European Commission

Feasibility study on an electronic identification, authentication and signature policy (IAS)



FINAL REPORT
A study prepared for the European Commission
DG Communications Networks, Content & Technology

Digital Agenda for Europe

This study was carried out for the European Commission by











Internal identification
Contract number: 30-CE-0413876/00-31
SMART 2010/0008

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN 978-92-79-31151-2
DOI: 10.2759/25928

© European Union, 2013. All rights reserved. Certain parts are licensed under conditions to the EU.
Reproduction is authorised provided the source is acknowledged.

Table of contents

1. SUMMARY OF THE STUDY GOALS AND SCOPE .....
1.1 Background of the Study .....
1.2 Scope of the Study .....
1.3 Role of this document in the Study .....

2. APPENDICES .....
2.1 Deliverable D.1: IAS in the European policy context .....
2.2 Deliverable D.2: IAS in Europe, an overview of the state of the art .....
2.3 Deliverable D.3: Proposal for a European IAS policy framework.....

1. Summary of the Study goals and scope

1.1 Background of the Study

The purpose of the present project, as described in the tender specifications, is to study the feasibility of a comprehensive EU legal framework that would apply to all electronic credentials needed to secure electronic transactions as well as the ancillary services needed to use them: electronic identification, authentication, signature, seals, certified delivery and a voluntary official email address. The perspective of the legal framework would be to facilitate the smooth working of electronic transactions in the internal market. In other words, it would be based on article 114 of the Treaty on the Functioning of EU (TFEU).

The Digital Agenda confirms that "*Electronic identity (eID) technologies and authentication services are essential for transactions on the internet both in the private and public sectors. Today the most common way to authenticate is the use of passwords. For many applications this may be sufficient, but more secure solutions are increasingly needed. As there will be many solutions, industry, supported by policy actions – in particular eGovernment services - should ensure interoperability based on standards and open development platforms.*"

The Commission, therefore, will "*In 2011 propose a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems*". This Study aims to provide inputs for this action.

1.2 Scope of the Study

The scope of this study is to determine if and how a comprehensive European IAS framework could be formed, including the legal, technical and trust components required for such a framework.

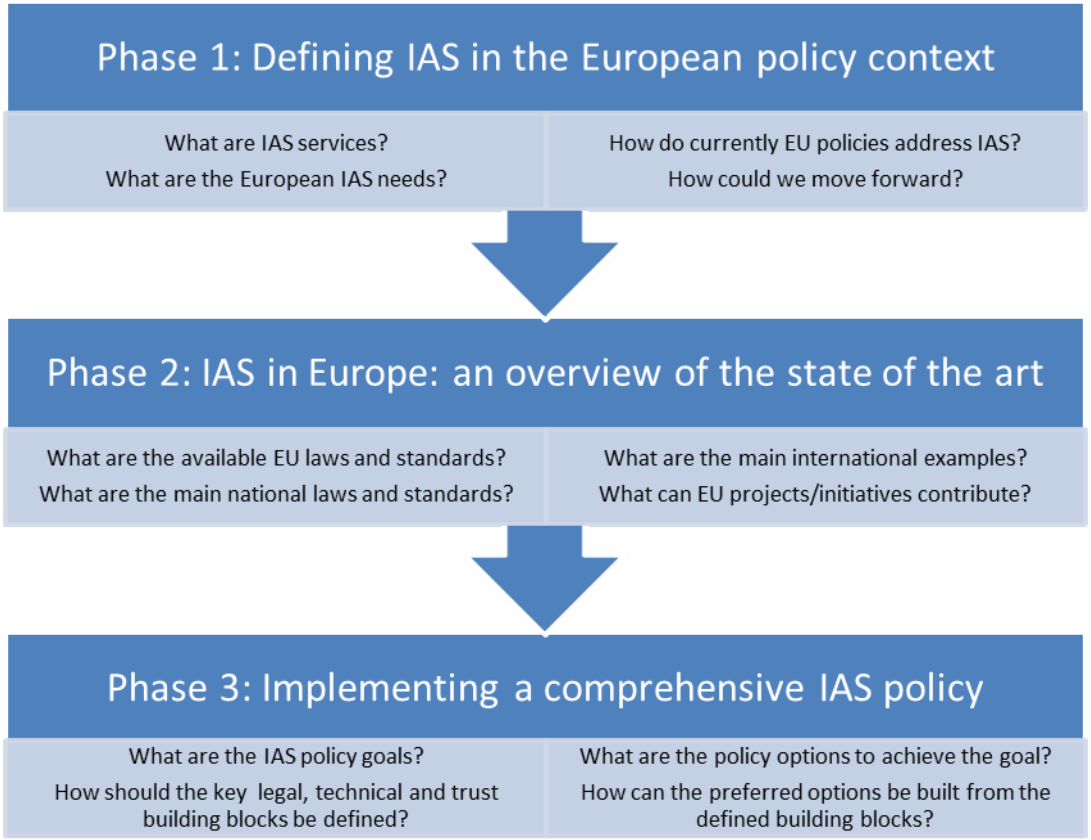
Each of these components will be defined by the study team, in a way that will allow them to serve as building blocks and to be combined into a comprehensive policy framework covering IAS services and ancillary services.

The study should culminate in a recommendation from the study team to the Commission on how a complete and functioning legal, technical and trust framework for IAS services could be constructed. This recommendation should build on consultations of selected experts through direct discussions and workshops, as well as the feedback received through the Commission's 2011 public consultation on electronic identification, authentication and signatures.

In this way, the study team aims to provide an immediately usable proposal, while optimally allowing the Commission room to adapt to future policy discussions or changed policy preferences.

1.3 Role of this document in the Study

Apart from a general on-going support task to the Commission, the present Study consists of three tasks that correspond to a logical phase in the study. The phases and tasks can be graphically summarized as follows:



The current document corresponds to all phases in the overview above and contains the final versions of the deliverables produced during the three phases. This Final Study Report contains the following documents:

- Deliverable D.1.1.b: IAS in the European policy context
- Deliverable D.2.2.b: IAS in Europe, an overview of the state of the art
- Deliverable D.3.2.b: Proposal for a European IAS policy framework

2. Appendices

2.1 Deliverable D.1.1.b: IAS in the European policy context

2.2 Deliverable D.2.2.b: IAS in Europe, an overview of the state of the art

2.3 Deliverable D.3.2b: Proposal for a European IAS policy framework

Study on an electronic identification, authentication and signature policy (IAS)

IAS in the European policy context

Final Version (D.1.1.b)

20 February 2013











This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the general invitation to tender of the Directorate-General Information Society and Media, n° SMART N° 2010/008. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.

Table of contents

1. SUMMARY OF THE STUDY GOALS AND SCOPE 4
1.1 Background of the Study 4
1.2 Scope of the Study 4
1.3 Role of this document in the Study 5

2. DEFINING IAS 7
2.1 What are IAS services? 7
2.2 Putting the basic definitions in a services perspective 24
2.3 Interim Observations 32

3. POLICY NEEDS FOR IAS IN THE DIGITAL SINGLE MARKET 35
3.1 How do IAS services fit in the Digital Single Market? 35
3.2 Needs for a functioning IAS internal market 41
3.3 The international dimension: needs and challenges 42

4. REVIEW OF PAST IAS POLICY: SCOPE, IMPACT AND CHALLENGES 43
4.1 Analysis of the impact of EU policy on IAS: how (in)complete is the picture? 43
4.2 Identification of key gaps 49

5. THE ROAD AHEAD 61
5.1 How useful is the eSignatures Directive as a starting point for IAS regulations? 61
5.2 Weaknesses of the eSignatures Directive – lessons learned 64
5.3 What are the alternatives? 68

6. CONCLUSIONS 70
6.1 IAS – summary of challenges and goals from a policy perspective 71
6.2 Perspectives for a future comprehensive trust services framework 73

7. APPENDICES 76
7.1 Abbreviations 76
7.2 Workshop report: analysis of comments received 78
7.3 Sources of IAS use cases 82

1. Summary of the Study goals and scope

1.1 Background of the Study

The purpose of the present project, as described in the tender specifications, is to study the feasibility of a comprehensive EU legal framework that would apply to electronic assertions needed to secure electronic transactions as well as the ancillary services needed to use them: electronic identification, authentication, signature, seals, certified delivery. The perspective would be to facilitate the smooth working of electronic transactions in the internal market. In other words, it would be based on article 114 of the Treaty on the Functioning of EU (TFEU).

The Digital Agenda confirms that "*Electronic identity (eID) technologies and authentication services are essential for transactions on the internet both in the private and public sectors. Today the most common way to authenticate is the use of passwords. For many applications this may be sufficient, but more secure solutions are increasingly needed. As there will be many solutions, industry, supported by policy actions – in particular eGovernment services - should ensure interoperability based on standards and open development platforms.*"

The Commission, therefore, will "*In 2011 propose a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems*". This Study aims to provide inputs for this action.

1.2 Scope of the Study

The scope of this study is to determine if and how a comprehensive European IAS framework could be formed, including the legal, technical and trust components required for such a framework.

The study should include recommendations on how a complete and functioning legal, technical and trust framework for IAS services could be constructed. This recommendation should build on consultations of selected experts through direct discussions and workshops, as well as the feedback received through the Commission's 2011 public consultation on electronic identification, authentication and signatures.

1.3 Role of this document in the Study

The present Study mainly consists of three tasks that correspond to a logical phase in the study. The phases and tasks can be graphically summarized as follows:

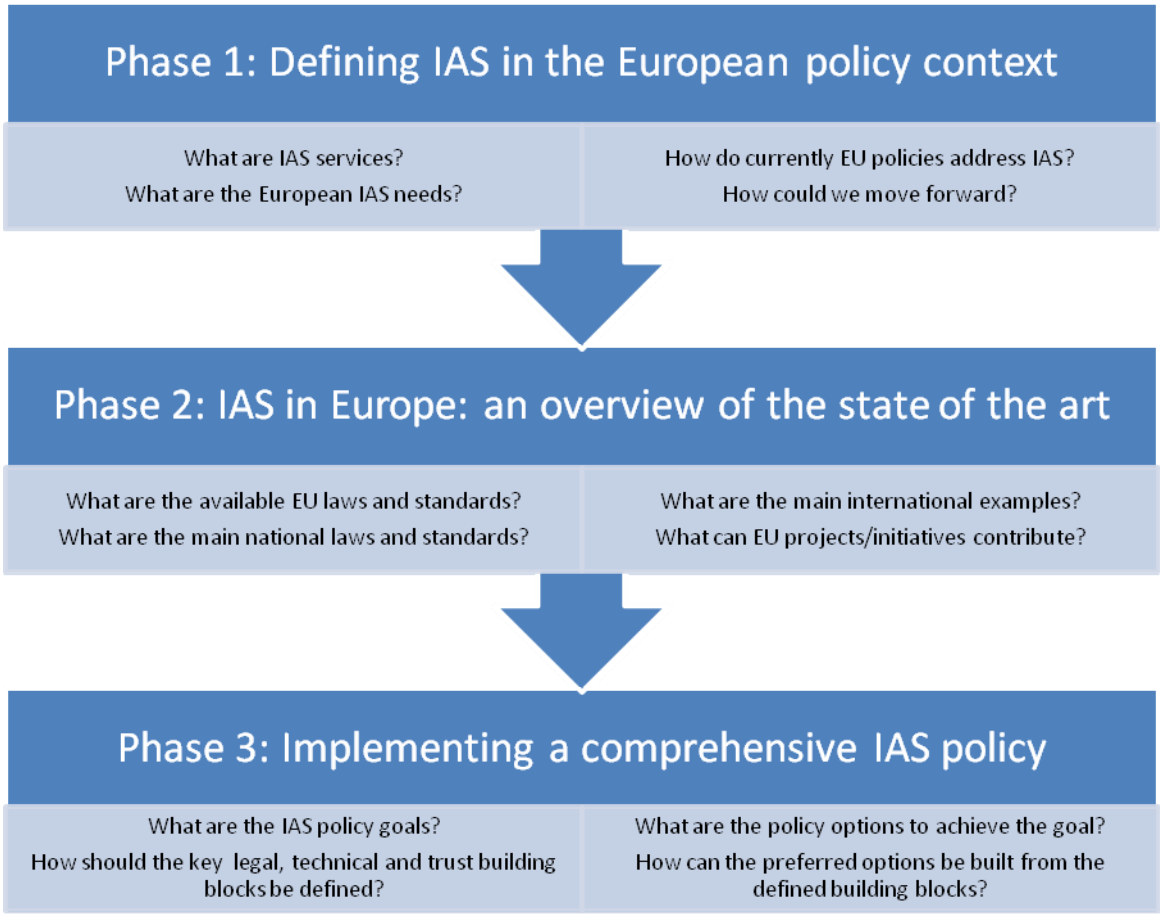


Figure 1: IAS study phases

The current document is Deliverable 1.1 - IAS in the European policy context, and corresponds to Phase 1 in the overview above. The goal of this report is to create the basis for the development of a comprehensive policy framework, specifically by:

- **Defining IAS**: it is absolutely crucial that participants in the IAS policy debate have a clear and common understanding of IAS concepts. Section 2 will therefore consist of elaborating the study team's understanding of the main notions, and building up, from the industry and legal standards, the definitions aimed to serve as common basis and language.

- **Understanding European IAS policy needs**: in order to define a comprehensive IAS policy framework, it must first be clear what the European needs and ambitions

in this area are. This will be analyzed in Section 3 of the report, building on the relevant sections of the Digital Agenda.

- **Determining to what extent the existing IAS policy framework in Europe already covers these policy needs**: It is important to understand the impact of this framework on IAS, and to determine what the gaps (if any) are. This will be examined in Section 4 of the report.
- **Establishing a road forward**: if there are indeed gaps between IAS policy needs and the current framework, we will need to determine how these can be resolved. While a comprehensive vision on this topic will be developed in Phase 3 of the Study, we can already define in Section 5 of the present document what the main conceptual options are.

This document has been finalized in two iterations:

- A draft version (D.1.1) outlining the study team's initial thoughts and opinions on the four aspects outlined above. This draft was presented to the Stakeholders for discussion.
- A final version (D.1.1.b) based on the feedback received.

As indicated in the graphic above, this report has been used as one of the key inputs for the recommendations of phase 3.

2. Defining IAS

2.1 What are IAS services?

With regard to defining IAS services, the core challenge is twofold:

- there are too many and often even different, conflicting or overlapping definitions of the basic terms;
- the fields of identity, authentication and signature are highly linked in practise while bearing their own differences.

However considering (i) the current move towards the rationalisation of the entire eSignature standardisation framework in the context of the execution of Mandate M460[1], (ii) the recent EC Decisions enabling Member States harmonising the publication of trust information on supervised or accredited certification services supporting electronic signatures and hence rationalising somehow the related trust framework, (iii) the political decision to better and further address IAS from a policy perspective and establishment of further legal measures as confirmed in the Digital Agenda for Europe[2], the European eGovernment Action Plan[3] and the Single Market Act[4], (iv) the execution of the present study aiming to adequately support this legal track, arriving at a common semantic basis is difficult but clearly necessary.

There will be rarely a better opportunity and momentum for establishing a sound and consistent set of definitions between all legal, technical and trust frameworks.

We will elaborate in this section the terminology and definition building blocks we need for the study on the basis of the eSignature Directive 1999/93/EC, the Modinis study[5] (covering exclusively the identification and authentication aspects) and the draft rationalised

---

[1] Mandate M460 is a standardisation mandate given end 2009 by the EC to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of information and communication technologies applied to electronic signatures. For further information see: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/standardisation/index_en.htm

[2] Digital Agenda for Europe COM(2010)245 of 19 May 2010: key actions on PSCs, e-ID, eSignatures.

[3] European eGovernment Action Plan COM(2010)743.

[4] Single Market Act COM(2011)206, 13 April 2011 - priority action on Digital Single Market (section 2.7).

[5] Modinis Study on Identity Management in eGovernment – Common terminological framework for interoperable electronic identity management, v2.01, November 23, 2005.

framework for electronic signature standardisation (DSR/ESI-000099)[6] and related standards, while rationalising and arbitrating when facing conflicting or overlapping definitions.

Entity & Identity

The first basic term we will here define is the term 'entity'.

Entity: means any natural or legal person or any information system that shall be characterised through a collection of identity attributes of which at least one subset of such identity attributes uniquely represents it.

We believe important, as stressed in Modinis, to keep this definition open to any type of person (including natural persons of course but also legal persons or public sector bodies) while further defining other types of entities (e.g. computers or other forms of machinery, digital resources or processes) as covered by any "information system" as defined in Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[7].

The following definition of 'identity' is also based on the Modinis definition.

Identity: The identity of an entity means the collection of all the entity's identity attributes.

An entity has only one such collection or set of all its identity attributes; to this extent one can say that one entity has only one identity. Each of the identity attributes from this collection needs not necessarily be unique to that entity but some and often several sub-sets of such identity attributes can uniquely identify an entity.

Unique Identity: means a collection of an entity's identity attributes that uniquely represents that entity.

---

[6] Draft Rationalised Framework For Electronic Signature Standardisation (DSR/ESI-000099) available from http://portal.etsi.org/stfs/STF_HomePages/STF425/STF425.asp and elaborated in the context of Mandate M460.

[7] Defined as 'any device or group of inter-connected or related devices which performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance'; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT

Sub-sets or collection of an entity's identity attributes that does not uniquely identify an entity are often called "partial identities".

Identity Attribute: means a distinct, measurable, physical or abstract named property belonging to an entity.

Common examples of such identity attributes include name, surname(s), nationality, date and place of birth, address, biometric data, professional or honorific title, gender, age statement, ..., but also other characteristics such as, possession of a public/private key pair, a delegation, a grant could be considered as identity attributes. A unique identifier is a special type of identity attribute that, on its own uniquely identifies an entity.

Identity Attribute Assertion: means an electronic attestation which links one or more identity attributes to a unique identity of an entity and confirms the identity of that entity.

The term assertion is preferred to the term 'credential' which is often misused or misunderstood. Such electronic attestation may not be delivered under the form of digital certificates, which is the most common type in a PKI world, but under other forms of signed statements (i.e. X/C/PAdES formatted signatures, SAML messages, XACML statements). Digital Certificates and Attribute Certificates can be considered as special types of Identity Attribute Assertions as they mainly link a specific type of identity attribute, namely a signature verification data, to an entity. Mandates[8], authorisations[9] and other types of permissions[10] can also be seen as specific types of identity attribute assertions. Figure 2 below illustrates a non exhaustive list of different sub-sets of identity attribute assertions.

An **"official identity"** can be defined as an Identity Attribute Assertion delivered by or on behalf of a public sector body[11] acting as an Identity Attribute Assertion Provider[12].

---

[8] Mandate can be defined as a revocable role (i.e. a set of one or more authorisations related to a specific application or service) or a set of revocable roles which refer to one or more permissions granted by an identified entity to another identified entity to perform well-defined actions with legal consequences in the name and for the account of the former. [Modinis]

[9] Authorisation, here, refers to the permission of an authenticated entity to perform a defined action or to use a defined service/resource. [Modinis]

[10] Permission describes the privileges granted to an authenticated entity (e.g. priviledge with respect to low-level operations that may be performed on some resource such as read, write, delete, execute, create, etc.). [Based on Modinis]

[11] Defined in Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, as “the State, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies

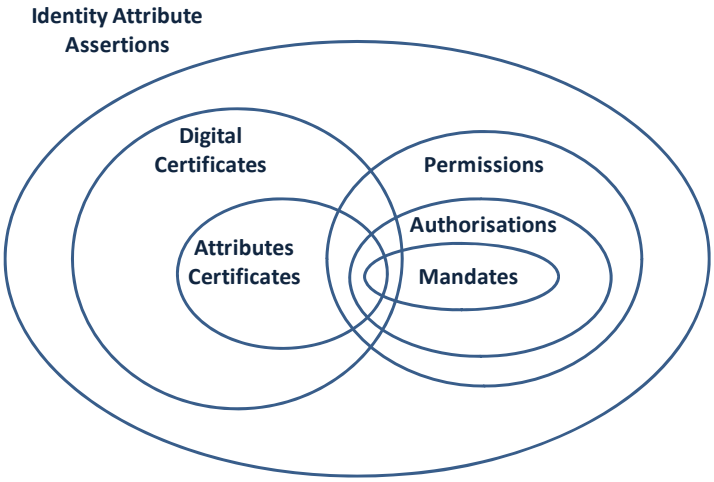


Figure 2: Identity Attribute Assertions

Identification can then be defined as the process of using claimed (e.g. by means of Identity Attribute Assertion) or observed attributes of an entity to deduce who the entity is. It can lead to a unique or a partial identity.

Authentication

Authentication is the corroboration of a claimed set of attributes or facts with a specified, or understood, level of confidence[5]. Authentication is typically divided into data authentication and entity authentication. We will also further define the concept of data authentication data as it will later serve as building block to define electronic signatures and clarify the distinction and interrelation between those concepts.

Entity Authentication: means the corroboration of the claimed identity of an entity and a set of its observed attributes. [5]

Data Authentication: means the corroboration that the origin and the integrity of data are as claimed. [5]

Data Authentication Data: means data in electronic form which are attached to or logically associated with other electronic data and which corroborates the identity of the entity at the

---

governed by public law"; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0098:EN:NOT

[12] See definition further in the text.

origin of the associated data and the integrity of the associated data.

The current definition of “electronic signature” in Directive 1999/93/EC (Art.2.1) (“data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”) is actually equivalent to the above “data authentication data” definition. This has been source of long misunderstanding between technical and legal worlds also linked to the fact that the most currently deployed PKI based technology for implementing rely on the exact same cryptographic operation for implementing electronic signatures and PKI based authentication.

We propose to add to the concept of electronic signature the expression of a consent, an intent or commitment. Of course the expression of such an explicit consent or commitment could be that the signature is created with no other purpose than authenticating the signatory as an entity. The definition of electronic signature is given later in the present section and other aspects of the legal issues related to the current definition of electronic signature in Directive 1999/93/EC are also discussed in Section 3.

Practical examples of use of data authentication data for not being an electronic signature are Message Authentication Codes, being key-dependent one-way hash functions which can be used to authenticate files between users

As in many cases a device is used to obtain such data or entity authentication, we further define the notion of authentication device.

Authentication Device: means configured tools, software or hardware used by an entity for the purpose of entity or data authentication.

Today these devices take many forms and involve one or more factors (the classic 'what you are', 'what you know', what 'you possess', and the more recent 'how you behave'), and support the corroboration of the claimed identity and the related relevant set of identity attributes, particularly it typically includes UserID/password, One Time Password (OTP) solutions, TAN cards, PKI based tokens and smart cards.

In a number of usage scenarios, the Authentication Device may require an interface device such as a keyboard, a biometric capturing device, or a card reader with or without a PIN-pad.

Authentication Interface Device: means configured tools, software or hardware used by an entity for the purpose of authentication in conjunction with an Authentication Device to facilitate or enable the use of the latter.

Signatures

Similarly to the previous identification and authentication related sets of definitions, the first basic term that we will here define is the term 'signatory'.

Signatory: means a person who holds a signature creation device and {acts, creates an electronic signature} either on his own behalf or on behalf of the natural or legal person or public sector body he represents. [5]

Note: text between { } designates that a choice should be made between several possible terms, in this latter choice, the underlined term is the one proposed.

The first occurrence of the word “person” is not qualified to be “natural” or “legal” person. The notion of person is interpreted differently in EU Member States. In some Member States a legal person is entitled to sign with the same rights and effects that a natural person. However if we later consider specific types of electronic signatures, namely “electronic seals” which are generated by signatories being legal person, public sector bodies[13], competent authorities, or public authorities, then either we enlarge this first occurrence of 'person' to 'natural or legal person' (with the “or” being also meant to consider cases for which this legal person is not an option in some Member States).

Electronic Signature: means data authentication data which {states, indicates the expression of, expresses} a {binding commitment, consent, intent, endorsement, adherence} from the signatory towards the associated data.

Note: text between { } designates that a choice should be made between several possible terms, in this latter choice, the underlined term is the one proposed.

[13] Defined in Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, as “the State, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law”; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0098:EN:NOT

This consent may be expressed in an explicit or implicit manner (while it would be far better being explicit). As explained previously and also as experienced in real life, electronic signature can be used for the purpose of entity authentication or for the purpose of data authentication; the desired goal would then be reflected in the expressed consent.

It is worth stressing the "universal" nature of electronic signature in the sense that it is applicable to any context and situation. Intrinsically, an electronic signature is of the same nature when used for eGovernment applications, for a private sector application or for any other type of use.

In order to address expressed market requirements and comments highlighted in the results of the Public Consultation, we introduce specific types of electronic signatures, namely “electronic seals” which are generated by signatories being legal person or public (sector) bodies.

Electronic Seal: means an electronic signature created by a legal person or a public sector body.

Similarly to what is done in Directive 1999/93/EC, we further refine the definition of advanced and qualified electronic signatures and electronic seals.

Advanced Electronic Signature ([14]): means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Advanced Electronic Seal: means an advanced electronic signature created by a legal person or a public sector body.

Qualified Electronic Signature ([15]): means an advanced electronic signature which is based on a qualified certificate [issued to a natural person] and which is created by a secure signature creation device.

Qualified Electronic Seal: means a qualified electronic signature for which the signatory is

[14] Directive 1999/93/EC, Art.2.2.

[15] Based on Directive 1999/93/EC , Art.5.1.

a legal person or a public sector body.

It can be observed that Directive 1999/93/EC, and the above definitions, defines electronic signatures in a broad and technology neutral way. It is the opinion of the IAS Study team that at the time of conducting our Study, the only viable large-scale implementation available is based on cryptography. Cryptographic primitives are available from various different mathematical families (e.g. RSA, ElGamal, ECC). These are based on different mathematical concepts (the hardness of factoring, the hardness of computing the discrete logarithm, and the hardness of finding points on elliptic curves). However, they offer comparable functionality.

While being then less technology neutral the following definitions are important and kept from Directive 1999/93/EC:

Signature Creation Data ([16]): means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.

Signature Creation Device ([17]): means configured software or hardware used to implement the signature creation data.

Secure Signature Creation Device ([18]): means a signature-creation device which meets the requirements laid down in *Annex III of Directive 1999/93/EC*.

Signature Verification Data ([19]): means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.

Signature Verification Device ([20]): means configured software or hardware used to implement the signature verification data.

The expression of a consent/intent/commitment as a condition of an electronic signature, is already present in some Member States implementation of Directive 1999/93/EC (e.g. in the

[16] Directive 1999/93/EC, Art.2.4.

[17] Directive 1999/93/EC, Art.2.5.

[18] Directive 1999/93/EC, Art.2.6.

[19] Directive 1999/93/EC, Art.2.7.

[20] Directive 1999/93/EC, Art.2.8.

Grand-Duchy of Luxembourg) and in signature related standards e.g. when combining ETSI TS 101 733 v1.2.2 definitions of "digital signatures" and of "signers":

- ***Digital signature****: data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient (ISO 7498-2).*
- ***Signer****: entity that creates an electronic signature. The Signer is the entity that initially creates the electronic signature. When the signer digitally signs over data using the prescribed format, this represents a commitment on behalf of the signing entity to the data being signed.*

Moreover the expression of a (signed) commitment is already a standardised feature of electronic signature formats whether based on XAdES, CAdES or PAdES profiles.

Furthermore, producing electronic signatures, data authentication data or authentication itself as an entity supposes the counterpart of verifying such electronic signatures, data authentication data and entity authentication which is the goal of so-called verifiers or relying parties. Both signers and authenticating parties on the one side and relying parties on the other side are likely to rely on one or more entities helping them to execute their task and to build trust relationships between them, the so-called trust service providers. Such entities support the signer/authenticating parties and verifiers by means of supporting trust services and related trust service tokens as tangibles outputs of such services. Such services typically include the provision of identity attributes assertions, in particular the provisions of digital certificates used to guarantee the identity of a signer or an authenticating party and their related services (e.g. registration services, certificate status validity services, certificate revocation services, repository services), the provision of time-stamping services as the notion of trusted time may be of critical importance when securing transactions and in particular electronic signatures and authentication, signature generation and signature validation services, archiving or information preservation services.

Trust Service Providers

The following definitions are proposed to serve as building blocks in the context of the study. They are mostly based on the current Draft Rationalised Framework For Electronic Signature Standardisation[6] and the EFVS study[21].

[21] EFVS Study Framework contract ENTR/05/58-SECURITY, SC N°14 – Final Report "Common Solution Model: Completion of the framework for Signature Validation Services", February 2010. http://ec.europa.eu/idabc/servlets/Docf934.pdf?id=32633.

Trust Service: means an electronic service which enhances trust and confidence in electronic transactions.

Note: Such trust services are typically but not necessarily using cryptographic techniques or involving confidential material.

Trust Service Provider: means an entity which provides one or more electronic Trust Services.

Trust Service Token: means a physical or binary (logical) object generated or issued as a result of the use of a Trust Service.

Note: Examples of binary Trust Service Tokens are Identity Attribute Assertion, like Certificates, CRLs, Time-Stamp Tokens, OCSP responses, Digitised Data, Registered Electronic Delivery and Information Preservation Record.

Similarly to the concept of qualified electronic signature, we will define:

Qualified Trust Service Token: means a Trust Service Token that meets the requirements laid down *in a specific annex/list*, and that is provided by a Trust Service Provider who fulfils the requirements laid down *in a specific annex/list* and that in consequence benefits from a legal certainty.

There is no concept of Qualified Trust Service Provider (TSP) but well of a TSP issuing Qualified Trust Service and Qualified Trust Service Tokens.

We can identify:

- Qualified Time-Stamp Token,
- Qualified Digitised Data,
- Qualified Certificate,
- Qualified Registered Electronic Delivery,
- Qualified Information Preservation Record,
- Qualified Identity Attribute Assertion,
- etc.

Trust Service Providers issuing certificates

We suggest replacing the concept of **Certification Service Provider** defined in Art. 2.11 of Directive 1999/93/EC as an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures by the concept of Trust Service Provider issuing certificates with the following definitions:

Trust Service Provider issuing certificates: means a Trust Service Provider who issues Certificates and provides related Certificate creation, assignment and life cycle management services.

Certificate: means an Identity Attribute Assertion which links signature verification data to a unique identity of an entity to which the signature verification data belongs.

An **Attribute Certificate** means a Certificate which links signature verification data to one or more identity attributes and confirms that those identity attributes belongs to the entity to which the signature verification data belongs.

Certificates and Attribute Certificates are special types of Identity Attribute Assertions as they link a specific type of identity attribute, namely a signature verification data, to an entity.

Electronic signature can be used for the purpose of entity authentication or for the purpose of authenticating data; it would then be reflected in the expressed consent as per the definition of "Electronic Signature". Using X.509 based Certificates and the related signature creation and verification data for the purpose of entity authentication means implementing electronic signatures (usually applied on random associated data) for which the expressed consent is limited to the scope and purpose of identifying the signatory authenticating itself through such means. It should be noted that the expression of this consent may be explicit or implicit but it should always be stated as clearly as possible.

Qualified Certificate ([22]): means a certificate which meets the requirements laid down in *Annex I of Directive 1999/93/EC* and is provided by a Trust Service Provider issuing certificates who fulfils the requirements laid down in *Annex II of Directive 1999/93/EC*.

We suggest to review the requirements currently laid down in those Annexes I and II as part of the Phase 3 of the IAS study.

Signature Generation and Validation Service Providers

Signature Generation Service Provider: means a Trust Service Provider which provides Trust Services that allow secure remote management of signatory's signature creation device and generation of electronic signatures by means of such a remotely managed

[22] Directive 1999/93/EC, Art.2.10.

device.

Those elements may rely on a Signature Policy that can be either explicit or implicit, be defined by the Signature Generation Service Provider (SGSP) or the relying party using the SGSP services or jointly negotiated by the parties.

Signature Policy: means a set of rules for the creation and validation of one or more electronic signatures that defines the technical and procedural requirements for creation, validation and (long term) management of this(these) electronic signature(s), in order to meet a particular business need, and under which the signature(s) can be determined to be valid.

There can be human readable or machine processable presentation of signature policies.

Signature Validation Assertion: means an electronic attestation provided by a Signature Validation Service Provider that confirms the results of the validation of an electronic signature.

Signature Validation Service Provider [based on EFVS study[21]]: means a Trust Service Provider offering the following services in relation to an electronic signature supported by certificates issued by certificate issuing services from TSP's issuing certificates (CAs):

a) Validation of the certificates supporting the electronic signature;

   Note: This validation step should be extended to include the certificate chain, starting from the signatory's certificate up to a trusted (root) CA certificate.

b) Validation of the electronic signature.

Those services ((a) and (b) above) may rely on a Signature Policy that can be either explicit or implicit, be defined by the SVSP or the relying party using the SVSP services or jointly negotiated by the parties.

It should be noted that Signature Validation Service Provider (SVSP) providing the above services may also provide extended services that may optionally include but not be limited to the following additional services:

- *Trusted Time services (e.g. Time-stamping services, Time-marking services);*
- *(Long term) Archiving of the signatures and/or signed documents;*
- *The extension of such signatures for preservation purposes;*
- *The maintenance of the signature/document formats;*
- *Any additional transactional service or delivery service related to the signed documents and signatures.*

Qualified Signature Validation Assertion: means a Signature Validation Assertion that

- meets the requirements laid down in a specific annex/list, including the provision to end-users with specific **guarantees with regard to the trustworthiness and legal reliability** of the electronic signature, i.e. assessing the legal value of the signature and providing an acceptable liability model that allows the relying party to rely legally on this statement; such guarantees can rely on statements made on some technical or legal requirements and/or quality criteria on certificates and electronic signatures, and
- is provided by a Trust Service Provider who fulfils the requirements laid down in a specific annex/list
- and that in consequence would benefit from a legal certainty.

This may involve all or a limited combination of rules described in more details in the EFVS study.[21]

Time-Stamping Service Providers

Time-Stamping Service Provider: means a Trust Service Provider which issues Time-Stamp Tokens.

This entity may also be referred to as a Time-Stamping Authority.

Time-Stamp Token: means a data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.

Information Preservation Service Providers

Information Preservation Service Provider (IPSP): means a Trust Application Service Provider which provides trust services to which information, among which documents, is entrusted in an agreed form (digital or analog) for being securely kept in digital form for a period of time specified in the applicable agreement; this service is expected to be able to exhibit all preserved information at any moment during, or at the end of, the preservation period.

Note: Cfr ETSI TS 101 533.

Registered Electronic Delivery Service Providers

Registered Electronic Delivery: means enhanced form of data transmitted by electronic means (ex. e-mail, document, message) which provides evidence relating to the handling of the data including proof of submission and delivery.

Registered Electronic Delivery Service Provider: means a Trust Application Service Provider which provides Registered Electronic Delivery trust services.

Identity Attribute Assertion Service Providers

Identity Attribute Assertion Provider: means a Trust Service Provider that provides Identity Attribute Assertions.

Supervision of Service Providers

The concept of supervision of service providers issuing qualified certificates is an essential building block of the current Directive 1999/93/EC as it allows implementation of a trust model of those qualified electronic signatures benefiting of an automatic equivalence to hand written signatures as explained further in the legal section of the present document.

However the implementation in practice of such a concept has lead to several issues:

- the co-existence and differences between the interpretation of an 'appropriate system that allows for supervision' (as introduced by Art 3.3 of the Directive) and of 'voluntary accreditation' (as defined in Art. 2.13 of the Directive) are not always, if ever, understood clearly, even by those who are in charge of such systems;
- the terms and definitions used are often overlapping or conflicting with the terminology used in the audit and assessment world;
- the divergence of implementation in practice of the concept of "appropriate [...] supervision" by Member States has lead to significant differences in the effective implementation of the controls underlying such a supervision ranging from very basic controls up to formal certification. The recent Diginotar case has, if nothing else, shown that there is a clear need for sufficiently effective supervision, since security

risks can have a very serious impact on the trustworthiness of CAs and on their economic utility.

Given the importance of supervision as a tool for establishing and maintaining trust in trust service providers, it is our strong belief that it is time to move towards a more structured and specified system for allowing effective, systematic, independent and documented supervision for obtaining evidence and evaluating such evidence objectively.

It is proposed that such a more structured and specified supervision system should be introduced for **qualified trust services**, while similar systems may be kept voluntary for non-qualified trust services.

The present document recommends the system to rely on **standardised conformance criteria** against which the (qualified) trust services (shall) will be assessed (audited) and that the assessment of conformance of trust services and providers of related trust services to the standardised conformance criteria (including standard policies and practices) is performed **by auditors** against **standardised conformance assessment processes**. These auditors should be "accredited" as operating to standard audit practices (e.g. by a National Accreditation Body such as UKAS in UK, ENAC in Spain, DAkkS in Germany, NAT in Hungary, full list at http://www.european-accreditation.org/content/ea/members.htm, as those National Accreditation Bodies operate under common practices and have cross recognition through the European co-operation for Accreditation (EA) and all are members of the International Accreditation Forum[23]).

It is expected that the MS Supervisory Body (i.e. the Administration in charge of the supervision) could rely on such accredited auditors, internally or externally if lacking relevant competencies themselves, who will be assigned, under a selection process to be defined, with the mission of the effective audit of the qualified trust services (mandatory) or of a non-qualified trust services upon request by the TSP providing such services (voluntary).

[23] The International Accreditation Forum, Inc. (IAF) is the world association of Conformance Assessment Accreditation Bodies and other bodies interested in conformance assessment in the fields of management systems, products, services, personnel and other similar programmes of conformance assessment. Its primary function is to develop a single worldwide program of conformance assessment which reduces risk for business and its customers by assuring them that accredited certificates may be relied upon.

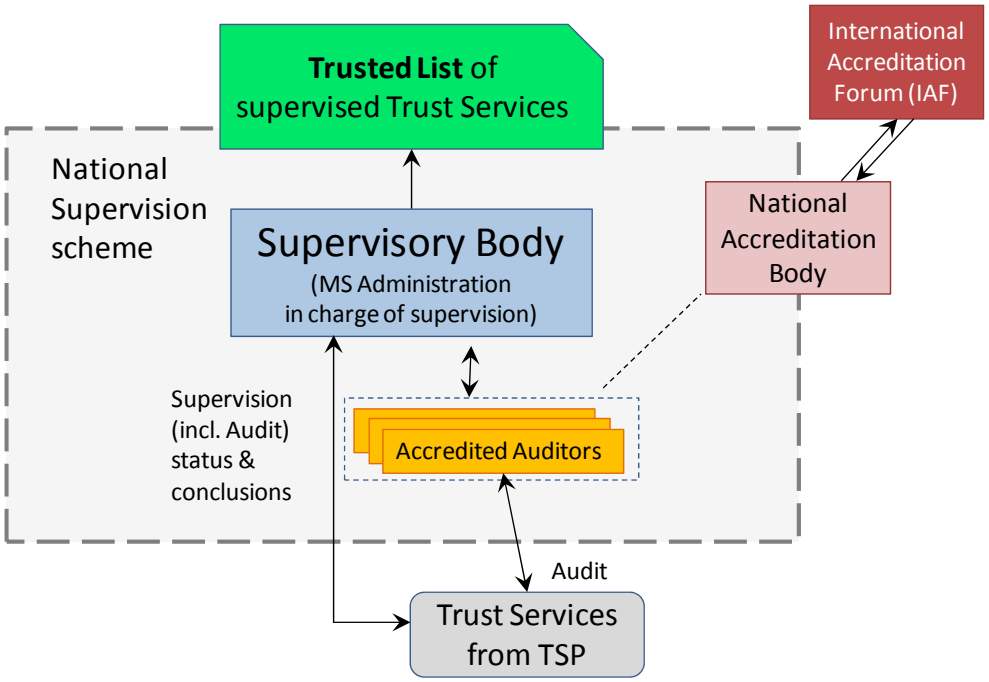


Figure 3

A possible supervision audit process flow is depicted in Figure 4 below and is based on the CROBIES study[24].

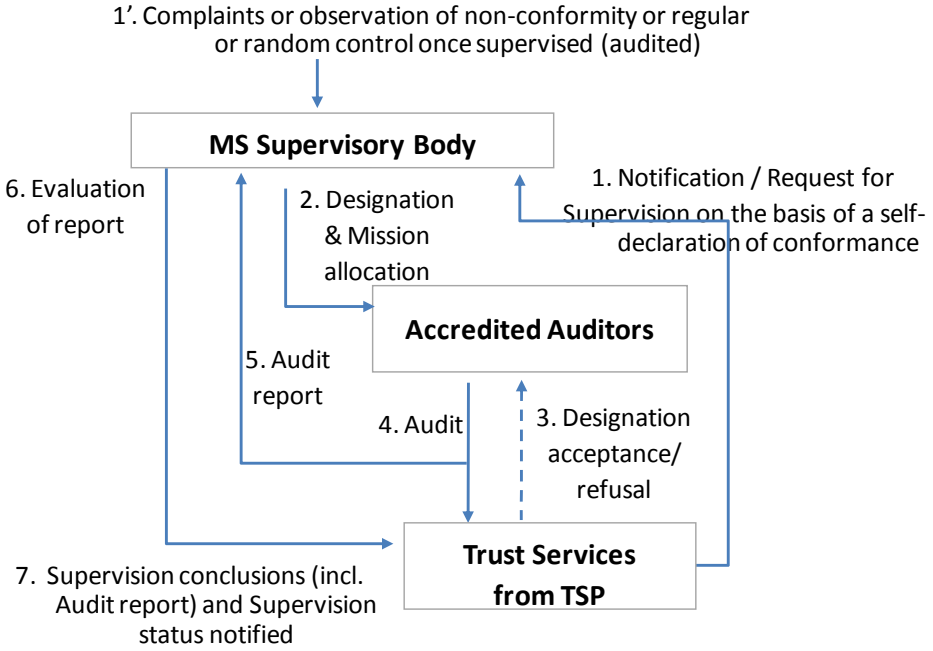


Figure 4

[24] Study on Cross-Border Interoperability of eSignatures (CROBIES), A report to the European Commission from SEALED, time.lex and Siemens (Version 1.0, 2010); available at http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm.

Supervision based on a common set of conformance criteria established on a standardised basis (i.e. in the context of mandate M460), specified per type of qualified trust service and based on a standardised control process (i.e. based on well-established audit practices), together with the inclusion of qualified trust services in national Trusted Lists will ensure a more efficient and safer market than it is today.

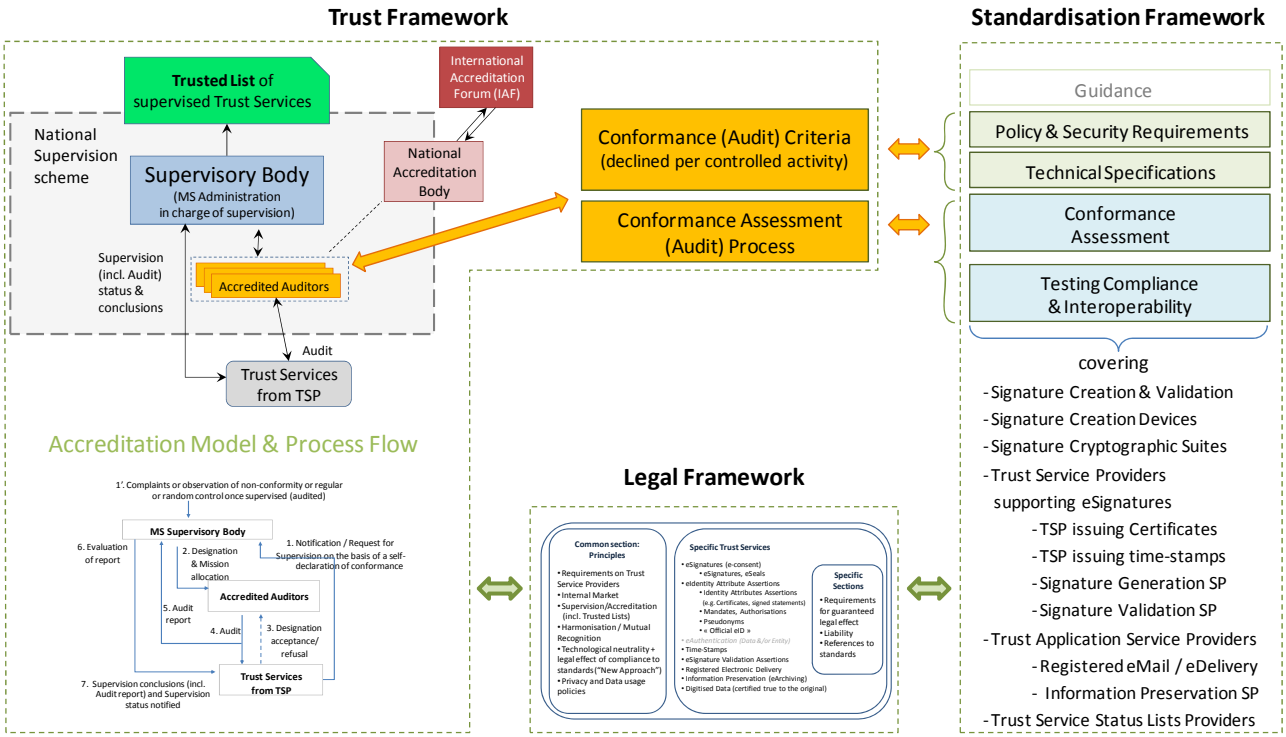


Figure 5

Trust Service Status Lists Service Providers

The following definitions are used

Trust Service Status List: means a signed list presentation of the trust service status information on which interested parties may determine whether a trust service is or was operating under the approval of any recognized scheme at either the time the service was provided, or the time at which a transaction reliant on that service took place.

This is the base concept from which Trusted List is a baseline profile applied to the context of Directive 1999/93/EC and CD 2009/767/EC amended by CD 2010/425/EU.

Trusted List: refers to a European Union Member State's "Supervision/Accreditation Trust Service Status List of certification services from Certification Service Providers, which are supervised / accredited by the referenced Member State for compliance with the relevant

provisions laid down in Directive 1999/93/EC".

Note: Based on CD 2009/767/EC amended by 2010/425/EU.

Trust Service Status List Provider: means a Trust Service Provider issuing a Trust Service Status List.

2.2 Putting the basic definitions in a services perspective

In this Study, the relationships and interactions between Electronic Identification, Authentication and Signature are initially considered from the basic isolated service perspectives. Subsequently we consider them from their overlaps.

Perspective 1 - Electronic Identification

We consider Electronic Identification the family of Use Cases for an "identifiable entity (Modinis term)" that address the lifecycle of collection of attributes, establishment, activation, modification, archival. We consider Electronic Identification as distinct from Electronic Authentication.

With regard to Electronic Identification, we distinguish between Electronic Identity Establishment, and Electronic Identity Use:

- **Electronic Identity Establishment** is addressed by an enrolment process that:
  - Captures the selected identity attributes. This may include biometric attributes. Such attributes should be derived from an authentic source.
  - Relates those attributes to a primary key (electronic identity primary key, i.e. an identifier consisting in itself a Unique Identity) for later retrieval. There is typically a repository or database that may be centralised or decentralised in nature.
  - May include:
    - Corroboration of different information sources as to confirm the identity that is to be established;
    - The allocation of identity attribute assertions and related authentication devices (e.g. an identity card, a social services card, userid and password or a token) for use in subsequent authentication.

- **Electronic Identity Use** contains a wide range of possible Use Cases where the electronic identity primary key (i.e. a Unique Identity), the related identity attributes, or additional information linked to the above are used. This includes “1:N” identification as in the context of law enforcement or border control.

Both establishment and use should take into consideration respect for privacy and consent. Consent of the identifiable entity may be present or absent, depending on the Use Case. It can be assumed to be present when e.g. enrolling for and collecting an employee identification badge. It may be absent when using the identity attributes of a drunk driver who tried to escape from the accident he caused.

Typical use cases include:

- Selection of beneficiaries (address, family status, age, etc) for e.g. a governmental benefit;
- Studies and evaluations for diverse purposes (public health, marketing campaigns, spam, …);
- Member recruitment;
- HR processing;
- Identification of citizens, migrants, and asylum seekers;
- Identification of criminals;
- Identity profiling;
- …

For a comprehensive list of sources of identity Use Cases, refer e.g. to the appendices.

When considering an identification scheme where all desired properties of ideal identity management are met such as uniqueness of an entity, persistency of identities, minimal disclosure of identity attributes, full user control, anonymity, data privacy, etc., one can consider and model as follows the way of addressing the basic identity building blocks and related services defined in the previous section.

Every person is unique in the World. The same uniqueness principle may apply whether dealing with natural or legal persons (including public sector bodies). This might be also applicable for a wide set of other types of entities or information systems when suitable and applicable. Uniqueness of natural persons is characterised by biometrical properties such as DNA, fingerprint, retina and many others or when ultimately required through a combination

of such means. Unfortunately today none of them is perfect with current state-of-the-art technology.

In the ideal world there would be a technology providing some inimitable unique identity (IUI)[25] to every natural person and have as properties to be:

- a Unique Identity of the entity it is related to;
- 100% unique to that entity;
- derived from biometric properties with 100% reliability for a lifetime;
- be as short as possible.

The same concept of IUI with such properties would be also somehow easier to be established for legal persons through a universal unique identification scheme while it may be that finding an agreement on such a scheme would take a long time and efforts[26].

However the current state-of-the art can certainly rely on the concept of Unique Identity[27] as defined in the previous section while trying to evolve towards Inimitable Unique Identity in the future, to allow **derivation** of such UI (or IUI) through one-way function resulting in a reasonably short and meaningless, hence anonymous and privacy enabling, string of bits, namely the **Unique Identity Derivation** (a special type of electronic identity primary key as named above, i.e. a special unique identifier consisting in itself a Unique Identity of the entity it is related to).

A certain degree of control, probably a full control, is desired by the person in question (or its authorised representatives) on such UI (or IUI) derivation process as the result will still consist in unique identities but of the type that can be more easily manageable and ensuring some anonymity to the entity it represents. Such derivation process could then be performed by the person itself or some entity the person trusts or needs to prove his identity (UI or IUI).

Identity Attribute Assertion Providers (that mat also be called Attribute Authorities in short) are Trust Service Providers that are trusted to provide Identity Attribute Assertions to entities, i.e. to assign identity attributes to persons (identified through their unique identities, UIs, or IUI, or derivations of such UIs or derivations of their IUI) in forms of assertions which bind the UI Derivation to a specific attribute with a certain degree of security, quality and assurance (e.g. integrity of the assertion, trustworthiness and authenticity of the Identity Assertion Service Provider, reliability of the assertion content and assignment process). This

[25] This concept is based on work and discussions with Tarvi Martens Director of SK, Estonia while slightly rationalised and generalised for application to a wider set of market, business, or social network implementations than the sole "official" governmental eID schemes.

[26] Initial work has been done in this area in the context of CEN CWA 16036: Cyber-Identity - Unique Identification Systems For Organizations and Parts Thereof, November 2009.

[27] i.e. a collection of an entity's identity attributes that uniquely represents that entity.

degree would ideally be 100% in the context of an official Governmental identification scheme but may vary between different levels in more relaxed market or business or social application domains. In practical terms such identity attribute assertions are **electronically signed** by the issuing Identity Attribute Assertion Provider. Such electronic signatures will naturally include expression of commitment related to the guarantee given by the IAAP on the level of assurance to be given to the assertion.

Different levels of granularity may also be implemented ranging from assertions binding only one identity attribute to a UI (or IUI) Derivation to assertions binding two or more attributes to the same UI (or IUI) Derivation.

A related feature of an ideal IAS system would be to allow the person (i.e. identified by the UI or IUI or a Derivation) to be in full control of its identity attributes and related assertions. In some cases attribute assignment may be carried out with the request of an authorised representatives (e.g. parents with regards to a child, legal representative with regards to a legal person), or by IAAP acting solely but with the consent of the person (e.g. citizenship, academic degree, professional qualification, medical status) but in all cases the person should have (sole) control on the usage of its attributes.

IAAP should follow the following rules and be accordingly supervised or controlled depending on the type and nature of the service (e.g. mandatory supervision for qualified service, industry certification or labelling for other market services):

- being obliged to keep attribute history,
- give out assertions (included historical) in real-time (to third parties) only with Permission of the identified person.

In other words – a person may but would never be obliged to carry or save his/her assertions. These may be reliably stored in IAAP systems and released to 3rd parties only when UI (or IUI) Derivation owner agrees. In some cases, the person might want some attribute (such as Public Key) to be available to anyone without Permission.

Anonymity and privacy can be achieved by generating as many derived UI (or IUI) Derivations, being anonymous in essence. A person could have multiple UI Derivations but still based on one of its UIs (or its IUI). The UI Derivation owner, i.e. the person to who it relates, is the only one who can prove if necessary (issuing IAAP, when such a Trust Service Provider is used, holds the secret by definition) that his/her UI (or IUI) is related to the UI (or IUI) Derivation. A person is free to choose whether other IAAP's are issuing assertions to his/her real UI or to some of his/her UI Derivation.

The concept, not new in essence, based on a rationalisation of the use of unique identifiers, is however simple and powerful enough to build sound basic building blocks when defining a common basis for a consistent IAS policy.

A Public Key (or more widely Signature Verification Data) **is a special identity attribute that can be asserted to UI (or IUI) Derivations by special IAAP's – the so-called Trust Service Providers issuing Digital Certificates.** Like any other assertion it does not need to contain any additional data. A person can be asserted with multiple Public Keys with multiple assertions, in this case Public Keys are practically named in distinguished manner (e.g. as “Public Key for Qualified Signature”, etc.).

The person has of course a sole control over Private Key(s) (Signature Creation data) associated with corresponding Public Key(s) (Signature Verification Data) and this is part of the assertion commitment given by the TSP issuing certificates when electronically signing the assertion(s).

Permissions for releasing individual assertions from IAAP's are created with Private Key(s) (Signature Creation Data). For example, if the person wants his/her Surname to be released to some 3rd_party then he/she uses a Private Key to sign Permission in form of

P [My_UIDerivation,”Surname”,3rd_person_UIDerivation,*timeframe, IAAP_UIDerivation*] .

This Permission can be used by the identified 3rd_person to request and get access to person’s surname by contacting the appropriate IAAP (I*AAP_UIDerivation*) in specified timeframe. The Permission can also specify historical time – e.g. “what my surname was 10 years ago”. Integrity and authenticity of the Permission can be verified using privately known or publicly available assertion of UIDerivation and Public Key from the issuing Trust Service Provider.

Such identity attribute assertions and the above explained mechanism can be advantageously used to build up simple but efficient, privacy enabled and powerful schemes for implementing mandates, authorisation, delegation of powers (and signatures) allowing decentralised models and empowering existing authentic sources to implement such models on the basis of mere electronic signatures.

Two (or even more) models may coexists, namely

- on the one side, an "official governmental based eID" model in which the IUI is established on a close to 100% certainty (or to the highest possible level) and a governmental eID authentication device and/or set of identity attribute assertions are delivered to citizen by an official IAAP allowing its owner to sign or authenticate him/herself with a maximal level of assurance for him/herself and relying parties, and
- on the other side, one or more "business application domain" driven model relying either on an UI Derivation of an officially established IUI or from an UI that is established on ad hoc basis with a certain level of assurance to build a "business application domain" electronic ID model, i.e. a device and/or set of identity attribute assertions that are delivered to the business application domain participants by a business entity acting as an IAAP. This can range from current low level assurance

identity based models on today's social networks, to models reaching banking sector quality requirements for securing eBanking applications.

These models can certainly coexists and also leverage one on the other (provided that it is the one with a lower level of assurance that can leverage the one having a higher level and that levels of the services or their components can be compared) and benefit from the same IAS policy model and being regulated accordingly when this is required and to the extent it is needed. Today some national eID models are evolving in that direction (e.g. German eID scheme). However the quality of enrolment and the quality of authentication are equally to be considered.

Perspective 2 - Entity Authentication

Entity authentication is the process of establishing an acceptable level of assurance that a claimed identity is genuine.

In the context of identity claims, it is common to refer to the parties as Claimant and Verifier. The Claimant is “claiming the identity”, typically using some form of identity attribute assertion. The Verifier is “verifying the claim”. They may call upon a third party services such as an IdP (identity Provider) during the protocol.

Identity Attribute Assertions may be based on something the claimant knows (a password or PIN), has (an identity authentication device), and is (static biometrics such as facial image, fingerprints, iris). More recently dynamic biometrics are being considered, such as gait (the patterns of movements of e.g. limbs).

The authentication may be mutual, where each party authenticates against the other. De facto this is done with protocols such as TLS/SSL. Multiparty arrangements are possible, where more than two parties are involved.

Obviously there exist scenarios where privacy needs to be preserved or enhanced. This is where we situate PETs (Privacy Enhancing Techniques). Such privacy may need to be guaranteed absolutely, or it may be conditional. In the latter case it may be revoked when certain conditions are met/unmet.

Typical Use Cases include:

- Demonstration of holding a credential for being eligible for benefits (address, family status, age, etc) by the claimant;
- Logon to an electronic Service Provider or eGovernment service;
- Managing the domotic services of your house;
- Internet buying;
- Internet selling (including reputation management aspects);

- Listening to streaming music through a paying subscription;
- Border control;
- Voting;
- Checking mail and voice-mail.

Taking privacy-preservation into consideration is possible in each of these Use Cases. If privacy-preservation would be part of the Use Case from one viewpoint, there might be complementary viewpoints that mandate privacy revocation. Consider computer-related crime in general, and particular identity impersonation, money laundering, paedophilic activities, cyber attacks, virus spreading or terrorist financing.

Perspective 3 - Signature creation

When a Signer signs, he performs a number of steps that create a signature which serves at authenticating the data to be signed and associates to it the expression of a consent or commitment to the signed data.

The first obvious use case for electronic signatures is to mimic the hand written signatures and hence the consent or commitment and aim of the signer may be that the electronic signature is meant and recognised as equivalent to a handwritten signature with a legal binding of the signer to the signed data.

Besides such an expected legal effect and scope of the signature, different natures or types of commitments may be associated to the signed data with or without the expression of a desired legal effect. This can range from positive or negative assertions or even mixing them to express more complex natures of the consent of signer to a signed data or document. This typically includes:

- Approval of the content and meaning of the signed data or document,
- Being the originator of the signed data or document,
- Signature is meant to authenticate the signer as originator and ensure the integrity of the data (with or without any other legal binding to the content of the signed data),
- Review and approval in a specific approval flow context,
- Signature of a contract,
- Signature of an official act,
- Signature with the aim of witnessing a data or an event or a document (e.g. being an agreement between two or more other parties),
- etc.

Typical use cases include the signing an electronic document (XML, PDF, MS-Word, …) in different application contexts in whatever type of electronically processed communication or

transaction (e.g. eBusiness, eBanking, eGovernment, eProcurement, eVAT, eGuichet, eProcedures, eHealth, eJustice, etc).

More often in electronic business processes, a single business process involves more than one but a combination of electronic signatures logically ordered the one to the other, in terms of timing and sequencing but also in terms of consent and commitments. The nature of the consent may then be much more complex.

As shown in the above described identification perspective, electronic signatures are intrinsically built on identification and authentication building blocks and services. Electronic signature can serve to secure and implement identity attribute assertions ranging from the assignment of "classic" identity attributes, digital certificates, mandates, authorisations, time related assertion (e.g. time-stamping), etc. but also be used as an authentication device on the basis of which the signatory's claimed identity can be corroborated by a verifier or relying party.

Perspective 4 - Signature validation

Signature verification consists in the simple principle of verifying an electronic signature through the use of privately or publicly available signature verification data known with a certain level of assurance to be associated to an identified entity who is in possession of the corresponding signature creation data used to generate the electronic signature to be verified.

This process may reveal to be a quite complex process on a technical basis depending on the technology being used for which each component or service supporting such a verification process must be adequately verified according to a certain set of rules or policies the verifier will rely on to be convinced that the electronic signature can be considered valid to a certain level of assurance.

The main difficulty in this process, besides the complexity inherent to the technology being used and its inherent interoperability issues[28], lies in the adequacy and consistency between the different assurance levels having been defined or not to qualify each and every component building block or services that supports the signature verification. This covers notably the quality, security or assurance level of the signature creation device, the digital certificate of the signer, the practices used by the issuing TSP to register the certificate

[28] To this extent a specific Specialist Task Force (STF) and associated efforts are currently deployed to fixing the specifications of signature validation procedures (See STF 427 QF3 aspects on the ETSI ESI STF 427 homepage (http://portal.etsi.org/stfs/STF_HomePages/STF427/STF427.asp). The fact that this type of efforts are still being needed for a quite mature 30 years old technology is quite revealing of the inherent complexity of such a process.

subscriber, to issue the certificate and to maintain and provide information about its validity status, the integrity and authenticity of the underlying identity attribute assertions whether related to the signatory itself or to the issuing IAAP or to any Trust Service Provider used in the signature creation or validation process (e.g. Signature Generation Service Provider, Signature Validation Service Provider).

So far no consistent model for establishing the level of assurance has been consolidated for the whole picture of such components underlying the signature creation and validation process. However some promising 4-level based schemes are emerging either from the Kantara or the STORK initiatives; even if they are limited somehow to the I and A aspects of an IAS model, it is worth to consider to establish and leverage on these models to build a pragmatic 4-level based Assurance Model for an IAS policy.

2.3 Interim Observations

Using the concepts outlined in the paragraphs above, following observations can be made:

Overlap is present in practise

As illustrated in the preceding sections, in many Use Cases, the usage of I, A and S overlaps significantly both from a conceptual and a practical perspective.

Solutions are in place but still lack interoperability

Large-scale identity and authentication systems have been build and are deployed, but today remain locked into their silo's. They include aspects of signatures as well. This is e.g. illustrated by:

- ICAO MRTD/PKD, arguably the largest identity and authentication system (or rather "system of systems") worldwide, but based on its own standards such as ICAO 9303 (globally based on PKI);
- SIM (Subscriber Identity Module) cards for mobile phones, with more than two billion cards in use worldwide probably the largest de-facto identity standard;
- The worldwide SWIFT system for global funds transfer is secured by PKI;
- The network of suppliers in the Defence's industry based it's security on PKI (TSCP – Transglobal Secure Collaboration Platform);
- The EU Digital Tachygraph system, with its EU-wide PKI (ERCA – European Root Certification Authority) and various cards, including driver identification cards.

Existing identity solutions are already widely diverging, as illustrated e.g. by the differences between the Belgian eID and the German ePA:

- The Belgian eID allows anybody who is physically in possession of the card to read the data on the card (obviously only the designated government entity can update the information);
- The German ePA only allows reading by authorised terminals, and for authorised purposes, and it generates different pseudonyms for different Use Cases to protect the privacy of its holder or allows revealing information on a need to know basis.

Interoperability is not supported except on pilot level

As demonstrated by the CIP-IST-Large Scale Pilot STORK[29], the definition of interoperability requirements is difficult but not impossible. STORK defines how a solution on cross-border level can make national eIDs interoperable without changing their systems and interfering on infrastructures. Some efforts are still needed to ensure the sustainability of its results.

When a large scale EU or global enterprise wants to manage the IAS aspects of employees, contractors and partners, it faces a highly diversified landscape in both legal and technical terms. This is highly inefficient and costly.

Social network solutions might fill voids and become de-facto standards

In the real world we observe Use Cases where e.g. a mobile phone number and the bill from the mobile operator are used to identity and authenticate a person when applying for a bank loan. Such Use Case is legally not regulated today, but fills a clear void. If e.g. Facebook or Google-based identities become widespread, they might fill this gap. Once such identities would be in use, they might set the de-facto standard, making regulation even harder.

Privacy preservation is mostly lacking in the current approach

Current solutions such as the above are not or rarely based on systems that take into account requirements for privacy preservation, minimum disclosure or consent.

A consistent set of basic definitions and concepts are required as a common basis for building consistent and a sound IAS policy

Current definitions, concepts and languages are often defined and understood differently between those legal, technical and trust worlds. We have started this study by establishing a first draft rationalisation of commonly adopted definitions while simplifying the picture in essence. The proposed concepts, definitions and related building blocks and services are aimed to support the implementation of a ideal world of electronic identity, authentication and signatures where all desired properties such as uniqueness of entities, persistency of

[29] Secure idenTity acrOss boRders linKed - www.eid-stork.eu.

identities, privacy, minimal disclosure of attributes, highest level of adequacy between the expected and experienced level of assurance when validating identities and electronic signatures, full user control, anonymity, etc. Today situation still differs from such an ideal world but it is believed that this is still realistically achievable with the current state-of-the art and future trends and emerging technologies (one of the objectives of Phase 2 is to assess such a fact).

3. Policy needs for IAS in the Digital Single Market

3.1 How do IAS services fit in the Digital Single Market?

Until recently, the role of IAS as a whole (covering electronic identification, authentication and signature services) has only been dealt with in a piecemeal fashion in European regulations. The main regulatory intervention has been the eSignatures Directive, which aimed to support the internal market for certification services, with a strong emphasis on eSignature services. Since the adoption of the Directive in 1999, several other legal instruments have referenced the eSignatures concepts established by the Directive (including e.g. the Sixth VAT Directive and the Public Procurement Directives), whereas identification and authentication have not been directly addressed.

It is however interesting to note that the 2007 Payment Services Directive (PSD) provides a definition of the concept of authentication, stating that "authentication" means a procedure which allows the payment service provider to verify the use of a specific payment instrument, including its personalised security features.[30] This definition of course uniquely targets the PSD context, meaning that it has a limited impact on other European policy areas.

However, policy focus on the importance of IAS services in the internal market has increased with the adoption of the Digital Agenda. The Digital Agenda was published as a Communication of the European Commission in 2010,[31] and contains the common European strategy for creating “a flourishing digital economy by 2020”. It outlines a number of policies and actions that support this objective, grouped around various action areas. For the purposes of this report, the most relevant action area relates to improving trust and security.

The Digital Agenda positions eSignatures in the broader context of trust and security challenges in the information society, which include such topics as misappropriation of identity, fraud, cyber crime, data protection, privacy-by-design, and critical information

[30] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, art. 4,19.;
see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:01:EN:HTML

[31] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe – 26.8.2010; COM(2010) 245 final/2.

infrastructure protection. ESignatures (and electronic identities) can be considered as mechanisms that can contribute to building viable solutions on each of these points.

The Agenda correctly stresses the necessity of ensuring the trustworthiness of technology as a prerequisite to its use in practice. Recognizing that the Directive has not been entirely successful in meeting its stated purpose of "facilitat[ing] the use of electronic signatures and contribut[ing] to their legal recognition" (article 1 of the Directive), the Digital Agenda proposes a revision of the eSignatures Directive, "with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems."

It is worth noting the phrasing of the proposed action set out in the Agenda: the revision should result in a legal framework for 'secure eAuthentication systems'. The Commission might have also simply called for a revision focusing on 'secure electronic signatures'. The broader terminology used in the Digital Agenda could be taken to suggest that electronic authentication services in a broader sense are now contemplated as an area where regulation might be beneficial and justified.

The specific challenges relating to electronic identification undoubtedly play a role in this particular phrasing. Indeed, the Agenda contains a further related action, namely to propose by 2012 a Council and Parliament Decision "to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents – issued by the public or the private sector)". This action could be used to address one of the current challenges in relation to electronic identification: while innovative EU projects (such as the large scale pilot STORK[32]) have developed functioning technical solutions to eID challenges, there is currently no broader legal or policy framework to move these pilots into operational solutions for the general public. The inclusion of this action in the Digital Agenda suggests that a Commission Decision could clarify this point, by ensuring at a minimum that Member States have a list of electronic identification methods from other Member States that they agree to treat as equivalent.

Thus, the Agenda seems to have a strategy to improve the trustworthiness of eAuthentication systems, albeit without specifying at this stage exactly what those systems might entail.

While this summary focuses on the trust and security aspects of the Digital Agenda, it should be recognized that the Agenda takes a much broader perspective, and correctly notes that the EU has in many respects failed to bring about a true Digital Single Market, in which on-line service borders are eliminated (or at least reduced) in the same way as for the offline single market.

[32] https://www.eid-stork.eu/.

Specifically, the Agenda notes that:

"[t]he internet is borderless, but online markets, both globally and in the EU, are still separated by multiple barriers affecting not only access to pan-European telecom services but also to what should be global internet services and content. This is untenable. First, the creation of attractive online content and services and its free circulation inside the EU and across its borders are fundamental to stimulate the virtuous cycle of demand. However, persistent fragmentation is stifling Europe's competitiveness in the digital economy. It is therefore not surprising that the EU is falling behind in markets such as media services, both in terms of what consumers can access, and in terms of business models that can create jobs in Europe. Most of the recent successful internet businesses (such as Google, eBay, Amazon and Facebook) originate outside of Europe. Second, despite the body of key single market legislation on eCommerce, eInvoicing and eSignatures, transactions in the digital environment are still too complex, with inconsistent implementation of the rules across Member States. Third, consumers and businesses are still faced with considerable uncertainty about their rights and legal protection when doing business on line. Fourth, Europe is far from having a single market for telecom services. The single market therefore needs a fundamental update to bring it into the internet era."

These observations can also be applied to eAuthentication services in general. The recent Public consultation on electronic identification, authentication and signatures[33] have provided some support of the Digital Agenda's statements from the perspective of others with an interest or concern in the matter, asking among other points which trust building services and credentials should be considered for regulation at the European level in order to ensure their cross-border use. The 418 respondents to the question provided the following replies:

For which of the following trust building services and credentials should legal or regulatory measures be considered at EU-level in order to ensure their cross-border use?

	Number of replies	% of total number of replies to this question
Certified electronic documents in general	270	64,59%
Electronic seals	216	51,67%
Time stamping	219	52,39%

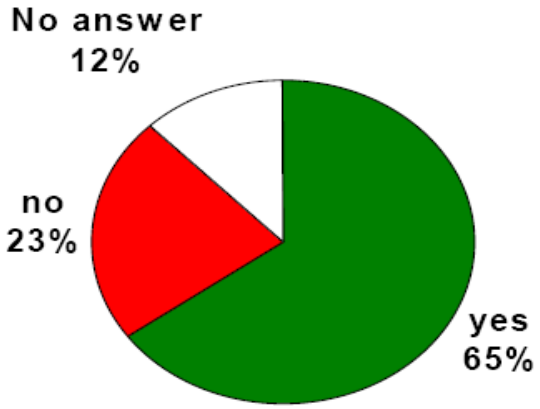
[33] For an overview of the consultation's questions, approach, and all received contributions, see http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision/pub_cons/index_en.htm.

Certified delivery of mail	195	46,65%
Authorisations/mandates	194	46,41%
Long term archiving	191	45,69%
Electronic transferable records	136	32,54%
Official delivery address	119	28,47%
Others (please list)	68	16,27%
Pseudonyms	67	16,03%
Anonymous agents	47	11,24%
None	26	6,22%

Thus, only 6,22% felt that no further trust services required any regulation. Respondents who chose this answer and provided additional comments frequently stated that regulations were unnecessary or too rigid, and that standardization, accreditation schemes and private sector initiatives would be adequate to address cross border challenges.

Among those who felt that new regulations could be valuable, certified electronic documents in general – without further definition in the consultation – were the main service type chosen for further regulation (64,59% of respondents), with electronic seals and time stamping each also being mentioned by more than half of respondents.

Do you see a need for additional legal or regulatory measures on eID at EU-level?

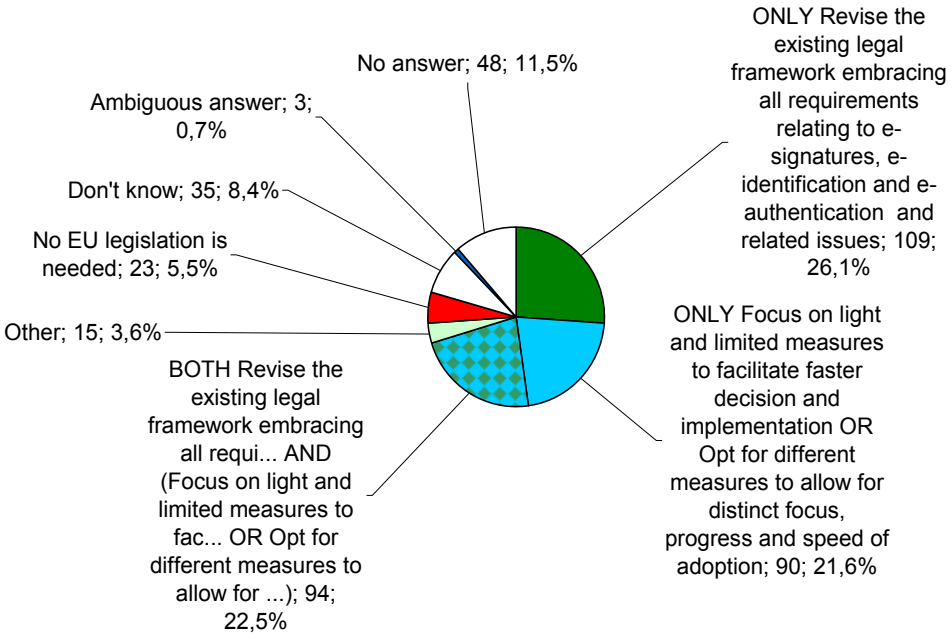


The fifth section of the consultation recalled the "Digital Agenda for Europe" communication in which the Commission has proposed two key actions directed at the creation of a well functioning digital single market with a view to eliminate the current barriers to the use of e-signatures, e-identification and e-authentication across Europe. Specifically, key action 3 of the Digital Agenda focuses on the revision of the eSignatures Directive, whereas key action 16 targets a Council and Parliament Decision to ensure the mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States.

In this context the respondents were asked what European Union legislative measures on e-signatures, e-authentication of natural and legal person claims as well as e-identification would be appropriate to best meet the challenges of the digital single market.

The responses received on the nature of necessary legal measures on e-signatures, e-identification and e-authentication show no clear indication.

Q23: What EU legislative measures on eID, e-sig, e-auth. would be appropriate?
(exclusive answers)



The main observation is that only 5,5% of the respondents feel that no legislation is needed, whereas the largest group of 26,1% considers a comprehensive legal framework to be most appropriate. 21,6% are in favour of lighter and more limited measures to facilitate faster adoption and implementation or preferred more specific targeted measures. 22,5% prefer at the same time a comprehensive approach but achieved by light or different means. Although 48,6% of respondents prefer a revised legal framework embracing all requirements relating to e-signatures, e-identification and e-authentication and related issues, the answers do not allow however to find out if a majority prefers a set of measures or an all-encompassing measure.

The pie chart above shows the answers of the respondents in a re-processed manner, where respondents could choose multiple answers to the following six options: "Revise the existing legal framework embracing all requirements relating to e-signatures, e-identification and e-authentication and related issues / Opt for different measures to allow for distinct focus, progress and speed of adoption / Focus on light and limited measures to facilitate faster decision and implementation / No EU legislation is needed / I don't know / Other".

Thus, it would appear that both the Commission and market players are aware of the importance of IAS services as a tool for enhancing trust and security in the Digital Single Market.

3.2 Needs for a functioning IAS internal market

If IAS services are indeed to play a role as trust/security enablers in the Digital Single Market as foreseen in the Digital Agenda, then a European policy framework is required that ensures that these services are understood and perceived as sufficiently trustworthy themselves.

This implies a common understanding on a number of key elements to be addressed by a comprehensive IAS approach, specifically:

- An unambiguous understanding of IAS services and ancillary services, including definitions of these services and an overview of how they relate. At present, only eSignatures have a common definition at the European level, and (as will be examined below), even on this topic some ambiguity remains.
- The policy goals that an IAS approach should cover, including such aspects as the enabling of the internal market, technological neutrality and legal reliability. These goals are currently dictated by the provisions of the Digital Agenda.
- The legal translation of these policy goals and requirements, stipulating the goal of the regulatory text, definitions of basic concepts, provisions on general obligations for trust service providers, data protection, liability, internal market rules, legal effect of services, any supervision/accreditation mechanisms, etc. A basis for this already exists via the eSignatures Directive. In the section below, we will examine to what extent the eSignatures Directive is adequate to address IAS challenges.
- The trust framework needed to support a comprehensive IAS approach. With respect to eSignatures, this has been implemented primarily through supervisory/accreditation mechanisms. However, these only relate to eSignatures, and not to identification or authentication services in general. A similar basis for common trust in the EU would appear to be required for IAS in general.
- The technical framework required to enable the comprehensive IAS approach, including standardisation needs. Again, much work has already been done at the European level with respect to eSignatures, but this is not the case for IAS services in general.

A common thread in this overview is the fact that these needs have been covered to a significant extent in the EU with respect to eSignatures, but not with respect to any other types of IAS services. It would seem that this is a gap that would need to be addressed in order to achieve the goals of the Digital Agenda.

3.3 The international dimension: needs and challenges

The summary of policy goals above focuses very strongly on the European Digital Single Market. However, IAS services do not – or at least should not – operate in European isolation. Markets are international, and any IAS policy approach adopted at the European level needs to recognize the importance of being able to align with international initiatives and good practices. This is crucial to avoid European IAS service providers becoming isolated from international markets.

Indeed, the Digital Agenda recognizes the importance of its international dimension in a separate chapter:

"2.8. International aspects of the Digital Agenda

The European Digital Agenda aims to make Europe a powerhouse of smart, sustainable and inclusive growth on the global stage. The seven pillars in the Digital Agenda all have international dimensions. The Digital Single Market in particular needs an external face because progress on many of the policy issues can only be made on an international level. Interoperability and standards recognised at the world scale can help promote more rapid innovation by lowering the risks and costs of new technologies. […]Thus an international dimension of the Digital Agenda in order to complete the actions above is crucial[…]."

This emphasis on the international dimension was also echoed in the aforementioned public consultation. As indicated in the summary[34], "*many responses made reference to the importance of international standardization, if possible supported through international agreements to use the same standards in international transactions. European standards should be promoted at the international level to support this process. This same observation was also made with respect to the information security and data protection aspects of eID, eSignatures and eAuthentication: while European collaboration and harmonization is beneficial and should be continued as a priority, a truly international framework would eventually need to emerge to address the challenges of the international economy. Several respondents however also warned against attempts to unilaterally impose European perceptions or solutions, as this could have an adverse impact on international trade*."

Thus, it is clear that any European IAS policy framework should be conceptually able to integrate seamlessly with international developments, in order to support not only the internal market, but also international markets.

[34] European Commission, Information Society and Media Directorate-General, Public consultation on electronic identification, authentication and signatures in the European digital single market - Overview of responses, Brussels, 12.8.2011, http://ec.europa.eu/information_society/policy/esignature/docs/pub_cons/consultation_summary.pdf, p. 30.

4. Review of past IAS policy: scope, impact and challenges

4.1 Analysis of the impact of EU policy on IAS: how (in)complete is the picture?

The primary EU instrument in the IAS domain thus far is undoubtedly Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (the eSignatures Directive). This Directive states its purpose in article 2: it aims “to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market.”

The Directive aimed to ensure that legal uncertainties surrounding the value of eSignatures would not become a barrier to the budding eSignatures market in the European Union, or perhaps more accurately, that such uncertainties could reasonably be kept to a minimum. The elimination of any kind of legal uncertainty was (and remains) a practical impossibility, due to the large variety of approaches to eSignatures and their technical characteristics. The European law maker had to tread a fine line between flexibility (allowing different technologies with different degrees of reliability) and legal certainty (ensuring the predictability of the legal value of at least some types of eSignature).

This resulted in the compromise that is now relatively well known. Conceptually, the Directive creates two fundamental eSignature types, on the basis of which a third type can be built:

1. The basic e-signature concept, i.e. data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;

2. The advanced e-signature concept, i.e. an electronic signature which:

(a) is uniquely linked to the signatory;

(b) is capable of identifying the signatory;

(c) is created using means that the signatory can maintain under his sole control; and

(d) is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

In practical terms, the advanced e-signature definition is technologically neutral. However, in the current state of the art it is only implemented through the use of cryptographic technologies.

3. The advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, commonly referred to as qualified electronic signatures. This is also the terminology that will be used in this article.

When considering legal certainty however, the Directive contains only two tiers:

1. All eSignatures benefit from a non-discrimination rule (article 5.2), meaning broadly that their legal effectiveness and admissibility as evidence in legal proceedings cannot be denied merely on the grounds of being electronic or of not complying with one of the requirements for qualified signatures. Of course, this does not eliminate the possibility of eSignatures being rejected for any number of other reasons, including for instance the use of insufficiently reliable technologies, taking into account all circumstances which are relevant to the case (e.g. the behaviour of the parties after an e-signature has been created).

2. Only qualified signatures benefit from the presumption of equivalence rule (article 5.1), meaning that these signatures are automatically considered to satisfy the legal requirements of a signature in the same manner as a hand written signature, and that they are always admissible as evidence in legal proceedings.

In effect, the system of legal certainty in the Directive is remarkably binary: qualified signatures are endowed with apparent legal certainty, and other types of eSignatures are not. This situation can be affected substantially by additional rules, such as by specific laws declaring other forms of e-signature to also be equivalent to hand written signatures, or more typically by contractual arrangements in which the relevant parties make separate arrangements on the legal validity and admissibility of eSignatures in advance.

The conceptual framework in European e-signature laws is thus very much centered around eSignatures as a tool for emulating hand written signatures. While the market access and internal market rules (articles 3 and 4 of the Directive) apply to all types of certification service providers and certification services, the only provision in the Directive that governs the legal effect of these services is focused on achieving equivalence with hand written signatures. This observation may appear to be trivial, but it is not. From a technical perspective, the cryptographic process of signing specific data can serve many other functions which have little to no logical connection to a hand written signature. As examples, one might consider:

- The identification of a person (entity authentication) may use identical technologies, yet there is no intention of achieving equivalence to a hand written signature.

- The use of electronic stamps or seals, where a entity signs a document to authenticate it on behalf of a legal person (e.g. a company seal or administrative stamp), or even on behalf of an computer system or process, in which hand written signatures may be entirely inappropriate or even nonsensical as an analogy.
- Authorization management, where the user wants to demonstrate a certain legal mandate (e.g. to confirm the status of doctor, lawyer, notary public, etc) or access/usage right (e.g. the status of employee, citizenship, or simply of being an adult). In these cases, equivalence to a hand written signature may not necessarily be the desired goal.
- Time stamping, where the equivalence to a hand written signature is irrelevant, since the only intention is to add a trustworthy time reference to a specific transaction.

The Directive is much less relevant to all of these functions. This is not to say that it has no effect on them:

- First, the e-signature itself is defined as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication" (emphasis added). This definition makes no explicit or implied reference to the purpose of creating a substitute for a hand written signature; indeed, based on this terminology alone, all of the examples above could be said to be covered by the definition of an electronic signature, since they are all methods of authentication (either entity authentication or data authentication).[35]
- Second, the notion of a "certification-service-provider" is very broadly defined in the Directive as "an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures" (emphasis added). Again, the definition is so broad that virtually all types of authentication service providers could be said to be covered.

None the less, even under this broad interpretation of the Directive's terminology, the Directive does not provide a comprehensive material legal framework for the services mentioned above. Admittedly, the market access and internal market provisions of the Directive (mainly article 4.1) apply, meaning that Member States may establish the rules which apply to service providers established on their territories, and that they may not restrict the provision of services originating from another Member State. This is of course vitally important, given the Digital Single Market ambitions of the Digital Agenda.

However, with respect to the legal value of trust services, the relevant provisions of the Directive (article 5 of the Directive) are only meaningful when the signatory aims to create a

[35] Patrick Van Eecke, *De handtekening in het recht, Van pennentrek tot elektronische handtekening* [The signature in a legal context, from scrawl to electronic signature], Larcier, 2004, 420 (608),and Stephen Mason, *Electronic Signatures in Law*, (2nd edn, Tottel, 2007), 4.5 also illustrate this issue.

substitute for a hand written signature. In all the other examples mentioned above, it is impossible on the basis of the Directive to link any legal value to a service, other than perhaps to state that its electronic nature does not invalidate it outright. As legal support to a trust service goes, this would appear to be a relatively weak endorsement.

In conclusion, the implicit focus of the Directive is quite clearly on enabling electronic tools that emulate traditional hand written signatures to be recognized as a form of eSignature. It aims to achieve this effect through a number of simple and logical rules and principles.

The rules established by the Directive address the legal, technical and trust landscape required to allow an interoperable eSignatures market to function, with a strong focus on electronic signatures. The conceptual framework (definitions of e-signature tiers and CSPs) has already been briefly explained above, as has the approach of the legal effect of eSignatures. However, the other building blocks also deserve some consideration, if only to help explain why the Directive has not been able to achieve the desired purpose.

As a basic foundation of the Directive, the free market principle (or more truthfully: the internal market rules) are a logical consequence of treating certification services as a market service. To enable the internal market, it is vitally important that Member States cannot set arbitrary barriers to foreign CSPs. This goal has been implemented via article 4 of the Directive, declaring that “[e]ach Member State shall apply the national provisions which it adopts pursuant to this Directive to certification-service-providers established on its territory and to the services which they provide. Member States may not restrict the provision of certification-services originating in another Member State in the fields covered by this Directive.” CSPs are thus largely governed by a country-of-origin rule, which ensures that they do not need to comply with 27 materially different sets of rules if they choose to operate in all 27 Member States.

As a technical tool, advanced eSignatures also require a minimum common technical framework to ensure their operation. This technical framework is not included directly in the Directive as such. Indeed, that would have been a poor strategic choice, given the relative procedural complexity of renegotiating a Directive, which would make it very difficult to keep the technical framework updated. Instead, the Directive contains only a fairly high level set of requirements in its four annexes, relating to:

Annex I: requirements for qualified certificates

Annex II: requirements for certification-service-providers issuing qualified certificates

Annex III: requirements for secure signature-creation devices

Annex IV: recommendations for secure signature verification

With respect to technical standardization, the Annexes do not aim to provide guidance for specific implementation or assessment activities, as they are far too generic for that

purpose. Instead, the Directive foresees the possibility of providing additional guidance through Commission Decisions, to be taken upon the advice of an "Electronic-Signature Committee" created under article 9 of the Directive, thus colloquially known as the "Article 9 Committee". This Committee may:

- clarify the requirements laid down in the Annexes;
- clarify the criteria that Member States should apply when designating a body to determine the conformity of secure signature-creation-devices with the requirements of the Directive;
- clarify "generally recognized standards for electronic signature products", notably by establishing and publishing reference numbers of such standards in the Official Journal of the European Union. When this has been done, the internal market provisions of article 3.5 require the Member States to presume that meeting those standards also implies compliance with the requirements laid down in Annex II, point (f) (relating to the requirement for CSPs issuing qualified certificates to use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them), and in Annex III (requirements for secure signature-creation devices).

Through this process, The Commission adopted two Decisions: Decision 2000/709/EC[36] establishing the minimum criteria for conformity assessment bodies, and Decision 2003/511/EC[37] publishing reference numbers to three generally recognized standards[38] for electronic signature products which create a presumption of compliance with part of the qualified electronic signature requirements. Perhaps surprisingly, neither one of these

[36] 2000/709/EC: Commission Decision of 6 November 2000 on the minimum criteria to be taken into account by Member States when designating bodies in accordance with article 3(4) of Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures (notified under document number C(2000) 3179) (Text with EEA relevance) OJ L 289, 16.11.2000, p. 42–43.

[37] 2003/511/EC: Commission Decision of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council (Text with EEA relevance) (notified under document number C(2003) 2439) OJ L 175, 15.7.2003, p. 45–46.

[38] Notably the following standards: CWA 14167-1 (March 2003): security requirements for trustworthy systems managing certificates for electronic signatures - Part 1: System Security Requirements; CWA 14167-2 (March 2002): security requirements for trustworthy systems managing certificates for electronic signatures - Part 2: cryptographic module for CSP signing operations - Protection Profile (MCSO-PP); CWA 14169 (March 2002): secure signature-creation devices.

Decisions was ever updated, despite developments in global e-signature standardization initiatives.[39]

Finally, the Directive also incorporated a trust infrastructure to support certification service providers. Essentially, the trusted (or untrusted) state of an electronic signature is a function of many factors, one of which is the role of a trusted third party. In the absence of a trusted third party (e.g. a simple e-signature consisting of a text file appended to an e-mail, where the text file and e-mail are both solely created by the signatory), an e-signature has a limited ability to provide confidence in the text that has been signed, where the authenticity of the e-mail is uncertain. In those cases, the signature amounts to little more than the word of the signatory, which was already reflected in the signed text without any signature. Through the involvement of a trusted third party (such as the CSP issuing signature certificates in a PKI-based advanced e-signature system), relying parties have a more substantial anchor to which they can attach confidence. If they know that the issuer is trustworthy, then that removes at least one possible area of doubt.

A significant issue is how a relying party can determine whether such a trusted third party is in fact to be trusted.[40] The Directive provides a solution to this question through the concepts of supervision, conformity determinations and accreditation:

- Member States must establish appropriate supervision schemes, in which (at a minimum) CSPs established within their borders that issue qualified certificates to the public are supervised (article 3.3 of the Directive). Since qualified certificates are a prerequisite to creating qualified signatures, this implies that qualified signature solutions by definition benefit from some degree of supervision, thus improving their trustworthiness.
- As noted above, the second component of a qualified signature (apart from the qualified certificate) is the use of a secure signature-creation-device. The Directive specifies that Member States can designate bodies with assessing the compliance of such devices with the requirements of the Directive (as laid down in Annex III). Such findings of conformity are to be recognized in all Member States (article 3.4).
- Finally, Member States are also allowed to introduce “voluntary accreditation schemes aiming at enhanced levels of certification-service provision” (article 3.2 of the Directive). Member States can use such schemes to institute quality labels, or to define ‘trust levels’ of signature types in an effort to make the market more

[39] For list of standards across the globe, see the second deliverable of this Study (“D2.1 – IAS in Europe: an overview of the state of the art”)

[40] On this topic, note chapters 11, 12 and 13 in Stephen Mason, *Electronic Signatures in Law* and Patrick Van Eecke, *De handtekening in het recht, Van pennentrek tot elektronische handtekening* [The signature in a legal context, from scrawl to electronic signature], Larcier, 2004, 543-560

transparent and intuitive to consumers and service providers. It is important to recognize that “enhanced levels of certification-service provision” does not necessarily imply a high reliability of e-signature solutions; even basic (non-advanced) eSignatures may be subject to voluntary accreditation, irrespective of their objective reliability. The Directive requires that the conditions related to such schemes must be “objective, transparent, proportionate and non-discriminatory”, to avoid market distortions. However, since accreditation schemes are by definition established at the national level, they tend to enable trust at the expense of interoperability, since foreign service providers are less likely to have a business case for seeking voluntary accreditation in another Member State, even if their signature solutions objectively meet or exceed the requirements of the voluntary scheme.

On the basis of these trust enablers, each Member State *must* have a supervisory body to supervise CSPs issuing qualified certificates to the public. In addition, it *may* also have an accreditation body to manage any voluntary accreditation scheme, and it *may* have one or more conformity assessment bodies to determine the compliance of any supposed secure signature creation devices. Conceptually, this approach is sound, as it ensures that the legal and technical framework are linked through a workable supervisory framework.

Thus, the Directive provided a basic legal framework that established the main legal, technical and trust building blocks. While clearly slanted towards state of the art PKI solutions, this was considered to be appropriate to sustain an interoperable eSignatures market.

4.2 Identification of key gaps

A cursory examination of current EU initiatives involving or requiring the cross border use of eSignatures (e.g. in relation to e-procurement, e-justice, e-invoicing, the implementation of the Services Directive, or any exchange of authentic e-documents) shows that the eSignature Directive has largely failed to achieve this objective of an interoperable eSignatures market. Even leading initiatives in this area are still developing or piloting solutions, twelve years after the adoption of the Directive. Solutions for cross border interoperability either require closed contractual frameworks – essentially cutting out the influence of the Directive to a large extent – or abandon the high-security, high-certainty goals of the Directive by adopting simple (non-PKI) e-signature solutions or by reducing the trust assurances to relying parties. In effect, even if one accepts that the eSignature Directive has helped create a market for advanced eSignature services at the national level, any beneficial effect on the internal market (i.e. at the cross border level) is modest at best.

A number of factors can be identified that may be partly responsible for the lack of an internal market for advanced eSignatures, or more generally for the lack of cross border interoperability. It is important to recognize that not all of these factors are related to the EU framework for eSignatures as briefly described above. For one, it is inherently difficult to provide an appropriate legal framework in a technological area which evolves very quickly, notably in order to respond appropriately to security challenges. This is especially true in relation to electronic signatures, where new standards are continuously developed and algorithms are deprecated when weaknesses become apparent.

Apart from technical complexity, the European advanced eSignature market in 1999 was also still developing rapidly, with relatively little services being made available as stand-alone products for the public in most EU Member States. Finally, as was already noted in the introduction to this report, the business case for the advanced eSignatures as a separate service (i.e. in isolation from applications in which they are intended to be used, such as e-banking) remains uncertain. All of these elements made it inherently complex to create a legal framework that would enable a flourishing internal market for advanced e-signature services.

Nevertheless, the current EU framework is clearly also not without its flaws, and a number of issues can be clearly linked to the lack of an internal market.

Already in 2003, an exhaustive study on the legal and market aspects of electronic signatures conducted on behalf of the European Commission and available on-line, pointed to some flaws of the current legal framework on e-signatures.[41] The study came to the following findings, which are still relevant today:

- "The study team found out that most of the EU Member States have, more or less **faithfully, transposed** the Directive into national legislation. In addition, many of the non-EU countries surveyed have based their own electronic signatures and delivery of signature related services legislation on that of the EU Directive. From a technical point of view the Directive has even influenced international standardization initiatives, such as the IETF standardization work on Qualified Certificates. It is clear that the **Directive has influenced** legal and technical activities outside of the European Union boundaries. New terminology introduced by the Directive (especially Qualified Certificate, Advanced Electronic Signature, Certification Service Provider) has been taken on board by the EEA countries, Switzerland, the Accession and the Candidate countries.

[41] Study on The legal aspects of the application of Directive 1999/93/EC and on the practical applications of the electronic signature (Member States, EEA, Candidate countries), A report to the European Commission from K.U.Leuven, Landwell, HN Consulting and Secorvo (version 1.0, 2003), see http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf .

- Although the broad lines of the Directive have been respected by the Member States when transposing the Directive, a number of issues have nevertheless been identified as problematic. These problems can mainly be attributed to a misinterpretation of the Directive's wording, which in turn leads to divergences in national laws and/or divergences in the practical application of the rules.

- Regarding the market access rules as stipulated by Article 3 of the Directive, the following remarks need to be made. The good news is that for the moment, none of the Member States surveyed submit the provision of certification services by providers established in another Member State to **prior authorization**, thus formally respecting Article 3.1 on market access. It is, indeed, perfectly possible for a CSP established in one Member State to provide certification services in another Member States, without having to ask the prior permission of a national authority. This was not possible everywhere in Europe before the Directive was issued and transposed.

- On the other hand, various Member States have established **supervision schemes** that are very close to prior authorization, and are possibly infringing Article 3.1 provisions. Given that CSPs have been established in all but a few of the countries surveyed and given that the majority of supervision schemes are still in the very early stages of development, it is impossible to compare yet the practical implications of the supervision systems. Nevertheless, it has become obvious that there are very important divergences between the various supervision schemes in the Member States. Although the effect of these divergences remains limited, since most of the CSPs still operate exclusively in their home country, the divergences will begin to show a negative impact once European or non-European providers start to launch more cross-border certification services across the EU.

- Also, the Directive's rules on **voluntary accreditation** seem to be misunderstood by national governments. Many European countries wrongfully consider voluntary accreditation schemes as a means of controlling whether or not a Certification Service Provider operates in compliance with the provisions of the Directive. Another alarming observation is that the voluntary accreditation schemes, in many European countries, are in practice, not really voluntary. A typical example being that many national e-government programmes only accept accredited CSPs to participate in the programme, and thus indirectly oblige a CSP to get an accreditation. This evolution is certainly not in line with the Directive's vision.

- Concerning the so-called "**public sector exception**" of Article 3.7, which allows Member States to make use of electronic signatures in the public sector subject to possible additional requirements, we have seen divergences in both the interpretation and implementation of this provision. It seems clear that in many countries the use of electronic signatures in the public sector is subject to additional

(security) requirements. Communicating electronically with public authorities is in many European countries possible only through the use of signatures based on Qualified Certificates issued by an accredited CSP. Member States need to be reminded that applying additional conditions can only be justified by objective reasons and should only relate to the specific characteristics of the application concerned. Also, Member States need to ensure that basic competition rules are not being infringed by their initiatives.

- As to the **conformity assessment of secure signature-creation devices** many countries seem quite reluctant to designate their own designated bodies for SSCD assessment. This may be due to the very high SSCD security requirements and the lack of active manufacturers in most countries. Another reason is the very large resources needed for operating an assessment body. The process of assessing a product is usually extremely expensive as well as time-consuming. Two further reasons why vendors are sometimes reluctant to have their products assessed is that an assessment is often only valid for a fixed amount of time (the product needs to be re-assessed), and a conformity assessment "freezes" a product so that it cannot be changed (e.g., in order to apply a security patch) without making invalid the assessment. Consequently, although but a small number of SSCDs have been assessed; all of these have been assessed by a relatively small number of designated bodies. Only in Austria, Germany and the Czech Republic has the number of products assessed been higher than two. In some countries (Austria, Germany) signature products other than SSCDs have been assessed as well

- The **non-discrimination principle of electronic signatures**, as regulated by Article 5.2 of the Directive, has been taken over by national legislators. However, the transposition of Article 5.2 has not always been explicitly done and in those countries with an explicit transposition the scope of Article 5.2 has not always been covered in its entirety. It is not yet clear whether this rather vague transposition in some countries has a practical impact on the legal use of electronic signatures. Thus, how electronic signatures will be treated in future national legislation and case law requires close monitoring.

- It would be too premature to jump to early conclusions on judges' position vis-à-vis electronic signature given that to date there are but a few legal cases on this subject. Indeed, until recently, the sample of **case law** tackling directly or simply evoking electronic signatures issues is still too small and fragmented to be considered as representative enough of the judge's mind in this area.

- As to the **legal effect of Qualified Electronic Signatures** (the ones regulated by Article 5.1 of the Directive), there has been a general tendency in the majority of European countries to explicitly recognise the equivalence between a handwritten

signature and a specific “type” of signature by imposing the same or slightly different conditions than the ones stipulated in Article 5.1. It is, however, important to know that the Directive obliges Member States only to make sure that a Qualified Electronic Signature is legally speaking treated in the same way as a handwitten signature, but that it does not regulate the legal use and consequences of a handwritten signature itself, and thus not the legal consequences of the Qualified Electronic Signature either. The legal use and consequences (which transactions need a signature, which evidential value is given to a signature, etc) remains a nationally regulated matter.

- Qualified electronic signatures need to be in compliance with the requirements as stated by the first three **Annexes** of the Directive. It is, therefore, important that the Annexes are correctly transposed into national legislation. The implementation of **Annex I** is very similar in most of those countries. The only risk is related to interoperability problems which might occur if technical implementations of Annex I diverge by, for example, not using ETSI TS 101 862, or any other common format for encoding the requirements of Annex I. The Commission should therefore promote the use of interoperability standards for the technical implementations of Annex I. For the implementation of **Annex II**, implementation levels are sometimes quite varying, meaning that the establishment and running of a CSP will differ considerably. Any organization wishing to establish a CSP business in several countries must therefore adapt itself to different requirements and procedures. Product vendors will also have difficulties building products for this very fragmented market. In addition, several countries put additional detailed and unnecessary requirements on the CSP, thus creating barriers for the establishment of a CSP. The Commission should therefore point out any unnecessary and excessive requirements for CSPs, which might be perceived as market obstacles. For the implementation of **Annex III**, there is also evidence of fragmentation. The requirements for SSCDs are, for example, much higher in Austria and Poland than in some other European countries. As far as **Annex IV** is concerned, Article 3.6 is very clear. The list contains only recommendations, which have to be taken into account by the Member States and the European Commission when they work together in order to promote the development and the use of signature-verification devices. They can, in our opinion, not be changed into obligatory requirements at a national level, as some Member States have done.

- With very few exceptions, all European countries have provided for a special **liability** provision transposing Article 6 of the Directive into national legislation. Within the European Union, the respective liability clauses of the EU Member States have followed the wording and rationale of Article 6. In cases where transposition was not explicit, the general tendency has been to provide stricter liability clauses, by

broadening the scope of application of the Article, notably, by extending the list of liability causes as laid down in the Directive.

- All countries under examination have prescribed in their national laws rules on the legal recognition of **foreign (non-EEA) Qualified Certificates** in their territory. Only Ireland, the UK and Malta, do not distinguish between domestic and foreign Qualified Certificates. Most of the EU and EEA countries have faithfully transposed the conditions of Article 7 into their national legislation. In the Accession and Candidate countries the situation appears to be somewhat more complicated.

- The implementation of the **data protection** rules of Article 8 into national legislation apparently did not pose any real difficulties. Some countries, though, did not correctly implement article 8.2 of the Directive. In those countries, a CSP is not obliged to follow the stricter data protection rules, whereas a CSP established in another Member State must adhere to its national rules. This may give rise to complaints of unfair competition in that it could act as an obstacle trade within the internal market. Further discussion also needs to centre on whether the stringent rules of Article 8.2 for CPS issued certificates to the public, (such as obligation to for direct personal data collection), are realistic, given that most CSP data is obtained from third parties such as a local registration authority. The use of a **pseudonym** in a certificate is allowed in all but two of the countries surveyed. Only Estonian and Bulgarian electronic signature legislation forbids the use of pseudonyms in their national rules on Qualified Certificates. Many countries explicitly require the disclosure of real names to the public authorities upon request and under strict conditions.

- An important question, which needs to be posed, is what does the **use of electronic signatures in Europe** really mean? The number of supervised and accredited CSPs issuing Qualified Certificates in the European countries varies considerably from country to country, with many countries having either no or only one CSP. In the few countries where any larger numbers of Qualified Certificates have been issued, this is almost exclusively due to some form or another of government promotion. There is currently no natural market demand for Qualified Certificates and related services. The largest application area in Europe for electronic signatures is generally linked to e-banking applications in a closed user environment, and thus outside the scope of the Directive. Within the scope of the Directive, very few applications are in use today and they are almost wholly limited to e-government.

- It is interesting to note that many application service providers currently on the market falsely believe that their applications require Qualified Electronic Signatures as a minimum in order to be legally compliant, leading to **unnecessary costs and complexity** on planning and designing for the use of Qualified Electronic Signatures.

- Technology evolves rapidly and in the near future many electronic signature technical solutions will be based on **new technological developments**, such as new secure PC environments, mobile signatures and signature servers. Consequently, supervision bodies, designated bodies and others involved in the regulation of Qualified Electronic Signatures should look at these technologies with an open mind and not restrict security assessments to what is known and available today.

- The lack of **interoperability**, both at national and cross-border level, is a big obstacle for market acceptance and the proliferation of electronic signatures. It has resulted in many isolated "islands" of electronic signature applications, where certificates from only one CA can be used for one application. In a few cases only can certificates from multiple CAs be used for multiple applications. Much more should therefore have been done earlier at a European level to promote interoperability.

- The EESSI (European Electronic Signature Standardisation Initiative) programme has developed some 30 **standards** that are Directive compliant. However, the fact that article 3.5 of the Directive does not allow to refer to all standards, as well as the delay in developing the standards and having their references published in the Official Journal, has led to a situation whereby several countries have either developed their own technical interpretations of the Directive, (leading to varying requirements in different countries), or else have waited for standards to be developed, leading to a vacuum for product and service vendors on the market. Not until the publication of references to standards in the Official Journal in July 2003 has there been any clarity on the standards acceptable to all Member States. Another risk relating to interoperability is that currently only one set of standards related to Qualified Electronic Signatures (based on PKI) currently exists, which may hinder further technologies being used for Qualified Electronic Signatures. Furthermore, due to the limitation of the A9C mandate, it has proven impossible to refer to additional standards."

Another exhaustive study of these issues and their effect was conducted on behalf of the European Commission in 2010 under the acronym CROBIES (Study on Cross-Border Interoperability of eSignatures), which is available for online consultation.[42] Briefly summarized, the CROBIES study identified, amongst other things, the following weaknesses and criticisms:

---

[42] Study on Cross-Border Interoperability of eSignatures (CROBIES), A report to the European Commission from SEALED, time.lex and Siemens (Version 1.0, 2010); available at http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm.

- The **legal framework is unclear and ambiguous** on certain important points. For instance, opinion is split in the Member States on the question of whether the concept of a 'signatory' can include legal entities, i.e. whether an e-signature can be ascribed directly to a company rather than to the person signing on behalf of that company. Similarly, it is still debated whether a secure-signature-creation device (SSCD) must undergo an affirmative conformity assessment by a designated body, or whether such an assessment is merely advisable to remove or reduce doubts on its status.
- The **technical framework is outdated** and does not link clearly to legal requirements. The Commission Decision above only references three specific standards which are partially outdated and do not unambiguously apply to some advanced e-signature creation approaches. For instance, the use of mobile telephones or HSMs (Hardware security modules) is increasingly popular in the advanced e-signature market, yet these are not clearly addressed by the referenced standards.[43] Furthermore, the EU standardization landscape is highly complex: beyond the aforementioned three standards, there are around 30 other standardization projects whose link to specific legal requirements is not clear. The fact that Commission Decisions under the Directive can only create a presumption of compliance with the requirements of Annex II(f) and Annex III of the Directive, and not with other requirements, makes it even harder to assess any formal value to these standardization documents.
- The **trust framework is too vague** to create justifiable trust in the internal market. As described above, CSPs issuing qualified certificates to the public are subject to national supervision schemes. However, the Directive merely requires that these supervision schemes are 'appropriate', without providing guidance to the Member States as to what this entails. As shown in the CROBIES study, national requirements range from a simple notification letter to the supervision body to full and periodically recurring audits, creating an uneven trust landscape, not to mention internal market distortions. Apart from this inequality, there was no homogeneous way for relying parties to determine whether a CSP was indeed supervised in practice, since supervision bodies did not have a common communication strategy on this issue. This problem was only addressed in October 2009 – ten years after the adoption of the Directive – when a Commission Decision[44] issued against the

[43] For instance, see Frederic Stumpf, Markus Sacher, Claudia Eckert and Alexander Roßnagel, 'The creation of Qualified Signatures with Trusted Platform Modules', *Digital Evidence and Electronic Signature Law Review*, 4 (2007) 61 – 6.

[44] Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market, OJ L 274, 20.10.2009 p. 36

backdrop of the Services Directive required supervising bodies to use a common trusted list approach to publicly announce the supervision status of their CSPs. Prior to that time, relying parties would need to check the supervision status of a CSP manually each time they wanted to rely on a signature. Similarly, when SSCDs have undergone conformity assessments (the need of which is already unclear, as noted above), there is no common approach to publish this status, and no way to keep this status updated over time as potential weaknesses threatening the SSCD status are uncovered.

Clearly, the legal, technical and trust frameworks established by the eSignature Directive have their flaws. It should be noted however that these flaws primarily apply to qualified signature solutions, since questions related to supervision and SSCDs are much less relevant to other signature types. Nonetheless, since the eSignature Directive only created a clear and predictable legal effect for these types of signatures, this can be considered a real weakness.

While important, these problems could be fixed through limited changes and updates of the legal, technical and trust framework. There is, however, a broader weakness in the Directive, which would require substantially greater changes. As noted above under the description of the scope of the Directive, its provisions clearly focus principally on electronic signatures as a substitute for hand written signatures. This emphasis disregards the reality that finding a substitute for hand written signatures is only one possible application of certification services.

As described in the definitions section above (Section 2 of this document), the relationship between eSignatures and other services (including identification, time stamping, electronic registered mail etc) is more nuanced. eSignatures are ultimately an assertion, generated by a combination of tools (e.g. SSCD, card reader, keys) and services (e.g. certificate issuance, time stamping). Only a few of these tools and services have been regulated by the current eSignatures Directive, despite the fact that all of them are being used on the European internal market today. eSignatures both build on these other tools and services, and serve as a building block for others, without these tools and services being regulated. In other words, the eSignatures Directive focuses on one link in a chain, without considering the full picture.

(Corrigendum to Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the points of single contact under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market (OJ L 274, 20.10.2009) OJ L 299, 14/11/2009 P. 0018 – 0054); as amended by the Commission Decision of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States, OJ L 199, 31.7.2010, p. 30.

The main question is what the European policy goals with respect to this full chain of products and services should be. If the goal is merely to ensure that these products and services related to eSignatures can benefit from a formally free market, then the eSignatures Directive is largely adequate. Clearly, the Directive is not perfect in this respect. Market distortions remain due to e.g. the differences in supervision regimes at national level, meaning that two otherwise identical CSPs in two different Member States might be subject to vastly different supervision requirements, thus creating additional expenses and a competitive disadvantage for CSPs in stricter countries. Similarly, the internal market clause does not have a clear impact on public sector applications (e.g. for eGovernment services), as Article 3.7 of the Directive leaves a fairly vague margin of appreciation for Member States to impose additional requirements on eSignatures used in public sector services. As a result, it is frequently unclear whether restrictions imposed by Member States are a legitimate application of Article 3.7, or a violation of the Directive's rules.

None the less, in spite of these clear shortcomings which still need to be rectified, the Directive already includes market access rules and internal market principles (Articles 3 and 4) that apply to certification-service-providers and certification-services in general. This would include IAS service providers and IAS services in general, without any limitation towards eSignatures. As a result, prior authorisation schemes for such services would not be permitted (Article 3.1), nor any other type of restriction towards the provision of such services originating in another Member State (Article 4.1), and the service providers would largely be subject to the laws of the Member State in which they are established (Article 4.1). Finally, the free circulation of electronic-signature products is guaranteed by (Article 4.2).

Thus, a free market for IAS services in general has already been established to a large degree. However, with respect to eSignatures, the Directive made a further choice to not only open the market, but also to assign a legal value to certain eSignatures, based on a series of requirements and obligations, especially with respect to CSPs issuing qualified certificates to the public. This second facet has not been regulated for other IAS services. The question is whether it should also be a European policy goal to also go one step further for these other IAS services, by e.g. also set minimum standards and requirements for other tools and services in order to provide them with a clear legal value as well.

A strong argument can be made for this position. As noted above, more and more IAS services are emerging on the European market. If the only common European regulation relates to free market access, Member States may introduce national regulations that specify requirements in order to achieve a certain legal effect (although they may obviously not impose requirements for merely being allowed to provide services within their borders, as this would be contrary to the Directive's free market rules). However, such regulations can also distort the European internal market for IAS services: even if an IAS service provider is allowed to provide services in other Member States (as guaranteed by the

eSignatures Directive), it cannot provide guarantees with respect to the legal value of its services, at least not without assessing this against local legislations. Worse yet, such legislation may be contradictory between countries, meaning that a service provider would at the very least need to modify its service offering on a per country basis, or simply be unable to benefit from any legal value in some Member States. De facto, this is a significant disruption of the IAS market in Europe.

From that perspective, the Directive's primary focus on eSignatures as a substitute for hand written signatures means that it is unable to create trust at the European level in IAS service providers. This would suggest that the current situation is contrary to the goals of the Digital Agenda, and that a broader approach is required.

As an example, an eSignature as a substitute for a hand written signature is only meaningful if it can be adequately linked to a signatory, either as an identifiable individual, or at least by a pseudonym. Indeed, the eSignature Directive recognizes this issue, as it defines certificates as electronic attestations "which link signature-verification data to a person and confirm the identity of that person" (article 2.9). Similarly, advanced[45] signatures under the Directive must (amongst others) be "uniquely linked to the signatory"[46] and " capable of identifying the signatory" (article 2.2). Thus, when eSignatures are intended to emulate hand written signatures, identification is a prerequisite. Yet the Directive does not address how this should be done, other than to note that the use of pseudonyms in certificates "should not prevent Member States from requiring identification of persons pursuant to Community or national law" (recital 25). This requirement is echoed in Annex II (d) in relation to qualified signature certificates, noting that CSPs must "verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued." Identification (either as an independent process preceding the issuing of signature certificates or as a separate type of authentication service) is not harmonized by the Directive in any meaningful way.

The same observation applies to time stamping, another type of certification service that supports the determination of the authenticity of eSignatures. The value to be given to an eSignature is partly predicated on the mechanism used to reliably determine when it was created. This is a crucial question, since relying parties mainly need to be able to assess whether an eSignature was valid at the time it was created, not merely at the present time (which may be years later). The time factor is an important pillar to the trustworthiness of

[45] Interestingly, no such requirement applies to the base notion of "electronic signatures", for which the Directive requires that they 'serve as a method of authentication' in general. This is in line with the observation made above, namely that electronic signatures in general could be interpreted to cover *any* application of authentication services, but that the Directive only provides a meaningful legal framework for eSignatures as a substitute for hand written signatures.

[46] For a critical analysis of this concept, see Stephen Mason, *Electronic Signatures in Law*, 4.9.

eSignatures and a valuable certification service in its own right. Again, the Directive does not cover this aspect in a meaningful way.

Other ancillary services build on these tools: electronic archiving depends on time stamping,[47] and electronic registered mail requires both reliable identification of the signatories (senders and recipients alike) and time stamping. In the absence of the basic tools, the derivative services cannot be created either.

In short, it is important to recognize that eSignatures are a component of an ecosystem of certification services. When the Directive covers only one element of that ecosystem (and imperfectly at that, as argued above), new market distortions will inevitably arise. Some Member States have already made the decision of creating their own national legal frameworks for some of these certification services, including time stamping, electronic registered mail and archiving. In the absence of harmonizing provisions at the European level, this is creating new internal market barriers: a "qualified time stamping service" in Member State A may have no legal value in Member State B, either because Member State B has no legal framework for this type of service, or because the legal framework is different. In practical terms, the time stamping service provider has no way of learning about possible issues other than to seek legal advice on a country by country basis, in order to discover whether its service has any value outside of its national borders, and what changes might be necessary to satisfy national legal requirements. This would appear to be a textbook example of the type of barrier that the European internal market should aim to avoid.

Based on these observations, it would appear that the eSignature Directive is in serious need of review, at a minimum to fix the smaller issues mentioned above. However, this may also be a good opportunity to broaden the legal framework to ensure that certification services are more comprehensively covered and to avoid further barriers in the internal market. Obviously, the lessons learned from the eSignature Directive should be considered if this broader approach is taken.

---

[47] Stefanie Fischer-Dieskau and Daniel Wilke, 'Electronically signed documents: legal requirements and measures for their long-term conservation' *Digital Evidence and Electronic Signature Law Review*, 3 (2006) 40 – 44

5. The road ahead

5.1 How useful is the eSignatures Directive as a starting point for IAS regulations?

The Digital Agenda has unambiguously announced a revision of the eSignature Directive, which will probably strive to fix at a minimum the shortcomings summarized elsewhere in this report, together with a possible Decision to ensure mutual recognition of certain eIDs between Member States. This would undoubtedly be a good step forward for the EU. None the less, a broader approach seems equally viable, building on the observation that e-authentication systems (to use the terminology of the Digital Agenda) are similar in most respects, but differ in small important details.

This can already be witnessed in the terminology as discussed above: the definition of an electronic signature as presented by the Directive ("data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication") is broad enough to potentially cover eSignatures (in the equivalent-to-hand-written sense), eID and time stamping, among many others. It is worth considering whether a similar policy framework is also possible, and even desirable, for these related services.

As a starting point, it is possible to consider prior experiences across the Member States. The need for a legal framework for ancillary services (time stamping, company seals, electronic registered e-mail, long term archiving) has been known for some time, and some Member States have been active in this field. To name but a few examples:

- Austria, as one of the leading EU Member States in this area, has implemented legislation regulating not only eSignatures, but also electronic identification, through the 2004 eGovernment Act.[48]
- Belgium adopted a generic legal framework for certain trusted services in 2007,[49] including electronic registered mail, time stamping and electronic archiving. Despite a recent update for the rules on electronic registered mail in 2010 (integrated into the general eSignatures Act), executive rules were never fixed, and the law remains largely inoperative at present. However, new legislation in this area is planned for the near future.

[48] E-Government-Gesetz.

[49] Wet van 15 mei 2007 tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten/ Loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance.

- The Czech Republic has implemented rules for time stamping in its eSignatures Act of 2000.[50] Interestingly, the law uses the same logic and terminology ('qualified time stamp') that is also in vogue for eSignatures.
- Estonia, as another technology leader in the EU, has a legal framework[51] that supports (and indeed requires) time stamping, digital stamps (advanced eSignatures created by legal entities), and official e-mails.
- Similarly, Finland has adopted an Act on strong electronic identification and electronic signatures.[52]
- Germany likewise introduced the notion of qualified time stamping in its eSignatures Act.[53]
- Italian law contains rules on electronic registered mail.[54]
- The Slovakian eSignatures Act contains specific rules for time stamping.[55]
- The Slovenian eSignatures Act recognizes the concept of a time stamp as being comparable to advanced eSignatures, with the same rules applying by changing those things which need to be changed;[56]
- Finally, the Spanish Act on Electronic Citizen Access to Public Services[57] recognizes eSignatures, e-seals (company signatures), and time stamping.

This listing is neither fully up to date nor exhaustive. Its purpose is merely to illustrate that a significant and increasing number of Member States have recognized the important role of e-authentication systems other than mere eSignatures, and that they have provided a legal

---

[50] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu).

[51] Digitaalallkirja seadus, RT I 2000, 26, 150.

[52] Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, 7.8.2009/617.

[53] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) vom 16.5.2001 (BGBl. I S. 876).

[54] Through the Codice dell'Amministrazione Digitale (the current version is Decreto Legislativo 30 dicembre 2010, n. 235); Roberta Falciai and Laura Liberati, 'The Italian certified e-mail system', *Digital Evidence and Electronic Signature Law Review, 3 (2006) 50 – 54.*

[55] Zákon č.215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov –The Slovakian Act ('as amended' or 'v znení neskorších predpisov') was consolidated in 2009 (§9 of this Act still explicitly refers to time stamping (Časová pečiatka – time stamping)), see http://www.zbierka.sk/zz/predpisy/default.aspx?PredpisID=208862&FileName=zz2009-00076-0208862&Rocnik=2009.

[56] Zakon o elektronskem poslovanju in elektronskem podpisu.

[57] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

framework for such services. When doing so, these laws are often integrated or at least closely aligned with general eSignature rules.

This is important for two reasons. First, it suggests that the principles and challenges for various e-authentication systems are similar, and that it might be possible to address them in unison. Second, it also shows a potential internal market barrier. If time stamping service provider A can guarantee the legal value of its services in one country (for instance, because it is considered a qualified time stamping service in that country) but not in another country (for instance, because that country has no rules, or worse yet, different ones), then that creates a market barrier. This is a challenge for the EU to address, as it was an almost identical observation that lead to the adoption of the eSignatures Directive.[58]

Indeed, if we look at the conceptual needs behind a comprehensive IAS policy as listed above, we already commented that all of these were already addressed (even if imperfectly) by the eSignatures Directive:

- An unambiguous understanding of IAS services and ancillary services
- The policy goals that an IAS approach should cover, including such aspects as the enabling of the internal market, technological neutrality and legal reliability.
- The legal translation of these policy goals and requirements, stipulating the goal of the regulatory text, definitions of basic concepts, provisions on general obligations for trust service providers, data protection, liability, internal market rules, legal effect of services, any supervision/accreditation mechanisms, etc.
- The trust framework needed to support a comprehensive IAS approach.
- The technical framework required to enable the comprehensive IAS approach, including standardisation needs.

At least theoretically, this suggests that it would be possible to apply the same approach to a comprehensive IAS framework.

[58] For example, see the table of diverging national legislations on p. 4-5 of the 1998 Proposal for a European Parliament and Council Directive on a common framework for electronic signatures, at http://ec.europa.eu/information_society/policy/esignature/docs/com1998_0297en.pdf. The table is strikingly similar to the list above.

5.2 Weaknesses of the eSignatures Directive – lessons learned

The overview above suggests that the regulatory approach of the eSignatures Directive might be applied to IAS services in general. However, it should also be recognize that the eSignatures Directive has a number of weaknesses that would need to be addressed in future policy initiatives. For a full analysis of these, we can refer to earlier studies referenced above. In the section below, some of the main lessons learned are summarized, based on the conclusions and recommendations of these earlier studies.

5.2.1 Supervision of CSPs

- The European Member States have always had difficulties in striking a balance between “appropriate supervision” of Certification Service Providers and the prohibition to submit their activities to prior authorization. It would therefore be useful to publish guidelines on how the supervision can be organized in order to make it conform to the Directive’s provisions.
- The guidelines to be published by the European Commission can also be used to clarify a number of currently unresolved legal issues in this area. One of the most difficult questions is to know what the notion of “establishment on the territory” in practice means for a Certification Service Provider (for example, certificate issuer established in one Member State but collaborating with registration authorities, directory service providers, etc. in other Member States: who is in charge of the supervision?).
- Not all Member States have established a scheme for the appropriate supervision of CSPs issuing Qualified Certificates to the public. This would need to be rectified, because this situation creates the possibility for CSPs established in those Member States to issue Qualified Certificates to the public in other Member States without being submitted to appropriate supervision. This harms the trust model behind the Directive.
- Ideally the supervision schemes in the Member States should be harmonized, at least to a certain degree.
- Since EESSI already has published a number of valuable documents in this area it is recommended that supervisory authorities be encouraged to make use of these specifications. Use of such specifications by supervisory authorities has to be closely monitored.

5.2.2 Voluntary accreditation

- Measures should be taken in order to clarify the vision of the European legislator with regard to voluntary accreditation schemes for Certification Service Providers. Specifically, cross-border accreditation should be encouraged as a way of facilitating interoperability. The Commission should, on the other hand, discourage as much as possible the establishment of *national* accreditation schemes for Certification Service Providers issuing Qualified Certificates to the public.
- The Commission should stimulate the clustering of efforts on a Community level. The objective should be to establish a limited number of high quality European accreditation schemes, preferably focusing on or specialising in specific categories of certification services for application domains.

5.2.3 Secure signature-creation devices.

- Partly because the Directive currently sets very high requirements on SSCDs, such devices still find their way to the market too rarely. In order to stimulate the production of secure signature-creation devices, the requirements for formal assessment need to be more homogeneous, clear and flexible in the future. The procedures for obtaining a conformity declaration should be shorter and less costly. The European Commission should support every effort in this direction.
- As to the rules to be followed by the designated conformity assessment bodies, the Commission should provide coordination and guidance. The Commission Decision of 2000 on the minimum criteria when designating conformity assessment bodies is a valuable first step but needs to be pursued. The independent, transparent and non-discriminatory character of the assessment procedure should ideally be monitored.

5.2.4 Public sector exception

- The Commission should clarify the interpretation of the conditions that are needed before the Member States can use the “public sector exception” of Art. 3.7 of the Directive. Member States should be made aware that the non-discrimination rule of Art. 5.2 of the Directive applies not only to the private but also to the public sector. This provision of the Directive can be misused to justify a lack of interoperability in eGovernment applications, which is hardly the intent of the European lawmaker.

- Efforts towards improvement of interoperability between e-government programmes and particularly between their electronic signature applications should be supported or initiated at a European level.

5.2.5 Qualified Electronic Signatures

- With regard to Art. 5.1 there is primarily a need for clarification about the scope of this provision. It should be made clear to all interested parties that 1) “qualified electronic signature” is not a synonym of “legally valid electronic signature” and 2) fulfilling the requirements of a qualified electronic signature is one – but by no means the only - way to allow equivalence to handwritten signatures.
- From a European perspective the success of Art. 5.1 depends entirely on the availability of a very well standardized and easily recognisable European qualified electronic signature, including not only criteria for creation devices and certificates but specifying the complete signature chain. Recent efforts in the context of the Services Directive (such as the aforementioned establishment of national trust lists) can serve as significant enablers in this respect; and similar initiatives could be considered for other requirements with respect to qualified electronic signatures, such as SSCDs.
- Member States should be made aware that the concept of the qualified electronic signature is mainly useful for cross-border transactions in Europe. It serves as a “passport” that guarantees in every Member State the application of the rules applicable to handwritten signatures.
- The Annexes have been more or less literally transposed into national legislation by virtually all the countries surveyed. The remaining task is to make sure that the implementation gets streamlined throughout Europe. Every effort in this direction should be supported. National implementations of the Annexes have, on the other hand, to be firmly discouraged.
- The Commission should take action against those Member States who have not correctly transposed the Annexes by, for example, translating the recommendations of Annex IV into requirements for qualified electronic signature at a national level.

5.2.6 Non-discrimination rule

- With regard to the application of Art. 5.2 there is a primary need for clarification. All interested parties should be better informed about the objective and the scope of this provision.
- The Commission should systematically examine if the Member States have issued legislation referring to Qualified or Advanced Electronic Signatures and detect where such references don't comply with the rule of Art. 5.2.

5.2.7 Standardization

- The Commission and Member States must ensure that all Member States correctly implement the presumption of conformity with standards referenced in the Official Journal. This has not always been the case in all Member States.
- The Commission and Member States should encourage further work on standards related to Annex II (f) and Annex III, in order to promote the use of alternative technologies for qualified electronic signature. Although the present standards are mostly technology neutral (within the framework of PKI), they still favour the use of smart cards as SSCDs, for example.
- The long-term maintenance of the standards referenced in the Official Journal must be ensured, either by transferring the current CWAs to a more permanent body, for example ETSI, or promote the CWAs to European Norms.
- The Commission must urgently ensure the acceptance of a common specification for algorithms and parameters, as well as a common maintenance procedure for that specification.
- The complex areas of archiving and long-term validation of electronically signed documents are often perceived as obstacles for the use of electronic signatures. The Commission should promote work on guidelines and standards in these areas.
- The Commission and the Member States should find mechanisms to promote/recommend the standards for interoperability already developed by ETSI within the framework of EESSI.

5.2.8 Data protection

- It is necessary to ensure that any electronic authentication process complies with personal data protection requirements. The current European regulatory framework is very much focused on the use of identity certificates. In recent years, attention has shifted towards better privacy protection in the online environment. Research has been done on various possibilities combining electronic authentication with the needs for anonymity or the use of multiple virtual identities. The efforts of the European Union to promote advanced personal data protection for its citizens should not be contradicted by its regulatory framework for electronic authentication. Closer examination is needed on the possibilities to combine anonymity and pseudonymity with the provisions of the eSignatures Directive.

These lessons should be taken into account for any future update of the eSignatures Directive, and especially when contemplating the extension of the eSignatures Directive to cover other IAS services.

5.3 What are the alternatives?

The overview above shows that the regulatory approach of the eSignatures Directive, while having clear weaknesses to be addressed, could conceptually be applied to other IAS services as well. However, it should also be recognized that there are alternative approaches, and that a single comprehensive legal framework (an 'IAS Directive', with national 'IAS supervisory bodies' and European generally recognized 'IAS standards') may not be the most effective approach. All alternatives need to be duly recognized.

Conceptually, a number of options are available to the Commission. Apart from the two default policy options (i.e. the 'no policy option' of having no framework at all, and the 'status quo option' of keeping the eSignatures Directive as is), the following possibilities are theoretically available:

- A lighter, simpler eSignatures framework, based e.g. on the 2001 UNCITRAL Model Law on Electronic Signatures[59], at the exclusion of any other IAS services;
- A light IAS framework based on the New Approach regulatory style;
- Making only minimal changes to the eSignatures Directive to address some of the shortcomings mentioned above, but without further touching upon other IAS services;

[59] See http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2001Model_signatures.html

- Adopting separate directives (or other regulatory instruments) for each IAS service to be covered as the need is recognized (an eSignatures Directive/Decision, an eID Directive/Decision, a Time stamping Directive/Decision, etc.). A mixture of these instruments could also be considered, as is suggested by the actions of the Digital Agenda (which suggests a revision of the eSignatures Directive without speculating yet on what the result would be; and a Decision on the mutual recognition of eIDs);
- Adopting a comprehensive IAS Directive.

In the following steps of this Study, we will develop and assess the possible options for a future IAS policy framework.

6. Conclusions

The current Directive is very strongly focused on one IAS business model, namely the provision of services aiming to create eSignatures as substitutes for hand written signatures, which was the centre of the attention from 1998 and 2000 but which has progressively been replaced by a much more heterogeneous and complex IAS market situation. The regulatory framework thus includes, for example, quite detailed rules for certificate providers issuing signature certificates to the public but does not deal with other categories of IAS or trust service providers. The regulatory needs relating to other categories of trust service providers are nevertheless at least as urgent as those with regard to certification authorities. There is, for example, a clear need for regulation dealing with archival service providers, or with registered mail services. From a users' perspective it is difficult to understand why such services remain completely unregulated, while at the same such a complex regulatory framework has been established for issuers of certificates.

In the table below, the main policy goals with respect to IAS services are summarized, along with a brief mapping to the current scope of the eSignatures Directive, and a high level proposal for expanding the scope of the eSignatures Directive to cover other IAS services, while addressing the weaknesses of the current legal framework as described above.

6.1 IAS – summary of challenges and goals from a policy perspective

General Policy objective: "to facilitate the smooth working of electronic transactions in the internal market" (as noted in the Tender specifications for this Study) This implies that IAS services should be addressed as a **market service**, and that the goal of a European policy framework for IAS should be to **enhance trust in IAS services** for users				
Specific policy objectives as described in the Digital Agenda	Free internal market for IAS services (i.e. no prior authorisation or legal restriction; and application of country of origin rules)	Free internal market for IAS products (i.e. free circulation of compliant products)	Cross-border legal acceptance of IAS (i.e. legal validity of IAS services should not be questionable)	Promoting the market IAS related services and products (i.e. legal framework for IAS must be conducive to enable trust)
Does the current legal framework match the policy objectives? Current Directive limited to "data authentication" (cfr recital 4 and 8)	Free internal market for certification services (no authorisation, country of origin) See art. 3.1 and art. 4.1	Free internal market for signature products (no authorisation, country of origin) See art. 4.2	Cross-border legal acceptance of electronic signatures See art. 5	Promoting the market of data authentication related services and products See recital 11
Challenges in relation to eSignatures based on the current Directive	Ambiguities lead to diverging application (supervision processes and criteria)	Ambiguities lead to diverging application (assessment requirements, processes and criteria)	Ambiguities lead to diverging application (SSCD requirements, supervision processes)	Too many ambiguities; bad alignment between legal, technical and trust framework.

Challenges in relation to IAS based on the current Directive	Limited difficulties, but internal market obstacles for IAS services may be created through national laws	Internal market obstacles due to ambiguity of the scope of the provisions of the Directive: are IAS services other than eSignatures affected and how? This is uncertain.	No cross-border legal acceptance of other IAS related results (time-stamp, seal, archive, …)	No promotion of other IAS products and services. The current Directive does not enable this in any meaningful way
Envisaged legal framework for IAS services: what changes are needed?	Broaden the scope of the internal market clauses. Ensure that IAS services are unambiguously covered.	Broaden the scope of the internal market clauses Ensure that IAS products are unambiguously covered.	Introduce legal acceptance clause for other IAS results and introduce similar minimum requirements for IAS results	Promote the market of other IAS products and services
How can changes be implemented?	Option 1: broaden definition of certification service provider or broaden definition of electronic signature (currently limited to 'data authentication') Or Option 2: introduce new definitions for IAS service providers	Option 1: broaden definition of electronic signature product Or Option 2: introduce new definition for IAS products	Implement similar regimes as for electronic signatures, i.e. combination of general acceptance clause and equivalence clause for other IAS services. Establish equivalent requirements for other IAS services.	Make reference to other IAS services and products in recitals Ensure scope of internal market clauses also includes IAS services and products

Clearly, while the eSignatures Directive is a conceptually sound model, further IAS guidance is needed in order to enable trust in IAS market services, as required by the Digital Agenda. Existing practices and examples will be identified and assessed in Deliverable 2 of this Study, and policy options will be defined in deliverable 3, along with a proposal for a suitable legal framework for IAS services.

6.2 Perspectives for a future comprehensive trust services framework

While more precise proposals for a future trust services framework will be developed in future deliverables of this Study, the viability of a model based on the approach of the current eSignatures Directive can already be briefly demonstrated in this section, building on some of the observations made above.

The definitions provided in Section 2 of this document can be used as a basis for the establishment of a new IAS policy. Considering the IAS policy challenges and goals as described above, the figure below provides an illustration of a possible structure for a future IAS trust services framework, which would need to be implemented in practice through appropriate legal, technical and organisational outputs.

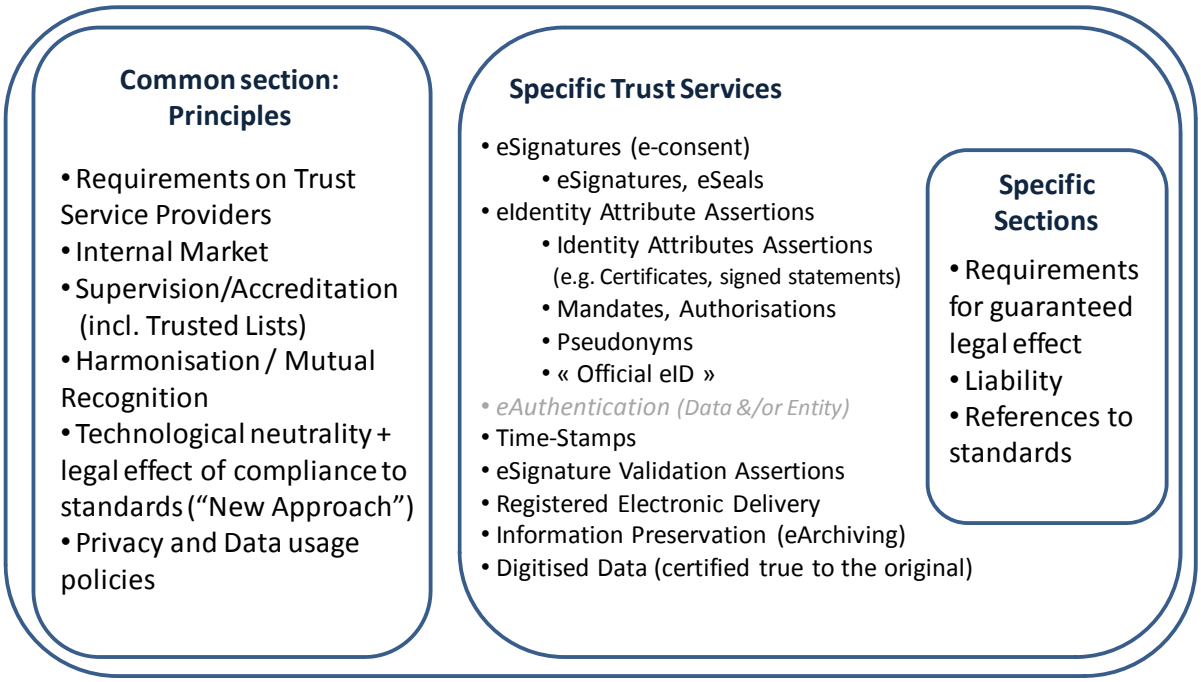


Figure 8

As the above figure illustrates, it should conceptually be possible for a future IAS policy framework (including the legal translation of this policy into e.g. a Directive or a Decision) to establish a series of common principles for all trust services, and to define the unique characteristics of each trust service in a separate section. These trust service specific sections could be structured as listed in the figure above. A first trust service type would then correspond to electronic signatures (as currently also covered by the eSignatures Directive), establishing rules for different types of signature (from simple to qualified, as well as depending on the type of signatory –

signature or seal), the signature creation devices and Signature Generation Service Providers. The second section would cover among other elements TSPs issuing certificates.

As is currently already the case for eSignatures, specific provisions would apply to trust service tokens that meet the requirements laid down in a specific annex/list ("qualified tokens", in analogy with qualified signatures), and which would be provided by a Trust Service Provider who fulfils the requirements laid down in a specific annex/list (analogous to CSPs issuing qualified certificates to the public under the present Directive), so that these tokens can then benefit from a predictable and harmonized legal value. If desired, policy provisions and technical requirements could be aligned on multiple levels of assurance (LoA), as illustrated in the Table 1 below.

	ESig	ESeal		Time-Stamp	Digitised Data	Digital Certificate	RED	RED receipt	I.P. Archive	IAA	SCD/ACD	Signature Validation Assertion
Qualified (LoA4)	AdESig + QC + SSCD	AdESeal + QC + SSCD		QTST	QDD	QC (corresponds to QCP+ certificate policy)	QRED	QREDreceipt	QIPA	QIAA	SSCD/ SACD	QSVA
	Equivalent to Handwritten signature	Legal Certainty		Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty	Legal Certainty
LoA3	$AdESig_{QC}$	$AdESeal_{QC}$				(corresponds to QCP certificate policy)						
LoA2	AdESig	AdESeal				(corresponds to NCP+ or NCP certificate policy)						
LoA1	ESig	ESeal				(corresponds to LCP certificate policy)						

Table 1

Obviously, it is not necessary for multiple levels of assurance to be defined for each type of trust service (indeed, for some trust services the existence of multiple levels of assurance may not be meaningful), but the model is flexible enough to allow this if desired, or to allow standardisation bodies to standardise on these matters. For some service types, including specifically electronic identification, this is an important asset.

The model may also be further aligned to the "quality classification scheme for eSignature elements" defined in CROBIES[24] WP 5.2 (depicted here below) and the "eSignature Business factors" approach underlying a business guidance approach to electronic signature implementation as annexed to the ETSI/CEN Draft Special Report Rationalised Framework for eSignature standardisation[6].

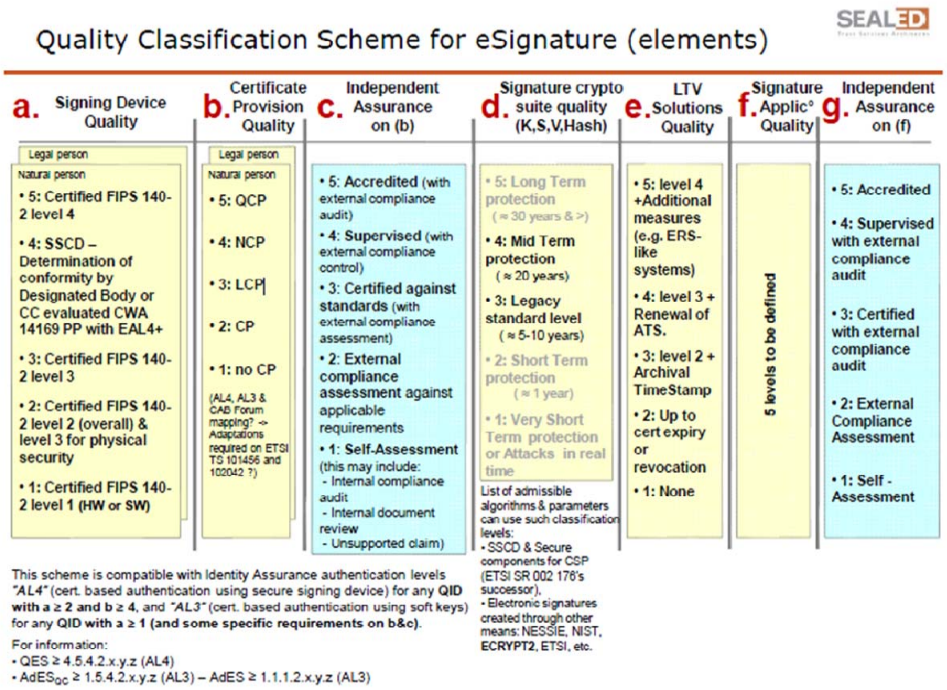


Figure 9

Clearly, there are many ways to formalize and structure this vision, as already explained above (see Section 5.3 - What are the alternatives?), and difficult choices will need to be made on the types of trusted services to be covered by a future European IAS policy framework. This question will be examined and addressed by future deliverables of this study. None the less, the brief outlined presented above may serve as an illustration that a comprehensive trust services framework based on a set of common principles appears to be conceptually viable, and would be capable of addressing the European policy goals in this area.

7. Appendices

7.1 Abbreviations

AdES	covers $AdES_{ig}$, $AdES_{eal}$, and $AdES_{tamp}$
AdESeal	Advanced Electronic Seal
AdESig	Advanced Electronic Signature
AdEStamp	Advanced Electronic Stamp
$AdES_{QC}$	Advanced Electronic Signature supported by a Qualified Certificate
CRL	Certificate Revocation List
IAA	Identity Attribute Assertion
IAAP	Identity Attribute Assertion Provider
IPSP	Information Preservation Service Provider
IUI	Inimitable Unique Identity
OCSP	Online Certificate Status Protocol
PKC	Public Key Certificate
QC	Qualified Certificate
QES	Qualified Electronic Signature
RED	Registered Electronic Delivery
REM	Registered Electronic Mail
SGSP	Signature Generation Service Provider
SP	Signature Policy

SSCD	Secure Signature Creation Device
SVSP	Signature Validation Service Provider
TASP	Trust Application Provider
TL	Trusted List
TSL	Trust-service Status List
TSP	Trust Service Provider
TSP_{PKC}	Trust Service Provider issuing Public Key Certificates
TSP_{QC}	Trust Service Provider issuing Qualified Certificates
TSSLP	Trust Service Status List Provider
TSSP	Time Stamping Service Provider
TST	Time Stamp Token
TSrT	Trust Service Token
UI	Unique Identity

7.2 Workshop report: analysis of comments received

7.2.1 Scope of the present section

The IAS Study team committed to send to the Commission updated and finalized deliverables D1 and D2 integrating the feedback received at the Study workshop held in Brussels on 3rd of October 2011 as well as integrating feedback received after the workshop via the IAS Study website or any other means of communication.

Surprisingly, most of the received comments do not specifically relate to deliverables D1 and D2, but are rather oriented towards the description of gaps identified in the Directive 1999/93/EC and / or are focusing on topics that respondents found relevant to introduce in the framework of a new Regulation on IAS.

The present section bundles the received inputs and classifies them into considerations that have an impact on D1 and/or D2 on one hand, and elements that are more relevant to take into account for the establishment of the new Regulation on IAS.

In particular, the present section distinguishes elements that impact D1 and/or D2 directly and proposals or comments that cannot be taken up directly, while providing an explanation why these proposals or comments cannot be taken into account.

Based on the conducted review of the feedback and inputs received, it appears that the general observations and analysis of the study team's first report were relatively widely accepted as valid and that most of the relevant proposals were either already present in the deliverables, or that they relate specifically to the definitions in D1.

Thus, instead of amending D1 with each and every respondent's proposals (which are occasionally contradictory between the various correspondents and do not take into account the subsequent discussions with the Commission), the IAS team prefers to keep the initial terminology without modifying D1. Any modifications would create the risk of some respondents feeling that definitions are moving away even further from their inputs than before. Rather than introducing such harmful dichotomy, the IAS team prefers to consider the initial D1 definitions as a starting point for the establishment of the definitions, considering that the proposals from the respondent, when relevant, have been taken into account for building the ad-hoc deliverable together with the outputs of the discussions with the Commission.

7.2.2 Summary workshop feedback

a. Topics to consider for the IAS regulation

Firstly, it is clear that the general observations and analysis of the study team's first deliverable D1 were relatively widely accepted as valid. Notwithstanding smaller concerns highlighted in the "IAS project Workshop report" delivered to the Commission in October 2011 – notably with respect to the importance of context and the role of eConsent as an element of eSignatures – the report therefore seems fundamentally suitable as a basis for taking the study to the next stages.

For those next stages however, and notably with respect to the drafting of policy proposals, several concerns were raised. A red thread within these comments was the need to retain a 'light touch' framework, and notably to ensure that not all details are set in stone by future regulations. Thus, the study team will need to state carefully why certain proposals would be necessary and proportionate to achieve the EU's policy goals, in order to ensure that it remains as 'light touch' as possible without endangering the achievement of these policy goals.

A similar observation was also made with respect to the scope of future proposals. The extension of regulations to cover electronic identification and ancillary services causes some concerns with some of the stakeholders. It is often not yet clear what the market for these services is, or indeed whether there is a significant market for them, and the regulatory framework should take care not to disrupt the evolution of these markets by creating (rather than removing) barriers. However, other comments go in a diametrically opposite direction, pleading for this extension as ancillary services are intrinsically linked to eSignatures and already covered by national/local rules.

Finally, stakeholders repeatedly emphasized the need to ensure that the IAS framework (including legal and technical aspects) is capable of aligning with international evolutions. The key goal is interoperability on an international market, and the creation of a European island of harmonized service should be avoided.

b. Specific comments and impacts on D1 and D2

A few very specific comments were raised during the workshop, specifically with regard to the terminology used in IAS D1:

- A series of comments recommends tackling privacy more closely, in particular by considering concepts like "untraceably", "transparency", "anonymity", "pseudonymity", etc.

- Some of the core concepts within D1 are questioned as they should also consider the processes and context; context is an important factor for defining identity, and this is currently not recognized in the definitions.

In addition, with regard to the initiatives to consider in IAS D2:

- A participant recommends that IAS team takes into account several initiatives not mentioned yet in D2. In particular, NATO is also developing a plan for "managing access to global commons" (incl. cyberspace). They are looking to establish standards as part of an international cyber security strategy. Also, a recent Interpol study showed through two reports on identity fraud that ID fraud is a top enabler for crime, leading to parliamentary initiatives.

  Outcome: *These projects are not mentioned as such. Identity fraud should be fought amongst other with a sound IAS regulatory framework, but requires a separate framework upstream from generic IAS rules, and is thus considered as beyond the scope of the IAS study.*

- A participant recommends that the IAS team takes into account the ABC4trust initiative.

  Outcome: This project is already mentioned in D2.1.

7.2.3 Specific feedback received from individual experts

The study team received further feedback after the workshop from individual experts, largely in the form of written contributions. The received feedback is analysed in the sections below per respondent. Before exploring them in some detail, it is however worth highlighting some trends that deserve more emphasis, as most of the respondents share a convergent opinion on these topics.

- A large concern for privacy is expressed – in relation of Identification and Authentication especially – and most of the respondents draw our attention to the principles of "privacy by design" and "user-centric privacy", based on minimal data disclosure technologies (on a need-to-know basis), zero-knowledge cryptography, combined or not with the intervention of identity provider, untraceability, untrackability, anonymity, pseudonymity, etc. A few respondents explicitly refer to the ABC4Trust initiative active in that field.

- Many comments insist on the need to deal with the legal entity signature (or eSeal).

- Some of the comments suggest that besides considering a regulation on IAS, one also needs to consider the relevance and potential benefits of having no regulation.

Finally, it is worth noting that the concept of “consent” as being inherently linked to eSignatures is debated. Some respondents are strongly in favour of unambiguously binding an eSignatures with “consent” (or “commitment” or “intention to sign”) of the signatory on the signed data, while others are reluctant as this would limit the scope of the eSignature concept in general.

7.3 Sources of IAS use cases

FIDIS	Future of Identity in Information Society – www.fidis.net	Cases: • fidis-wp2-del2.2_Cases__stories_and_Scenario.pdf • fidis-wp2-del2.6_Identity_in_a_Networked_World-UseCases.pdf
Modinis (2005-2007)	https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome	
Prime	"Privacy enhancing identity management" research project – FP6 – www.prime-project.eu	Cases: • https://www.prime-project.eu/prime_products/reports/reqs/pub_del_D2.2.a_ec_WP2.2_v5_Final.pdf
PrimeLife	The FP7 continuation of Prime – www.primelife.eu	
STORK	Secure idenTity acrOss boRders linked - www.eid-stork.eu	Cases: - D4.2 Final Report on eID Process Flows - D7.4 Common specifications A2A - List of Commission A2A services of Common Interest
TAS3	Trusted Architecture for Securely Shared Services – www.tas3.eu	


DLA PIPER


SEALED
Trust Services Architects


time.lex


PRICEWATERHOUSECOOPERS


SG
A

Study on an electronic identification, authentication and signature policy (IAS)

IAS in Europe:

an overview of the state of the art

Final Version (D 2.2.b)

18 January 2013











This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the general invitation to tender of the Directorate-General Information Society and Media, n° SMART N° 2010/008. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.

Table of contents

1. SUMMARY OF THE STUDY GOALS AND SCOPE 5
1.1 Background of the Study 5
1.2 Scope of the Study 5
1.3 Role of this document in the Study 6

2. OVERVIEW OF CURRENT LEGISLATIVE LANDSCAPE AT NATIONAL, EU AND INTERNATIONAL LEVELS 8
2.1 Relevant laws in Member States: scope, impact and gaps 8
2.1.1 Austria 8
2.1.2 Belgium 13
2.1.3 Czech Republic 25
2.1.4 Estonia 29
2.1.5 Finland 30
2.1.6 France 36
2.1.7 Italy 42
2.1.8 Romania 45
2.1.9 Slovakia 50
2.1.10 Slovenia 52
2.1.11 Spain 53
2.2 Relevant laws from outside of the EU: scope, impact and gaps 56
2.2.1 Brazil 56
2.2.2 Malaysia 59
2.2.3 United States of America 61

3. OVERVIEW OF CURRENT NORMATIVE LANDSCAPE AT EU LEVEL 65
3.1 eSignature standardisation framework 65
3.1.1 Mandate M460 - a Rationalised Framework for European eSignature standards 65
3.1.2 Inventory of eSignature standards 71
3.1.3 Work Programme 72
3.2 Identity and Authentication standardisation framework 72
3.2.1 ETSI SIM 72
3.2.2 ETSI identity pre-standardisation efforts 73
3.2.3 CEN initiative in standardising cyber identity and unique identification of legal person and parts thereof 73
3.2.4 CEN TC 224 WG's 74

4. LEADING STUDIES, PROJECTS AND POLICY INITIATIVES 79
4.1 Identity and Authentication 79
4.1.1 The private sector perspective: scope, impact and lessons learned 79
4.1.2 The public sector perspective: scope, impact and lessons learned 81
4.1.3 The service supplier/vendor perspective: scope, impact and lessons learned . 86
4.1.4 The academic perspective 89
4.1.5 Beyond the EU Member States 91
4.2 eSignatures 94
4.2.1 European Commission driven actions 94
4.2.2 Use of eSignatures in Large Scale Pilots: scope, impact and lessons learned 100
4.2.3 European sector specific initiatives 102
5. CONCLUSIONS 103

1. Summary of the Study goals and scope

1.1 Background of the Study

The purpose of the present project, as described in the tender specifications, is to study the feasibility of a comprehensive EU legal framework that would apply to electronic assertions needed to secure electronic transactions as well as the ancillary services needed to use them: electronic identification, authentication, signature, seals, certified delivery. The perspective would be to facilitate the smooth working of electronic transactions in the internal market. In other words, it would be based on article 114 of the Treaty on the Functioning of EU (TFEU).

The Digital Agenda confirms that "*Electronic identity (eID) technologies and authentication services are essential for transactions on the internet both in the private and public sectors. Today the most common way to authenticate is the use of passwords. For many applications this may be sufficient, but more secure solutions are increasingly needed. As there will be many solutions, industry, supported by policy actions – in particular eGovernment services - should ensure interoperability based on standards and open development platforms.*"

The Commission, therefore, will "*In 2011 propose a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems*". This Study aims to provide inputs for this action.

1.2 Scope of the Study

The scope of this study is to determine if and how a comprehensive European IAS framework could be formed, including the legal, technical and trust components required for such a framework.

The study should include recommendations on how a complete and functioning legal, technical and trust framework for IAS services could be constructed. This recommendation should build on consultations of selected experts through direct discussions and workshops, as well as the feedback received through the Commission's 2011 public consultation on electronic identification, authentication and signatures.

1.3 Role of this document in the Study

The present Study mainly consists of three tasks that correspond to a logical phase in the study. The phases and tasks can be graphically summarized as follows:

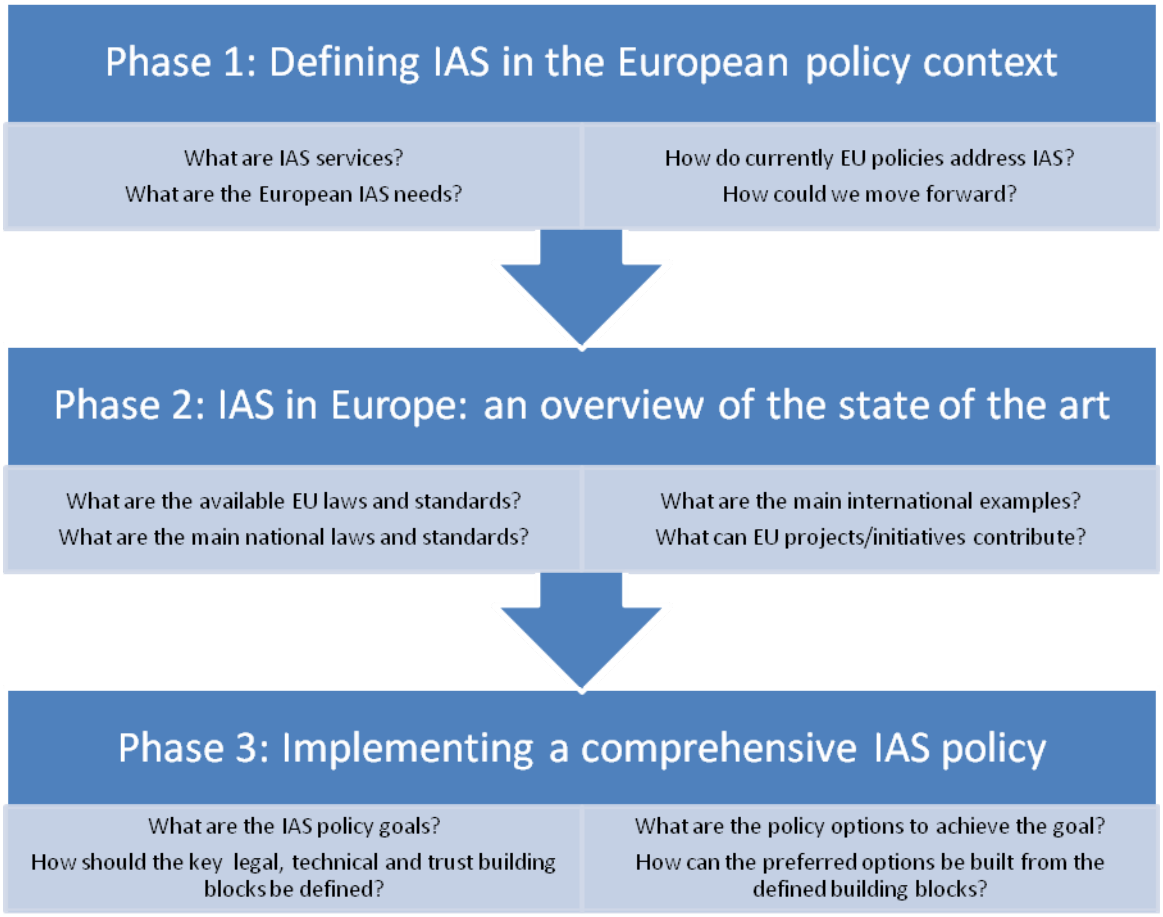


Figure 1: IAS study phases

The current document is Deliverable 2.1 - IAS in Europe: an overview of the state of the art, and corresponds to Phase 2 in the overview above. The goal of this report is:

- to **provide a summary** of the main IAS initiatives from a legal, technical and policy perspective that may impact the creation of a comprehensive European IAS framework. Specifically, this report will attempt to identify the main relevant past realisations, their scope, and any lessons learned.
- on the basis of this overview, this report will then **identify any gaps** to be filled or **inconsistencies** to be harmonized.

- finally, the overview of past initiatives (including laws and standards) can serve to **identify good practices**, which might prove useful **as a model for IAS policy at the European level**.

This document has been finalized in two iterations:

- An initial draft version of D.2.1. This document outlines the study team's initial thoughts and opinions on the four aspects outlined above. This draft was presented to the Stakeholders for discussion.
- Based on the feedback received, a final version has been produced. The analysis of the feedback received from experts and from the workshop shows that the initial deliverable D.2.1 considers the state-of-the in the field of IAS in a quite complete and appropriate manner as the comments from the experts and the workshop refer either (mostly) to initiatives already considered in the deliverable or (sometimes) to initiatives out of scope of the study. For the details on each and every feedbacks and justification on the reason why some comments can eventually not be considered within D2, the reader is invited to read the document annexed to the final version of D1.1.

As indicated in the graphic above, this report is one of the key inputs for the recommendations of phase 3. Specifically, the good practices identified in this report have been a valuable input for drafting EU policy recommendations that are grounded in national practice and experience.

2. Overview of current legislative landscape at national, EU and international levels

2.1 Relevant laws in Member States: scope, impact and gaps

As has already been briefly signalled in the first deliverable of this study, several Member States have gone beyond the scope of the eSignatures Directive by implementing a legal framework that more profoundly impacts IAS services, e.g. by providing requirements for time stamping services, electronic registered mail, or certain subcategories of eSignatures (e.g. company seals or public sector signatures).

Clearly, these laws can be very instructive as examples to any future European IAS regulatory initiatives, by highlighting how services can be defined, what requirements (if any) should be imposed, and what legal effect (if any) should be attached to them. In the sections below, we will examine the relevant legislations of Member States who have taken such a more extensive approach towards IAS.

It should be emphasized that the overviews below are likely not complete. It has been drafted based on an extensive review by the study team of available literature; however, given the relative novelty of this policy area, it is not unlikely that some legal initiatives may not be included in the list below.

2.1.1 Austria

a. General approach and scope of legislation

As one of the EU's leading countries with respect to eGovernment, Austria has adopted legislation regulating not only eSignatures through the eSignatures Act (*Signaturgesetzes*[1]), but also electronic identification, through the 2004

[1] See http://www.signatur.rtr.at/en/legal/sigg.html

eGovernment Act (*E-Government-Gesetz*[2]). Both of these expand significantly on the basic scope of the eSignatures Directive:

- the eSignatures Act introduces rules for time stamping (*Zeitstempeldienste*), including qualified time stamping (*Qualifizierte Zeitstempeldienste*);
- the eGovernment Act supports the use of the Citizen Card (*Bürgerkarte*) concept, i.e. the use of a means of authentication (not necessarily in the form of a smart card) for the purposes of identification, electronic signing and storing representation data[3]. Thus, apart from general eSignature rules, the Act also provides rules with respect to identity and authenticity (§2-3). Furthermore, as an eGovernment act, it also provides rules for a specific category of signatures for civil servants (the *Amtssignatur,* §19) and for the authenticity of printouts of electronic documents (§20).

For the eSignatures Act, the added value compared to the eSignatures Directive can be summarized as follows:

- the entire Act is stated to apply equally to CSPs issuing qualified signature certificates or qualified time stamping certificates (§1.3);
- the qualified time stamp (*qualifizierter Zeitstempel*) is defined in §2.12 as "an electronic assertion stating that specific electronic data has been presented at a specific point in time, which meets the security requirements of this Federal Act and of any regulations issued on its basis";
- high level requirements for qualified timestamping service providers are stated in §10, focusing on the requirements to implement appropriate security guarantees to ensure the accuracy and authenticity of its assertions, and in documenting its approach to ensuring the reliability of its services through its policies. Trustworthy systems, products and processes must be used for the creation and storage of timestamps that provide protections against modification that ensure technical and cryptographic security. Signature creation data are to be kept secret, and the TSP must ensure that qualified time stamp data cannot be forged or manipulated without detection.

---

[2] See http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230

[3] See http://ec.europa.eu/idabc/servlets/Doc097b.pdf?id=32320

- Both for qualified signatures and qualified time stamps, the security requirements of §18 must be met. This paragraph also allows the adoption of more specific security requirements, and requires conformity assessment bodies to determine compliance.
- More specific requirements have been set through the eSignature Ordinance[4], for which §11 defines requirements for qualified time stamping. These include notably:
- The mandatory use of an SSCD, and compliance with algorithms and parameters specified in Annex to the Ordinance;
- The use of certificates that are intended specifically and exclusively for the purposes of time stamping, and which have been marked as such;
- Data and time must be asserted in CET, specifically in summer time; any other time zones must be specifically mentioned;
- The TSP may not allow deviation from the real time exceeding one minute;
- Any restrictions in the availability over time of the service must be explicitly communicated.
- Interestingly, the legal effect of qualified time stamping is not defined along with the legal effect of qualified electronic signatures (§4), nor anywhere else in the Act, other than in the definition of the qualified time stamp itself ("stating that specific electronic data has been presented at a specific point in time").

With respect to the eGovernment Act, the approach can be briefly summarized as follows:

- The Act defines crucial concepts such as identity, unique identity, identification, authenticity and authentication in §2. The following definitions are used:
    - "Identity": the designation of the individuality of those involved by characteristics that are particularly well suited to allow them to be distinguished from others; including through such characteristics as

[4] See http://www.signatur.rtr.at/en/legal/sigv.html

their name, date and place of birth, but also the company number or alphanumerical numbers;

- o "Unique identity": the designation of the individuality of those involved by one or more characteristics, allowing them to be uniquely distinguished from all others;
- o "Identification": the process of validating or establishing the identity;
- o "Authenticity": the truthfulness of a declaration of will or of an act, in the sense that the claimed author can be determined to be the actual author;
- o "Authentication": the process of validating or establishing authenticity.

- A Citizen's card is in turn defined as a logical unit that allows the creation of a qualified signature and which contains a so-called 'identity link' (*Personenbindung*), and which may also contain representation data.
- The identity link is issued by the sourcePIN (*Stammzahl*) Register Authority. It is a signed SAML record containing:
  - o the sourcePIN which is the citizen's unique identifier derived from the Central Resident Register (or the Supplementary Register)
  - o the citizen's name and date of birth
  - o data that links the identity link to the qualified certificate stored on the token
  - o the signature of the sourcePIN Register Authority
- The sourcePIN may only be stored in the identity link in the citizen card, thus is under sole control of the citizen. SourcePINs otherwise benefit from explicit legal protections (§12).
- The eIDM model implemented using the citizen cards is based on sector-specific PINs that are derived from the sourcePINs. Using cryptographic one-way functions the sector-specific identifiers are calculated so that the citizen is uniquely identified in one sector, but identifiers in different sectors cannot be unlawfully cross-related. The Sector Delineation Regulation (E-Government-Bereichsabgrenzungsverordnung - E-Gov-BerAbgrV) defines 26 sectors of State Activity so that within each sector using the same identifier no data protection issue is caused.

- In electronic communication with the public sector, access rights to personal data can only be granted if the unique identity and the authenticity of the access request can be demonstrated. Identification is however not a routine process: the Act specifies that it may only be requested by a public authority insofar as this is necessary in the course of its official function (§3).

- Despite the designation of being an eGovernment Act, it also specifies certain rules for using the citizen card in the private sector (§14-15). Companies can use the citizen card to derive private sector-specific PINs that are unique within their sphere, but cannot be cross-linked with identifiers of other entities.

- For electronic signatures created by public administrations, so-called “official signatures” (*Amtssignatur*) have been defined in the eGovernment Act (§18). Official signatures are indicated by an attribute in the certificate (an object identifier). They serve to facilitate recognition of the fact that a document originates from an authority. The official signature is represented in the electronic version of the document by an image which the authority has published on the Internet. Furthermore, the public authority is required to provide information on how to validate the signature.

- Finally, the eGovernment Act specifies that eDocuments signed with an official signature have equal legal value to official attestations (*öffentlichen Urkunde*) (§19). The print-out of the document itself must indicate a website where it can be electronically validated.

b. Lessons learned

Both Acts are very instructive on a number of points:

- With respect to the eSignatures Act, the simple integration of qualified time stamping (and only qualified time stamping, without any nonqualified level) is interesting. The legal effect is indirectly stated, namely by noting its function in the definition, and through its security requirements (e.g. allowing only one minute of deviation with the actual time). Otherwise, very few additional provisions appear to have been necessary, in comparison to the generic eSignatures rules.
- With respect to the eGovernment Act, the definitions are highly instructive, especially the distinction between identities and unique identities. The implementation is very privacy oriented and reliable, building on official identity registers and obfuscating the primary identity number through a mechanism of context specific derivative numbers via the identity link. However, this is also an approach which may be harder to transpose to other countries, given the reliance on pre-existing infrastructure (notably reliable identity registers and a unique identification number) implemented through Citizen Cards.
- The official signature is an interesting concept, especially in combination with the eDocument validity and validation information obligations (i.e. their legal equivalence to official attestations and the support for validation of print-outs, which facilitates the transition between paper and electronic documents).

2.1.2 Belgium

a. General approach and scope of legislation

(a) Applicable legislation

The first legal instrument of relevance is the **preliminary draft** of a bill which would expand the scope of the current E-signatures Act of 9 July 2001 by integrating ancillary services such as electronic archiving and electronic registered mail in the current E-signatures Act. Due to ongoing difficulties with the government in Belgium,

there has been a delay in reviewing and adopting legislation which are deemed to be non-urgent.

A part of this preliminary draft, namely the chapter on electronic registered mail, was introduced in the Act of 13 December 2010 since this fit in with the liberalisation of the postal sector. This new legislation modified the act governing the organisation of postal services in Belgium and introduced legal constraints for the electronic registered mail in the Act of 9 July 2001. "Electronic registered mail" was defined as "any service of electronic data transfer that includes a lump sum guarantee against the risk of loss, theft or damage of the data, in which the sender, possibly at his request, receives proof of sending and/or of delivery to the addressee. Under the modified E-signatures Act, electronic registered mail was considered to meet the requirements of registered mail, unless further regulatory requirements apply. In the absence of such requirements, electronic registered mail will be usable in all cases where traditional registered mail is legally required.

The constraints included in the Act of 13 December 2010 were to be effective on 30 June 2011. Unfortunately, Belgium passed the legislation forgetting to notify the European Commission and without following the provided procedure under the "transparency" European Directive saying that any Act for the information society domain must be notified to the European Commission and is subject to a standstill period of 3 months to give the Commission the time to develop an opinion on the compliance of the Act at the European level. The Act of 13 December 2010 did not comply with this standstill obligation and was published without notification and therefore the Act was withdrawn. Nevertheless, the preliminary draft still awaits approval by the Belgian government and is expected to be implemented into national law in the near future.

Apart from this preliminary draft, there is also a second legal instrument which requires mentioning, namely the **Belgian Act of 15 May 2007** concerning the establishment of a legal framework for certain trusted service providers. The Act foresees that for each of the services specific provisions must be determined in executive (royal) decrees, at the latest on 1 December 2007.

However, due to the long-lasting difficulties within the Belgian government (or lack thereof), the Act never fully entered into force due to missing executive (royal) decrees.

What follows is a summary of the most noteworthy provisions of these two legal instruments.

(b) Preliminary draft

New definitions – The Act introduces a number of new concepts and also further specifies and/or broadens a number of existing notions:

- "**Certification service provider**" is broadened by the following lyrics in italics: each natural or legal person who issues and manages certificates, *or provides electronic archiving services or services of electronic registered mail*, or other services regarding electronic signatures.

- The concept of "**administration**" is broadened and adapted by the following lyrics in italics: *the services of the General Directorate Energy of the FPS Economy, S.M.E.s, Self-Employed and Energy* which is charged with the tasks regarding accreditation and verification of the certification service providers which issue qualified certificates, *qualified electronic archiving services or services of qualified electronic registered mail services* and are established in Belgium.

- The definition of "**electronical archiving service**" is added and defined as "service which primarily exists of retaining electronic data and which is provided by a certification service provider of which is exploited for the own account of a natural or legal person."

- The definition of "**electronic registered mail service**" is added and defined as "service provided by a certification service provider regarding the transfer of electronic data which exists of safeguarding on a flat-rate basis against the risks of loss, theft or damage of the data, whereby the sender, where appropriate upon his request, receives an acknowledgement of the delivery and/or of the order of the sending to the addressee."

- The definition of "**qualified electronic archiving service**" is added and defined as "electronic archiving service provided by a certification service provider who meets the requirements set forth in Annex V of this Act or which is exploited for its own account by a natural or legal person which meets the requirements of abovementioned Annex, except for the letters l, m and n."

- The definition of "**qualified electronic registered mail**" is added and defined as "electronic registered mail service which is provided by a certification service provider who meets the requirements set forth in Annex VI of this Act."

Scope – The scope of the preliminary draft is broadened (in comparison to the current legislation) by adding, apart from electronic signatures, electronic archiving and electronic registered mail. The tasks of the certification service providers, as mentioned in the Act, is broadened from only providing (qualified) certificates for electronic signatures to providing (qualified) certificates for electronic archiving services and electronic registered mail services.

The possibility for the King to require additional demands in a Royal Decree for the use of electronic signatures in the public sector is broadened to the option to requiring additional demands also for qualified electronic archiving services or services of qualified electronic registered mail.

The scope of chapter V of the Act is broadened from only applying to certification service providers which issue certificates, to certification service providers which also provide qualified electronic archiving services or qualified electronic registered mail services.

New provisions – A number of new provisions has been introduced by the Act. Firstly, the Act foresees that the certification service provider which provides qualified electronic archiving services or qualified electronic registered mail services to the public, can be held liable for the damage he inflicts to each entity or natural or legal person which is due to the non-compliance of the requirements set forth in respectively Annex V or Annex VI of the Act, unless the certification service provider can demonstrate that there is no negligence on his behalf. Such certification service provider can determine the restrictions on the use of his service, provided that these restrictions are recognizable to third parties. The certification service provider is not liable for damage resulting from the use of the service whereby the indicated restrictions of use are transgressed.

It was also added that in the event an acquisition of the activities of a certification service provider is not possible, the certification service provider must inform the users of his services of the termination of his services without delay and offer them the possibility to transfer the files to another service provider within two months at no additional cost or to have the retained data returned.

The following provision on documents accepted as proof was added: "Subject to the application of the specific legal and regulatory requirements a transcript realised by means of a qualified electronic archiving service is considered to constitute a trustworthy and sustainable transcript in the sense of article 1335bis of the Civil Code."

The following provision was also added: "The explicit or implicit requirement of a registered mail can be met provided that the sender used an electronic registered

mail service. Subject to the application of specific legal or regulatory requirements regarding registered mail, a qualified electronic registered mail is considered to meet the explicit or implicit requirement of a registered mail."

Finally, when the contract regarding the electronic archiving is terminated, for whatever reason, the provider of the electronic archiving service cannot invoke a retention right on the data towards the recipient of the service. At the termination of the electronic archiving contract, for whatever reason, the provider of the electronic archiving service must ask the recipient of the service by registered mail what should happen with the data which were given to him. In the event the recipient fails to answer within three months, the service provider may proceed with the destruction of the data, provided that there is no explicit prohibition from a judicial authority or competent administration to do so.

Requirements for certification service providers – Annex V, containing the requirements for certification service providers of qualified electronic archiving services, and Annex VI, containing the requirements for certification service providers of qualified electronic registered mail services, are added. Both Annexes include requirements of reliability, security, transparency and financial stability (including liability insurance), and also describes at a high level which organisational processes are required to implement the services. More specifically, the certification service providers must:

a. Demonstrate that they are sufficiently trustworthy to provide certification services.

b. Only retain and consult the data insofar it is necessary for the execution of the service.

c. Taking into account the state of the art, take all adequate technical and organisational measures to secure the data against accidental or unauthorised destruction, loss, modification, damage or access by unauthorised third parties.

d. Apply the necessary measures to detect the normal and deceitful transactions to which the data are subject. The certification service provider must, to the extent possible, identify those who perform such transactions. He must register these data, ensure the dating of the data and retain the registered data during the entire retention period of the data concerned.

e. Take the necessary measures to keep the data legible at least during the legal or regulatory or contractual term.

f. Apply the necessary measures, taking into account the state of the art, to avoid any modification of the retained electronic data during the retention, consulting or transfer, except for the modifications regarding the carrier or the electronic format of the data.

g. Return the requested data in a legible and usable format as discussed with the recipient, within a reasonable period of time upon request of the recipient of the service.

h. Implement a system which prevents the voluntarily destruction of the archived data in order to completely or partially repair the data.

i. Work with specialised personnel, and where appropriate with subcontractors, who have the specific knowledge, experience and qualifications necessary for carrying out their services, and to submit them to a confidentiality obligation.

j. Use a dating system by means of electronic registration based on the coordinated universal time each time the date and/or time must be determined.

k. Use, when scanning original paper documents, a system which reproduces the original document in electronic format in a trustworthy manner.

l. Offer transparency towards the recipients regarding the offered provision of services.

m. Demonstrate impartiality towards the recipients of their services and towards third parties.

n. Dispose of sufficient financial means to be able to provide the service in accordance with this Act and its executive decrees and particularly to be able to manage liability for damage, by in any case be covered by an adequate insurance.

o. At the time of sending of the message, provide the identified addressee with a proof of sending, including an electronic signature in the sense of article 4 §4 of this act or any other procedure which is contractually acknowledged as equal to a handwritten signature, indicating:

- the identification of the service provider: trade name, address and electronic address;

- the name of the recipient (addressee) as reported by the sender;
- the date and time on which the message was processed by the system.

p. Guarantee the originality of the data by means of adequate security techniques, taking into account the state of the art.

q. Allow the sender to be correctly identified and the moment of sending be correctly indicated.

r. Prior to the sending being delivered, with or without proof of sending, appropriately verify the identity of the addressee of the electronic registered mail, or where appropriate the identity of the proxy.

s. Upon request of the sender, and depending on the circumstances, deliver the proof of sending or refusal of the message by the addressee, of the proof of non-delivery. This proof is provided with the date on which the message was received or refused by the addressee and contains an electronic signature of both the service provider and the addressee in the sense of article 4 §4 of this act, or any other procedure which is contractually acknowledged as being equal to a handwritten signature. The proof of non-delivery must be provided after expiration of a term of fifteen days, starting from the date of sending of the message.

[*Please note: requirements d - h and k: N/A for certification service providers of electronic registered mail; requirements o - s: N/A for certification service providers of electronic archiving*]

Verification and sanctioning – Since the scope of the Act would be broadened to, apart from electronic signatures, also electronic archiving and electronic registered mail, the verification and sanctions as specified in chapter VII of the Act also apply to the certification service providers of electronic archiving services and electronic registered mail services.

(c) Act of 15 May 2007

Definitions – Each of the four services covering electronic data are defined in the Act. The definitions align with the definitions included in the Belgian Act of 11 March 2003 on the legal aspects of information society services. In practice anyone, either

legal or natural person, can be a recipient of a trusted service. The trusted service may be used for either professional or other purposes.

- "**Provider of electronic archiving service**": each natural or legal person which, usually in exchange for a remuneration and upon request of the recipient of the service, provides *electronic archiving services, whereby the retaining of the electronic data constitutes an essential element of the offered service*. This definition covers anything which can be retained by a service provider in one way or another, regardless of the carrier (CD-rom, hard drive, etc.) or regardless of the type of data (documents, connection data, etc.). The definition does not entail that the offered archiving service must be the principal activity of the service provider. Important to mention is that the electronic archiving of authentic deeds and documents which concern tax, judicial or social matters are explicitly excluded from the scope of the Act.

- "**Provider of electronic time registration service**": each natural or legal person which, usually in exchange for a remuneration and upon request of the recipient of the service, provides *services regarding the time registration of a set of electronic data*. This definition is very broad in a sense that it allows any service to be eligible for electronic time registration. However, this definition does not indicate which method(s) of time registration can be used. The Explanatory Memorandum clarifies this point by indicating that especially time stamping must be considered. This technique of time stamping does however not register or date electronic data, as is incorrectly suggested in the definition. In reality it is a technique whereby the hash value of a file is sent to a server. The server will then return a digitally signed certificate with the exact time indication. The time is taken over from the atomic clock.

- "**Provider of electronic registered mail service**": each natural or legal person which, usually in exchange for a remuneration and upon request of the recipient of the service, provides a *service existing of safeguarding on a flat-rate basis against the risks of loss, theft or damage, whereby the sender, or when appropriate upon his request, receives a proof of the delivery and/or of the order of the sending to the addressee*. The way of defining electronic registered mail services copies the procedure which is applied for physical registered mail. The functions aspired by the physical registered mail are not necessary implemented in an identical way in an electronic environment. Proof of sending and reception in such environment is mostly taken care of on the level of the server, through automatic and secured audit trails.

Functional equivalence is not achieved by copying the formal procedure but by starting from the functions which have to be achieved.

- "**Provider of service regarding the temporary blocking of sums of money**": each natural or legal person which, usually in exchange for a remuneration and upon request of the recipient of the service, *in light of an agreement concluded electronically and on a distance , provides a service aiming to block a sum of money which is deposited by the recipient of the service, and on the depositing of that sum of money to the addressee who is bound to deliver a good or a service in case the latter does not comply with his obligation*. The purpose of this service is to block the purchase price on the account of a neutral third party in order to prevent that bad faith sellers would receive money without ever delivering the goods or services.

Scope – The Act applies to trusted service providers who are established in Belgium. Trusted service providers who are established elsewhere therefore do not need to comply with the provisions of the Act, and therefore cannot provide services which are compliant with the Belgian standards to generate certain legal consequences.

The Act relates in particular to four services which cover electronic data, namely archiving, time registration, registered mail and temporary blocking of sums of money. Trusted service providers, such as notaries or banks, will have to apply divergent rules depending on whether they process paper or electronic documents.

A number of minimum quality standards is required, which are common to all four trusted services. The minimum quality standards concern (i) impartiality, (ii) data processing, (iii) transparency, (iv) expertise, (v) confidentiality and (vi) liability for damage. These quality standards resemble the requirements included in Annex V and Annex VI of the preliminary draft as discussed above. To each of the quality standards, a system of verification and criminal sanctioning is linked.

In addition to the quality standards which are set forth in the Act, executive (royal) decrees were expected to set forth specific provisions for each of the four services, and to determine the legal value attributed to the data which is electronically archived, electronically time stamped or sent through electronic registered mail. In addition, these decrees were also planned to determine the verification and notification procedures of which the Administration disposes, as well as the criminal sanctions which can be imposed. Because of the fact that this Act was drafted very quickly due to urgency, the Act relied on executive decrees for the further elaboration of the legal framework. However, these executive decrees were never taken and therefore the Act lacks effectiveness.

Another point of criticism regarding this Act is that it is not entirely consistent with the philosophy of the European legislation in this domain since it hampers the cross-border provision of services on a European or global scale. This was also included in the European Commission's remarks on the preliminary draft of this Act.

Quality standards – The quality standards must be seen as a completion of the obligations to which the service providers were already subject based on general contract and liability legislation as well as legislation on commercial practices and information society services. The quality standards are in turn completed by the system of verification and criminal sanctions.

The legislator is of the opinion that in the event these quality standards are complied with, this will attribute legal consequences to the electronic documents, data or sendings. For instance, regarding electronic archiving, the electronically archived document will be considered equal to the paper archived document, until evidence of the contrary. Concerning the electronically registered mail, the service will be estimated to fulfil the same functions as are traditionally attributed to the traditionally registered mail, until evidence of the contrary.

- **Impartiality**: the trusted service provider must demonstrate impartiality towards the recipients of their services and towards third parties. This implies that the trusted service provider must abstract its own financial dependence from that of the client. Since it is not specified what "impartiality" really implies and who are considered to be "third parties", it is advised to assess the impartiality of the trusted service provider on a case by case basis.

- **Data processing**: Subject to the application of the Data Protection Act of 8 December 1992, the trusted service provider cannot withhold the received data for any purpose. This provision not only implies that the data processor must comply with the provisions of the Data Protection Act, but also that the data processor and the data controller (person responsible for the data processing) must conclude an agreement stipulating the liability of each of the parties involved. This obligation is sanctioned with a criminal penalty (namely a fine up to 137.500 EUR). In addition, the trusted service provider must, taking into account the state of the art, apply reasonable measures to secure the received data and in particular prevent the data from being transformed, damaged or made accessible to unauthorised third parties. This security obligation applies to both personal data and other data.

- **Transparency**: the trusted service provider must offer to the recipients of the services, prior to the contract being concluded, direct access to the

following information, which must be formulated in a clear and comprehensible way:

- the exact way and conditions of the use of the services;
- the functioning and accessibility of the services;
- the security measures taken;
- the notification procedure regarding incidents, complaints and disputes;
- the offered guarantees;
- the scope of their liability;
- the scope of the insurance coverage;
- the exact operation modes and conditions of the trusted service, including the imposed restrictions regarding the use thereof, especially concerning the legal consequences attached to the trusted service; relevant elements of that information must, upon request, also be put at the disposal of third parties who rely on the trusted service;
- in the event the trusted service has been notified, the accreditation number received by the service provider from the Administration.

This transparency obligation should allow recipients of the trusted services to make an informed decision on which trusted service provider they prefer to rely on, which is why the transparency obligation is formulated as a pre-contractual information obligation. Trusted service provider should carefully oblige this transparency obligation, as it is sanctioned with a fine of up to 55.000 EUR.

- **Expertise**: the trusted service provider is expected to work with personnel which disposes of the specific skills necessary for the provision of the services. The legislator does not confer any concrete requirements, so it is up to the trusted service provider to personally determine of which skills his personnel must dispose to adequately provide the services.
- **Confidentiality**: the trusted service provider must submit its personnel to a confidentiality obligation. Although this is not specifically mentioned in the Act, it can be derived from this provision that the trusted service provider is

also personally bound to treat the data received with confidentiality. More specifically all data which can be expected to have a confidential or sensitive nature fall under this confidentiality obligation. This obligation also applies to all information exchanged during the pre-contractual phase. In practice this implies that the trusted service provider will need to include confidentiality clauses in the employment contracts with his personnel or temporary workers, and will have to install additional organisational measures. This obligation is not specifically sanctioned by the Act, so that there has to be reverted to the general liability provisions of civil law to see which sanctions apply.

- **Liability for damage**: the trusted service provider must dispose of sufficient financial means to be able to provide the service in accordance with this Act and its executive decrees and particularly to be able to manage liability for damage, by in any case be covered by an adequate insurance. It has not been further specified what must be understood by "sufficient financial means".

Verification measures – The Act foresees a warning procedure initiated by the Minister of Economy or the civil servant appointed by him, whereby the offender is demanded (by registered mail with receipt of by delivery of a copy of the report in which the factual elements are determined, or by electronic registered mail) to terminate the infringing act. This allows the offender to comply with the provisions of the act without risking the criminal sanctions of the Act.

The civil servants appointed by the Minister of Economy are authorised to detect and identify the acts prohibited under this act. The detection and identification by the civil servants is supervised by the attorney general or the federal attorney.

In the event the damage inflicted to a third party is fully repaired, the civil servants appointed by the Minister of Economy may suggest to the offender the payment of a sum of which the payment will cancel the criminal proceedings. The amounts are to be determined by executive decree, and cannot be inferior or higher than the minimum and maximum fines foreseen by the Act. The offender is not obliged to consent to the proposition of settlement and is free to choose to defend himself during criminal proceedings.

Sanctions – The Act foresees fines from 1.375 up to 137.500 EUR for persons infringing the quality standards and for hindering the detection and identification by civil servants of prohibited acts. In the event of a criminal conviction it is advisable to inform the recipients of the trusted service on this, by affixing or publishing the judgment in newspapers or elsewhere.

2.1.3 Czech Republic

a. General approach and scope of legislation

(a) Electronic signatures

Legislation – The legal framework on electronic signatures in the Czech Republic is provided by the Electronic Signatures Act 227/2000 Coll. Ordinances belonging to this Act are the Ordinance on electronic filling rooms 496/2004 Coll., Ordinance on qualified certification service providers procedures 378/2006 Coll., and the Government Decree 140/2000 Coll. on the list of free trade licences. The (very limited) Government Decree 495/2004 Coll. implements the Electronic Signatures Act and lays down rules for public authorities in very general terms. The Decree further specifies which authorities have to provide electronic access and which information they have to provide.

Due to lack of power and resources of the Ministry of Informatics (which was closed in 2007 and competences were transferred to the Ministry of Interior), the attempts in the Czech Republic to establish a centrally coordinated e-government failed. Consequently, the other administrative bodies created their projects independently of the wishes of the Ministry of Informatics. At this moment, the e-government is created by many applications developed in different ways by different public administration bodies. This however is not a coordinated process but rather a natural growth of applications of resorts that depend on activities of responsible persons in those administrative bodies.[5]

Electronic signatures – The Act provides a definition for electronic signatures and introduces a system of qualified electronic signatures and accredited qualification service providers issuing qualified certificated, qualified system certificates (which can be issued to legal entities) and qualified time stamp tokens. As regards to electronically exchanging information with public authorities, the Act foresees that the use of electronic signatures in the public sector may be subject to additional requirements. More specifically, only certified electronic signatures and qualified certificates issued by accredited providers of certification services can be used for electronically exchanging information with public authorities. In addition, the certificate has to contain a social security number.

Electronic signatures are defined in accordance with the Directive, however, the definition does not contain any requirement on the specific type of electronic

[5] IDABC, Study on Mutual Recognition of eSignatures: update of Country Profiles - Czech country profile, July 2009, p. 4.

signature, nor on certification service providers issuing non-qualified certificates. However, the Act does contain requirements for advanced electronic signatures, namely:

- the electronic signature is linked to the signatory;
- the electronic signature is capable of identifying the signatory in relation to a data message;
- the electronic signature has been created and attached to a data message using means that the signatory can maintain under his sole control; and
- the electronic signature is linked to the data message to which it relates in such a manner that any subsequent change of the data is detectable.

Summarised, electronic signatures are only accepted in the event a person or entity is requesting for information without any document needing to be signed. Advanced electronic signatures are accepted only in a few cases (such as electronic invoicing). Consequently in most cases the only legal solution is to use electronic signatures based on qualified certificates issued by an accredited certification service provider. However, the use of qualified electronic signatures is not required by any act so in reality they are not often used.

Although the Act does not foresee a long term validity for electronic signatures, there are however technical solutions, such as long term signatures. These technical solutions are specified in ETSI standards but from a legal point of view it has not been specified as to how those standards should be used.

Electronic marks – Electronic mark is the designation of an electronic signature based on a qualified certificate. Further to defining electronic signatures, the Act also defines the concept of electronic marks as "data in electronic form which are attached to or logically associated with a data message and meets the following requirements:

- the electronic mark is unequivocally linked to the marking person (a natural person, legal person or government body that holds an electronic mark creation device and marks a data message by an electronic mark) and are capable of identifying that person by means of a qualified system certificate;
- the electronic mark has been created and attached to a data message using an electronic mark creation device that the marking person can maintain under its sole control;
- the electronic mark is linked to the data message to which it relates in such a manner that any subsequent change of the data is detectable.

The marking person is subject to a number of obligations, such as notifying the certification service provider who has issued the qualified system certificate without delay in the event there is a risk of abuse of its electronic mark creation data. Electronic mark creation data is unique data which is used by the marking person to create electronic marks.

The use of an electronic mark based on a qualified system certificate and created using an electronic mark creation device shall enable it to be verified that a data message has been marked with an electronic mark by a marking person.

Qualified time stamps – Qualified time stamps are defined as "a data message which has been issued by a qualified certification service provider and which links data in electronic form to a moment in time in a trustworthy manner, and guarantees that that data existed in electronic form before the given moment in time.

Qualified certification service providers – Qualified certification service providers are charged with issuing qualified certificates and identifying the person concerned. The law does not specify any conditions hereto so it is up to the certification service provider to decide. In practice all qualified certificates are issued after personal appearance. The only exception hereto is when a person already has obtained a certificate that is still valid and wishes to have a new certificate with the same data; in this case that person can use the already issued certificate to sign the request.

The E-government Act 300/2008 (Act on Electronic Communication and Authorized Conversion of Documents) enables natural and legal persons to communicate with public authorities by electronic means by creating a framework for electronic communication between state authorities, territorial autonomies and public authorities, as well as for their electronic communication with natural and legal persons**.** The Act establishes an electronic delivery system ("Data Boxes") for communication with public authorities as well as for authorised conversion of the documents (from paper to electronic form and vice versa). These so-called Data Boxes are best to be compared with an email account, which is made mandatory for public administration bodies and for legal entities, and is voluntary for natural persons. The Data Boxes supplements the communication which was delivered through ordinary mail and enables electronic communication with public authorities.

Electronic signatures will play an important role both from a delivery and conversion point of view. The delivery system will deliver both signed and unsigned messages. While the authentication to the system can replace an electronic signature for citizens, who do not have to sign the messages while using the system, the documents sent from the public authorities to the citizens must always be signed. Apart from this, the system will attach a qualified timestamp to each message. The authorised conversion of the documents will enable to convert the paper documents

into the electronic form and vice versa with the converted documents having the same legal effects as the original document. Both electronic signatures and qualified timestamps will be used for this process. The details regarding the use of the Data Boxes information system are further explained in the Ordinance 194/2009.

Among e-government applications using the electronic signatures are public procurement, e-health, e-justice, tax portal and the Czech security administration. When using electronic signatures for e-government applications there is generally only one possibility: it must be an advanced electronic signature based on a qualified certificate issued by an accredited certification service provider. Czech Republic does not provide for any requirement regarding advanced electronic signatures (except for the definition) nor on certification service providers issuing non-qualified certificates.

Qualified certificates and qualified system certificates can be issued to any person (qualified system certificate can also be issued to a legal entity), even to persons belonging to another country. The latter will only constitute a problem in the event the user from that other country does not have a qualified certificate issued by a qualified certification service provider accredited in the Czech Republic, since this is a general requirement to use certificates issued by an accredited certification service provider in e-government applications.

(b) Electronic archiving

The **Act on Archiving and Record Management** 499/2004 (as amended by the Act 190/2009) provides a framework for document archiving in general and electronic archiving in particular, as well as for the management of databases, the rights and obligations of authorities dealing with documents, and the processing of personal data.

The Act on National Registers 111/2009 (as amended by the Act 227/2009) deals with the process regarding the electronisation of public administration. The Act defines the content of national registers and lays down the rights and obligations regarding the creation, use and operation of the system. The National Registers Authority, an autonomous organisation body of the state and the administrator of the basis information system, was established by this Act.

2.1.4 Estonia

a. General approach and scope of legislation

Legislation and scope – The E-signatures Directive was transposed into Estonian legislation through the Digital Signatures Act of 8 March 2000 (as amended in January 2009). The Act grants similar legal value to digital and handwritten signatures, in both public and private sectors, provided that they comply with the requirements set forth in the Act and unless otherwise specified. The Digital Signatures Act also foresees an obligation for all public institutions to accept digitally signed documents.

Electronic signatures – An electronic (digital) signature is defined as "a data unit, created using a system of technical and organisational means, which a signatory uses to indicate his or her connection to a document." The requirements mentioned above include that the electronic signature must enable unique identification of the signatory, enable determination of the time at which the signature is given and link the electronic signature to data in such a manner that any subsequent change of the data or the meaning thereof is detectable. In the terms of the E-signatures Directive, the Estonian Digital Signatures Act only regulates advanced electronic signatures. Other types of electronic signatures can of course be used, but the Act does not confer them legal power.

As regards to the legal effect, electronic signatures are equalised with handwritten signatures. Nevertheless, if it is proved that the private key (signature creating device) was used for giving the signature without the consent of the holder of the corresponding certificate, the digital signature cannot be considered as having the same legal consequences as the handwritten signature. In this event, the certificate holder shall compensate damage caused to another person who erroneously presumed that the signature was given by the certificate holder, if the private key was used without the consent of the certificate holder due to the intent or gross negligence of the certificate holder.

Digital stamps ("digital seals") – In addition to electronic signatures, Estonian legislation also foresees the use of digital stamps. Digital stamps are technically equal to electronic signatures but have a legally different significance, since they can be performed without the direct consent of a physical person and consequently allowing for automated stamping. Although digital signatures have been used for many years, they only received legal effect in January 2009 by the amendment of the Digital Signatures Act, which foresees in a definition of the notion of digital stamp in order for forthcoming legislation to use the notion. Certificates for digital stamping

can be issued to both legal and natural persons, by a certification service provider. It is expected that the public sector will find a number of new applications for the use of digital stamping and therefore increase the market in this area.

Certification service providers – The competence of the certification service providers in Estonia is regulated by the Act, which includes requirements and regulates the supervision. A certification service provider must be a legal entity with a regulated minimum share capital. It must be registered with the National Certificate Service Provider Registry and carry out an annual audit to ensure both organisational and systematic reliability. In addition, certification service providers are required to be covered by a liability insurance to safeguard against compensating faults made while providing the service. It must be emphasized that under the current Digital Signatures Act, certification service providers may only certify persons identifiable by name and identification code. The issuance of certificates to pseudonyms is currently not covered by the Act, even though It was discussed in parliament during the law adoption process (where it was deemed to constitute an unnecessary risk).

Certificates issued by a certification service provider are valid as of the beginning of the period of validity set out in the certificate but not before entry of the corresponding data in the database of certificates which is maintained by the issue of the certificate.

Time stamping service providers – The Digital Signatures Act also foresees a framework for time stamping service providers, for which the requirements are generally the same as the requirements for certification service providers. The Act defines a time stamp as "a data unit which is created using a system of technical and organisational means which certifies the existence of a document at a given time." The Act does not specify a time stamp further into detail, but states that they must be bound to the time stamped data and be issued in such a manner as to preclude the possibility of changing the data undetectably after obtaining a time stamp.

2.1.5 Finland

a. General approach and scope of legislation

The current legal framework in Finland for e-identification and e-signatures is provided by the Finnish Act on Strong Electronic Identification and Electronic Signatures (617/2009) ("the Identification Act"), which entered into force on 1

September 2009 and replaced the repealed Act on Electronic Signatures (14/2003) which implemented the E-signatures Directive.

Definitions – The Identification Act includes a number of interesting concepts, which are defined as follows:

- "**Strong electronic identification**" means the identification of a person and the verification of the authenticity and validity of the identification by an electronic method based on at least two of the following three alternatives: (a) password or something similar that the identification device holder knows; (b) chip card or something similar that the identification device holder has in his possession; or (c) fingerprint or some other characteristic identifying the device holder.

- "**Identification device**" means objects or identifying data or characteristics that together form the identifiers, identification devices and verification devices required for strong electronic identification.

- "**Identification method**" means the entirety of the identification device and system required to create an individual strong electronic identification event.

- "**Identification service provider**" means a provider offering services for strong electronic identification to service providers using them or issuing identification devices to the general public or both. He must meet the following requirements:

  (a) he must be of age;

  (b) he must not have declared bankruptcy;

  (c) operating capacity must not be restricted.

  In addition, the identification service provider must be trustworthy. He cannot be deemed trustworthy if he has been convicted of a crime by a court of law during the past five years, or has been fined during the past three years for a felony that would make such person obviously unfit to act as an identification service provider, or is he has previously acted in a way that would make such person an obviously unfit identification service provider.

- "**Identification method**" means the entirety of the identification device and system required to create an individual strong electronic identification event. The identification method must meet the following requirements (can possibly be complemented with requirements of Ficora):

(a) the relevant method shall be based on initial identification, where the relevant data can be verified afterwards;

(b) the method shall unambiguously identify the identification device holder;

(c) the method is sufficiently secure to ensure that only the identification device holder can use the device; and

(d) the method is sufficiently secure and reliable, taking into consideration the relevant technical threats to data security.

- "**Identification device holder**" means a natural person to whom the identification service provider has issued an identification device based on an agreement. The identification device holder shall use the device according to the terms and conditions of that agreement. If the device is not used in accordance with the terms and conditions set forth in the agreement, the identification service provider has the right to cancel or prevent the use of the device. In the event the identification device holder has lost the identification device or if it is in the unauthorised possession of another person, he must immediately upon detection notify the identification service provider or a designated party of this.

- "**Initial identification**" means the verification of the identity of the applicant for an identification device in connection with the acquisition of the device.

- "**Certificate**" means an electronic verification that confirms the identity or confirms the identity and links the data for verifying a signature to the signatory, and that can be used for strong electronic identification and electronic signatures. With the help of a certificate, it is possible to verify a person's identity, or verify an identity and link the verification data to the signatory of the signature. In addition to the public key, the certificate also contains other data, such as the name of a person or organisation, the day the certificate was granted, the last day of validity or the individualised serial number.

- "**Qualified certificate**" means a certificate that has been issued by a certification service provider and includes an indication of the fact that the certificate is a qualified certificate, details of the certifier and the state in which the certifier is based, the signatory's name or a pseudonym, the signature verification data which corresponds to the data in the signatory's possession used for creating the signature, the period of validity of the certificate, a symbol identifying the certificate, the certification service provider's advanced electronic signature, potential limits on use of the

qualified certificate, and any special information on the signatory, should this be necessary.

- "**Certification service provider**" means a natural person or legal person who offers certificates to the general public.

Scope – The objective of the Act is to create common rules for the provision of strong electronic identification services. It will likewise promote the provision of identification services and the use of electronic signatures. The Act is founded on the principle that users must be able to trust information security and protection of privacy when they use strong electronic identification services.

Although the Act contains few surprises regarding electronic signatures, it is nevertheless interesting because of its provisions on electronic identification. The Act introduces the concept of "strong electronic identification", which means the verification of the identity of a person by an electronic method. It enables consumers to certify their identity safely as they use various electronic services, since through strong electronic identification, the identification device and its user can ultimately be connected to the person's true identity. The identification device used for strong electronic identification are bank identifiers used by banks, the Population Register Centre's citizen certificate and telecom operator's mobile certificates.

Electronic signatures – The Act confirms the principle set forth by the Directive that electronic signatures are legally just as binding as traditional handwritten signatures on paper contracts/documents, and introduces the concept of "strong electronic identification". Furthermore, the Act takes into account the EU Digital Agenda objectives which aim at an EU-wide, cross-border identification solutions based on reliable national identification systems.

The Act comprises the idea that an electronic signature based on strong electronic identification can justifiably be considered to provide stronger legal proof of an identified person's will to be bound by a specific agreement (either on the person's behalf or on behalf of a company or other legal entity represented by that person), than a traditional handwritten signature on a paper contract document, which can be more difficult to later link to a specific person, e.g. based on handwriting samples, than an electronic signature based on strong electronic identification.

General guidance and monitoring of strong electronic identification and electronic signatures is the responsibility of the Ministry of Transport and Communications. It is the responsibility of Ficora (Finnish Communications Regulatory Authority) to monitor compliance with the Act, and if required, Ficora will issue technical orders regarding reliability and data security requirements for identification service providers and certification service providers offering qualified certificates. Finally, the

Data Protection Ombudsman is responsible for monitoring compliance with the provisions of this Act regarding personal data.

Ficora has the right to obtain the necessary information for performing its tasks from identification service providers and certification service providers offering qualified certificates; Ficora also has the right to inspect the identification service provider or his services, if it has reason to suspect that they have materially breached the Act. Ficora shall perform a yearly audit of the certification service provider issuing qualified certificates.

Requirements – The Act stipulates the requirements for a device for creating safe signatures. Such device shall be able to ensure in a sufficiently reliable manner that:

- the data used for the creation of the signatures is unique, that it will remain confidential and that it cannot be deduced from any other data;
- the signatures are protected against forgery;
- the signatory will be able to protect the data used for the creation of a signature against use by others; and
- it will not alter the information to be signed nor will it prevent the information from being presented to the signatory prior to signing.

Ficora may appoint notified bodies (private or public institutions) which will assess whether the device for creating signatures meets the abovementioned requirements.

A qualified certificate may be issued by a certification service provider other than those based in Finland provided that he is based in a member state of the EEA and is a member of a voluntary accreditation system in a member state of the EEA. The certificate must meet the requirements applicable to qualified certificates in the country where he is based and must be guaranteed by a certifier who is based in a member state of the EEA and who meets the national requirements in the country in question. In the event the signatory has a weighty reason to suspect the unauthorised use of data for creating a signature, or any other reason for doing so, the certification service provider can, upon request of the signatory, cancel the qualified certificate.

A certification service provider issuing qualified certificates must submit a written notification to Ficora, prior to the commencement of the operation.

Obligations – The Act sets forth a number of obligations to be complied with by the identification service providers, and more specifically an identification service provider must:

- Notify the commencement of identification services by written notification to the Ficora, including the name and contact information of the service provider, information about the services and about the requirements for the identification method and identification service provider;
- Disclose to the applicant, prior to entering into an agreement for an identification device, information about the service provider, the services offered and their prices, the identification principles (define how the provider will perform its obligations set out in this Act and which lay down the conditions governing access to their identification services by service providers using strong electronic identification), the rights and responsibilities of the parties, potential limits of liability, complaint and dispute settlement procedures, potential restraints and restrictions on use regarding legal transactions, and other potential terms of use related to the identification device;
- Ensure that its personnel has adequate expertise, experience and competence;
- Dispose of sufficient financial resources for the operation and for covering possible liabilities for damages;
- Protect personal data and ensure adequate information security, and notify without any undue delay service providers using its services, identification device holders and Ficora of severe risks and threats to its data security.
- Be responsible for the reliability and functionality of services and products provided by people working for him.

Notification – Service providers offering strong electronic identification and qualified certificates must submit a notification to Ficora. Ficora maintains a public register on identification service providers and certification service providers offering qualified certificates. It also monitors that identification service providers and certification service providers offering qualified certificates comply with the obligations imposed on them by the legislation.

Consumer complaints – Ficora also acts as the appellate authority in matters concerning the operations of identification service providers and certification service providers offering qualified certificates, as well as electronic signatures based on qualified certificates. Consumers may contact Ficora if they suspect that the identification service provider acts against the legislation or regulations regarding strong electronic identification and electronic signatures.

Ombudsman – The Data Protection Ombudsman monitors the compliance of provisions concerning personal data by virtue of the Act on strong electronic identification and electronic signatures. Ficora and the Data Protection Ombudsman collaborate with the Financial Supervisory Authority, the Finnish Competition Authority and the Consumer Agency when performing supervision tasks.

Liability – The signatory is liable for damages from any unauthorised use of data that is used for creating an advanced electronic signature certified by a qualified certificate until the request for cancelling the certificate has been received by the certification service provider.

A certification service provider offering qualified certificates shall be liable for damages to someone relying on the qualified certificate if:

- data marked on the qualified certificate was incorrect at the time of issue of the certificate;
- the qualified certificate does meet the requirements set forth by the Act;
- the person identified in the qualified certificate did not, at the time of issue of the certificate, have in his or her possession the data used for creating the signature corresponding to the signature verifying data as stated or defined in the certificate;
- the creation and verification data created by a certification service provider or its subcontractor are inconsistent;
- the certification service provider or its subcontractor did not cancel the qualified certificate as provided in the Act.

Criminal sanctions – The provisions on penalties for infringements of this Act are provided in the Criminal Code and the Personal Data Act.

2.1.6 France

a. General approach and scope of legislation

(a) Electronic signatures

Legislation – France has transposed the E-signatures Directive through the **E-signatures Act of 13 March 2000**, which adapted the Civil Code rules of evidence, in order to make electronic documents and signatures legally acceptable. The Act

changed articles 1316, 1316-1, 1316-2, 1316-3, 1316-4 et 1326 of the Civil Code and introduced the legal equality of an electronic signature and a traditional, written signature. It includes a presumption of reliability of which the conditions are set forth in the Civil Code, and of which the burden of proof rests on the signatory.

Other relevant legislation regarding electronic signatures is the following:

- The **Act of 21 June 2004** on trust in the digital economy (n° 2004/575), which contains the legal framework for the development of e-commerce services in France. Among others, this Act regulates the liability of certification service providers issuing qualified digital certificates (article 33).

- The **Decree of 30 March 2001** (n°2001/272), which contains technical specifications on electronic signatures and distinguishes the electronic signature from the secured electronic signature (signature électronique sécurisée). The electronic signature is the signature complying with the conditions set forth in the Civil Code, while the secured electronic signature in addition also complies with the requirements specified in the Decree, and is presumed to be reliable (fiable), which shifts the burden of proof of reliability of the signature in the event of a dispute before a court.

  The Decree specifies the requirements of the secured electronic signature, which cover on the one hand the hardware and software (certified by the Administration) used to create the secured electronic signature, and on the other hand the content and the quality of the electronic certifications delivered by the certification service providers. The Decree further specifies the framework of the activities of the service providers which have to freely carry out their activity. From the moment they meet all the requirements, the service providers can demand to be acknowledged as being certified, which generates the presumption of compliance with the requirements of the Decree.

- The **Ordinance of 26 July 2004** with regard to the qualification of certification service providers issuing digital certificates and to the accreditation of the bodies in charge of the evaluation of the certification service providers describes the national scheme for the qualification of certification service providers issuing qualified certificates as defined in article 6 of the Decree 2001-272. The scheme is completed by a posteriori control by the DCSSI (Direction Centrale pour la Securité des Systèmes d'Information), as provided by article 9 of the Decree 2001-272.

- The **Ordinance on electronic interactions** between public services users and public authorities and among public authorities of 8 December 2005 (n° 2005/1516) (the so-called Teleservices Ordinance) attributes the same legal force to an electronic signature on public documents as that of a hand-written signature.

  Article 8 stipulates that the documents of administrative authorities may be subject to an electronic signature. The electronic signature is considered to be legally valid provided that it applies a procedure, in accordance with the provisions on the general security repository, which allows the identification of the signatory, guarantees the link of the signature with the document to which it is attached and ensures the integrity of the document.

  Article 9 - III foresees that the security products and the trusted service providers may obtain a certification which certifies their compliance with the security level of the general security repository. The Decree of 18 April 2002 (n° 2002-535) specifies the conditions for the attribution of such certification. The deliverance of such certification may, as regards to the trusted service providers, be confided to entrusted to a private body authorized for this purpose.

Initiatives – In addition to legislation, France has also been working on further elaborating the operation of e-government. In particular, in October 2008 the "Digital France 2012" project was adopted, which sets up a series of objectives to be reached by 2012. The project aims at generalising electronic authentication means such as the national eID card. The result of the efforts is reflected in the central portal www.service-public.fr/demarches24h24/, through which the French government offers a large series of electronic services to citizens, professionals and local communities. Among the most frequently used services are requests for birth certificates, notifications of a home address change and access to health insurance accounts.[6]

Reliability – Pursuant to the decree of March 30, 2001, an electronic signature is presumed reliable if it is created by using a "secured" signature creation device and based on a qualified certificate. French law does not use the terms electronic signature or advanced electronic signature as stated in the Directive on electronic signatures but rather the term "secure". So, as to be secure, the electronic signature shall be:

---

[6] IDABC, Study on Mutual Recognition of eSignatures: update on Country Profiles - French country profile, July 2009, p.5.

- uniquely linked to the signatory;
- created using means that the signatory can maintain under their sole control; and
- linked to the data to which it relates, in such a manner that any subsequent change of the data is detectable.

Issues – New legislative initiatives on electronic signatures have faced opposition from the National Data Processing and Liberties Commission (CNIL), which is concerned about the possible threat to privacy that the use of electronic signatures could pose. It is particularly opposed to the use of an individual's social security code as a mode of identification of the signatory, as is the Data Protection Authority. The National Data Processing and Liberties Commission has questioned the compatibility of such a provision with proper protection of personal data.

(b) Electronic archiving

[*The following information does not entirely apply to the archiving of electronic public archives, which are subject to specific provisions on storage and instalment. The destruction of electronic public archives, in whatever format, without the prior authorisation of the archiving administration constitutes a crime*.]

Legislation – The Act of 13 March 2000 contains multiple provisions relating to the law of evidence. It amends the French Civil Code: article 1316-1 allows an electronic document as proof to the same extent as a written document on paper format, provided that the document is retained in such conditions which guarantee the integrity of the document. Article 1348 specifies what constitutes an authentic copy.

Article L 134-2 of the Consumer Code, introduced by the Act of 2004 on trust in the digital economy, imposes the archiving of a written document which proves the existence of any contract drafted on an electronic format and concerning an amount above a certain threshold. This threshold is set at 120 EUR by the Decree of 16 February 2005 (n°2005-137). This provision, which particularly concerns e-shops on the Internet, envisages facilitating settlement of disputes. The legal storage term for the archiving is 10 years, which corresponds to the prescription term for contracts.

Regarding electronic archiving, a set of non-binding standards provide companies with a guideline for electronically archiving their documents, such as:

- Standard NR Z 42-013, published in 1999, is the most well-known in France. It specifies the technical and organisational measures allowing to guarantee

the integrity of the documents during their registration, storage and restitution.

- Standard NF Z 43-400.

The OAIS (Open Archive Information System) is a conceptual model designed to manage, archive and preserve numerical documents for a long term. It corresponds to the ISO 14721:2003 standard (Space data and information transfer systems - Open archival information system - Reference model).

Types of archives – The French data protection authority, the National Data Protection and Liberties Commission (CNIL Commission Nationale de l'Informatique et des Libertés), recommends to holders of numerical data to adopt an archiving policy which varies depending on the nature of the archived data (current archives, intermediary archives and final archives), in order to reconcile the needs of the exploitation of the data with the right to privacy and the right to be forgotten. To do so, the CNIL uses the three categories of archives defined in the Heritage Code:

- current archives, e.g. data relating to a client in light of a contract;
- intermediary archives, which are of administrative importance for the services concerned: the retention term is fixed by the applicable prescription provisions;
- final archives, which are of historic, scientific or statistic importance: can be retained indefinitely.

The current and intermediary archives can only be stored for the term necessary for their processing, which is specified on the declaration with the CNIL. The data controller must therefore proceed to the destruction of these archives in a timely manner. The intermediary archives are intended to be used by only certain services, for instance by the legal department. Managing the access security must ensure that only these authorised persons have access to these data.

Archiving electronic mail – Archiving electronic mail meets different needs stemming from IT departments as business departments. Three types of electronic mail archiving are preferred by over one company in two. The most frequent used type of electronic mail archiving can be qualified as "economical" archiving and responds to the issues of management and cost reduction induced by the increasing augmentation of electronic mail which generates important storage costs as well as a congestion within email inboxes. Such archiving projects are often initiated by IT departments and can thereafter give rise to other archiving projects generating from other departments within a company.

The two other types of archiving, more considered by the organisations than actually deployed, assimilate to the "regulatory" archiving and the "probative" archiving. Although both are quite similar, the first can be distinguished by its mandatory character, which is due to a number of laws and regulations obliging certain companies to retain their electronic mail which are specifically identified (invoices, payroll, etc.) for the event of an external verification. This type of archiving is mostly used by sales departments. In the event of "probative" archiving, the company takes on a preventative approach by installing tools which allow it in case of a dispute to identify the documents necessary as evidence. This type of archiving is mostly used by legal departments.

(c) Electronic registered mail

Legislation – **Article 1369-8 of the French Civil Code** already provided a provision regarding electronic registered mail, however only five years later an executive decree was promulgated. The **Decree of 2 February 2011** (n° 2011-144) sets out the requirements with regard to the identification of the third party responsible for mailing (its legal status and contact details must be detailed), sending registered mail by electronic means (identification of both sender and recipient, with or without acknowledgment of receipt, warranty for loss, theft or deterioration, etc.).

The decree also provides for specific procedures and timeframes for the recipient to accept or refuse the registered e-mail. While the purpose of the above measures is to adapt the legal requirements to the digital environment (especially in the light of the increasing importance of the conclusion and performance of contracts through electronic means), these conditions appear to be quite demanding so that they are expected to dampen the interest in using electronic registered mail in contrast to traditional registered mail.

Parties involved – Three parties are concerned when sending an electronic registered mail: an operator, a sender and a recipient. The Decree specifies which information must be provided and which transactions must be carried out by each of the parties. The recipient will be able to accept or refuse the electronic mailing of the registered letter, after notification at the time of delivery. In practice, the operator will notify (e.g. by email) the recipient that he has an electronic registered letter addressed to him. The recipient then has 15 days to decide whether or not he wishes to receive the electronic registered letter, or whether he prefers receiving a traditional (paper) registered letter. It must be emphasized that in a B2B context, the

professional who receives an electronic registered letter does not have the option to refuse this electronic format.

From the moment of the sending of the electronic registered letter to its recipient, the operator must inform the sender on this. To do so, the operator must specify the sending number, the date and the time of sending and, possibly, the name of the postal service provider charged with printing the electronic registered letter on paper. The recipient authenticates himself in order to read the letter, which implies the use of an electronic signature with storage of the numeric imprint guaranteeing the integrity of this letter.

The storage term for the operator is maximum one year. This short storage term may lead to problems in the event of legal proceedings, which can last for years and in light of which it is recommended to both the sender as the recipient to conserve the tracks of their correspondence with the operator.

Issues – The Decree also contains a few topics which fall into a "grey" area regarding their interpretation. For instance the notification of the recipient indicating his decision regarding the refusal of the electronic registered letter. If this notification is sent by traditional electronic mail, is lost or has been filtered as spam, is it acceptable to then state that the registered letter has never been claimed? Another example of a "grey" area is the idea of sending the electronic registered letter on a paper format upon request of the recipient. This generates an economic issue, since this choice or option does not belong to the person paying for the electronic registered mail service. This option for the recipient could lead to the result that in the end sending an electronic registered letter could turn out to be more expensive than a regular registered letter.

2.1.7 Italy

a. General approach and scope of legislation

The Italian legislation, and in particular the Code of Digital Administration ("*Codice dell'Amministrazione Digitale*"[7], hereinafter the "Code"), regulates both electronic

[7] Legislative Decree of 7 March 2005, nr. 82, available at http://www.digitpa.gov.it/principali-attivit/codice-dellamministrazione-digitale#art48-com1.

signature and electronic identification. In particular, as regards ancillary services needed to secure electronic transactions, the Code sets forth rules in the field of:

- Electronic registered e-mail ("*posta elettronica certificata*"), defined as the communication system able to certify the sending and delivery of an e-mail (art. 1, nr. 1, *v-bis* of the Code). According to this provision, the certification establishes a value of full legal evidence. According to the spirit and goals of the Code, and more specifically as provided for under art. 48, nr. 1, of the Code, documents that need a certification of sending and delivery can be sent through electronic registered e-mail (as preferred means of communication) with, as a general rule, the same legal value of communications sent through (registered) mail (see art. 48, nr. 2, of the Code);
- Time stamping ("*validazione temporale*"), defined under art. 1, nr. 1, *bb* of the Code as the result of the electronic procedure to assign a date and a time to an electronic document. Here too the certification has the value of full legal evidence. No further rules are provided by the Code.

The electronic registered e-mail is declared to be the preferred means of communications between (i) different branches of the public administration (art. 47, nr. 1, of the Code) and (ii) the public administration and the citizens and companies[8], provided that the citizen/company obtained an electronic registered e-mail address and that this address has been registered in specific dedicated databases (not clearly defined by the law, namely by the Law Decree of 29 November 2008, nr. 185 that mentions these databases: it can be inferred from the law that these databases include the Companies Registry and the lists of members of liberal professions kept by professional associations (art. 6 of the Code). The databases can be consulted and processed by the different branches of the public administration in accordance with the provisions set forth by the National Data Protection Authority (art. 6, nr. 1-bis, of the Code).

As regards companies, the possession of an electronic registered e-mail address is compulsory and companies established before 28 November 2008 must communicate this e-mail address to the Companies Registry before 29 November 2011 (art. 16, nr. 6, of Law Decree of 29 November 2008, nr. 185, converted into

[8] The Code sets forth that the submission and exchange of applications, declarations and documents between companies/enterprises and public authorities is done exclusively on electronic way (art. 5-bis of the Code).

Law of 28 January 2009, nr. 2[9]). Members of liberal professions enrolled in a registry, such as lawyers, accountants, etc. must also have such an address, according to nr. 7 of the abovementioned art. 16.

Citizens in general terms are not obliged to have an electronic registered e-mail address but they may get one (and in this case they may use it only to communicate with the public authorities). Public administrations as well shall have an electronic registered e-mail address that shall be published in the Internet site of the public authority concerned (art. 54, nr. 1, *d*, of the Code).

It is also important to highlight that applications and declarations submitted to the public authorities through electronic registered e-mail are legally valid and accepted provided that the authentication tokens have been issued through the previous identification of the holder and that the system administrator certifies this (art. 65, nr. 1, *c-bis*, of the Code).

The technical rules regarding the electronic registered e-mail have been provided for by the Decree of the President of Republic of 11 February 2005, nr. 68[10], that establishes the principle that both private entities and public authorities can be providers of electronic registered e-mail services, that providers established in another EU Member State can also operate in Italy if they meet the requirements under their national law that are equivalent to those provided by the Decree and that respect the technical rules applicable in Italy (art. 15, nr. 1). Thus, the law already includes internal market provisions.

The Code is also focused on the electronic identification, defined under art. 1, nr. 1, *u-ter*, as the validation of the data given in an exclusive and unequivocal way to a subject in order to allow the identification in the electronic systems through adequate technologies (also to the ends of guaranteeing access security). The main identification tokens are the national e-ID card and the so-called National Services Card ("*Carta nazionale dei servizi*", issued by some local public authorities according to their will). Both may contain the credentials required for electronic signature – please refer to art. 66 of the Code).

b. Lessons learned

It can be pointed out that:

[9] The text is available (in Italian) at http://www.parlamento.it/parlam/leggi/09002l.htm.

[10] The text is available (in Italian) at http://www.digitpa.gov.it/sites/default/files/normativa/DPR_11-feb-2005_n.68.pdf.

- Interoperability among electronic registered e-mail systems issued by providers located in other EU Member States is limited, since the foreign provider must comply with the technical requirements applicable in Italy in order to provide e-mail services that are fully recognizable by Italian public authorities. Thus, the impact of the internal market clause in the act is rather limited.
- The approach in Italy is not oriented towards an open market, but rather towards enabling/facilitating reliable communication with the public sector. This also explains why e.g. take-up of official mail addresses for companies is not voluntary.
- The adoption of the national e-ID card is not yet fully complete and in any case the card, together with the National Services Card, may eventually serve as e-signature token (in this sense the Code does not clearly provide that these cards are e-signature tokens). On the other side, the Code states that these cards are the access instruments to the online services of public authorities when the electronic identification is requested.

2.1.8 Romania

a. General approach and scope of legislation

The primary eSignatures law in Romania is the Law no. 455 / 2001. However, two separate laws have been implemented in addition, which cover electronic time stamping (Law No. 451/2004[11]; sometimes also referred to as 'temporal marking' after the Romanian terminology in the law – *Lege privind marca temporalã*) and

[11] See http://www.glin.gov/download.action?fulltextId=231816&documentId=122121&glinID=122121 for a full text version in Romanian; or http://www.digisign.ro/uploads/Lege451_marcare_temporala_EN.pdf for an informal translation in English.

electronic archiving (Law no.135 / 2007[12] - *Lege privind arhivarea documentelor în formă electronică*).

The main observations in relation to Law No. 451/2004 (the time stamping act) can be summarized as follows:

- The time stamp (*marca temporală*) is defined as "a collection of electronic data, uniquely attached to an electronic document; it certifies that certain electronic data were presented at a given moment to the time stamping services provider" (article 2b);
- The law introduces a concept of 'time base' (*baza de timp*), which is the unitary system of temporal reference which all the time stamping service providers refer to, i.e. the common time point of reference (article 2d); the administrator/supplier of this 'time base' is to be appointed by a regulatory and supervisory authority (article 9);
- The law appoints the same regulatory and supervisory authority as in the eSignatures act as being competent for time stamping as well; (article 2e); time stamping service providers must notify their activities to this authority 30 days in advance (article 6). The authority will set the minimum set of procedures for time stamp creation and for control procedures, and is competent for monitoring adherence to these obligations.
- The content of a time stamp is regulated in article 3, and consists of :
    - a) the stamp attached to the electronic document subject to stamping;
    - b) date and time related to the document subject to stamping, expressed in universal time;
    - c) information that uniquely identifies the time stamping services provider;

[12] See http://www.glin.gov/download.action?fulltextId=231937&documentId=198225&searchDetails.searchAll=true&summaryLang=en&search=&glinID=198225&searchDetails.queryString=pubno%3A%22345%22&searchDetails.hitsPerPage=10&fromSearch=true&searchDetails.offset=130&searchDetails.sortOrder=default&searchDetails.queryType=BOOLEAN&searchDetails.showSummary=true&searchDetails.activeDrills= for a Romanian version, and http://www.digisign.ro/uploads/Lege135_arhivare_electronica_EN.pdf for an unofficial English language translation.

- d) the registration number in the registry of the time stamping services provider.

- High level security requirements are defined in the Act; these are similar to the high level requirements defined for qualified eSignature service providers in the Directive. However, it is worth noting that the time stamping act does not distinguish qualified/non-qualified levels.

- Liability provisions are set in article 10 of the act, and are largely identical to those for qualified eSignature service providers under the eSignatures Directive. Specifically, the time stamping services provider is liable for any damage caused to any person who bases its conduct on the legal effects of the timestamp:

  - a) in terms of accuracy, at the issuing time of the timestamp, for all the information it contains;

  - b) in terms of ensuring that when the timestamp is issued, the provider identified therein owned the generation data of the timestamp corresponding to the timestamp verification data, stipulated in this Law;

  - c) in terms of fulfilling all obligations stipulated in art. 3-8.

  The time stamping services provider is not liable under paragraph (1) if it proves that, in spite of its due diligence, it could not prevent the damage.

- Technical and methodological rules are set through a separate decree, namely Decision no.896 of 2 October 2008[13]. Article 19 of this Decision directly references ETSI and ISO standards in relation to time stamping; there is thus already an alignment to European and international standards.

With respect to the e-archiving act (Law no.135 / 2007), the following points are worth noting:

- The scope of the Act is stated as being the generation, storage, access and use of electronic documents archived or that are to be archived in electronic

[13] See http://www.glin.gov/download.action?fulltextId=196944&documentId=215798&glinID=215798 for the full version in Romanian

archives (article 1); and compliance with a second act (the National Archives Law no. 16/1996) is required (article 2).

- The law provides definitions for a number of key concepts, including electronic archives administrator, electronic archives, electronic archiving services provider, and electronic archiving system. The following definitions are used:
    - electronic archives administrator – natural or legal person accredited by the specialized regulatory and monitoring authority to administer the electronic archiving system and the documents archived in the electronic archives;
    - electronic archives – the electronic archiving system, along with all archived electronic documents;
    - electronic archiving services provider – any and all natural or legal persons accredited to provide electronic archiving services;
    - electronic archiving system – electronic IT system dedicated to the collection, storage, organization and categorizing of electronic documents in order to store, access and edit them;
- The act is market based: archiving services are available to anyone (public or private sector, article 4), and no prior authorization can be required (article 5, based on the provisions of the eSignatures Directive). None the less, supervision is required by a regulatory and supervisory authority, which is (as with time stamping) the same authority as for CSPs providing qualified signature certificates to the public; archiving service providers must notify their activities to this authority 30 days in advance (article 6). The authority will set the minimum set of procedures for time stamp creation and for control procedures, and is competent for monitoring adherence to these obligations. Changes in security practices must be notified to the authority.
- The act has detailed provisions for including a document in an electronic archive (article 7 and following), which include the requirement of the document being signed by the submittor and by the archive administrator. The administrator has to attach a sheet to each document specifying:
    - a) the owner of the electronic document;
    - b) the issuer of the electronic document;
    - c) the holder of the right to dispose of the document;

- d) the history of the electronic document;
- e) the type of electronic document;
- f) the classification level of the electronic document;
- 7. g) the digital format the electronic document is archived in;
- 8. h) the key words required for the identification of the electronic document;
- 9. i) physical storage medium localization elements;
- j) sole identifier of the electronic document within the electronic archives;
- k) document's issue date;
- l) archiving date;
- m) document's maintenance term.

- Interestingly, the law can be applied to electronically archive paper documents, as requirements for this conversion process are also included (article 8.3).
- Storage requirements are regulated separately (article 12), and include e.g. the requirement to maintain and deposit the source code for all relevant software with the National Archives. In this manner, retrieval possibilities are protected. The archiving service provider must similarly ensure the availability of software that would allow the electronic documents to be viewed, reproduced and stored (article 13).
- Access rules are similarly fixed (article 14), specifically the right for the document owner to set access conditions.
- High level obligations are defined in the law itself; as for time stamping, technical and methodological rules are set through a separate decree, namely through Ministerial Ordinance nr. 493/15.06.2009[14].

[14] See http://www.pdf.com.ro/help-center/46-legislatie/120-ordinul-ministrului-mcsi-nr-493150620 09-privind-normele-tehnice-i-metodologice-pentru-aplicarea-legii-nr-1352007-privind-arhivarea-documentelor-in-form-electronic for a full version in Romanian

b. Lessons learned

The following points are of particular interest in the aforementioned laws:

- It is worth noting that Romania has opted for three separate acts on eSignatures, time stamping and electronic archiving. None the less, they all have a market focus (i.e. they are not eGovernment specific), and share the same major principles, which also become clear by the cross references in the time stamping and e-archiving acts to the eSignatures act (e.g. the use of a common supervisory authority;
- Both the time stamping and the e-archiving acts introduce only one category of time stamping service provider, without distinguishing e.g. qualified and non-qualified levels. However, the implementation of the acts follows the same logic as for CSPs providing qualified signature certificates to the public under the eSignatures Directive. I.e., the logic of both acts is based around a single model with predictable levels of reliability.
- The e-archiving act is particularly interesting due to its extensive coverage of all major concerns (creation, storage and access), and due to the possibility of electronically storing paper documents.
- Finally, it is worth noting that neither law defines a clear legal effect for their services other than by defining what the service is. In other words, neither of these laws contains a legal equivalence rule.

2.1.9 Slovakia

a. General approach and scope of legislation

The Slovak Act on electronic signature ("*Zákon č.215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov*", Act nr. 215 of 15 March 2002[15]) provides for rules regarding time stamping ("*Časová pečiatka*"), whose condition of applicability is the existence of an electronic document, of a private key and of a public key (§ 9 of the Act). The time stamp designed by the Slovak

[15] The English version is available at http://www.ictparliament.org/node/1980. The Slovak version is available at http://www.nbusr.sk/ipublisher/files/nbusr.sk/elektronicky-podpis/zakony_ep/215_2002.pdf.

lawmaker is based on similar terms and technologies as the electronic signature, since the time stamping operates thanks to a private key, produced by an accredited authority, and by a public key, which has a qualified certificate issued by an accredited certification authority.

In fact, the act does not make systematic distinctions between time stamping and eSignatures, considering one as an application of the other. E.g. an “accredited certification service” is defined by the act as “the issuance of qualified certificates, the annulment of qualified certificates, providing lists of annulled qualified certificates, acknowledging the existence and validity of qualified certificates, searching for and providing issued qualified certificates, and the issuing and authentication of time stamps”. The same supervisory authority is competent for supervising and regulating time stamping activities as well (article 10).

The definition for a time stamp is very closely aligned with the definition of an electronic signature. Article 9 states that a time stamp is “an information attached to an electronic document or logically linked to it otherwise and must comply with the following requirements:

> (a) it may not be produced effectively without knowledge of a private key intended for this purpose and without an electronic document;
>
> (b) on the basis of the knowledge of the public key belonging to a private key used in producing it, it is possible to authenticate that the electronic document to which it is attached or logically linked otherwise is equal to the electronic document used for its execution;
>
> (c) an accredited authority has produced it using a private key intended for this purpose;
>
> (d) it may be executed solely by using a security equipment for time stamp executing pursuant to Article 2, paragraph (x); the generally binding legal regulations issued by the authority shall stipulate details concerning the requirements for such a security equipment;
>
> (e) an accredited certification authority has issued a qualified certificate to the public key belonging to a private key used for executing it;
>
> (f) it enables unequivocally to identify the date and the time when it has been executed.

The Act sets also rules about archive maintenance under § 18 of the Act. Certification authorities have the obligation to store for at least ten years the following items: (i) documentation concerning the organizational, technical and

security means; (ii) originals of applications for issuance of certificates with the documents proving identity of the applicant; (iii) documentation relating to annulled certificates. Storing can be done also in electronic form in a secured environment.

b. Lessons learned

The Slovak legislation is interesting in the sense that it strongly aligns the rules for electronic signatures and time stamping. For time stamping, no qualified level is foreseen; only a basic concept for which the legal effect is already included in its definition.

2.1.10 Slovenia

a. General approach and scope of legislation

The relevant legislation in Slovenia is the Electronic Commerce and Electronic Signature Act of 23 June 2000[16] ("*Zakon o elektronskem poslovanju in elektronskem podpisu*") which regulates the use of time stamps ("*časovni žig*"). Time stamp is defined by the Act under art. 2, nr. 5, as an electronically signed certificate of the certification service provider confirming the content of the specific data at the alleged time. Therefore it is conceptually very close to the notion of electronic signature, and in fact the law only states that the provisions regulating e-signature certificates and qualified certificates shall *mutatis mutandis* apply to the time stamp and to the services concerning it (art. 25 of the Act).

It is important to stress that a qualified certificate is required to give legal effectiveness and admissibility as evidence to the time stamp, as provided under art. 15 of the Act. From an organizational perspective, certification service providers do not need prior authorization to perform their activities, but they must report the beginning of performing of the activities to the Ministry for Economy (see art. 18 (1) and (2) of the Act). Thus, the supervisory rules are comparable to those for eSignature certificate issuers.

As regards archive maintenance, certification service providers who issue qualified certificates must store all relevant information concerning qualified certificates for as

[16] The English version is available at http://www.ictparliament.org/node/1951. The Slovenia version is available at http://www.uradni-list.si/1/objava.jsp?urlid=200498&stevilka=4284.

long as the data, marked with the time stamp to which the qualified time stamp is referred, will be stored, and at least for five years from the issuance of the certificate (art. 35 (1) of the Act). The information, listed explicitly by the Act under art. 35 (2), can be recorded electronically.

b. Lessons learned

The Slovenian legislation about e-signature and related tools is highly focused on security, which is well defined and regulated in the Act itself. However, the most remarkable aspect is the highly summary way in which time stamping is dealt with by the act: other than the definition, the only provision in relation to time stamping is the statement that the provisions regulating e-signature certificates and qualified certificates shall *mutatis mutandis* apply to the time stamp and to the services concerning it (art. 25 of the Act). Thus, a substantial degree of flexibility and interpretation remains.

2.1.11 Spain

a. General approach and scope of legislation

IAS services are affected by two different pieces of legislation in Spain:

- The Act on Electronic Signature ("*Ley de firma electrónica*") – law nr. 59/2003 of 19 December 2003[17]; and
- The Act on Citizens electronic access to public services ("*Ley de acceso electrónico de los ciudadanos a los servicios públicos*") – law nr. 11/2007 of 22 June 2007[18].

The Act of 2003 regulates *inter alia* the adoption of a national e-ID card, which allows the holder to electronically sign documents, since the card includes e-signature tools, as set forth by art. 15 (1) of this law. The Act under art. 16 (2) states that the government shall assure that the e-signature tools included in the e-ID card

[17] The text is available in Spanish at http://noticias.juridicas.com/base_datos/Admin/l59-2003.html.

[18] The text is available in Spanish at http://noticias.juridicas.com/base_datos/Admin/l11-2007.html.

are compatible with the e-signature tools that are generally adopted and accepted. On the basis of the information provided by the Spanish government, the certificate stored in the chip of the e-ID card is a qualified e-signature certificate[19].

The Act of 2007 on the other side is applicable only to the relations between public administrations and between citizens on one side and public administrations on the other side, as clearly indicated by art. 2 (1) of the law. According to this law, public administrations must accept electronic signatures that meet the requirements of the law of 2003 as identification tools and as means to prove the authenticity and the integrity of electronic documents (see art. 13 (1) of the law). The e-signatures that shall be accepted by public authorities are several: not only those whose certificate is included in the e-ID card but also other advanced e-signatures, as well as other e-signature systems that are used by the citizen (and that are not advanced or qualified electronic signatures), as pointed out by the second paragraph of art. 13.

Apart from the basic signature concept, the law also regulates the notion of an e-seal, as a signature created by public administrations, which are linked only to the administration itself (art. 18 of the law). Every public officer then may sign e-documents with his/her electronic signature (eventually using the signature whose certificate is included in his/her e-ID card), as pointed out by art. 19 of the 2007 Act.

Time stamps (*sellado de tiempo*) are also regulated by the Act of 2007, and are defined by the Annex (point *s*) of the law as "*accreditation by a trusted third party of the date and time of performance of any operation or transaction by electronic means*". They are used in case of submission of electronic applications and documents by citizens to a public administration, since in this case the public authority will stamp the applications and documents with the day and hour of submission (see art. 25 (3) of the 2007 Act). In principle, the adoption of a time stamp on an administrative e-document is compulsory when the nature of the document requires its use, as indicated by art. 29 (2) of the law.

b. Lessons learned

The Spanish approach to electronic signature and related tools seems to be flexible enough to stimulate competition between certificate providers in the market. However, it is interesting to note that the time stamping concept was not introduced

[19] http://www.ads.gov.ba/v2/attachments/658_09_National_Strategy_on_eID_Sarajevo.pdf (last retrieved on 26 Oct. 11).

in the primary eSignatures Act, but rather in the Act on Citizens electronic access to public services, indicating a public sector rather than market focus.

2.2 Relevant laws from outside of the EU: scope, impact and gaps

Apart from the aforementioned European initiatives, lessons can possibly also be learned from the way non-EU countries have dealt with IAS challenges through their respective legislations. In the sections below a number of interesting examples will be explored a bit further

2.2.1 Brazil

a. General approach and scope of legislation

Brazil is one of the forefront countries in the field of e-government in South America (see for instance the e-vote applied in the whole country for elections of political bodies, or the real estate e-registration system[20]) and therefore the country has a complex legislative and regulatory set of rules in the field of e-signature, which also extend to ancillary fields such as notably time stamping.

Among the several legal sources applicable in the field, a central position is taken by the "*Medida provisória*" (Provisional Measure) nr. 2.200-2 of 24 August 2001[21] which creates the infrastructure of Brazilian public keys for e-signature, called ICP-Brasil[22]. The infrastructure, according to art. 1, shall guarantee the authenticity, integrity and legal validity of electronic documents, of support applications and of applications that use digital certificates, as well as the realization of secure e-transactions. ICP-Brasil is a body managed by a board whose members are appointed by the President of Republic, as provided for by art. 3.

[20] For a list of legislative measures in the field of e-government in Brazil please refer to http://www.certisign.com.br/certificacao-digital/legislacao/nacional (last retrieved on 28 Oct. 11).

[21] The text is available in Portuguese at https://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm.

[22] For more information please refer to http://www.iti.gov.br/twiki/bin/view/Certificacao/WebHome (last retrieved on 28 Oct. 11).

The structure of the digital certificate system in Brazil is composed of two pyramidal levels:

- The Root Certificate Service Provide ("*Autoridade Certificadora Raiz*", hereinafter RCSP) at the top level. The RCSP in practice is the ITI ("*Instituto Nacional de Tecnologia da Informação*", National IT Institute[23]), and
- Several Certificate Service Providers ("*autoridades certificadoras*").

According to art. 5, the RCSP shall emit, send, distribute, revoke and manage the certificates of the certificate service providers at the lower level. Furthermore, the RCSP manages the list of certificates that have been granted, revoked and lost but it cannot provide final users with digital certificates (art. 5, second paragraph). As provided for under art. 6, only certificate service providers can emit, send, distribute, revoke and manage final users' certificates.

Art. 10, § 1, is of pivotal importance since it states that electronic documents signed with a certification process made available by ICP-Brasil (in other words with a digital signature whose certificate has been granted by a certificate service provider that is part of the ICP-Brasil system) are deemed to be authentic as regards the signatories of the document, in light of the provision of art. 219 of the Civil Code (that says that "*the declarations contained in signed documents are deemed to be authentic in relation to the signatories*"). Thus, eSignatures laws in Brazil focus more on the legal impact on the declarations, rather than on the legal value of the signature itself.

Time stamps are regulated as well in Brazil, namely by the following administrative acts enacted by the managing board of ICP-Brasil:

- "*Resolução*" (Decision) nr. 78 of 31 March 2010[24];
- "*Resolução*" nr. 69 of 13 October 2009[25];
- "*Resolução*" nr. 60 of 28 November 2008[26].

---

[23] http://www.iti.gov.br/twiki/bin/view/Main/WebHome

[24] The text is available in Portuguese at http://www.iti.gov.br/twiki/pub/Certificacao/Resolucoes/Resolucao78.pdf

[25] The text is available in Portuguese at http://www.iti.gov.br/twiki/pub/Certificacao/Resolucoes/Resolucao69.pdf

These legal sources are reflected in the ICP-Brasil's document "*Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil*" (General View about the System of Time Stamps in the ICP-Brasil, DOC-ICP-11, version 1.2, of 5 April 2010[27]). Time stamps are provided for by third trusted parties called "*Autoridades de Carimbo do Tempo*" (time stamps service providers), controlled and audited by the RCSP (see § 1.3). According to § 1.4 the use of time stamps is not compulsory and e-signatures are valid even if they are not associated with a time stamp.

The certificate system for time stamps is pyramidal as well in the sense that at the top of the structure there is the RCSP acting as "*Entidade de Auditoria do Tempo*" (Time Auditing Entity) that audits and synchronizes the time stamp service providers. The system operates thanks to and in connection with "*Sistemas de Auditoria e Sincronismo*" (Auditing and Synchronization Systems, linked to an atomic clock) that make sure that the time stamps are correct and precise.

As regards online identification and authentication, and more precisely as regards e-ID documents, there exist different forms of electronic documents in Brazil that allow identification of the holder and signature of e-documents, thus conferring to the document the same legal value as documents with an handwritten signature.

Actually there is no national ID document linked to a unified federal citizens' database, or better, this system (called "*Registro de Identidade Civil*", Register of Civil Identity) is under implementation that started its test phase in 2011 and will last nine years[28]. Therefore, in the future Brazil will have a national e-ID card with a chip where a certificate for electronic signature will be stored.

Actually, however, citizens and companies must use other tokens to electronically sign documents, such as *inter alia* the e-CPF[29] for physical persons and the e-CNPJ[30] for legal persons.

---

[26] The text is available in Portuguese at http://www.iti.gov.br/twiki/pub/Certificacao/Resolucoes/Resolucao_60.pdf

[27] The text is available in Portuguese at http://www.iti.gov.br/twiki/pub/Certificacao/DocIcp/DOC-ICP-11_-_Versao_1.2.pdf

[28] For more information and for a list to legislative references please refer to http://portal.mj.gov.br/ric (last retrieved on 28 Oct. 11).

[29] *Cadastro de pessoas físicas* (Register of physical persons), used for tax purposes.

[30] *Cadastro nacional da pessoa jurídica* (Register of legal persons), used for tax purposes.

In order to obtain a certificate for electronic signature ("*certificado digital*"), i.e. one of the abovementioned tokens, the applicant must choose one between the several certification service providers recognised and approved by ICP-Brasil, as pointed out above. Certification service providers can be (and in practice are) both private and legal entities (as provided for by art. 8 of the abovementioned "*Medida provisória*" nr. 2.200-2). The user is free to select which token he needs and/or for which purpose he requires the certificate (e.g. certificate for e-justice services, for e-health services etc.). After the real verification of the holder's identity, the certification is granted by the certificate service provider so that the holder can be identified and authenticated online and can sign electronic documents.

b. Lessons learned

The main lessons that come from Brazil are:

- The e-signature system adopted in Brazil is open in the sense that private operators can participate in the market as certificate service providers, but at the same time there is a strong control by a centralised and public authority (the ITI acting as RCSP at the top of the hierarchical structure). This allows competition in the market but at the same interoperability between different e-signature systems is assured. On the other hand, it also means that a single entity exercises control over the entire market.
- The approach to the legal value of eSignatures is somewhat different compared to that of the eSignatures Directive: whereas the European model focuses on the value of the signature itself, the Brazilian model looks at the impact on the signed information.
- The introduction of a unified national e-ID card with a certificate for electronic signature has been planned (and the implementation phase started in 2011). However, the introduction of a national e-ID card requires a major reform in the system of citizens' national registries, which has been planned as well. The implementation phase of these major reforms is expected to last nine years.

2.2.2 Malaysia

a. General approach and scope of legislation

Malaysia has adopted legislation in relation to eSignatures as early as 1997 (the Digital Signature Act 1997[31], expanded by the eSignatures Regulation 1998[32]). The latter is especially instructive with respect to time stamping, as Part IX of the Regulation relates exclusively to time stamping, and contains rules with respect to:

- Regulation 58. Use of time-stamps.
- Regulation 59. Effect of time-stamp by recognised date/time stamp service.
- Regulation 60. Stages of certificate of recognition for date/time stamp services.
- Regulation 61. Qualification requirements for recognition.
- Regulation 62. Functions of recognised date/time stamp service.
- Regulation 63. Chargeable fees.
- Regulation 64. Application for certificate of recognition.
- Regulation 65. Information required for establishment stage.
- Regulation 66. Information required for operation stage.
- Regulation 67. Issue and renewal of certificate of recognition.
- Regulation 68. Revocation of certificate of recognition.
- Regulation 69. Surrender of certificate of recognition.
- Regulation 70. Register of Recognised Date/Time Stamp Services.

The legal effect of time stamps (Reg. 59) is addressed in a very straightforward manner, noting that:

> (1) The date and time time-stamped on a document and digitally signed by a recognised date/time stamp service shall, unless it is expressly provided

[31] See http://www.skmm.gov.my/link_file/the_law/NewAct/Act%20562/Act%20562/a0562.htm

[32] See http://www.skmm.gov.my/link_file/the_law/NewAct/Act%20562/Rules%20&%20Regulations/pua%20359y1998/pua359y1998bi/pua0359y1998.htm

otherwise, be deemed to be the date and time at which the document is signed or executed.

(2) The date and time time-stamped on a document and digitally signed by a recognised date/time stamp service shall be admissible in evidence in all legal proceedings without further proof.

Requirements for time stamp service providers are also defined (Reg.60) at a high level. It is noteworthy that Malaysian regulations require local offices or local partnerships with Malaysian entities; thus, they are not focused on encouraging open markets. Foreign service provider may however get accreditation if they comply with Malaysian legal requirements (Part X of the Regulations). Service providers are required to obtain a certificate of recognition, which is issued by the Malaysian Communications and Multimedia Commission (MCMC). The MCMC thus acts as a supervisory authority, albeit within a clear prior authorisation scheme.

With respect to the functionalities of time stamp service providers, the Malaysian Regulations (Reg.62) require service providers to publish hash values of stamped documents in a recognized repository, as a method of ensuring that time stamps can be validated independently.

b. Lessons learned

The legal framework in Malaysia with respect to time stamping is relatively straightforward and seems to be compatible with the existing European approach in relation to eSignatures. Notably, the definition of a legal effect of time stamps can be particularly useful as a good practice model for European policy initiatives.

2.2.3 United States of America

a. General approach and scope of the legislation

(a) Legislation on electronic signatures

In the US, a number of legal instruments provide a regulatory framework for electronic signatures. Apart from these federal laws, each State can proclame state legislation regarding the subject. What follows is a brief summary of each of the most relevant US acts regarding electronic signatures.

- The **Electronic Signatures in Global and National Commerce Act**, enacted on 30 June 2000, is a federal acts facilitating the use of electronic records and electronic signatures in both interstate and foreign commercial transactions by attributing the validity and legal effect to contracts entered into electronically. This act lays out the guidelines for interstate commerce, and assimilates electronic signatures and records with their paper equivalents.
- The **Uniform Electronic Transactions Act**, which has been adopted by 48 US states, aims at aligning the differing state laws over areas such as retention of paper records and the validity of electronic signatures, and supports the validity of electronic contracts as a viable medium of agreement.
- The **Digital and Electronic Authentication Law** (also referred to as SEAL) was adopted in 1998 and sought to update the Bank Protection Act in regards to electronic authentication techniques by financial institutions (1968). The law foresees different forms of electronic authentication, such as biometric, clickwrap, password, public key infrastructure and security token.
- The **Government Paperwork Elimination Act** (1999) requires federal agencies to use electronic forms, electronic filing and electronic signatures (when practicable) to conduct official business with the public.

(b) Other initiatives

In April 2011, the White House issued its "*National Strategy for Trusted Identities in Cyberspace - Enhancing Online Choice, Efficiency, Security and Privacy*" (hereinafter "Strategy").

This document aims at securing online transactions for businesses and individuals, and introduces the concept of an "**Identity Ecosystem**". This implies an online environment where individuals and organisations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities — and the digital identities of devices.

The Identity Ecosystem is designed to securely support transactions that range from anonymous to fully-authenticated and from low to high-value. It will offer, but will not mandate, stronger identification and authentication while protecting privacy by limiting the amount of information that individuals must

disclose. The Identity Ecosystem is built around four guiding principles, namely:

- the enhancement of privacy and support of civil liberties;
- identity solutions must be secure and resilient;
- ensure policy and technology interoperability among identity solutions;
- the Identity Ecosystem must be developed from identity solutions that are cost-effective and easy to use.

In its Strategy, the White House indicates the key players within the Identity Ecosystem[33]:

• An **individual** is a person engaged in an online transaction Individuals are the first priority of the Strategy;

• A **non-person entity (NPE)** may also require authentication in the Identity Ecosystem NPEs can be organizations, hardware, networks, software, or services and are treated much like individuals within the Identity Ecosystem NPEs may engage in or support a transaction;

• The **subject** of a transaction may be an individual or an NPE;

• **Attributes** are a named quality or characteristic inherent in or ascribed to someone or some-thing (for example, “this individual’s age is at least 21 years”);

• A **digital identity** is a set of attributes that represent a subject in an online transaction;

• An **identity provider (IDP)** is responsible for establishing, maintaining, and securing the digital identity associated with that subject. These processes include revoking, suspending, and restoring the subject’s digital identity if necessary

• The identity provider may also verify the identity of and sign up (enrol) a subject. Alternatively, verification and enrolment may be performed by a separate **enrolling agent;**

[33] White House, *Strategy for Trusted Identities in Cyberspace*, April 2011, p. 21 - 22.

• IDPs issue **credentials**, the information objects used during a transaction to provide evidence of the subject's identity. The credential may also provide a link to the subject's authority, roles, rights, privileges, and other attributes;

• The credential can be stored on an **identity medium**: a device or object (physical or virtual) used for storing one or more credentials, claims, or attributes related to a subject Identity media are available in many formats, such as smart cards, security chips embedded in personal computers, cell phones, software based certificates, and Universal Serial Bus (USB) devices. Selecting the appropriate identity medium and credential type is implementation-specific and depends on the risk tolerance of the participating entities;

• A **relying party (RP)** makes transaction decisions based upon its receipt, validation, and acceptance of a subject's authenticated credentials and attributes. Within the Identity Ecosystem, a relying party selects and trusts the identity and attribute providers of their choice, based on risk and functional requirements. Relying parties are not required to integrate with all permutations of credential types and identity media. Rather, they can trust an identity provider's assertion of a valid subject credential, as appropriate. Relying parties also typically need to identify and authenticate themselves to the subject as part of transactions in the Identity Ecosystem. Relying parties can choose the strength of the authentication and attributes required to access their services;

• An **attribute provider (AP)** is responsible for the processes associated with establishing and maintaining identity attributes. Attribute maintenance includes validating, updating, and revoking the attribute claim. An attribute provider asserts trusted, validated attribute claims in response to attribute requests from relying parties. In certain instances, a subject may self-assert attribute claims to relying parties. Trusted, validated attributes inform relying parties' decision to authorize subjects;

• **Participants** refer to the collective subjects, identity providers, attribute providers, relying parties and identity media taking part in a given transaction;

• A **trustmark** is used to indicate that a product or service provider has met the requirements of the Identity Ecosystem, as determined by an accreditation authority. The trustmark itself, and the way it is presented, will be resistant to tampering and forgery; participants should be able to both visually and electronically validate its authenticity. The trustmark helps individuals and organizations make informed choices about the Identity Ecosystem-related practices of the service providers and identity media they select.

3. Overview of current normative landscape at EU level

3.1 eSignature standardisation framework

As the result of the standardisation mandate M460 of the European Commission to the European Standardisation Organisations, the current European eSignature standardisation framework is today in the first stage of a complete rationalisation process aiming to overcome identified issues with regards to mutual recognition and interoperability of eSignatures and to ensure its effective and practical use in business driven implementations.

Despite some successful and widely adoption of very specific standards, this rationalisation is an essential step towards the emergence of a sound EU standardisation framework contributing to the consistent mapping between the related legal, technical and trust requirements that will induce a sound market for the cross-border use and interoperability of electronic signatures offering (business) stakeholders the sufficient certainty and mutual recognition of accordingly implemented electronic signatures throughout Europe.

3.1.1 Mandate M460 - a Rationalised Framework for European eSignature standards

a. The background

At the end of the last century, the European Electronic Signature Standardization Initiative (EESSI) was launched as a result of two specific mandates from the Commission[34,35] to coordinate the European Standardization Organisations CEN and ETSI in developing a number of standards for eSignature products that could ease the adoption of electronic signatures into the market, facilitate the

[34] **EESSI Mandate M279**, Mandate to CEN, CENELEC and ETSI in support of a European legal framework for electronic signatures, European Commission, 1998.

[35] **EESSI mandate M290,** Mandate addressed to CEN, CENELEC and ETSI in support of the European legal framework for electronic signatures- Phase 2: Implementation of the work programme resulting from mandate M279 and presented in Section 8.3 of the (draft) report prepared by EESSI, European Commission, 1999.

interoperability of eSignature based solution and services, and map technical and industry driven policy requirements to Directive 1999/93/EC on a Community framework for electronic signatures.

The current state of the European eSignature standardisation as a result of EESSI and some continuation work from ETSI and CEN includes a variety of eSignature related topics covering also ancillary services to eSignature.

While being quite limited in scope, the mapping between legal provisions from Directive 1999/93/EC and the EESSI derived eSignature standardisation framework were materialised by Commission Decision 2003/511/EC, on generally recognised standards for electronic signature products. This decision namely published "generally recognised standards" for electronic signature products in compliance with article 3(5) of the Directive but on a very limited scope (i.e. limited to SSCD requirements, Annex III of Directive, and requirements on trustworthy systems, Annex II.f). The wide set of other requirements were not formally mapped and leaving all other legal provisions and requirements laid down in Directive 1999/93/EC with unclear directions on what specifications would meet these requirements despite the fact that the EESSI eSignature standardisation framework also covered ancillary services to eSignature and a quite complete set of technical provisions with regards to eSignature creation, verification and preservation.

Emerging cross-border use of eSignatures and the increasing use of several market instruments (e.g. Services Directive, Public Procurement, eInvoicing) that rely in their functioning on eSignatures and the framework set by the Signature Directive emphasized problems with the mutual recognition and cross-border interoperability of eSignature.

Acknowledging the need to address the legal, technical and standardisation related causes of these problems, the Commission launched a study on the standardisation aspects of eSignatures[36] which concluded that the current multiplicity of standardization deliverables together with the lack of usage guidelines, the difficulty of access, the current academic approach and lack of business orientation, the numerous options and latitude for divergent interpretations and different technical implementations were detrimental to the interoperability of eSignature, and formulated a number of recommendations to mitigate this. Furthermore, the

[36] "Study on the standardisation aspects of e-signatures", SEALED, DLA Piper et al, 2007 (http://ec.europa.eu/information_society/policy/esignature/docs/standardisation/report_esign_standard.pdf).

Commission evaluated the EESSI process resulting in recommendations to improve its openness[37].

In addition, as many of the current eSignature standardisation documents did not reach the level of European Norms (ENs), their status may be considered to be uncertain.

Subsequently, the Commission launched the CROBIES[38] study to investigate solutions addressing some specific issues regarding interoperability and cross-border use of eSignatures and in particular profiles of qualified certificates and signature formats, (mutual) recognition of signature creation devices as secure signature creation devices in the sense of Directive 1999/93/EC, widely divergent implementation of 'appropriate' supervision practices in Member States, as well as common formats for providing trust status information about supervised / accredited certification services issuing qualified certificates or ancillary services supporting eSignatures.

Consequently, the European Commission issued Standardisation Mandate 460[39] to CEN, CENELEC and ETSI to update the existing eSignature standardisation deliverables, suggesting the establishment of a fully rationalised framework, including implementation guidelines, to overcome all these issues within the context of the Signature Directive, while taking into account its possible revision.

CEN, CENELEC and ETSI responded to M460 by setting up a two-phase approach starting first with defining such a rationalised framework and fixing quickly what could be quickly fixed on the basis of CROBIES suggestions and defining an associated future work programme aiming to address any elements identified as missing in this rationalise framework. Such a programme should then be executed in a second phase leading to a fully consistent and efficient set of rationalised European eSignatures standards that could be far more easily adopted by the market and lead to effective cross-border and interoperable eSignatures contributing greatly to a safer and successful eSociety.

---

[37] Evaluation of the standardization procedures in the context of the European electronic signature standardization initiative, Jos Dumortier, 2002.

[38] "CROBIES: Study onCross-Border Interoperability of eSignatures", Siemens, SEALED and TimeLex, 2010 (http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm).

[39] Mandate M460: "Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the Field of Information and Communication Technologies Applied to Electronic Signatures"

(http://ec.europa.eu/information_society/policy/esignature/eu_legislation/standardisation/index_en.htm).

The first phase of mandate M460 execution by CEN and ETSI is in its final drafting stage and drafts are being made available accordingly for:

- The Draft Rationalised Framework for eSignature standardisation[40]
- Quick fixes on **General Guidance and Requirements on Certificate Service Provider (CSP) conformity assessment**[41] whose objective is to produce a common basis for guidance on conformance assessment, including requirements on auditors, for all forms CSPs including qualified, nonqualified, time-stamp, and validation authorities.
- Quick fix on **Interoperable qualified certificate profile** whose objective is to update the qualified certificate profile standards[42] to address concerns identified in the CROBIES report. This includes issues related to identification of legal and physical entities in relation to these standards as well as updated requirements on current standardized information, which identifies that a certificate is a qualified certificate and to link the certificate with use of a Secure Signature Creation Device (SSCD), which is needed to avoid uncertainty over the acceptability of the signature in relation to legal requirements.
- Quick fix on **Procedures for Signature Verification** whose objective is to develop a technical specification specifying how to verify a digital signature within a given policy context.
- Quick fix on **Signature algorithms maintenance** whose objective is to maintain the guidance on signature algorithms.
- Quick fix on **electronic signature profile**[43] whose objective is to specify a Baseline Profile (ETSI Technical Specifications) for all the Advanced Electronic Signatures, i.e. CAdES, XAdES, PAdES and ASiC (Associated Signatures), which corresponds to the minimum basic requirements in the context of the "Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market" (EU Services Directive henceforth), and provide the same basic features with minimal number of options or no options at all. There will be two versions of the four deliverables

---

[40] ETSI STF425: http://portal.etsi.org/stfs/STF_HomePages/STF425/STF425.asp, and in particular the Draft Special Report is available from: http://portal.etsi.org/stfs/STF_HomePages/STF425/DSR_ESI_000099v000002.zip.

[41] ETSI STF 427: http://portal.etsi.org/stfs/STF_HomePages/STF427/STF427.asp, and in particular: http://portal.etsi.org/stfs/STF_HomePages/STF427/DTS-ESI-000075v000002.zip

[42] ETSI TS 101 862 and ETSI TS 102 280.

[43] ETSI STF 426: http://portal.etsi.org/stfs/STF_HomePages/STF426/STF426.asp.

C/X/PAdES and ASiC baseline-profiles, respectively considering the short-term signature verification requirements only[44] and the second will contain the short-term and a long-term signature base-line profile.

- Quick fix on the **testing of electronic signature standards**[45] whose objective is to develop:
  - technical specifications on conformance testing for the XAdES baseline profile as specified as a result of the above related quick fix on electronic signatures profiles",
  - a conformance testing tool for the XAdES baseline profile , and
  - an interoperability test event on PAdES signatures and ASiC - Associated Signature Containers.
- Quick fix on updating CD 2003/511/EC referenced documents, namely CWA 14169:2004, CWA 14167-1:2003, CWA 14167-2:2004 and CWA 14167-4:2004 in view of the future update of this Decision as foreseen in the Action Plan on eSignatures & eIdentification[46].

b. The proposed Rationalised Framework

The first draft of the proposed Rationalised Framework was published for stakeholders review end of August 2011[47].

In line with European Commission M460, the objectives of the rationalisation of the structure and presentation of the European Electronic Signature standardisation documents are:

- To allow business stakeholders to more easily implement and use products and services based on electronic signatures through the use of a radical business driven and guidance approach.

---

[44] ETSI ESI approved version available on: http://portal.etsi.org/stfs/STF_HomePages/STF426/STF426_Deliv_2011-09-13.zip

[45] ETSI STF 428: http://portal.etsi.org/stfs/STF_HomePages/STF428/STF428.asp.

[46] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on an ***Action Plan*** *on esignatures and e-identification to facilitate the provision of cross-border public services in the Single Market*, **COM(2008)798** of 28.11.08.

[47] Draft Special Report is available from: http://portal.etsi.org/stfs/STF_HomePages/STF425/DSR_ESI_000099v000002.zip.

- To facilitate mutual recognition and cross-border interoperability of eSignatures.
- To simplify standards by reducing unnecessary options and avoiding diverging interpretations of the standards.
- To target a clear status of European Norm for standardisation deliverables whenever applicable.
- To facilitate a global presentation of the eSignature standardisation landscape, the availability and access to the standards.

The first visible implementation of this last objective is the set-up of an eSignature standards portal accessible from www.e-signatures-standards.eu.

It is worth noting that the rationalised framework has been organised around 6 (functional) areas and 5 types of documentation, namely Guidance documents, Policy and Security Requirements, Technical Specifications, Conformance Assessment Guidance, and documents related to the testing of compliance and interoperability of products and services against requirements and specifications.

The 6 proposed areas for standardisation of eSignatures are the following:

1. **Signature Creation and Validation:** focusing on standards related to the creation and validation of electronic signatures, covering (i) expression of rules and procedures to be followed at creation, verification and for preservation of eSignatures for long term, (ii) signature format, packaging of signatures and signed documents, and (iii) protection profiles for signature creation/verification applications.
2. **Signature Creation Device**: focusing on standards related to SSCD's as defined in the Signature Directive, on signature creation devices used by Trust Service Providers as well as other types of signature creation devices.
3. **Cryptographic Suites**: focusing on aspects related to the use of signature cryptographic suites[48].
4. **Trust Service Providers supporting eSignatures:** including TSPs issuing Certificates, Time-Stamping Services Providers, TSPs offering signature validation services, TSPs offering remote signature creation services (also called signing server).

[48] I.e. the suite of eSignature related algorithms including key generation algorithm, signing algorithms with parameters and padding method, verification algorithms, and hash functions.

5. **Trust Application Service Providers:** covering Trust Service Providers offering value added services applying electronic signatures and that relies on the generation/verification of electronic signatures in normal operation (e.g. registered e-delivery services of electronic documents and messages, as well as long term archiving services).

6. **Trust Service Status (List) Provider**: This area covers the standardisation related to the provision of trust service "approval" status lists.

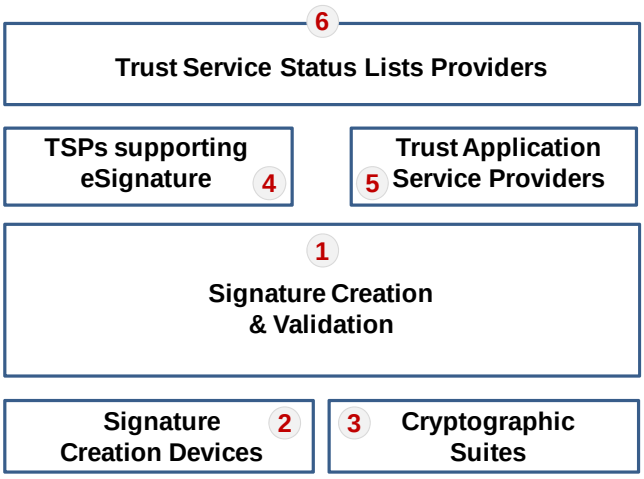


Figure: Overview of the eSignature standardisation Rationalised Framework (source ETSI)

3.1.2 Inventory of eSignature standards

As an input to the rationalisation of the current European eSignature standardisation framework, M460 driven ETSI STF 425 initiated a worldwide inventory with regards to electronic signature standards and related standardisation documents and published the interim results of such an inventory end August 2011. This inventory includes standards, publicly available and regulatory specifications from the International, pan European, national and sector (e.g. banking, e-invoicing, biopharmaceutical) domains.

It is not the purpose of the present document to redo or reformulate the work done in ETSI but to refer to this essential piece of work. This inventory is available from the ETSI STF 425 webpage[49] and from the eSignature standards dedicated website www.e-signatures-standards.eu.

[49] ETSI STF 425: http://portal.etsi.org/stfs/STF_HomePages/STF425/STF425.asp.

3.1.3 Work Programme

It is expected that 2 or 3 years would be needed to fully overcome the current issues and achieve a complete execution of the Work Programme leading to a fully coherent and business exploitable European eSignature Standards.

The challenge will mainly consist in providing of course a sound standardisation framework but also in setting up a smooth migration and transition from the current implemented (even if limited) market to the future requirements, while mapping closely to the future IAS policy framework and leveraging on and providing a commonly defined basis to the existing Trusted Lists model (as per CD 2009/767/EC amended by CD 2010/425/EU) for providing a common and harmonised way of providing trust related information on any type of supervised/accredited trust services.

3.2 Identity and Authentication standardisation framework

At EU level, the main efforts are concentrated in:

- ETSI's long standing introduction of identity and authentication in the form of the SIM (Subscriber Identity Module) and the more recent pre-standardisation "Group Specifications" for Identity management ; and
- CEN TC 224 (personal identification, electronic signature and cards and their related systems and operations);

Both the SIM-oriented and the emerging ETSI work is specifically oriented towards the telecommunication services industry, and to our understanding does currently not target broader acceptance.

The CEN Technical Committee 224 has produced standards such as the ECC (European Citizen Card) standard which particularly target Electronic Identity and Authentication.

As a significant amount of influential work has been done in the past outside Europe, we included a short summary of this in appendix.

3.2.1 ETSI SIM

ETSI defined the Subscriber Identity Module for GSM 2G in 1990, and the 3GPP defined the USIM in 1999. While the term SIM refers both to hardware and software, the term USIM only refers to the software application for Subscriber Identification which is executing on the UICC (the hardware). The current core specification is 3GPP TS 21.111.

With regard to identification and authentication, the standards define mechanisms and protocol exchanges, but not the algorithms. The operators have the choice for making this selection. Many operators rely on symmetric algorithms such as Milenage, which is related to the well-known Rijndael.

3.2.2 ETSI identity pre-standardisation efforts

ETSI has completed its Identity Management pre-standardisation specifications supporting interoperability and access control early 2011. These specifications are mainly focused on the telecom industry.

These specifications aim to simplify how users get authorized access to services and data beyond enterprise boundaries. They also support more privacy thus reducing the concerns in deploying these technologies.

This series of five pre-standardization specifications (known as Group Specifications) marks the end of the first phase of a transfer of European R&D projects of the European Commission's 6th and 7th Framework projects into specifications for industrial use.

The specifications were created by ETSI's Industry Specification Group on 'Identity and access management for Networks and Services' (ISG INS).

This first set of group specifications support interoperability and incorporate privacy into the telecoms services and networks domain. For example, Group Specification GS INS 001 on Identity Management (IdM) interoperability between Operators or Internet Service Providers (ISPs) and Enterprise provides mechanisms, interfaces and protocols allowing scenarios where third party providers share attributes with the operator, or reuses its authentication. A typical instance is Single Sign-On, a procedure by which a user gains access to all authorized communication services, thus avoiding the need for repeated authentication. GS INS 003 on distributed user profiles defines the relationship between access control and societal privacy needs and the associated legal framework.

3.2.3 CEN initiative in standardising cyber identity and unique identification of legal person and parts thereof

Unique persistent identification of business entities by recognised bodies and the verification of such identifications in trustworthy registers are a prerequisite for interoperability in electronic communications and transactions in open user groups.

It is likely that standards for electronic business exchange may mandate the use of unique identifiers in certain fields but do not specify how they can be decoded and resolved without a bilateral agreement. CWA 16036 aims to discuss these issues and provide standardisation bodies with proper recommendations to achieve this goal. This document gives guidance on unique identification systems currently in use or emerging for organizations and parts thereof, covering organizational and operational rules and processes to enable interoperability across multiple organization identification schemes. It includes an analysis of existing systems and proposes recommendations on how to achieve interoperability among them by using meta-identification systems.

This quite interesting, and we believe essential, exploratory work and recommendations for supporting interoperability and cross-border use of identification schemes whether used for identification, authentication or eSignature purposes must be continued and extended to natural persons.

3.2.4 CEN TC 224 WG's

This CEN Technical Committee deals with personal identification, electronic signature and cards and their related systems and operations. Its structure is depicted on their website as follows:

CEN/TC 224 - Structure

Secretariat	Chairperson	Secretary
AFNOR	Mr D.Lescribaa	Ms C.De Condé

SC/WG	Title
CEN/TC 224/WG 16	Application Interface for smart cards used as Secure Signature Creation Devices
CEN/TC 224/WG 15	European citizen card
CEN/TC 224/WG 18	Interoperability of biometric recorded data
CEN/TC 224/WG 17	Protection Profiles in the context of SSCD
CEN/TC 224/WG 6	User Interface
CEN/TC 224/WG 5	
CEN/TC 224/WG 11	Transport applications
CEN/TC 224/WG 9	Telecommunication applications

Figure: CEN/TC224 structure

We consider the following WG's particularly relevant from an IAS perspective:

- CEN TC224/WG 15 European citizen card or ECC

- CEN TC224/WG 16 Application Interface for smart cards used as Secure Signature Creation Devices
- CEN TC224/WG 17 Protection Profiles in the context of SSCD
- CEN TC224/WG 18 Interoperability of biometric recorded data

In this TC, following standards were recently published:

- EN 1332-1:2009 Identification card systems - Human-machine interface - Part 1: Design principles for the user interface
- CEN/TS 15480-3:2010 Identification card systems - European Citizen Card - Part 3: European Citizen Card Interoperability using an application interface

Furthermore, following standards are in progress:

- prCEN/TS 15480-4 : Identification card systems - European Citizen Card - Part 4: Recommendations for European Citizen Card issuance, operation and use
- prEN 14169-1: Protection Profile for Secure Signature Creation Device - Part 1: Overview
- prEN 14169-2: Protection Profile for Secure signature creation device - Part 2: Device with key generation
- prEN 14169-3: Protection profiles for secure signature creation device - Part 3: Device with key import
- prEN 14169-4: Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application
- prEN 14169-5 Protection profiles for secure signature creation device - Part 5: Device with key generation and trusted communication with signature-creation application
- prEN 14169-6Protection profiles for secure signature creation device - Part 6: Device with key import and trusted communication with signature-creation application
- Security Requirements for Device for Authentication - Part 1: Protection profile for core functionality

- Security Requirements for Device for Authentication - Part 2: Protection profile for extension for trusted channel to certificate generation application
- Security Requirements for Device for Authentication - Part 3: Additional functionality for security targets
- prCEN/TS 15480-1 rev Identification card systems - European Citizen Card - Part 1: Physical, electrical and transport protocol characteristics
- prCEN/TS 15480-2 rev Identification card systems - European Citizen Card - Part 2: Logical data structures and security services
- Personal Identification - Harmonization and interoperability of slap-ten print capture for Biometrics
- EN 14890-1:2008/prA1 Application Interface for smart cards used as Secure Signature Creation Devices - Part1: Basic services
- EN 14890-2:2008/prA1 Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services
- prEN 16248-1 Security requirements for device for authentication - Part 1: Protection profile for core functionality
- prEN 16248-2 Security requirements for device for authentication - Part 2: Protection profile for extension for trusted channel to certificate generation application
- prEN 1332-4 rev Identification card systems - Man-machine interface - Part 4: Coding of user requirements for people with special needs
- prCEN/TS 15480-5 Identification card systems - European Citizen Card - Part 5: General Introduction" (ECC-5)

a. WG15 European citizen card

Within WG15, the documents

FprCEN/TS 15480-4 / ECC-4: "Part 4: Recommendations for European Citizen Card issuance, operation and use“ as well as FprCEN/TS 15480-2 / ECC-2: "Part 2: Logical data structures and security services."

prCEN/TS 15480-1 / ECC-1 "Part 1: Physical, electrical and transport protocol characteristics“ (under revision).

CEN/TS 15480-3:2010 / ECC-3 "Part 3: European Citizen Card Interoperability using an application interface“ was published 13/09/2010.

Finally, with regard to prCEN/TS 15480-5 ECC-5 “Part 5: General Introduction” the NWI proposal was accepted on 20/06/2011.

b. WG 16 Application Interface for smart cards used as Secure Signature Creation Devices (SSCD)

With regard to WG16 status, following statuses are relevant:

For documents EN14890-1"Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services” as well as for EN14890-2 "Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional services“ “a revisions have been accepted on 23/02/2011

The TC224 Secretary is also asked to proceed to the PWI consultation on alignment with relevant ETSI standard to include the following topics:

- Web services on card
- Context specific authentication protocols for SSCDs for adoption on smart card
- Algorithm paper ETSI TS 102176 with liaison/participation to the relevant standardization bodies.

c. WG 17 Protection Profiles in the context of SSCD

With regard to the status of WG17, following documents are under approval

- prEN14169-1 "Protection Profile for Secure Signature Creation Device - Part 1: Overview”

d. WG18 Interoperability of biometric recorded data (prEN14169-3, prEN14169-4, prEN14169-5, and prEN14169-6)

WG18 is a new WG composed since 2010. Following documents are relevant:

- prEN14169-3 “Protection profiles for secure signature creation device - Part 3: Device with key import“

- prEN14169-4 “Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application“
- prEN14169-5 “Protection profiles for secure signature creation device - Part 5: Device with key generation and trusted communication with signature-creation application”
- prEN14169-6 “Protection profiles for secure signature creation device - 6: Device with key import and trusted communication with signature-creation application"

The new work item “Recommendations for using biometrics in European automated border crossing” is approved and officially opened (100% of positive votes, 6 countries committed to participate: Germany, United Kingdom, Austria, Netherlands, Spain and France). The resolution 857 is approved and the work item is opened within the CEN/TC224/WG18.

4. Leading studies, projects and policy initiatives

4.1 Identity and Authentication

4.1.1 The private sector perspective: scope, impact and lessons learned

a. Basic aspects

The private sector's use of identity and authentication services varies across the industry segments. In most if not all cases there is use of government identification documents during the hiring process of employees. As these hiring processes also gradually move to the Internet, electronic identification is making inroads there. The identity of the applicant is today still usually confirmed during the (mostly traditional) employment contract signing.

An issue that many international enterprises face is the following scenario:

- An employee is hired by company 1 in the group, HR processing is done in country 1;
- The employee is fired e.g. for misconduct, HR in country 1 flags him as no longer to be considered fit for hiring;
- The employee is hired by company 2 in the same group in country 2, HR processing is done in country 2;
- As HR processing is not consolidated, the fact that this employee is rehired is only discovered after a too long period.

Furthermore once the applicant needs to be brought on-board into the electronic business systems of his employer, the situation quickly becomes complicated in most cases. Many large private sector enterprises are structure in multiple tiers, such as the group (or HQ) level, the functional business unit level (which may or may not be structured according to national boundaries), affiliates, and business partners. The relation with the latter varies widely in terms of width and depth. Across these tiers staff, contractors and even automated software processes need to access and exchange information. Today, much of such information is still managed in technology silos (ERP's such as SAP and Oracle, various platforms

such as mainframe, Unix, Windows, and using a multitude of application servers etc). These silos are rooted in different technologies, whose identity and authentication technologies where not at all intended to be interoperable. Most large-scale enterprises recognized the need from both regulatory and efficiency/effectiveness perspectives to establish more unified identity and authentication solutions, including e.g. SSO (Single Sign On). However, in many enterprises, this is far from realised as it is both complex and expensive.

b. Projects

In many sectors (e.g. the Financial, the Telecom, the Healthcare and the Pharmaceutical Sectors), most enterprises launched an IAM (identity and access management) initiatives, often running for 3-5 years or longer. In many enterprises, these projects are currently still ongoing. More often than not today's status is that a selective part of the applications is covered for a selection of internal users. And while some company's indeed already succeeded at opening up e-Services for their external customers, there are still numerous companies where this is definitely not the case.

A significant interest is now spurred for the 'Identity as a Service" concept, particularly in the context of Cloud computing. In such a case, an enterprise needs to bridge both internal and external services (hosted in-house, externally and "in the cloud"), as well as internal and external identity providers.

c. SWIFT's approach

It is remarkable that SWIFT has taken a slightly different approach for managing the interaction with their customers, because they prefer to focus on eSignature more than anything else. SWIFT offers their customers the 3SKey (SWIFT Secure Signature Key) which allows PKI signatures to be created on the basis of an anonymous credential (private key and certificate) stored in a token. It does not contain the name of any individual but just a Unique ID that is used by 3SKey subscribers to associate the 3SKey user with the certificate. The activation process does not require the supply of any identification information about the 3SKey user, and the business credential is entirely anonymous.

4.1.2 The public sector perspective: scope, impact and lessons learned

a. Electronic ID

Electronic ID cards were introduced in the late 1990 by various Member States. This included the Finish eID card (December 1999), the Estonian eID card (January 2002), the Austrian citizen card (from 2003, with mass-rollouts from 2005), the Italian CIE / CNS (test phase 2003 for CIE), and the Belgian eID card (2002/2003). They were heterogeneous from a technology perspective, using smartcards (AT, BE, EE, ES, FI, GE, IT, PT, SE, ….), Mobile eID's (AT, EE, FI, LU, NL, NO, UK, …), allowing soft certificates (ES, SE, SI, …), or even username/password (NL, UK, …). They were issued by the public sector, the private sector or a combination. They are issued at federal, local, and regional levels. Finally, they also make different use of identifiers which can be horizontal (across the country), sector-specific or a combination.

For an overview, see the document "State of play concerning the electronic identity cards in the EU Member States (Brussels, 31 May 2010) 9949/10", from the European Council. [50]

As many Use Cases were identified that require cross-border usage of eID's, with it came the need for interoperability. However, this should be balanced with the requirements for Data Protection.

b. STORK

The STORK project does not change the Member State situations, but aims at interoperability. Running mainly from February 2009 through May 2011, it addressed functional design, technical design (borrowing heavily from SAML V2 for the actual protocols), implementation, exploitation (including pilots) and evaluation. As the proof of the pudding is in the eating, originally five pilots were selected: cross border authentication, safer chat, eID Student Mobility, eID electronic delivery and EU Citizen Change of Address. Integration of eID into the EC's ECAS authentication service was added as a sixth pilot.

In general, STORK assumes a citizen has online-access with eID, and considers the following use cases:

1. Authentication: in an online access to a service provider;

[50] See http://www.statewatch.org/news/2010/jun/eu-council-ID-cards-9949-10.pdf

2. Attribute Transfer (STORK defines eID as the identifier (e.g. national citizen ID), the rest" (name, date of birth, qualification, …) are attributes)
3. Attribute Verification: is a certain attribute presented by the citizen correct?
4. Certificate Verification.

When analysing the various eID implementations across the Member States, it can be observed that server-side solutions, client-side solutions and combinations are used. Some governments selected smart card based eIDs, which led to the introduction of client-side middleware to shield the card's implementation specifics from the application. Some governments introduced server-side middleware to cater for client-side independence from multiple tokens. Most solutions were established well before there was a common middleware standard.

Around 2006, the multipart standard ISO/IEC 24727 for middleware ("Identification Cards - Integrated circuit cards programming interfaces") was introduced by Task Force 9 of ISO/IEC JTC 1 SC 17/WG 4. It builds upon ISO/IEC 7816, with a focus on services and interfaces, aims to be card type neutral, contact and contactless agnostic. Its goal is to foster interchangeable and interoperable implementations for identification, authentication, and signature services. The standard made its way into many fields, including the US FIPS 201 (PIV) and the European Citizen Card. However, many national eID solutions were already established prior to the existence of this standard.

As a consequence, STORK had to create a model that could accommodate the various existing models. They based their design on two interoperability models, referred to as Middleware (MW) and Pan-European Proxy Services (PEPS). Common to those models are the two fundamental actors, the Citizen and the Service Provider. Citizen and Service Provider may reside in the same or in different countries. It has to be noted that besides Austria and Germany, Member States have opted for the PEPS approach. The existing technical implementations of eIDs in the Member States led to 4 possible combinations of MW and PEPS (PEPS=>PEPS, MW=>MW, MW=>PEPS, PEPS=>MW).

For example in the case of a Citizen of country-1 equipped with a PEPS (PEPS-C), wanting to use the services of a Service Provider in country-2, also equipped with a PEPS (PEPS-S) the following happens:

- The Citizen contacts the Service Provider's application, which decides to require eID-based authentication;

- As the Citizen is from another country than the SP, the authentication is rerouted by the SP to his national PEPS (PEPS-S);
- the PEPS-S will reroute to the PEPS-C in the Citizen's country, which will interact with the Citizen to create the appropriate authentication assertion;
- This assertion will be presented by the Citizen to the Service Provider, which evaluates it to decide whether he wants to accept it as a valid authentication response.

There is a strong dependence of the above scenario on electronic signatures, as such authentication responses are essentially electronically signed XML assertion. The consumer of the response should obviously verify the signature and validate it against revocation services.

The expression SPware was introduced to indicate the combination of client and server-side middleware, required to interface with a Service Provider. To provide a MW access at a PEPS or a PEPS interface at the SPware side, the concept of a Virtual Identity Provider was introduced. The Austrian SPWare MOA-ID is actually the main precursor for the STORK V-IDP. For example in the case of an Austrian student authenticating towards a Swedish university, the Swedish university will first query the Swedish PEPS, who needs to contact the Austrian "identity provider", which is based on a MW model (i.e. the student's card expects an SPware environment to function). The Austrian "identity provider" will present itself as a Virtual IdP to respond to the request from the Swedish PEPS. The scenario is further similar to the preceding one.

The technical implementations of the STORK building blocks in the pilots rely on the SAML 2.0 protocol suite from OASIS. The Use Cases are based on two SAML profiles, the "Web Browser SSO" Profile, and the "Holder of Key Web Browser SSO" Profile. The bindings onto communication protocols are based on HTTP-Post and SOAP Binding. The request/response protocols for obtaining an authentication assertion are based on the Authentication Request Protocol. The latter was amended to include Attribute Query. Finally, at the lowest level, the SAML Authentication and Attribute Assertions are used.

As a consequence, we now observe cross-border electronic services e.g. in the context of the general provision of services to citizens or enterprises. For example the Austrian *www.help.gv.at* portal allows authentication via eID, mobile or non-Austrian eID via STORK.



Figure: eIDentification and Authentication with Austrian eID card, mobile phone or via STORK on www.help.gv.at

Demonstrators for cross-border electronic services include national portals from Austria (help.gv.at), Estonia (eesti.ee), Germany (mein-service-BW), Portugal (portaldocidadao.pt) and the UK, one regional portal from Catalonia in Spain and one specific service for compliance activities for working in Belgium (limosa.be). For example an Estonian citizen can select his home country on the limosa.be site, and will be offered the possibility to authenticate with his national eID.

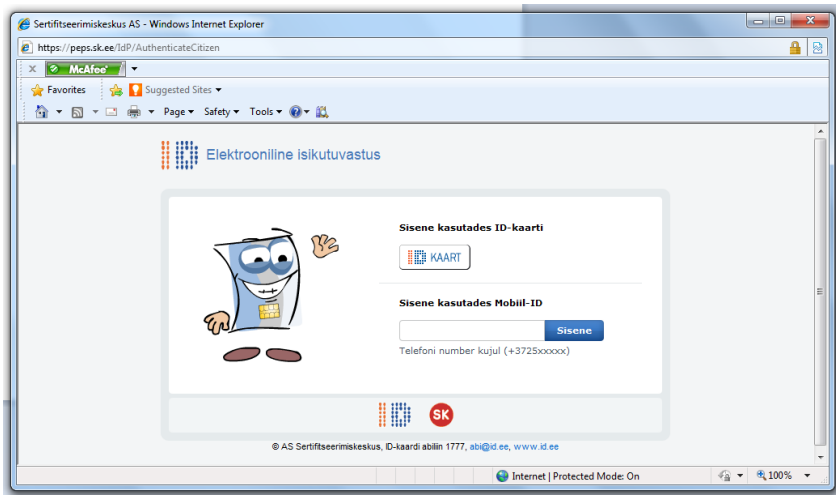


Figure: eIDentification and Authentication with Estonian eID card originating at www.limosa.be

This allows the citizen from the other Member State to prepare and process his compliance to local social requirements in Belgium.

c. SPOCS

Simple Procedures Online for Crossborder Services (SPOCS) is a pilot project launched by the European Commission that runs from 2009 through 2012. It aims to remove the administrative barriers European businesses face in offering their services abroad. SPOCS is expected to further enhance the quality of electronic procedures completion and has been designed for businesses that have an interest in cross-border activities. It will allow them to meet all the administrative obligations through a single contact point that will be available online.

The Points of Single Contact (PoSC) act as intermediaries between service providers and the national public administrations. These single intermediaries are designed to allow businesses to complete electronically all the relevant administrative procedures, such as obtaining authorisations to start an activity, which are necessary for providing their services in another EU country.

SPOCS benefits from the results achieved by its sister projects, STORK (on electronic identity) and PEPPOL (on electronic procurement), in relation to mutual recognition for the use of electronic identity and signatures. It will be implemented in different phases and a special emphasis will be drawn on the development of common specifications and tools for electronic services, such as technical and semantic interoperability, the promotion of electronic documents (eDocuments) and the creation of a services directory.

As such it is obvious that identity, authentication and signature are prerequisites for electronic document delivery as envisaged in SPOCS.

d. PEPPOL

PEPPOL, the **P**an-**E**uropean **P**ublic **P**rocurement **O**n**L**ine project, was initiated in 2008. It aims at expanding market connectivity and interoperability between eProcurement communities. PEPPOL enables access to its standards-based IT transport infrastructure through access points, and provides services for eProcurement with standardised electronic document formats (based on UBL and CEN/BII).

PEPPOL facilitates the pre-award and post-award procurement process with standardised components by focussing on the most complex eProcurement elements (marked yellow in the graphic below):

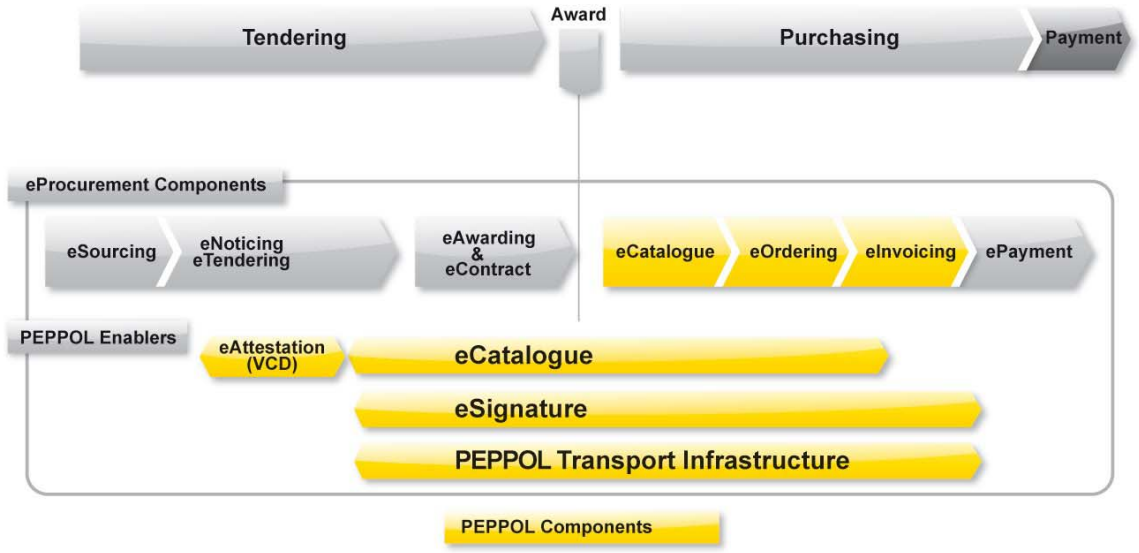


Figure: Peppol Components

As such, identification of the transacting partners as well as eSignatures are parts of the PEPPOL ecosystem.

4.1.3 The service supplier/vendor perspective: scope, impact and lessons learned

a. The inside-to-outside approach

To manage identity and authentication within an enterprise or public institution, most entities make use of specific solutions from vendors and service suppliers which they implement in-house. These solutions were originally established to manage the internal population, and have gradually been expanding to serve external populations as well.

Within the scope of market-oriented product and services, there is an abundance of vendors in the IA market. A significant market share is held by Siemens (Dir-X based product suite), Oracle/Sun (OIM/OAM/OIA), IBM (Tivoli family), Microsoft, and Evidian. Many IA products of today have a history that reflects the numerous mergers and acquisitions in the IA vendor space. This is e.g. illustrated by the original Netscape Directory Server, whose concepts continued into iPlanet, later into Sun, and recently into Oracle. SAP acquired MaXware, essentially a company

based on an Enterprise Directory product to integrate IAM functionality in their business solutions.

There is significant room to offer IAM functionality as a service, and this can be considered an emerging market.

When an application provider offers his services over the Internet or in the cloud, he is facing the challenge of integrating his customer's identity, authentication and authorisation system with his service offer. This leads to the requirement to build a 'circle of trust', or a federation. In such a federation, trust services are required as a foundation for the IdPs (Identity Providers) that offer identity and authentication.

Integration requirements when companies move services to the cloud obviously increase the identity and authentication aspects, as well as the data protection aspects.

b. The outside-to-inside approach

The social network applications were originally seen as 'external' to an entity's population. Their growth brought a need to address identity, authentication and authorisation (IAA) requirements. For example Facebook continuous to improve their IAA solutions:

- In 2006, the first version of the Facebook API was introduced, enabling users to share their information with the third party websites and applications. Many companies leveraged these APIs, allowing users to connect their identity information from Facebook, such as basic profile, friends, photos information and more, to third party websites, as well as desktop and mobile applications.
- In 2007, Facebook Platform was launched, which allowed third party developers to build rich social applications within Facebook. It uses the OAuth 2.0 protocol for authentication and authorization
- In 2008 Facebook Connect was introduced which enabled third party websites to implement more features of Facebook Platform off of Facebook. It builds further on the OpenID and OAuth concepts.
- In the post http://developers.facebook.com/blog/post/534/ is stated *"By October 1, 2011, we require that all website and canvas apps must exclusively support OAuth 2.0 (draft 20). All canvas apps must use the signed_request parameter. This also implies that old, previous versions of our SDKs will stop working, including the old JavaScript SDK. "*
- As such we assume that at the time of putting together this study report, Facebook was strongly favouring Oauth 2.0.

As specified in draft RFC "The OAuth 2.0 Authorization Protocol draft-ietf-oauth-v2-12", OAuth includes four roles working together to grant and provide access to

protected resources (i.e. access restricted resources which require authentication to access):

- resource owner - An entity capable of granting access to a protected resource.When the resource owner is a person it is referred to as an enduser.
- resource server - The server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens.
- Client - An application making protected resource requests on behalf of the resource owner and with its authorization.
- authorization server - The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization.

The Facebook implementation of OAuth aims to give the user control over what a third party app can do with his information. It involves three different steps: user authentication, app authorization and app authentication. User authentication ensures that the user is who he claims to be. This may already be performed in a step prior to the user wanting to access the third party app. App authorization ensures that the user knows what data and capabilities he is providing to the app. App authentication ensures that the user is giving their information to the appropriate app. Once these steps are complete, the app issues a user access token that enables you to access the user's information and take actions on their behalf.

Furthermore, Facebook launched “Connect with Facebook”, referred to (http://developers.facebook.com/docs/guides/web)”.

This builds further on the concepts from OpenID and Oauth to give users the ability to take their identity and social graph with them around the Web. The objective is that Facebook users represent themselves with their real names and real identities and take their identity information with them including profile information, profile picture, name, friends, photos, events, groups, and more. It remains to be seen to what extent this is embraced by the user community. In this field there is a clear potential for cross-over with the diverse identification and authentication services that are at the disposal of the end user. They may have use cases where they prefer to use a simple userid and password, and other use cases where they prefer to rely on a private sector or government supplied eID.[51]

[51] Note that PAYPAL is also using a similar approach making use of OpenID and OAuth.

4.1.4 The academic perspective

a. ABC4TRUST – Attribute-based Credentials

The goal of ABC4Trust (https://abc4trust.eu) is to address the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials (ABC). So far credentials such as digitally signed pieces of personal information or other information used to authenticate or identify a user where not designed to respect the users privacy. They invariably reveal the identity of the holder even though the application at hand often needs much less information, for instance only confirmation that the holder is a teenager or is eligible for social benefits. In contrast to that, Attribute-based Credentials allow a holder to reveal just the minimal information required by the application, without giving away full identity information. These credentials thus facilitate the implementation of a trustworthy and at the same time privacy-protecting digital society.

Today there are only a handful of proposals of how to realize an ABC. Notable is especially the appearance of two technologies, IBM's Identity Mixer (Camenisch) and Microsoft's U-Prove (Brands).

The objectives of ABC4Trust are to define a common, unified architecture for ABC systems to allow comparing their respective features and combining them on common platforms, and to deliver open reference implementations of selected ABC systems and deploy them in actual production pilots allowing provably accredited members of restricted communities to provide anonymous feedback on their community or its members.

ABC4Trust develops and trials an ABC enabled architecture and related application pilots. This will result in important input for the design of the upcoming electronic identity management infrastructure, and e.g. the related European Large Scale Action (ELSA).

The relationship with IAS lies particularly in their introduction of new paradigms such as anonymous credentials and selective disclosure of attributes. This can be expected to drive new security expectations from end users and policy makers.

b. TAS³ - Trusted Architecture for Securely Shared Services

This IST FP7 funded Integrated Project (http://tas3.eu) runs from Jan 2008 through Dec 2011. It focuses on federated identity management and aims to integrate adaptive business-driven end2end Trust Services based on personal information as well as Semantic integration of Security, Trust, and Privacy components. It

addresses four layers: Authentication for federated identities, Authorization for federated attributes, Trustworthiness & Reputation scores, and finally Data Protection policy enforcement.

TAS³ focuses on a Trusted Employability Platform and a Healthcare Demonstrator Platform.

The relationship with IAS lies particularly in how they address federated identities, federated attributes and "trustworthiness". These can equally be expected to drive new security expectations from end users and policy makers.

c. PrimeLife

PrimeLife is the FP7 continuation of Prime in FP6. It runs from March 2008 for 40 Months. PrimeLife is addressing the core privacy and trust issues pertaining to the challenges related to protecting the autonomy and control of users over personal information in daily interaction over the Internet. This raises substantial new privacy challenges such as how to protect privacy in emerging Internet applications such as collaborative scenarios and virtual communities, and how to maintain life-long privacy.

Its long-term vision is to counter the trend to life-long personal data trails without compromising on functionality. It will build upon and expand the FP6 project PRIME that has shown how privacy technologies can enable citizens to execute their legal rights to control personal information in on-line transactions.

The main objective of the project is to bring sustainable privacy and identity management to future networks and services:

- Fundamentally understand privacy-enhancing identity management 'for life' (practical life, throughout life & beyond)
- Bring privacy to the web and its applications
- Develop and make tools for privacy friendly identity management widely available

Resolving these issues requires substantial progress in underlying technologies. PrimeLife aims to substantially advance the state of the art in the areas of human computer interfaces, configurable policy languages, web service federations, infrastructures and privacy-enhancing cryptography.

The relationship with IAS lies particularly in how they address privacy-enhancing identities. This is a fundamentally different approach because such identities will be able to engage in transactions that do require proof of certain identity aspects or attributes only, while further guaranteeing privacy. These can equally be expected to

drive new security expectations from end users and policy makers alike, for example in the broad area of e-democracy.

4.1.5 Beyond the EU Member States

Outside the EU there are many remarkable I, A and S initiatives. We highlight one selected initiative, the eID and signature interoperability framework that is currently under construction in the GCC, as it is both technologically advanced and bears strong resemblance to the EU Member States situation.

a. The GCC approach

GCC is the acronym for Gulf Cooperation Council including six countries namely, Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates. The number of GCC population is estimated to be around 40 million people (GCC Portal, 2011). GCC citizens can usually travel freely between member states without the need for visas, and can use either their passports or national identity cards for border crossings. All GCC countries have initiated a national identity card programs with smart cards, biometrics, and PKI.

The majority of GCC states have developed e-identity service models with varying levels of complexity, including Qatar, Saudi Arabia, United Arab Emirates, Oman, and Kuwait. They introduced projects to accelerate the adoption of e-identity in their local societies mainly in the context of e-government. Among these projects, GCC countries are working to develop a common e-identity infrastructure that will enable the authentication of GCC citizens by any service provider at a member state e.g., border control, public services, etc. In light of the imminent requirement to enable e-identity on the GCC level, interoperability represents a major challenge.

While all GCC e-identity cards are ISO 7816 standard compliant, certain characteristics of the GCC cards are issuer specific, as a consequence of the proprietary applications (i.e. applets). These applications have their own file layouts and communicate via a dedicated set of APDUs (Application Protocol Data Units). All GCC countries developed middleware applications to enable interaction and access to their electronic identity cards. These are not necessarily compatible.

The following typical building blocks are present:

- e-identity common middleware: software libraries exposing the e-identity card business functions to service providers.

- e-identity discovery service: a server dedicated to discovering the target e-identity to query the client terminal in order to execute a specific card transaction.
- e-Identity Validation Gateway (VG): a Server exposing the e-identity scheme owner card validation services as web services available over the cloud.

b. The UAE approach

UAE is a pioneer in its biometric implementation. It has integrated multiple biometric technologies in critical infrastructure systems in the last decade, including:

Iris recognition

At the country's entry points, all visitors are required to undergo an iris scan. The UAE began the implementation of iris recognition technology at its borders in 2001 to inhibit illegal entry of persons in the country. The UAE was the first in the world to introduce such a large scale deployment of this technology. Today, all of the UAE's land, air and sea ports of entry are equipped with iris systems. UAE iris watch-list database is currently most likely the largest in the world, both in terms of number of iris records enrolled (more than 2.3 million people) and number of iris comparisons performed daily.

Facial Recognition

Facial recognition (facial on the move) has been implemented at UAE airports in 2008 to enhance security procedures and detect persons who might pose a threat to the country. The system allows identification checks to be performed from a distance without a person's active participation. The system helps inspectors at control points inside the airports to implement continuous and proactive checks designed to immediately detect persons who should be denied entry or detained.

Fingerprint based - Electronic Gates

UAE has another biometric application working at its airports; namely biometric based electronic gates (e-gate). The e-gate facility which was first introduced in 2002 in Dubai International Airport, is the first airport in the region and the third in the world offering this service to travellers. The service is basically available for quick passage through passport control. The electronic gate uses fingerprint biometrics to automatically process all registered passengers arriving and leaving from any of the UAE airports. This is a passenger clearance system that considerably accelerates the movement of traffic through electronic screening of passengers' data with the help of a smart card. It was estimated that more than 4 million travellers used electronic gates in 2010.

Electronic Passport

The UAE government is in the process of launching its new electronic (biometric) passport. The new passport contains biometric information mainly fingerprints and an ICAO standard photograph.

The information on the chips can be scanned and verified at airports, other ports and border posts.

PKI technology is used to sign the electronic data stored in the passport microprocessor chip. This is expected to enhance the current security features of passports and provide greater protection against tampering and reduce the risk of identity fraud. The issuance process is linked with the expiry of the existing passports as it will be replaced with the electronic ones. The biographical and fingerprint data are pulled electronically from the national identity register.

National Identity Register

Another large scale biometric program was launched in 2003. The program aims to set up a national identity register and to enrol an estimated 9 million population in the country. This program, which is also referred to by the UAE government as the national identity management infrastructure, aims to serve multiple strategic objectives. The primary objective was to set up a government entity that has an imperative role as the single source for personal identity provision in the Country.

Federal DNA Project

The government has begun a DNA identification database development in 2010. The project which is still in its pilot phase, targets to collect DNA samples of 10 million people both national citizens and foreign residents in the next few years. The federal DNA database is primarily seen to contribute to areas related to crime detection and identification of criminals. The market in the UAE has seen some trails of biometrics in public and private sectors however they were primarily limited to the field of physical access control. The application of the new UAE biometric identity card capabilities, to provide secure identification and personal verification solutions, is envisaged to improve public acceptance of the technology and vitalise electronic transactions.

c. The UAE eID

UAE issues a smart cards to its citizens and residents. It is Java based and serves the dual purpose of an application platform as well as secure storage. The application platform allows algorithms to run on the card. The secure storage

enables tamper proof storing of identity data including biometric data. The UAE was one of the early adopters of match-on-card feature. This feature enables fingerprint Match-on-Card user authentication as an alternative and to complement smart card PIN verification. This in turn gives access to the digital certificates on the card that can then be used for logon, digital signature, file encryption, secure VPN access among other services.

This solution provides a secure two or three factor authentication capability. The card is a hybrid smartcard that also contains PIN protected personal data including digital certificates, and the holder's biographical data and two best fingerprints. The card is envisaged to be the only acceptable identity document to access any government and some critical private sector services like the financial sector.

The multi-application card is designed to be compliant with the two major industry standards: the "Global Platform Card Specification Version 2.0.1", and the "Visa Card Implementation Requirements Configuration 1-Compact". Both the Java Card Runtime Environment (JCRE) and the Global Platform (GP) standards contribute to the security features of the UAE National ID card. Java provides cryptographic mechanisms and enforces firewalls to protect applications and maintain data and operation security within the multi-application shared card space. The GP 2.0.1 specifications extend the Java Card cryptographic authentication mechanisms to ensure dynamic and secure loading/ updating of individual applications in the dynamic and multi-applet Java Card. There are five applets on the card: ID and ePurse applet, PKI applet, Match on Card applet for the biometrics, eTravel Applet for ICAO, and a MIFARE Applet for public transport. Communication with the card can only be established using the SDK/Tool Kit distributed by the government.

For more information we refer to the article "Towards Federated e-Identity Management across GCC – A Solution's framework" by Dr Ali M. Al-Khouri and Malek Bechlaghem.

4.2 eSignatures

4.2.1 European Commission driven actions

At EU level a set of significant initiatives have been implemented since the emphasising of interoperability and mutual recognition barriers, whether technical or

legal, to the (cross-border) use of electronic signatures[52], starting with the **Action Plan on eSignatures and eIdentification to facilitate the provision of cross-border public services in the Single Market** published in 2008. It assumed that the creation of a comprehensive and pragmatic framework to achieve interoperable eSignatures (and eID) would simplify access of enterprises and citizens to cross-border electronic public services and would also benefit to B2B and B2C transactions and that the cross-border use of QES and AdES based on QC could be improved very quickly because of their clear legal status under Directive 1999/93/EC and the substantial existing standardisation work.

In support of this Action Plan, the Commission launched the **CROBIES Study[53]** to analyse the requirements and establish a general strategy for cross-border use of QES and AES based on QC *within* the existing legal framework set by the Directive. The CROBIES study concluded that a recast of the existing legal, standardisation and trust frameworks related to ES, supported by appropriate promotional and educational efforts, is essential to improve interoperability and cross-border use of ES. However CROBIES focused in five working packages (WP) on several "quick-win" actions that could improve some very specific aspects of the interoperability, cross-border use and mutual recognition of QES and AES based on QC *within* the current legal framework:

1. WP1. A proposal for a **common model for supervision and accreditation** of certification service providers issuing qualified certificates (and other services ancillary to e-signatures) because Directive 1999/93/EC does not specify how supervision should be organised.

2. WP2. The establishment of a **"Trusted List" for certification services issuing qualified certificates**. The resulting deliverable was the key

[52] Preliminary Study on Mutual recognition of eSignatures (2007): This study collected and analysed information on eSignatures approaches in eGovernment applications in the Member States and determined interoperability barriers and potential solutions.

Study on Mutual recognition of eSignatures (2009): This study updated country profiles in order to improve information on the advanced electronic signatures in use in eGovernment applications.

Study on the Standardisation aspects of eSignatures (2007): This study analysed the use made by enterprises, market players and other stakeholders of the standard referenced by Decision 2003/511/EC and other related standards resulting from EESSI and subsequent ESO's works in that matter. It assessed whether the business model chosen by Directive 1999/93/EC was still relevant given the technological developments. It concluded that the current EU eSignature standardisation landscape is too complex to use due to the multiplicity of documents, the lack of business orientation and usage guidelines, the difficulty of access and formulated recommendations to overcome these issues.

[53] http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm.

technical input for the establishment of **CD 2009/767/EC amended by CD2010/425/EU** that obliges MS to accept certain eSignatures (if these are required) and establish a common template and set of specifications for the establishment, maintenance and publication of Trusted List (TLs) indicating the supervision/accreditation status information on certification services issuing qualified certificates and on a voluntary basis on other supervised / accredited ancillary services to eSignatures.

3. WP3. A proposal for an **interoperable qualified signature certificate profile** to improve the provision, in both machine processable and human readable ways, of information on the qualified status of a certificate and on the indication that the e-signatures it support are created by a secure signature creation device as defined by Directive 1999/93/EC

4. WP4. A proposed framework for **interoperable Secure Signature Creation Devices**. Although Annex III to the Directive gives high level requirements for secure devices and specific standards were developed for their assessment, interpretation and implementation at national level still varies quite widely. To resolve this issue, CROBIES formulated recommendations for a homogeneous interpretation of the Directive at the European level.

5. WP5. A proposed model for providing **guidelines and guidance** for implementation of cross-border and interoperable e-signatures. CROBIES also proposed a **quality classification for e-signatures** as well as a means to maintain a European list of recommended **cryptographic algorithms** for e-signature.

The recommendations on the recast of the European eSignature standardisation landscape was put into practice through the issuance by the European Commission of the **Standardisation Mandate 460**[54] to CEN, CENELEC and ETSI to update the existing eSignature standardisation deliverables, suggesting the establishment of a fully rationalised framework, including implementation guidelines, to overcome all these issues within the context of the Signature Directive, while taking into account its possible revision. See section 3.1.1 for more details.

In 2010, the Commission released a **Digital Agenda for Europe**[55], being Europe's strategy for a flourishing digital economy by 2020. It consists of seven action areas, two of which relate to eAuthentication (Key Action 3) and eIdentification (Key Action 16). The Commission acknowledged that despite the existing key single market

[54] Mandate M460: "Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the Field of Information and Communication Technologies Applied to Electronic Signatures"

(http://ec.europa.eu/information_society/policy/esignature/eu_legislation/standardisation/index_en.htm).

[55] A Digital Agenda for Europe, 2010. The Digital Agenda is one of the seven flagship initiatives of the Europe2020 Strategy, the EU's growth strategy for the coming decade. See http://ec.europa.eu/information_society/digital-agenda/index_en.htm

legislation, online transactions are still too complicated and fragmented markets limit the demands for cross-border transactions. Therefore, it announces as a "Key Action 3" under the first pillar a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems.

Furthermore, initiated by IDABC, the Commission launched the **EFVS Study**[56] to examine the existing issues from the perspective of signature validation at the European level and to assess the legal, operational and technical feasibility of a European scale eSignature verification functionality. The study analysed selected existing eSignature verification solutions on the market, examined the feasibility and need for a common EU validation solution but concluded that in the current environment of missing legal regulations for Signature Validation Service Providers, inappropriate standards and a trust framework on an ad hoc basis it is virtually impossible to design comprehensive and durable validation solutions with a general EU level impact. Therefore, the Study stated the need for a broader perspective and proposed as well a comprehensive revision of the existing legal, technical and trust framework.

On 18 February 2011, the European Commission launched[57] in the context of the Digital Agenda for Europe[58] a **Public Consultation regarding electronic identification, authentication and signatures**[59], which closed on 15 April 2011. The purpose of the public consultation was to provide input for policymakers on how electronic identification, authentication and signatures can contribute to deliver the European digital single market. The European Commission also invited representatives from the public and private sectors and academia to a **stakeholder workshop**[60] on 10 March 2011 to debate on what legislative measures are needed

---

[56] EFVS study: description, analysis and assessment reports: http://ec.europa.eu/idabc/en/document/7764.html.

[57] See the press release at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/198&format=HTML&aged=0&language=EN&guiLanguage=en

[58] See http://ec.europa.eu/information_society/digital-agenda/index_en.htm.

[59] See http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision/pub_cons/index_en.htm

[60] Stakeholders workshop Digital Agenda for Europe: electronic identification, authentication and signatures in the European digital single market: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision/ws_3_2011/index_en.htm.

to address the challenges ahead. The objective of the workshop was to offer an interactive forum to exchange views and to confront different positions on the questions raised in the public consultation.

The European Commission received more than 400 contributions from a wide range of actors, including Member States, EU and national organisations, regional and local authorities, business and professional federations, individual companies, NGOs, and many European citizens. Most contributions were made via the Commission's online consultation tool (IPM — Interactive Policy Making), and several others were sent in as separate submissions.[61] Roughly half of the submissions originated from these organisations, with the other half of the respondents being from individual citizens.

Main findings on IAS usages

The overall usage of e-IAS tools by the respondents is reported to be relatively high (around 80 %), with responses showing no significant difference between organisations and individuals. IAS tools are mainly used for securing transactions and guaranteeing the integrity of electronic documents. Over 80% of respondents consider eGovernment and eBanking as the major application areas, emphasizing the importance of ensuring integrity and security in these domains.

eSignatures tailored to face the challenges of the digital single market

When examining how the respondents perceived the impact and role of eSignatures on the Digital Single Market, almost 80% of respondents estimated that take-up was low, characterising it as marginal or moderate. The most frequently indicated causes for this relatively low success rate were (1) the limited number of services requiring eSignatures; (2) insufficient user friendliness; (3) cross-border interoperability issues.

As the main interoperability challenges to be fixed by future initiatives, respondents refer to the heterogeneous approach to security requirements in different Member States, unclear terminology (both in the eSignatures Directive and in national implementations), and insufficient harmonisation of profiles of qualified certificates.

Generally, respondents suggested that future regulations could improve interoperability by eliminating ambiguities and reducing national divergences. In particular, 87% of respondents replied that EU legislation should also address ancillary services like certified e-documents, time stamping, mandates, e-seals, certified document delivery or archiving, whereas only 5% entirely opposed new

[61] Contributions can be accessed online at: http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision/pub_cons/index_en.htm

regulatory initiatives. Finally, 61% favoured the introduction of eConsent as a building block in EU eSignature legislation.

From a technical point of view, when analysing the options for addressing eSignature challenges, opinions are less clear. Only 32% of respondents are in favour of a creating a central EU signature validation service. Similarly, 50% of respondents believe that a common European eSignature security classification scheme would be useful.

Other topics found more universal support, such as supporting mobile devices as IAS tools (favoured by 82% of the respondents), and maintaining or keeping the EU's high "qualified" signatures security, as expressed by 66% of respondents (as opposed to the 16% who would prefer relaxed requirements).

Principles for future e-identification and authentication legislation and policy

The consultation gauged opinion on the perceived need for legislative measures to address e-identification and e-authentication in particular, including the fundamental principles of such legislation, expected effects on the Digital Single Market, potential benefits for users, cross-sector interoperability and any lessons learned.

A large majority of 65% of respondents favoured EU legislation for electronic identification, whereas only 23% was against. Key areas to be covered by such legislation according to the respondents are notably data protection and privacy (78%), transparency (65%), and liability of the eID provider (59%). Affordability and cross-sector usability were considered important by 39%. Identity federation saw significantly more support (44%) than a centralised approach (23%). **Respondents thus clearly favoured an open, trustworthy and interoperable eID environment.**

Looking at the expected impact of legislative measures addressing mutual recognition and acceptance of eID across borders on the Digital Single Market, the main expected effects were an improvement of legal certainty (62,2%), a reduction of administrative burdens (60,8%), and the increase of cross-border mobility (59,1%). Economically, respondents expect that increased economies of scale (49%) will have a strong positive impact as eIDs would become useful of an increased number of applications.

Finally, respondents frequently stressed the importance of international standardization, if possible supported through international agreements to use the same standards in international transactions. IAS services are seen as an inherently international phenomenon, and European initiatives should be attuned to this reality.

On the practical side, in the context of the Services Directive (2006/123/EC) that obliges Member States to make sure that service providers (businesses) can complete the procedures and formalities that are necessary to start or carry out their activities with Member States' administrations via Points of Single Contact and by electronic means, including across borders, and in order to facilitate in practice the

cross-border use of e-procedures and in particular of e-signatures that can be required in the process of completing procedures, three Commission Decisions have been adopted: Commission Decision 2009/767/EC, amended by Decision 2010/425/EU and Decision 2011/130/EU. The first two CD's oblige Member States to accept certain eSignatures (if these are required) and establish a common template and set of specifications for the establishment, maintenance and publication of Trusted List (TLs) indicating the supervision/accreditation status information on certification services issuing qualified certificates and on a voluntary basis on other supervised / accredited ancillary services to eSignatures. **CD 2011/130/EU** obliges Member States by August 2011 to be able to technically process certain formats of advanced electronic signatures (AdES) when they verify documents signed electronically by public authorities in other Member States. This latter Decision constitutes a further step on the European level to facilitate the verification of eSignatures in the context of documents that service providers may be required to sign or have signed to complete procedures through the Points of Single Contact.

In order to implement Article 8 of the Services and the three implementing Decisions above, the Commission has already provided and is still providing some assistance to Member States via some practical **tools and open source software**, available through the OSOR platform, **related to Trusted Lists and to advanced e-signature creation/validation**. Such signature and verification signature tools are considered to be used by Large Scale Pilots such as SPOCS and eCodex.

The European Commission is also working on an **Electronic Signature Service Infrastructure (ESSI)** and related Application Platform to facilitate the introduction of electronic signatures in its own internal and external exchanges.

4.2.2 Use of eSignatures in Large Scale Pilots: scope, impact and lessons learned

Large Scale Pilot projects launched by the Commission and some Member States as part of the ICT PSP Programme are making use or are likely to make use of eSignatures, namely PEPPOL, SPOCS and eCodex.

A federated approach to cross-border validation of eSignature is currently tested within PEPPOL[62], the large-scale cross-border eProcurement pilot project launched in 2008. In order to avoid multiple validation efforts in all Member States which are

[62] PEPPOL website, www.peppol.eu.

the main obstacle to cross-border interoperability, it may be an option to delegate verification tasks to a centralised or distributed validation service mechanism. WP 1 of PEPPOL addresses a specific cross-border eSignature validation tool or, to be more precise, a validation infrastructure for eProcurement applications, mostly relying on a commercial service currently. However sustainability of the project is in question and although the EFVS Study did not preselect PEPPOL as a key solution because it operated as a mere pilot project without a functioning implementation at that time and was unlikely to implement a definitive liability model, the results of EFVS study should also feed into a further optimisation of PEPPOL.

SPOCS[63], another LSP project launched in May 2009, aims at improving the competitiveness of European businesses and particularly small and medium sized enterprises by enabling national and European businesses to benefit from available efficient and interoperable electronic procedures. SPOCS is expected to build the next generation Points of Single Contact within the meaning of the Services Directive for businesses across Europe. It will provide seamless electronic procedures by building cross border interoperability based on existing systems and solutions. The project has presented several deliverables on specifications of a European interoperability layer for eGovernment services which are currently undergoing review from the European Commission. Envisaging the role of standardisation bodies and the use of EC provided tools for creation and verification of electronic signatures during a joint SPOCS, ETSI and European Commission workshop in September 2011, it was confirmed that a joint collaboration is likely to produce a win-win approach benefiting from each other's experiences and lessons learned provided that such a joint collaboration could be extended as a standard way for EC projects to consult the standardization bodies and to reuse existing standards/tool in particular with regards to eSignatures. In particular ETSI will evaluate how to extend the Associated Signature Container (ASiC-E) standard to cover the SPOCS defined Omnifarious Container for e-Documents (OCD) format and future contacts regarding the full standardization of OCDs will be kicked off within ETSI. On the other hand it was recognised that the OSS signature creation/verification tools developed on behalf of the European Commission in the context of Services Directive would be considered to be used by SPOCS and by e-CODEX.

e-CODEX[64] is an e-justice project to improve the cross-border access of citizens and businesses to legal means in Europe as well as to improve the interoperability

[63] SPOCS (Simple Procedures Online for Cross-border Services) website: www.eu-spocs.eu

[64] e-CODEX website: www.ecodex.eu.

between legal principals. a functionality which provides an easier (digital) way to exchange legal information between EU-countries. The aim of the project is:

- Contributing to the implementation of the EU legal framework and the e-Justice action plan, in due respect of subsidiarity;
- Achieving interoperability between existing national judicial systems;
- Enabling all Member States to work together towards a more effective judicial system in Europe;
- Improving the effectiveness and efficiency of the processing of the increasing number of cross-border proceedings, especially in civil, criminal and commercial matters;
- Contributing to a safer environment for citizens inside the EU;
- Modernizing the judicial systems in Europe;
- Increasing collaboration and exchange between judicial systems of the Member States.

4.2.3 European sector specific initiatives

European work on eSignature and eID is particularly relevant in judicial matters, where the authentication of acts is essential. Therefore, the Council of Bars and Law Societies of Europe (CCBE)[65] seeks to assist the development of a safe and practical electronic environment for legal professionals throughout Europe. In order to enable interoperable eCommunication for lawyers, CCBE has proposed a European Framework System for electronic ID cards for lawyers with possibly optional ES functionality. With this system, the CCBE aims at supporting its member bars in the implementation of electronic ID card schemes and – at the same time – to make these schemes interoperable for lawyers throughout Europe.

[65] www.ccbe.org

5. Conclusions

While far from exhaustive, the overview of initiatives above – comprising legal texts, standardisation initiatives, pilot projects, reference implementations and sector specific policies – shows that the IAS domain has far outgrown the scope of past European IAS initiatives, as principally embodied in the eSignatures Directive. These initiatives are indicative of the state of the art with respect to electronic identification, authentication and signatures, and illustrate that there is a need to move beyond the current principal focus on electronic signatures.

With respect to legislative initiatives, this can be seen most clearly in the number of acts that address varieties of eSignatures (notably eSignatures created by legal entities or public administrations), as well as time stamping, electronic registered mail and electronic archiving. Regulation of electronic identification was however seen much less frequently; it is clear that this is still an area in full development, for which a need for regulatory intervention is much less manifest, and where such intervention will thus need to be more clearly justified.

These legal frameworks also offer some support to the observation made in the first report of this study that the issues and possible solutions for each of these areas are not too different from those for electronic signatures. In some cases, definitions (e.g. of time stamping) were only minor variations of the European eSignature vocabulary. In other areas too, the links were frequently clear, e.g. by the integration of eSignatures and time stamping in a single act, or by subjecting various types of service providers (eSignatures, time stamping, registered mail, archiving,…) to the supervision of the same supervisory authority.

These are all examples of the close links between various IAS services, and of the possibility of streamlining the legislative approach for all of them by applying the same legal and supervisory model. It is thus worth noting that these national laws offer a great deal of inspiration for any future European legislative initiatives: the descriptions in this report contain references to definitions of services, lists of obligations, liabilities and legal effects, which could be re-used (sometimes virtually without changes) for a similar European regulatory framework.

Perhaps most importantly, the existence of multiple such laws shows that in a significant number of Member States, there is a perception of a regulatory gap that is currently not addressed at the European level. The creation of national frameworks for IAS services without European coordination (other than, obviously, for electronic signatures) risks creating new barriers for service providers in this area, who will have to explore on a case by case basis (1) whether laws exist, and (2) whether they (are able to) comply with them. Thus, the risk of distortions of the internal market is very real. Furthermore, the proliferation

of national laws on IAS services in countries outside the European Union, providing legal certainty to those companies offering and using IAS-related services, may have an impact on the competitiveness of European companies not enjoying similar legal comfort.

Apart from the legal perspective, the overview in this report also examines the state of the art with respect to technical issues, including notably standardisation work. Not surprisingly, we can see that standardisation efforts have never been restricted to e-signatures as emphasized by the eSignatures Directive, and that relevant standards have been created for all types of IAS services. This is unsurprising, as the mere existence and use of these services – even outside the context of any (shared) legal framework – would present interoperability challenges that could only be addressed through technical standardization.

Current standardization efforts (including at the European level through mandate M460) therefore focus on rationalizing – i.e. streamlining, updating and aligning – the existing standardization framework, to ensure its completeness, relevance and practical applicability. Standards are thus also moving to match a more comprehensive perspective on IAS services.

It is worth noting that here too, there is a risk of creating a disconnect between laws and standards when laws do not recognize existing standards in any way. Indeed, this presents a real interoperability risk, as the overview above has shown that national laws (or more typically decrees and decisions issued on the basis of these laws) often reference existing standards as being required. Thus, the overview above supports the contention that the current rationalization exercise is necessary, but also that it will at some point require a clearer legal grounding, preferably at the European level, to support its impact in practice.

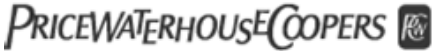
Finally, this report also examined a number of key ongoing pilot initiatives, projects and reference implementations (including notably the large scale pilots). The overview showed that these initiatives show great potential, and have often been successful in building workable solutions to real-life problems. What is however lacking, is a European policy framework through which they can be given a clear legal basis and further support for their sustainability and uptake in practice.

Globally, the picture offered by this overview is admittedly not comprehensive, but none the less persuasive. It shows that IAS services cover a much wider range of activities, in which legislations, standards and pilot projects have evolved beyond what the current EU legal framework can viably support. In order to avoid internal market barriers and to ensure that IAS services can get broader policy support in Europe, an update and expansion of the policy framework that covers these services – including eSignatures, time stamping, electronic registered mail, e-archiving, and electronic identification – will be necessary.


DLA PIPER


SEALED
Trust Services Architects


time.lex


PRICEWATERHOUSECOOPERS



Feasibility Study on an electronic identification, authentication and signature policy (IAS)

SMART 2010/0008

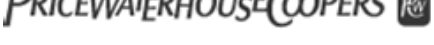
Proposal for a European IAS policy framework

Final Version (D3, Version 2b (final))
20 February 2013











This study was commissioned by the European Commission's Information Society and Media Directorate-General, in response to the general invitation to tender of the Directorate-General Information Society and Media, n° SMART N° 2010/008. The study does not, however, express the Commission's official views. The views expressed and all recommendations made are those of the authors.

Table of contents

1. SUMMARY OF THE STUDY GOALS AND SCOPE 9
1.1 Background of the Study 9
1.2 Scope of the Study 9
1.3 Role of this document in the Study 10

2. BUILDING BLOCKS FOR A FUTURE IAS POLICY FRAMEWORK 12
2.1 Building blocks for designing the future IAS Policy framework 12
2.1.1 From a legal point of view 13
2.1.2 From a technical point of view 14
2.1.3 From a trust point of view 15
2.1.4 From a practical and commercial point of view 15

3. RECOMMENDATIONS FOR BUILDING AN IAS REGULATION 17
3.1 Recommendations for an IAS Regulation 17
3.2 Ad-hoc support provided to the Commission 17

4. SUPERVISION ISSUES 19
4.1 Introduction 19
4.1.1 Trust services as key enablers in boosting use of online environment 19
4.1.2 Supervision and Trusted Lists as essential building blocks 23
4.1.3 Objectives for a sound Supervision system and Trusted Lists 25
4.2 Supervision in the proposal for Regulation 26
4.2.1 Supervisory body 26
4.2.2 Mutual assistance 27
4.2.3 Security requirements applicable to trust service providers 28
4.2.4 Supervision of qualified trust service providers 29
4.2.5 Initiation of a qualified trust service 30
4.2.6 Trusted Lists 31
4.2.7 Requirements for qualified trust service providers 31
4.3 A model for supervision of qualified trust service providers and qualified trust services they provide 33
4.3.1 Introduction 33
4.3.2 The “ISO Conformity Assessment” approach 33
4.3.3 The ISAE 3000 approach 36
4.3.4 The AICPA approach 37
4.3.5 The ISAE 3402 approach 39
4.3.6 The IFAC/IAASB/ISRS 4400 approach on “Agreed upon procedures” 39

4.3.7 Our proposal for a European Supervision Scheme for qualified trust service providers and qualified trust services they provide 39
4.4 Conclusions 44

5. IAS IN THE CLOUD 46
5.1 IAS in the Cloud, opportunities and challenges. 46
5.2 The Cloud's need for security is supported by IAS 47
5.2.1 Cloud service models 47
5.2.2 End user perspective 48
5.2.3 Management perspective 49
5.3 Cloud as an effective IAS services deployment model 50
5.3.1 Need for trust 50
5.3.2 Potential of an IASaaS model 50
5.4 Moving IAS into the cloud: legal issues 51
5.4.1 Data protection 52
5.4.2 Applicable laws 53
5.4.3 eSignature laws compliance 54

6. OVERVIEW OF DELEGATING AND IMPLEMENTING ACTS WITHIN THE REGULATION 55
6.1 Notification 55
6.2 Coordination 56
6.3 Supervisory body 58
6.4 Mutual assistance 60
6.5 Security requirements applicable to trust service providers 61
6.6 Supervision of QTSPs 63
6.7 Initiation of a QTS 66
6.8 Trusted lists 67
6.9 Requirements for QTSPs 68
6.10 Legal effects and acceptance of electronic signatures 69
6.11 QCs for electronic signature 70
6.12 Requirements for QSCDs 72
6.13 Certification of QSCDs 73
6.14 Publication of a list of certified QSCDs 74
6.15 Requirements for the validation of QeSs 75
6.16 Qualified validation service for QeSs 79
6.17 Preservation of QeSs 79
6.18 Legal effects of electronic seals 80
6.19 Requirements for QCs for electronic seal 81
6.20 Qualified electronic seal creation devices 83
6.21 Validation and preservation of qualified electronic seals 86

6.22 Requirements for qualified electronic time stamps 92
6.23 Legal effects and acceptance of the electronic documents 92
6.24 Legal effect of an electronic delivery service 93
6.25 Requirements for qualified electronic delivery services 94
6.26 Requirements for QCs for website authentication 95

7. ECONOMIC, SOCIAL AND ENVIRONMENTAL IMPACT OF A EUROPEAN FRAMEWORK FOR ANCILLARY SERVICES 98
7.1 Introduction 98
7.1.1 Context and objectives of the study 98
7.1.2 Overview of ancillary services 98
7.2 Drawing up the conceptual framework for REA 101
7.2.1 REA-question 101
7.2.2 Search process 101
7.2.3 Research findings 104
7.3 Discussion 127
7.4 References 129
7.4.1 Studies included in the Rapid Evidence Assessment 129
7.4.2 Other references 130

8. DISCUSSION ON A PAN-EUROPEAN EID SYSTEM, CHALLENGES AND OPPORTUNITIES 131
8.1 Introduction 131
8.1.1 Why do we need IAS for the information society - trusted communication and transactions 131
8.1.2 Current European legal framework 134
8.1.3 Existing IAS systems 136
8.1.4 Preliminary conclusion 141
8.2 Requirements for a pan-European eAuthentication system 142
8.2.1 User friendliness 142
8.2.2 Technologically neutral, interoperable, cross-applicable 143
8.2.3 Secure and reliable 144
8.2.4 Legally predictable 144
8.2.5 Scalability 144
8.2.6 Trust 145
8.2.7 Obstacles 146
8.3 Lessons learnt from .euTLD 148
8.3.1 Application to eID 151
8.3.2 The principles of a possible eID legal framework 152
8.4 Characteristics of a possible pan-European eAuthentication system 155
8.4.1 Inherent dilemma 155

8.4.2 Voluntary 155
8.4.3 User friendly 156
8.4.4 Secure 156
8.4.5 Privacy 157
8.4.6 Custom made 157
8.4.7 Portability 157
8.4.8 Drawbacks of the system 158
8.5 Conclusion 160
8.6 References 162

9. ANNEX A - RECOMMENDATIONS FOR AN IAS REGULATION 165
9.1 Building blocks for General Provisions 165
9.1.1 Possible provisions for scope 165
9.1.2 Possible provisions for definitions 166
9.2 Building blocks for Basic Principles 168
9.2.1 Possible provisions for market access 168
9.2.2 Possible provisions for Internal market principles 168
9.2.3 Possible provisions for non-discrimination principle 168
9.2.4 Possible provisions for generic quality requirements for trust service providers providing qualified trust services 169
9.2.5 Possible provisions for liability of qualified trust service providers 170
9.2.6 Possible provisions for data protection 170
9.2.7 Possible provisions for international aspects 171
9.2.8 Possible provisions for standardisation and presumption of conformity 171
9.3 Building blocks for the Supervision of qualified services 171
9.3.1 Possible provisions for Supervisory authorities 171
9.3.2 Possible provisions for independence and confidentiality 172
9.3.3 Possible provisions for duties 173
9.4 Building blocks for the establishment of a European Trust Services Committee / EU level governance framework 173
9.4.1 Possible provisions for European trust services committee 173
9.4.2 Possible provisions for independence 173
9.4.3 Recommendation on the possible tasks of the European trust services committee 174
9.4.4 Recommendation for international co-operation 175
9.4.5 Possible provisions for procedure 175
9.4.6 Possible provisions for reports 175
9.5 Building blocks for the regulation of Qualified trust services 176
9.5.1 Possible provisions for legal effects of electronic signatures 176
9.5.2 Possible provisions for legal effects of electronic seals 176

9.5.3 Possible provisions for quality requirements for qualified electronic signatures and qualified electronic seals 177
9.5.4 Possible provisions for legal effects of electronic identity attestations 178
9.5.5 Possible provisions for Quality requirements for qualified electronic identity attestations 178
9.5.6 Possible provisions for additional liability 179
9.5.7 Possible provisions for legal effects of electronic time stamps 180
9.5.8 Possible provisions for quality requirements for qualified electronic time stamps 181
9.5.9 Possible provisions for additional liability 181
9.6 Building blocks for the Regulation of Ancillary services 181
9.6.1 Possible provisions for legal effects of registered electronic mail 181
9.6.2 Possible provisions for quality requirements for qualified registered electronic mail 182
9.6.3 Possible provisions for requirements for qualified certificates 183
9.6.4 Possible provisions for secure signature verification 183

10. ANNEX B - ANNEXES TO CHAPTER ECONOMIC, SOCIAL AND ENVIRONMENTAL IMPACT OF A EUROPEAN FRAMEWORK FOR ANCILLARY SERVICES 184

10.1 Section A – Methodology used for Systematic Review/REA 184
Introduction to Systematic Reviews 184
Background to Rapid Evidence Assessments 185
10.2 Section B: Sources with indirect bearing on impact of Ancillary Services 186

11. ANNEX C - RECOMMENDATIONS FOR A EUROPEAN SUPERVISION SCHEME: PROPOSAL FOR CONFORMITY ASSESSMENT GUIDANCE 196

11.1 Introduction 198
11.2 Principles of the Supervision Scheme 198
11.3 Terminology, definitions and abbreviations 199
11.3.1 Terminology and definitions 199
11.3.2 Abbreviations 201
11.4 References 202
11.5 Conformity assessment model 202
11.5.1 Context 202
11.5.2 Description of the Assessment model 202
11.6 Responsibilities of the parties 204
11.7 Supervision process 205
11.7.1 Supervision process flow at a glance 205
11.7.2 Preparation 209
11.7.3 Initiation 210

11.7.4 Supervision Review 212
11.8 Requirements on Conformity Assessments 213
11.8.1 Conformity Assessment types 213
11.8.2 Conformity Assessment process 214
11.8.3 Requirements on multisite sampling 217
11.9 Events triggering assessments (incl. notification of changes, termination, incidents, complaints, at supervisory body sole's discretion, EC request) 219
11.10 Conformity Assessment Bodies 219
11.10.1 Recognition of Conformity Assessment Bodies - Requirements on NABs 219
11.10.2 Requirements on Conformity Assessment Bodies 219
11.11 Cross-border Assessment and Mutual Assistance 222

1. Summary of the Study goals and scope

1.1 Background of the Study

The purpose of the present project, as described in the tender specifications, is to study the feasibility of a comprehensive EU legal framework that would apply to electronic assertions needed to secure electronic transactions as well as the ancillary services needed to use them: electronic identification, authentication, signature, seals, certified delivery. The perspective would be to facilitate the smooth working of electronic transactions in the internal market. In other words, it would be based on article 114 of the Treaty on the Functioning of EU (TFEU).

The Digital Agenda confirms that "*Electronic identity (eID) technologies and authentication services are essential for transactions on the internet both in the private and public sectors. Today the most common way to authenticate is the use of passwords. For many applications this may be sufficient, but more secure solutions are increasingly needed. As there will be many solutions, industry, supported by policy actions – in particular eGovernment services - should ensure interoperability based on standards and open development platforms.*"

The Commission, therefore, will "*In 2011 propose a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems*". This Study aims to provide inputs for this action.

1.2 Scope of the Study

The scope of this study is to determine if and how a comprehensive European IAS framework could be formed, including the legal, technical and trust components required for such a framework.

The study should include recommendations on how a complete and functioning legal, technical and trust framework for IAS services could be constructed. This recommendation should build on consultations of selected experts through direct discussions and workshops, as well as the feedback received through the Commission's 2011 public consultation on electronic identification, authentication and signatures.

1.3 Role of this document in the Study

The present Study mainly consists of three tasks that correspond to a logical phase in the study. The phases and tasks can be graphically summarized as follows:

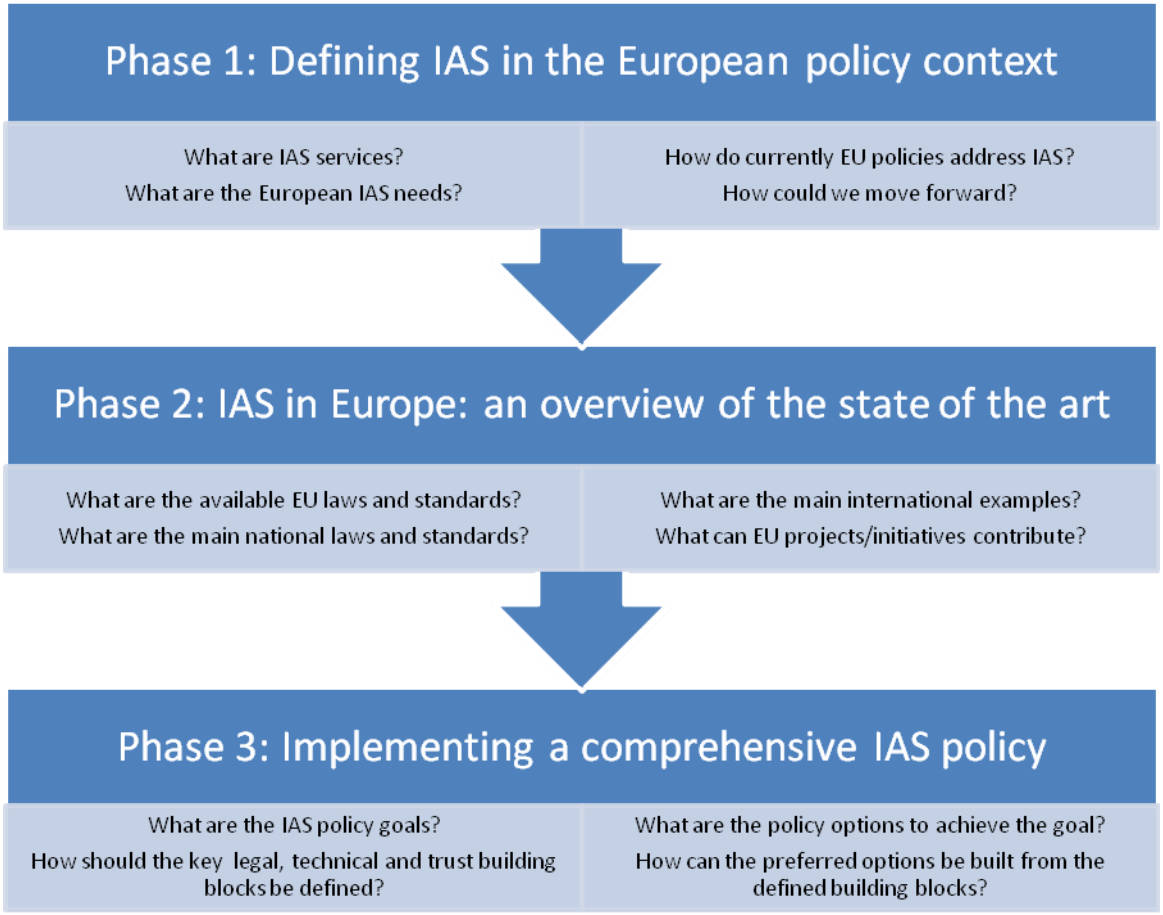


Figure 1: IAS study phases

The current document is Deliverable 3, v.2b - IAS in Europe: Proposal for a European IAS policy framework and corresponds to Phase 3 in the overview above. The goal of this report is to define specific building blocks for a comprehensive IAS approach, and to propose on how those building blocks should be combined into a complete and functioning legal, technical and trust framework.

The first aspect of this task (defining building blocks) involves the identification and definition of all elements that a comprehensive IAS approach would need to address, including notably:

- An unambiguous understanding of IAS services and ancillary services, including definitions of these services and an overview of how they relate to

each other (i.e. how electronic delivery services can depend on eID, eSignatures or time stamping).

- Input for the policy goals that an IAS approach should cover, including such aspects as the enabling of the internal market, technological neutrality and legal reliability.
- Input for the legal translation of these policy goals and requirements, such as draft recitals to be included in European legal texts, and draft proposals of legal provisions of a future regulatory framework.
- Input for the trust framework needed to support a comprehensive IAS approach, including any required supervisory/accreditation bodies at the European or national level, and including the potential role of private sector conformity assessment bodies.
- Input for the technical framework required to enable the comprehensive IAS approach, including an overview of standardisation needs and potential gaps.

In the second stage of this task (IAS policy proposal) the study team also provides its own proposal to the Commission on how those building blocks should be combined into an IAS 'house', based on its own analysis.

This document therefore contains recommendations of the study team on the future legal, technical and trust framework for IAS services. The various inputs of this document were drafted and developed in coordination with the European Commission, in the timeframe leading up to the publication of the Commission's Proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market[1]. For this reason, some of the inputs of this deliverable have been taken into account by the Commission, whereas others have been superseded by further policy developments since their production.

[1] See http://ec.europa.eu/information_society/policy/esignature/docs/regulation/com_2012_2038_en.pdf

2. Building blocks for a future IAS Policy framework

2.1 Building blocks for designing the future IAS Policy framework

The eSignature Directive 1999/93/EC has established a legal framework for the use of electronic signatures and certification services. Legal provisions were limited to an essential minimum in order to leave room for technical development potentialities.

While all Member States have implemented the general principles of the Directive, an analysis of the practical usage of eSignatures reveals a quite significant number of issues that today limit their interoperability and cross-border use.

They have resulted in very low level of high-volume market implementations, and current implementations of eSignatures are mainly experienced in a small number of eGovernment and isolated eBusiness sectors, mainly due to the fact that in such islands legal and technical uncertainties can be relatively easily reduced by imposing common rules.

The legal and administrative, as well as the technical and trust related barriers to the interoperability and cross-border use of eSignatures have been thoroughly synthesised in the September 2011 published "Digital Internal Market Study from the European Parliament[2]. It is not the purpose of the present document to restate all such barriers and their consequences; however the present section aims to list the various resulting actions that would be needed to overcome those barriers in terms of elements to be taken into account when designing the future IAS Policy framework.

2.1.1 From a legal point of view

From a legal perspective, the following needs have been identified and described:

---

[2] See "Digital Internal Market" paper from the European Parliament providing a good summary an overview of issues with regards to the internal market aspects and the interoperability and cross-border use of eSignatures as identified in CROBIES, EFVS, Study on Standardisation Aspects of eSignatures, and other relevant studies and papers. (Directorate General for Internal Policies, Policy Department Economic and Scientific Policy A: Digital Internal Market, IMCO, 2011, http://www.europarl.europa.eu/activities/committees/studies/download.do?language=en&file=41711#search=%20Digital%20Internal%20Market%20).

(1) Establish **common and specific requirements, obligations and liabilities for other eSignature ancillary services**[3] while reducing the level of interpretation of specific definitions or legal provisions for those very specific set of services.

(2) Reviewed set of **consistent definitions** (e.g. signatory being a natural or legal person, authentication versus eSignature, supervision versus voluntary accreditation, SSCD and related conformity assessment).

(3) Establish a **clear mapping between the legal provisions towards the (future) European standardisation documents** on eSignatures for all types of eSignatures components and related ancillary services.

(4) Analyse the **legal effect of compliance to standards** from a presumption of compliance with legal requirements up to a mandatory compliance.

(5) Reduce the legal uncertainty and pave the way towards a more conclusive trust framework for **AdES** and other ES which are not based on QC in order to increase their use in practice.

(6) Reduce the **legal uncertainties relating to the conformity assessments for SSCDs** and facilitate the identification of devices assessed as conform to the requirements (e.g. through harmonised publicly available lists of SSCD benefitting from a determination of conformity) and EU coverage of such assessments.

(7) Reducing the current diversity of national eSignature legal systems by reducing the current wide scope of discretion in implementing the current legal provisions related to eSignatures (e.g. using a Regulation instead of a Directive as legislative tool).

(8) Establish **common minimum requirements for supervision systems** of Trust Service Providers[4] supporting or built on electronic signatures (e.g. TSPs issuing certificates whether qualified or not, TSPs providing time-stamping services, TSPs providing Signature Generation Services, TSPs providing Signature Validation Services, TSPs providing Registered Delivery Services, TSPs providing eSignature long term preservation services) and ensuring more efficient mutual recognition and trustworthiness of such services. In particular the provision of freely available online certificate validity services without prior authentication or signed requests as well as

---

[3] Time-stamping services, (long term) preservation, signature validation services, signature generation services (also called signing servers).

[4] Trust Service Provider is used by preference against Certification Service Provider, see IAS Deliverable 1.1 for a full set of proposed definitions with regards to IAS concepts.

prompt notification of changes or compromises that could jeopardise the supervision/accreditation status of a TSP should be considered as requirements.

(9) Improve the mapping between legal provisions for reliable identification of signatory and to reliable identity management schemes through common minimum requirements ensuring interoperability, cross-border use and (personal) data privacy.

2.1.2 From a technical point of view

From a technical perspective, the following needs have been identified and described:

(1) Ensure the development of common, accepted and widely available true standards on eSignatures characterised by:

- as little as possible interpretation that may lead to divergent technical implementations jeopardising interoperability and cross-border use;
- as business oriented as possible rather than focusing on hypothetic and academic scenarios;
- the provision of sufficient guidelines and implementation support in particular for the creation and the validation of electronic signatures.

(2) The profiling of certificate fields and content should not allow divergent semantic interpretations of such fields and their content, in particular with regards to the signatory identity and the fact that it acts on its own behalf or on behalf of a legal or third entity, as well as to ensure specific minimum requirements with regards to their interoperability and validation.

(3) Complete the EU eSignature standardisation framework with regards to the provision by TSPs of other services than issuing certificates and in particular the Signature Creation Services and Signature Validation Services in a similar way to the considerable work done recently to standardise Registered Delivery Services of electronic document and messages.

(4) Eliminate barriers preventing specific sectors or domains of applications (e.g. eBanking) to make use of QES, in particular in connection with eID cards[5].

[5] These include the lack of cross-border PKI interoperability, the lack of control on the issuance of eID cards
deployed to the citizens by public authorities and other liability issues and the co-existence of European ES

2.1.3 From a trust point of view

From a trust perspective, the following needs have been identified and described:

(1) Leveraging on the existing Trusted Lists model as per CD 2009/767/EC amended by CD 2010/425/EU, for providing a common and harmonised way of providing trust related information on supervised trust services from TSPs while not being limited to issuance of QC. This will result from the establishment of common legal provisions and technical requirements on the provision of such services and the standardisation of those trust services types and related outputs (tokens).

2.1.4 From a practical and commercial point of view

From a practical and commercial perspective, the following needs have been identified and described:

Focusing on the existence of interoperability barriers on the cross-border level, there are still actions to be implemented in order to increase a wider and more practical use of eSignatures, and this of course in parallel to the legal, technical and trust oriented actions listed previously.

(1) Reduce or eliminate the possibility to not accept the presentation of electronic documents signed with eSignatures. Making such an acceptance obligatory could drastically increase the effective usage of eSignatures, in particular of QES (and potentially $AdES_{QC}$) in a cross-border context.

(2) Simplification to end-users and appropriate guidance for electronic signature implementation is required once legal, technical and trust frameworks will be made simpler and more consistent. In particular business driven guidance for use of electronic signatures should be made accessible to non-technical and business managers.

(3) Moreover, a **real consistency and mapping between** the legal, standardisation and trust **framework**. Together with a significant effort in **awareness, education and marketing activities for ES** as well as promotion regarding their cross-border use would be beneficial to the market, effective use of electronic signatures and lead to a safer digital society. In particular, users are also often not aware of the risks of unprotected electronic transactions and inadequate electronic evidence.

---

standards and the Banking sector's standards that all need to be followed, see Study on Standardisation Aspects of eSignature, 2007, Final Report, p. 57ff., 60.

(4) Increase **attractiveness of ES applications with clearly identifiable benefit** in particular for private users of ES. The existence of eGovernment ES applications alone will not sufficiently leverage the use of ES, as individuals generally do not have to consult public authorities very often. Thus additional attractive ES applications are necessary.

3. Recommendations for building an IAS Regulation

3.1 Recommendations for an IAS Regulation

The Tender Specifications required the contractor to elaborate building blocks for a legal framework on electronic identification-related credentials (e-identification, e-authentication, e-signature and ancillary credentials and services) with a view to removing interoperability barriers and facilitating the usage of these credentials.

More specifically, the contractor is expected to formulate proposals for policy options on electronic identification and authentication policy expanding appropriate existing provisions of the e-signature legal framework. The expansion of existing provisions may also include, where necessary, improving these provisions to create more legal certainty and to avoid cross-border interoperability barriers. For a number of IAS services, no provisions currently exist (e.g. with respect to time stamping), or existing provisions need to be clarified (e.g. with respect to the possibility for attributing electronic signatures directly to legal entities). In such cases, the contractor should formulate proposals for new (original) provisions.

The text in Annex: "Annex A - Recommendations for an IAS Regulation" contains a set of recommendations for building blocks and possible provisions for an IAS related legal framework. As noted in the introduction above, some of the inputs of this deliverable have been taken into account by the Commission, whereas others have been superseded by further policy developments since their production.

3.2 Ad-hoc support provided to the Commission

Throughout the duration of the project, the Study Team supported the European Commission in its drafting of a proposal for a Regulation on Trust Services.

The support essentially relates to the following topics:

- Validation of qualified electronic signatures,
- International aspects (Art.8),
- Article 14 - Supervision (13.1. and 15.5),
- Definitions in Regulation,
- Review of SME Panel questionnaire,

- Identification and authentication of organization and organization's websites,
- eSignature classification,
- Secure Signature Creation Device issues,
- Interpretation of article 20.1 of the proposed eIAS regulation.

4. Supervision issues

4.1 Introduction

4.1.1 Trust services as key enablers in boosting use of online environment

Building trust in the online environment is key to economic development. Lack of trust makes consumers, business and administrations hesitate to carry out transactions electronically and to adopt new services.

Enabling secure and seamless electronic interactions between businesses, citizens and public authorities, thereby increasing the effectiveness of public and private online services, e-business and e-commerce in the EU will only be possible through the adequate and efficient combination of sound legal, technical and trust frameworks for products and trust services supporting electronic identification, authentication and signatures.

Such products and trust services are not limited to the issuance and management of certificates, but also encompass any other ancillary services and products such as registration services, time-stamping services, directory services, electronic delivery services, computing services or consultancy services related to electronic signatures.

The proposal for a 'Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market'[6] adopted by the European Commission enhances Directive 1999/93/EC[7] and expands it to cover mutual recognition, acceptance at EU level and EU-cross border and cross-sector use of notified electronic identification and other essential related electronic **trust services**, focusing namely on "*any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signatures and for electronic seals*".[8]

Having confidence in those outputs of trust services, one needs to have confidence in the related trust services and that their providers have properly established and adequately implemented procedures as well as quality, security and protective measures in order to minimize the operational and financial threats and risk associated to provision of such

[6] COM(2012) 238 of 04.06.2012.

[7] OJ L 13, 19.1.2000, p. 12.

[8] For definitions of such outputs of trust service, refer to COM(2012) 238.

services and in order to meet the applicable legal requirements. It is only once having confidence in the soundness of the operational and technical implementation of such trust services, in their conformance to the legal requirements and in the fact that all this will lead to legal certainty that those trust services can be widely adopted to boost electronic transactions hence stimulating economic development.

To enhance people's trust in the internal market and to promote the use of trust services and products, the notions of qualified trust services and qualified trust service provider have been introduced in the Proposal for a Regulation on electronic identification and trust services for electronic transactions in the internal market (COM(2012) 238)[9], with a view to indicating requirements and obligations to ensure high-level security of whatever qualified trust services and products are used or provided. The Proposal provides the following definitions:

Article 3 Definitions

*(12) '**trust service**' means any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals;*

*(13) '**qualified trust service**' means a trust service that meets the applicable requirements provided for in this Regulation;*

*(14) '**trust service provider'** means a natural or a legal person who provides one or more trust services;*

*(15) '**qualified trust service provider**' means a trust service provider who meets the requirements laid down in this Regulation;*

Comment: the use of the wording "qualified trust service provider" may be interpreted in two ways when the adjective "qualified" applies to "trust service" or to "provider". It is expected that to be considered as a qualified trust service provider a trust service provider needs to provide one or more trust services that are either expressly foreseen by Regulation as qualified, or that a Member State has deemed to be qualified (like it has already happened with electronic delivery, time stamps and long term preservation, that have been regulated by single Member States as qualified services, and subsequently subsumed as qualified trust services in the Regulation. The

[9] See http://ec.europa.eu/information_society/policy/esignature/docs/regulation/com_2012_2038_en.pdf

Regulation shall not stifle innovation and the creation of new (and possibly more sophisticated) qualified trust services, that eventually will arise following the needs of a specific national legislation. *When* ***such a (national) qualified service does not arise mutual recognition issues, because it is used within one or more*** *isolated* ***single markets, there will be no need for intervention at EU level. But if (like it happens today with registered emails and time stamps) there will be lack of mutual recognition of services that are used in several member states, then the Commission, using the delegated powers and issuing implementing acts, shall intervene and dissolve the internal market barriers, transforming a national qualified trusted service into an EU qualified trusted service.***

Semantically this is not ensured by the above definition. It is suggested to update the definition as follows:

> ***(15) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services (according to the supervision scheme of at least one Member State) and meets the requirements laid down in this Regulation;***

It is not expected that a trust service provider can get a 'qualified' status and become a qualified trust service provider without providing any qualified trust service: there will be qualified trust services that are supervised only by one or more single member states (where issues of mutual recognition may arise), and qualified trust services that are expressly recognised by the Regulation or its delegated acts, where mutual recognition is mandatory for all member states. No identified set of requirements that could be considered for such purpose is defined in the proposal for Regulation COM(2012) 238 as all related requirements (in particular in Article 19) assume the provision of qualified trust services. However consideration (37) deals about "the qualified status of the service provider at the time of supervision", art. 16.4 states that a qualified trust service provider "shall lose its qualified status when it does not remedy to any failure to meet the Regulation requirements on them and on the qualified trust services they provide", and art.17.3. §2 states that "the supervisory body shall indicate the qualified status of the qualified service providers and the qualified trust services they provide in the trusted lists after the positive conclusion of the verification [...]". Currently Trusted Lists as they are defined in CD 2009/767/EC amended by CD 2010/425/EU give information only on the supervision/accreditation status of trust services including trust services issuing qualified certificates. No status is given to the trust service provider itself. Subsequently the supervisory body that wants to supervise a

new type of qualified trust service, shall provide a taxonomy of the service, to be included in the Trusted List as a national qualified trust service.

Any different solution, that privileges simple and straight classification of qualified trust services, to be provided "top down" by the Commission, will transform qualified trust services in a closed number, which will totally stifle innovation in the creation of new services in the EU: in practice it will mean, that in the future of the evolution of the qualified trust services, inputs for new services will come only from abroad the EU internal market. Today new qualified trust services have been created by national legislation (as it has happened at least in Germany, Austria and Italy, with registered emails, time stamps and long term preservation).

In the current proposal for Regulation COM(2012) 238:

- ***A trust service provider cannot be considered as a qualified trust service provider unless it provides a qualified trust service (according at least to one national supervisory body) and meet the requirements of the Regulation on both the provided qualified trust service and on itself, namely Art.19.2 requirements.***
- ***In the Trusted List, qualified status information will be given on a per qualified trust service basis and with regards to the trust service provider itself will either provide an explicit information on its qualified status or such information can be deterministically deduced from the status of its qualified trust services. A qualified trust service provider that fails to comply with requirements on Art.19.2 while providing one or more qualified trust services will lose the qualified status for itself and de facto for all its provided qualified trust services.***

Impacts on the current Trusted Lists format and procedures resulting from the proposal for Regulation COM(2012) 238 will be further discussed in the present document.

The proposed Regulation gives to such qualified trust services and their specific outputs a specific legal effect enhancing their legal certainty and admissibility over the EU, e.g.

- Art.20.2, a qualified electronic signature shall have the equivalent legal effect of a handwritten signature and, Art20.3, shall be recognised and accepted in all Member States;
- Art.28.2, a qualified electronic seal shall enjoy the legal presumption of ensuring the origin and integrity of the data to which it is linked and, Art28.3, shall be recognised and accepted in all Member States;

- Art.32.2, a qualified electronic time stamp shall enjoy the legal presumption of ensuring the time it indicates and the integrity of the data to which the time is bound, and, Art32.3, shall be recognised and accepted in all Member States;
- etc.

In general, it has to be clear, that a qualified trust service in order to be considered qualified, does not need to have any “legal effect” recognised: the added value of a qualified trust service is the creation of trust and confidence.

4.1.2 Supervision and Trusted Lists as essential building blocks

The concept of supervision of qualified trust services (e.g. issuing qualified certificates) is an essential building block of the current (Directive 1999/93/EC) and the future Regulation, or the future legal framework whatever shape it will take, as **it allows implementation** of a trust model of qualified trust services and of their outputs, e.g. those qualified electronic signatures benefiting of an automatic equivalence to hand written signatures.

As further confirmed in Consideration (37) of COM(2012) 238, "trusted lists are essential elements to build trust among market operators as they indicate the qualified status of the service provider at the time of supervision" and the qualified status of the qualified trust service they provide. While Consideration (37) of COM(2012) 238 continues by stating that "on the other hand they are not a prerequisite for achieving the qualified status and providing qualified trust services which results from respecting the requirements of this Regulation", relying on Trusted Lists is the only practical way for any relying party to ascertain the qualified status of a trust service and of its related output.

In the context of a qualified electronic signature, without any confirmation of the qualified status of the supporting qualified trust service (i.e. CA/QC certification service issuing qualified certificate for which the private key resides or not in a qualified signature creation device, SSCD in the current Directive), as being supervised by the MS Supervisory Body in charge of its supervision, the relying party can only rely on the claim from the trust service provider having issued the signatory's certificate. Without such confirmation, a relying party cannot make any decision on the fact that the received electronic signature is indeed supported by a qualified certificate and/or by a qualified (secure) signature creation device. Not having such confirmation does not imply that the received signature is not a QES or not an $AdES_{QC}$, as it may well be a QES or an $AdES_{QC,}$ but only that no informed decision can be made on the basis of available information, at least not without substantive and likely disproportionate efforts of the relying party. When a QES or an $AdES_{QC}$ is required (e.g. in the context of article 1.1 of CD 2009/767//EC amended by CD 2010/425/EU), in practice an electronic signature cannot be accepted unless such Trusted List based confirmation is

available. Having a confirmation of the qualified or non-qualified status of the supporting trust service (e.g. "supervisionrevoked" or "supervisionceased" status for a qualified trust service in the Trusted List) would be the only practical way to determine whether or not the electronic signature is a QES or an $AdES_{QC}$.

Issues with the current model

The concept of supervision of service providers issuing qualified certificates is an essential building block of the current Directive 1999/93/EC as it allows implementation of a trust model of those qualified electronic signatures benefiting of an automatic equivalence to hand written signatures.

However the implementation in practice of such a concept has led to several issues:

- the co-existence and differences between the interpretation of an 'appropriate system that allows for supervision' (as introduced by Art 3.3 of the Directive) and of 'voluntary accreditation' (as defined in Art.2.13 of the Directive) are not always, if ever, understood clearly, even by those who are in charge of such systems;
- the terms and definitions used are often overlapping or conflicting with the terminology used in the audit and assessment world;
- the divergence of implementation in practice of the concept of "appropriate [...] supervision" by Member States has led to significant differences in the effective implementation of the controls underlying such a supervision ranging from very basic controls up to formal certification. The recent Diginotar case has, if nothing else, shown that there is a clear need for sufficiently effective supervision, since security risks can have a very serious impact on the trustworthiness of CAs and on their economic utility.

Given the importance of supervision as a tool for establishing and maintaining trust in trust service providers, it is our strong belief that one must strengthen significantly the supervision model related to qualified trust service providers and to the qualified trust services they provide. This strengthening will aim to ensure the credibility and viability of the whole concept of qualified trust service provisioning aiming to enhance trust and confidence in electronic transactions and hence to ensure the security of the whole digital society. This strengthening requires defining a single supervision model common to all MS based on a more structured and specified system allowing effective, systematic, independent and documented supervision for obtaining evidence and evaluating such evidence objectively, in order to determine the extent to which the criteria a qualified trust service should meet are indeed fulfilled.

Such a **common supervision model** based on a common set of rules including common conformity criteria and common conformity assessment process rules, established on a

standardised basis (i.e. in the context of mandate M460[10]), specified per type of qualified trust service and based on a standardised control process (i.e. based on well-established audit practices), together with the inclusion of conformity statements of qualified trust services in national Trusted Lists will ensure a more efficient and safer market than it is today.

4.1.3 Objectives for a sound Supervision system and Trusted Lists

The minimal objectives and policy goals for setting up a sound supervision system based on a set of minimum requirements applicable to all MS Supervisory Bodies in charge of supervision of qualified trust service providers are the following:

- **Transparency**: As the rules and provisions EU supervision scheme for IAS trust services/products are to be made publicly available, this will make the EU supervision scheme and its related processes transparent.

- **Equality**: As the main goal is to prove/ensure that the EU Regulation is abided, the supervision scheme, including the (minimum) reference criteria and assessment process, have identical basis (are identical) to every (qualified) trust service provider, regardless the provider's goals and regardless the assessor.

- **Minimum level of security assurance**: This is achieved through the introduction of minimal criteria that need to be met.

- **Better preparation of qualified trust service providers**: By making public the supervision scheme, including the (minimum) reference criteria and assessment process, (qualified) trust service providers have the opportunity to better understand the content and purpose of the supervision, prepare themselves in advance to make wise decisions and investments when design its systems to meet the criteria and pass the supervision.

- **Trust establishment**: The supervision scheme is the basis to assure stakeholders and relying parties that supervised qualified trust service provider complies with it and that its supervised services are trustworthy.

- **Trust recognition**: The above goals and principles will facilitate international recognition of the EU MS supervision of qualified trust services and qualified trust service providers.

- **Qualified trust services supervision status information**: The actual status of supervision of a supervised qualified trust service from a qualified trust service provider shall be disclosed in the Trusted List of the Member State which is competent for such a supervision.

---

[10] See http://ec.europa.eu/information_society/policy/esignature/eu_legislation/standardisation/index_en.htm

4.2 Supervision in the proposal for Regulation

4.2.1 Supervisory body

In its Section 2 on "Supervision", Article 13 obliges Member States to establish supervisory bodies, based on Article 3(3) of Directive 1999/93/EC, clarifying and enlarging their remit with regard to both trust service providers and qualified trust service providers.

Article 13 Supervisory body

1. Member States shall designate an appropriate body established in their territory or, upon mutual agreement, in another Member State under the responsibility of the designating Member State. Supervisory bodies shall be given all supervisory and investigatory powers that are necessary for the exercise of their tasks.

2. The supervisory body shall be responsible for the performance of the following tasks:

(a) monitoring trust service providers established in the territory of the designating Member State to ensure that they fulfil the requirements laid down in Article 15;

(b) undertaking supervision of qualified trust service providers established in the territory of the designating Member State and of the qualified trust services they provide in order to ensure that they and the qualified trust services provided by them meet the applicable requirements laid down in this Regulation;

(c) ensuring that relevant information and data referred to in point (g) of Article 19(2), and recorded by qualified trust service providers are preserved and kept accessible after the activities of a qualified trust service provider have ceased, for an appropriate time with a view to guaranteeing continuity of the service.

3. Each supervisory body shall submit a yearly report on the last calendar year's supervisory activities to the Commission and Member States by the end of the first quarter of the following year. It shall include at least:

(a) information on its supervisory activities;

(b) a summary of breach notifications received from trust service providers in accordance with Article 15(2);

(c) statistics on the market and usage of qualified trust services, including information on qualified trust service providers themselves, the qualified trust services they provide, the products they use and the general description of their customers.

4. Member States shall notify to the Commission and other Member States the names and the addresses of their respective designated supervisory bodies.

5. The Commission shall be empowered to adopt delegated acts, in accordance with Article 38, concerning the definition of procedures applicable to the tasks referred to in paragraph 2.

6. The Commission may, by means of implementing acts, define the circumstances, formats and procedures for the report referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

4.2.2 Mutual assistance

Article 14 introduces an explicit mechanism of mutual assistance between supervisory bodies in Member States to facilitate the cross-border supervision of trust service providers. It introduces rules on joint operations and supervisory authorities' right to participate in such operations.

Article 14 - Mutual assistance

1. Supervisory bodies shall cooperate with a view to exchange good practice and provide each other, within the shortest possible time, with relevant information and mutual assistance so that activities can be carried out in a consistent manner. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the security audits as referred to in Articles 15, 16 and 17.

2. A supervisory body to which a request for assistance is addressed may not refuse to comply with it unless:

(a) it is not competent to deal with the request; or

(b) compliance with the request would be incompatible with this Regulation.

3. Where appropriate, supervisory bodies may carry out joint investigations in which staff from other Member States' supervisory bodies is involved.

The supervisory body of the Member State where the investigation is to take place, in compliance with its own national law, may devolve investigative tasks to the assisted supervisory body's staff. Such powers may be exercised only under the guidance and in the presence of staff from the host supervisory body. The assisted supervisory body's staff shall be subject to the host supervisory body's national law. The host supervisory body shall assume responsibility for the assisted supervisory body staff's actions.

4. The Commission may, by means of implementing acts, specify the formats and procedures for the mutual assistance provided for in this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

4.2.3 Security requirements applicable to trust service providers

Article 15 introduces an obligation for both qualified and non-qualified trust service providers to implement appropriate technical and organisational measures for the security of their activities. Furthermore, the competent supervisory bodies and other relevant authorities

must be informed of any security breaches. If appropriate, they will in turn inform other Member States' supervisory bodies and will, directly or via the trust service provider concerned, inform the public.

Article 15

Security requirements applicable to trust service providers

1. Trust service providers who are established in the territory of the Union shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to state of the art, these measures shall ensure that the level of security is appropriate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of adverse effects of any incidents.

Without prejudice to Article 16(1), any trust service provider may submit the report of a security audit carried out by a recognised independent body to the supervisory body to confirm that appropriate security measures have been taken.

2. Trust service providers shall, without undue delay and where feasible not later than 24 hours after having become aware of it, notify the competent supervisory body, the competent national body for information security and other relevant third parties such as data protection authorities of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.

Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the supervisory body concerned shall inform supervisory bodies in other Member States and the European Network and Information Security Agency (ENISA).

The supervisory body concerned may also inform the public or require the trust service provider to do so, where it determines that disclosure of the breach is in the public interest.

3. The supervisory body shall provide to ENISA and to the Commission once a year with a summary of breach notifications received from trust service providers.

4. In order to implement paragraphs 1 and 2, the competent supervisory body shall have the power to issue binding instructions to trust service providers.

5. The Commission shall be empowered to adopt delegated acts, in accordance with Article 38, concerning the further specification of the measures referred to in paragraph 1.

6. The Commission may, by means of implementing acts, define the circumstances, formats and procedures, including deadlines, applicable for the purpose of paragraphs 1 to 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

4.2.4 Supervision of qualified trust service providers

Article 16 sets out the conditions for the supervision of qualified trust service providers and qualified trust services provided by them. It obliges qualified trust service providers to be audited on a yearly basis by a recognised independent body to confirm to the supervisory body that they fulfil the obligations laid down in the Regulation. Moreover, Article 16(2) gives the supervisory body the right to carry out on-the-spot audits of the qualified trust service providers at any time. The supervisory body is also empowered to issue binding instructions to qualified trust service providers to remedy, in a proportionate manner, any failure to meet an obligation revealed by a security audit.

Article 16

Supervision of qualified trust service providers

1. Qualified trust service providers shall be audited by a recognised independent body once a year to confirm that they and the qualified trust services provided by them fulfil the requirements set out in this Regulation, and shall submit the resulting security audit report to the supervisory body.

2. Without prejudice to paragraph 1, the supervisory body may at any time audit the qualified trust service providers to confirm that they and the qualified trust services provided by them still meet the conditions set out in this Regulation, either on its own initiative or in response to a request from the Commission. The supervisory body shall inform the data protection authorities of the results of its audits, in case personal data protection rules appear to have been breached.

3. The supervisory body shall have the power to issue binding instructions to qualified trust service providers to remedy any failure to fulfil the requirements indicated in the security audit report.

4. With reference to paragraph 3, if the qualified trust service provider does not remedy any such failure within a time limit set by the supervisory body, it shall lose its qualified status and be informed by the supervisory body that its status will be changed accordingly in the trusted lists referred to in Article 18.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the specification of the conditions under which the independent body carrying out the audit referred to in paragraph 1 of this Article and in Article 15(1) and in Article 17(1) shall be recognised.

6. The Commission may, by means of implementing acts, define the circumstances, procedures and formats applicable for the purpose of paragraphs 1, 2 and 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

4.2.5 Initiation of a qualified trust service

Article 17 concerns the activity carried out by the supervisory body at the request of a trust service provider wishing to initiate a qualified trust service.

Article 17

Initiation of a qualified trust service

1. Qualified trust service providers shall notify the supervisory body of their intention to start providing a qualified trust service and shall submit to the supervisory body a security audit report carried out by a recognised independent body, as provided for in Article 16(1).

Qualified trust service providers may start to provide the qualified trust service after they have submitted the notification and security audit report to the supervisory body.

2. Once the relevant documents are submitted to the supervisory body according to paragraph 1, the qualified service providers shall be included in the trusted lists referred to in Article 18 indicating that the notification has been submitted.

3. The supervisory body shall verify the compliance of the qualified trust service provider and of the qualified trust services provided by it with the requirements of the Regulation.

The supervisory body shall indicate the qualified status of the qualified service providers and the qualified trust services they provide in the trusted lists after the positive conclusion of the verification, not later than one month after the notification has been done in accordance with paragraph 1.

If the verification is not concluded within one month, the supervisory body shall inform the qualified trust service provider specifying the reasons of the delay and the period by which the verification shall be concluded.

4. A qualified trust service which has been subject to the notification referred to in paragraph 1 cannot be refused for the fulfilment of an administrative procedure or formality by the concerned public sector body for not being included in the lists referred to in paragraph 3.

5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures for the purpose of paragraphs 1, 2 and.3 Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

4.2.6 Trusted Lists

Article 18 provides for the establishment of trusted lists containing information on qualified trust service providers who are subject to supervision and to the qualified services they

offer. This information must be made publicly available through a common template in order to facilitate its automated use and ensure an appropriate level of detail.

Article 18

Trusted lists

1. Each Member State shall establish, maintain and publish trusted lists with information related to the qualified trust service providers for which it is competent together with information related to the qualified trust services provided by them.

2. Member States shall establish, maintain and publish, in a secure manner, electronically signed or sealed trusted lists provided for in paragraph 1 in a form suitable for automated processing.

3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificate used to sign or seal the trusted lists and any changes thereto.

4. The Commission shall make available to the public, through a secure channel, the information, referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 38 concerning the definition of the information referred to in paragraph 1.

6. The Commission may, by means of implementing acts, define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).

4.2.7 Requirements for qualified trust service providers

Article 19 sets out the requirements the qualified trust service providers must meet in order to be recognised as such. It draws from Annex II of Directive 1999/93/EC.

Article 19

Requirements for qualified trust service providers

1. When issuing a qualified certificate, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom a qualified certificate is issued.

Such information shall be verified by the qualified service provider or by an authorised third party acting under the responsibility of the qualified service provider:

(a) by a physical appearance of the natural person or of an authorised representative of the legal person, or

(b) remotely, using electronic identification means under a notified scheme issued in compliance with point (a).

2. Qualified trust service providers providing qualified trust services shall:

(a) employ staff who possess the necessary expertise, experience, and qualifications and apply administrative and management procedures which correspond to European or international standards and have received appropriate training regarding security and personal data protection rules;

(b) bear the risk of liability for damages by maintaining sufficient financial resources or by an appropriate liability insurance scheme;

(c) before entering into a contractual relationship, inform any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service;

(d) use trustworthy systems and products which are protected against modification and guarantee the technical security and reliability of the process supported by them;

(e) use trustworthy systems to store data provided to them, in a verifiable form so that:

– they are publicly available for retrieval only where the consent of the person to whom the data has been issued has been obtained,

– only authorised persons can make entries and changes,

– information can be checked for authenticity;

(f) take measures against forgery and theft of data;

(g) record for an appropriate period of time all relevant information concerning data issued and received by the qualified trust service provider, in particular for the purpose of providing evidence in legal proceedings. Such recording may be done electronically;

(h) have an up-to-date termination plan to ensure continuity of service in accordance with arrangements issued by the supervisory body under point (c) of Article 13(2);

(i) ensure lawful processing of personal data in accordance with Article 11.

3. Qualified trust service providers issuing qualified certificates shall register in their certificate database the revocation of the certificate within ten minutes after such revocation has taken effect.

4. With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at any time at least on a certificate basis in an automated manner which is reliable, free of charge and efficient.

5. The Commission may, by means of implementing acts, establish reference numbers of standards for trustworthy systems and products. Compliance with the requirements laid down in Article 19 shall be presumed where trustworthy systems

and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the Official Journal of the European Union.

4.3 A model for supervision of qualified trust service providers and qualified trust services they provide

4.3.1 Introduction

The monitoring and supervision as model proposed in COM (2012) 238 aims to inspire trust. Taking a helicopter perspective, we see at least the following alternative approaches to inspire such trust, which are:

- The “ISO Conformity Assessment” approach;
- The ISAE 3000 approach;
- The ISAE 3402 approach;
- The AICPA approach;
- The ISRS 4400 approach on “Agreed upon procedures”.

4.3.2 The “ISO Conformity Assessment” approach

Within ISO, the conformity assessment policy development committee ISO/CASCO is both responsible for developing and making recommendations on conformity assessment policy to the ISO/CASCO membership and for developing conformity assessment standards and guides. Particularly relevant ISO standards include:

- ISO 17021 “Conformity assessment: Requirements for bodies providing audit and certification of management systems” (where the ISO 17000 series replaces EN 45000)
- ISO 27006 Requirements for bodies providing audit and certification of information security management systems.

It should be noted there was historically quite some confusion with regards to the related terminology.

- The term “Accreditation”
  - is used in conformity assessment regulations / standards to refer to checking capability of “Conformity Assessment Body”
  - is used in Directive 1999/93 as a form of conformity assessment
  - is not used in COM(2012) 238
- The term “Certification”
  - is used in conformity assessment to mean certification of conformity.
  - is used in Directive 1999/93 to relate to Certification Service Providers
  - is used in COM(2012) 238 with regards to the certification of Qualified Electronic Signature/Seal Devices to determine their conformity with applicable security requirements.

We will align our terminology on ISO/IEC 17000 which defines conformity assessment as: “demonstration that specified requirements relating to a product, process, system, person, or body are fulfilled”.

Certification of an entity (e.g. of a trust service provider) against a specific set of requirements or standard (e.g. ISO 27001) is performed by a certification body accredited for performing conformity assessments against such a specific set of requirements or standard (e.g. such as ISO 27001) by an Accreditation Body. Such an accreditation means that the accredited certification body has the authority, expertise and knowhow to go into organisations and assess them against the target requirements (e.g. of ISO27001). Only certification bodies can be accredited for a standard. It is a common misconception that organisations think that they can become e.g. ISO 27001 accredited. Accredited certification bodies undergo periodic assessments by their accreditation bodies, usually their National Accreditation Body.

Within Europe, the European cooperation for Accreditation (EA)[11] is the main institution that oversees the interactions and interoperability between the different European players,

[11] EA members:

AUSTRIA – **BMWFJ,** BELGIUM – **BELAC,** BULGARIA – **BAS,** CROATIA – HAA, CYPRUS – **CYS-CYSAB,** CZECH REPUBLIC - **CAI,** DENMARK – **DANAK,** ESTONIA – **EAK,** FINLAND – **FINAS,** FRANCE – **COFRAC**FYROM – **IARM,** GERMANY – **DakkS,** GREECE - **ESYD** HUNGARY - **NAT,** IRELAND - **INAB,** ITALY - **ACCREDIA,** LATVIA - **LATAK,** LITHUANIA - LA, LUXEMBURG – **OLAS,** MALTA – **NAB-MALTA,** NETHERLANDS - **RvA,** NORWAY - NA, POLAND - **PCA,** PORTUGAL – **IPAC,** ROMANIA – **RENAR,** SERBIA – **ATS,** SLOVAKIA – **SNAS,** SLOVENIA – SA, SPAIN – **ENAC,** SWEDEN – **SWEDAC,** SWITZERLAND – **SAS,** TURKEY – **TURKAK,** UNITED KINGDOM - **UKAS.**

mainly the national accreditation bodies. This network is well established, in particular in the area of ISO 27001.

The application of the ISO/CASCO model through EA onto the TSP universe can be depicted as the following generic model:

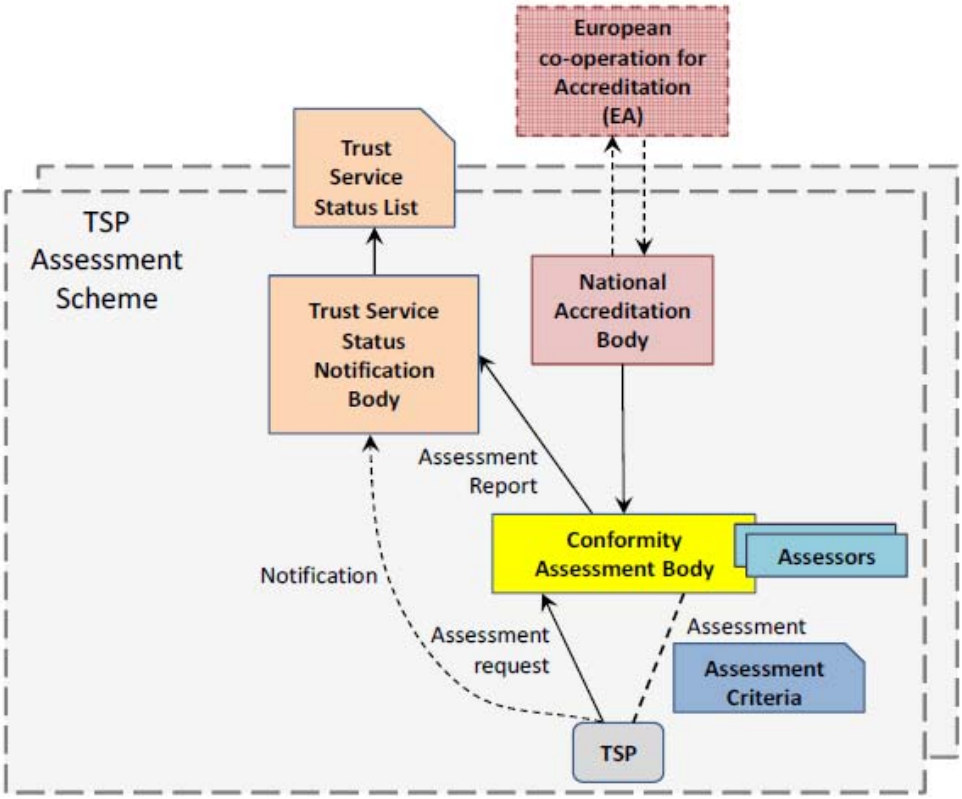


Figure 2

We consider this model as particularly relevant and the preferred approach to support the conformity assessment model underlying our proposed EU Supervision Scheme for qualified trust service providers and the qualified trust services they provide building up on the ETSI TS 119 403 generic model as well aligned to such ISO/CASCO model.

With regards to the conformity assessments determining that "appropriate Art.15.1 security measures" have been implemented by trust service providers with regards to the trust services they provide, the exact same model can apply.

4.3.3 The ISAE 3000 approach

The International Federation of Accountants (IFAC) operates a standards board, the International Auditing and Assurance Standards Board (IAASB). This IAASB issued the "International Standard on Assurance Engagements (ISAE) No. 3000, Assurance Reports on Controls at a Service Organization" originally in June 2000. The current version is "ISAE 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information - Proposed International Standard on Assurance Engagements (ISAE)", which is a 2011 exposure draft which will be finalised after all comments have been received and processed.

ISAE 3000's core part focuses on the requirements that allow a practitioner (i.e. an auditor) to express a degree of assurance over a subject matter. These requirements are structured as follows:

- Conduct of an Assurance Engagement in Accordance with ISAEs
- Ethical Requirements
- Acceptance and Continuance
- Quality Control
- Professional Skepticism and Professional Judgment
- Planning and Performing the Engagement
- Obtaining Evidence
- Considering Subsequent Events
- Other Information
- Description of Applicable Criteria
- Forming the Assurance Conclusion
- Preparing the Assurance Report
- Unmodified and Modified Conclusions
- Other Communication Responsibilities
- Documentation

Much attention is devoted to selecting the appropriate criteria to audit the subject matter (the topic of the audit), and to obtaining and evaluating evidence. ISAE 3000 offers the state-of-the-art framework in auditing, based on worldwide consensus.

For this reason we consider it relevant for our proposal.

4.3.4 The AICPA approach

Historically, the AICPA's "Statement on Auditing Standards No. 70: Service Organizations", commonly abbreviated as SAS 70 was a popular auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) with its content codified as AU 324. SAS 70 provided guidance to service auditors when assessing the internal control of a service organization and issuing a service auditor's report. SAS 70 also provides guidance to auditors of financial statements of an entity that uses one or more service organizations. Service organizations (also referred to as service providers) are typically entities that provide outsourcing services that impact the control environment of their customers. Examples of service organizations are insurance and medical claims processors, trust companies, hosted data centers, application service providers (ASPs), managed security providers, credit processing organizations and clearinghouses.

SAS 70 distinguished two types of service auditor reports:

- A Type I ("A report on controls placed in operation") service auditor's report includes the service auditor's opinion on the fairness of the presentation of the service organization's description of controls that had been placed in operation and the suitability of the design of the controls to achieve the specified control objectives.
- A Type II ("A report on controls placed in operation and tests of operating effectiveness") service auditor's report includes the information contained in a Type I service auditor's report and also includes the service auditor's opinion on whether the specific controls were operating effectively during the period under review.

The AICPA moved the guidance for Service Auditors to the "Statements on Standards for Attestation Engagements" (SSAE), naming the standard Reporting on Controls at a Service Organization. The "Statements on Standards for Attestation Engagements No. 16" (SSAE 16) was formally issued in June 2010 and became effective on 15 June 2011, taking over from SAS 70.

SAS 70 was replaced by two standards:

- ISAE 3402: International Standard on Assurance Engagements No. 3402, Assurance Reports on Controls at a Service Organization. ISAE 3402 is the international standard adopted by the International Auditing and Assurance Standards Board (IAASB).

- SSAE 16: Statement on Standards for Attestation Engagements No. 16 , Reporting on Controls at a Service Organization. SSAE 16 is the "local" standard adopted by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA).

To help CPAs (Certified Public Accountants) selecting the appropriate standard for a particular engagement, the AICPA has introduced the SOC (SERVICE ORGANIZATION CONTROL) reporting concept, and identified 3 different engagements (SOC 1, SOC 2 and SOC 3). Service Organization Control (SOC) reports are internal control reports on the services provided by a service organization providing information that users need to assess and address the risks associated with an outsourced service.

The "SOC" dimension distinguishes between reports on controls at a service provider that are:

- SOC 1 relevant to user entities' internal control over financial reporting
- SOC 2 relevant to non-financial controls
- SOC 3 focussed on security, availability, processing integrity, confidentiality, or privacy.

SOC 3 is based on the AICPA/CICA (Canadian Institute of Chartered Accountants) "Trust Services Principles" and Webtrust/Systrust.

Furthermore SSAE 16 carried over the distinction between Type I and Type II from the SAS 70 definitions. If a Service Organisation performs outsourced services that affect the financial statements of another Company (the ‘User Organization’), it is commonly requested to provide an SSAE16 Type II Report, especially if the User Organization is publicly traded.

So with regard to the AICPA/SAS70/SSAE 16 approach, the most relevant contribution could come from the SSAE 16 SOC 3 components. However, as they are rather geared towards the existing WebTrust/Systrust schemes, there would be significant efforts required to either adapt existing audit and control objectives or create those in such a way they would reflect the requirements of COM (2012) 238

For this reason we consider it less relevant for our proposal.

4.3.5 The ISAE 3402 approach

The International Federation of Accountants (IFAC) operates a standards board, the International Auditing and Assurance Standards Board (IAASB). This IAASB issued in

December 2009 the “International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization”.

ISAE 3402 was developed to provide an international assurance standard to allow public accountants to issue a report for use by user organizations and their auditors on the controls at a service provider that are likely to impact or be a part of the user organization’s system of internal control over financial reporting. As opposed to the AICPA’s broader SSAE 16, its focus is on financial reporting. It lacks the SSAE 16’s concepts of SOC 1, 2 and 3, which are the AICPA’s extensions to accommodate technological aspects.

For this reason we consider it less relevant for our proposal.

4.3.6 The IFAC/IAASB/ISRS 4400 approach on “Agreed upon procedures”

Finally, an approach can be based upon procedures agreed between the service provider and the auditor. Such an approach allows fine-tuning of scope and audit objectives to the largest extent possible. It is typically used to provide comfort to the service provider internally. It is less suitable to provide assurance towards external parties.

For this reason we consider it less relevant for our proposal.

4.3.7 Our proposal for a European Supervision Scheme for qualified trust service providers and qualified trust services they provide

From the way the COM(2012) 238 proposal for Regulation is proposing to organise those delegated acts and implementing acts, it is possible to establish a common European Scheme for supervision of qualified trust service providers and the qualified trust services they provide.

The present section proposes a concrete model for such a common "European Scheme for supervision of qualified trust service providers and the qualified trust services they provide", in accordance with the relevant articles from COM(2012) 238 [12]. The same model may be

[12] Those relevant articles are the following:

- COM(2012) 238, Art. 13.5 referring to delegated acts concerning the definition of procedures applicable to the supervisory tasks referred to in Art.15.2;
- COM(2012) 238, Art. 13.6 referring to implementing acts concerning the definition of the circumstances, formats and procedures for the report on the last calendar year's supervisory activities of each supervisory body, as referred to in Art.15.3;
- COM(2012) 238, Art. 14.4 referring to implementing acts concerning the specification of the formats and procedures for the mutual assistance provide in Art.14;

used to cover monitoring of trust service providers and in particular the verification of the compliance of trust service providers with Art.15 requirements from COM(2012) 238.

The proposed model builds upon work done in ETSI ESI with regards to general requirements and guidance for conformity assessment of trust service providers (ETSI TS 119 403), national supervision schemes, the COM(2012) 238 proposal for Regulation and the preferred ISO/CASCO approach described in Section 4.3.2. The proposed complete scheme may be integrated as such in an appropriate delegated or implementing act, or be included in the ETSI standardisation framework as an instantiation of ETSI TS 119 403[13].

It is believed that the establishment of such a common basis for supervision of qualified trust service providers and the qualified trust services they provide will not only serve to raise the level of confidence in these providers and services within the EU boundaries but will also serve as a benchmarking reference for the mutual recognition between EU services and those "qualified" trust services from 3rd countries or international organisations. Recognition of "qualified" trust services and trust service providers from 3rd country or international organisations that would be certified against the EU common supervision scheme or against an equivalent scheme by a conformity assessment body accredited by a national

---

- COM(2012) 238, Art. 15.5 referring to delegated acts concerning the further specification of the appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide as referred to in Art.15.1;
- COM(2012) 238, Art. 15.6 referring to implementing acts concerning the definition of the circumstances, formats and procedures, including deadlines, applicable for the purpose of Art.15.1 to 3;
- COM(2012) 238, Art. 16.5 referring to delegated acts concerning the specification of the conditions under which the independent body carrying out the audit referred to in Art.15.1 and in Art.16.1, and in Art.17.1 shall be recognised;
- COM(2012) 238, Art. 16.6 referring to implementing acts concerning the definition of the circumstances, formats and procedures applicable for the purpose of Art.15.1, Art.15.2 and Art.15.4;
- COM(2012) 238, Art. 17.5 referring to implementing acts concerning the definition of the circumstances, formats and procedures applicable for the purpose of Art.15.1 to 3;
- COM(2012) 238, Art. 18.5 referring to delegated acts concerning the definition of the information referred to in Art.18.1;
- COM(2012) 238, Art. 18.6 referring to implementing acts concerning the definition of the technical specifications and formats for trusted lists applicable for the purpose of Art.18.1 to 4;
- COM(2012) 238, Art. 19.5 referred implementing acts concerning the establishment of reference numbers of standards for trustworthy systems and products enabling presumption of compliance with requirements laid down in Art.19 where trustworthy systems and products meet those standards.

[13] ETSI TS 119 403 provides a general framework for the establishment of trust service provider assessment scheme whatever type of trust service and trust service provider, qualified or not, and not limited to the one covered by COM(2012) 238 proposal for Regulation. The proposed "European scheme for the supervision of qualified trust service providers and the qualified trust services they provide" is (as) compliant (as possible) with ETSI TS 119 403.

accreditation body participating to the European cooperation for Accreditation (and/or the International Accreditation Forum (IAF)[14]) to carry out such assessments would be facilitated.

Figure 3 illustrates the model for the European Supervision Scheme for the conformity assessment of qualified trust service providers and the qualified trust service they provide against the provisions and requirements laid down in the Regulation [ref.1].

Figure 4 illustrates the same model for the European Supervision Scheme applied for the confirmation of compliance through conformity assessment of trust service providers and the trust service they provide against the provisions and requirements laid down in the Regulation [ref.1 - in particular Art.15.1].

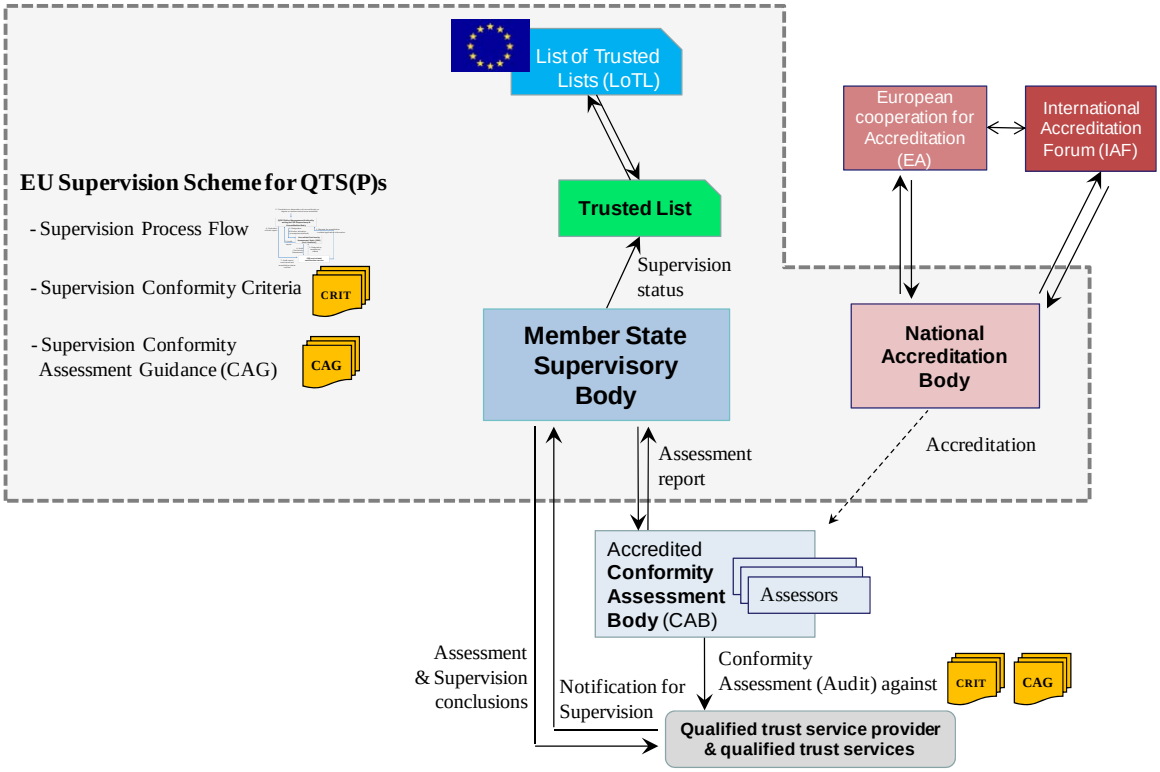


Figure 3: Model for European Supervision Scheme and related assessments - QTS(P)s

[14] The IAF is the world association of National (Conformance Assessment) Accreditation Bodies and other bodies interested in conformance assessment in the fields of management systems, products, services, personnel and other similar programs of conformance assessment.

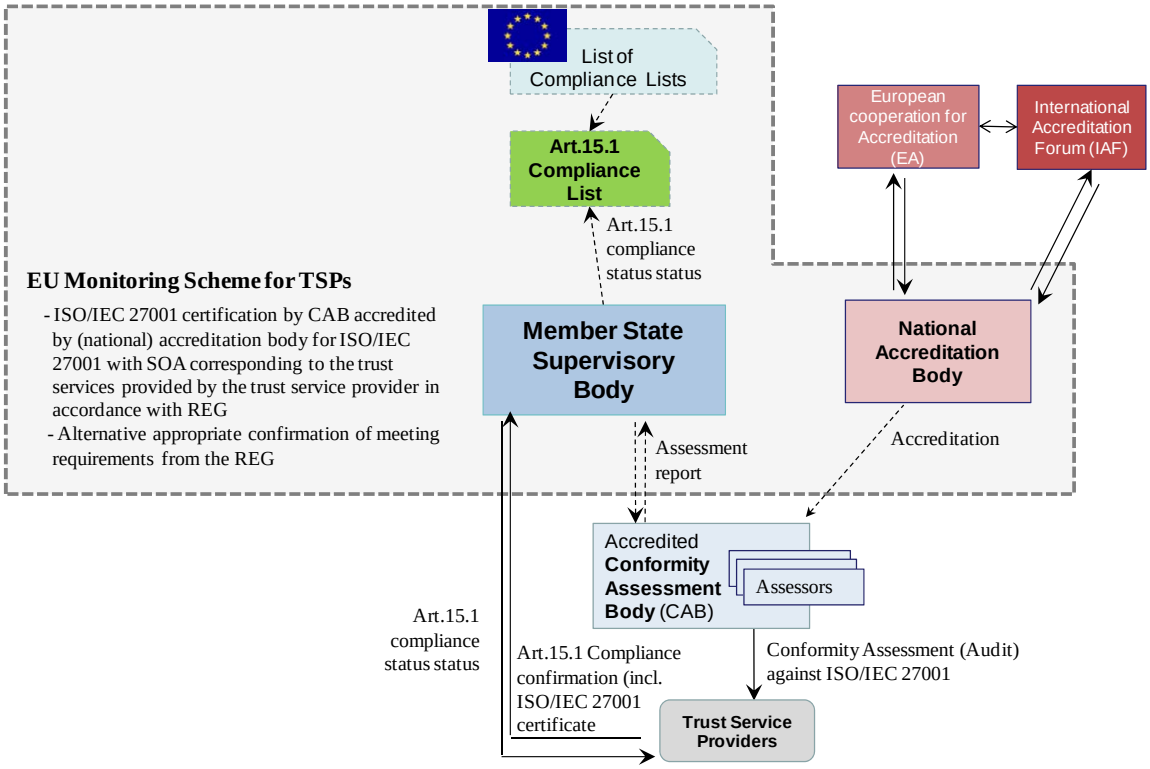


Figure 4: Model for European Supervision Scheme and related assessments - TSPs

Within the above described context and within each EU Member State, the European Supervision Scheme rely on the following elements:

- The **National Accreditation Body** (NAB): This is the sole body in a Member State that shall perform, with authority derived from the State, accreditation of conformity assessment bodies in the context of the Supervision Scheme. Such accreditation shall assess the competency of the accredited conformity assessment bodies to carry out assessments under the requirements identified in the Supervision Scheme.[15]

- **Conformity Assessment Bodies** (CAB): A conformity assessment body is an independent body of assessors which carries out the assessment of a qualified trust service provider and of the qualified trust services it provides against the requirements established in the Supervision Scheme, in particular against its conformity criteria and in accordance with its conformity assessment guidance. The competence of Conformity Assessment Body to carry out such an assessment is accredited by a National Accreditation Body. One or more Conformity Assessment Bodies may be accredited and hence recognised under the Supervision Scheme. The results of a conformity assessment executed by a conformity assessment body is notified to the Supervisory Body of the Member State in which the assessed qualified trust service provider is established. Conformity assessment bodies refer to

[15] The option has been made here to not allow, in the context of the present Supervision Scheme, Supervisory Bodies to play the equivalent role of the national accreditation body for evaluating the competence of a conformity assessment body to carry out a conformity assessment in line with the present European Supervision Scheme.

recognised independent bodies as referred to in Art.15.1, Art.16.1 and Art.17.1 of the Regulation [ref.1].

- The **Supervisory Body**: This is the body established in accordance with Art.13.1 of the Regulation and that are given all supervisory and investigatory powers that are necessary for the exercise of their task in accordance with the Regulation [ref.1]. With regards to qualified trust services and qualified trust service providers, the supervisory body shall be responsible for undertaking supervision of those qualified trust service providers established in their territory, and/or in the MS having designated this body to undertake supervision of qualified trust service providers established in the designating MS under the responsibility of the designating MS, and of the qualified trust services those qualified trust service providers provide. This supervision shall ensure that those qualified trust service providers and the qualified trust services they provide meet the applicable requirements laid down in the Regulation. All supervisory bodies from the EU shall abide by the Supervision Scheme for this purpose.

- **Trusted Lists**: The supervisory body shall also be the body responsible for the notification of the qualified status of the qualified trust service providers and the qualified trust services they provide in their national Trusted List in accordance with the Regulation [ref.1 - Art.18] and the present document. Qualified status result from the verification by the supervisory body of the compliance of the qualified trust service providers and the qualified trust services they provide with the requirements of the Regulation, such a verification being based on, e.g., the results of a conformity assessment performed by an accredited conformity assessment body.

  Similarly to the Trusted Lists, so-called "**Art.15.1 Compliance Lists**" could be used for the notification of the compliance status of the trust service providers with the Regulation [ref.1 - Art.15].

- The **List of the Trusted Lists** (LOTL) is an additional important element in the Supervision Scheme. In order to allow access to the trusted lists of all Member States in an easy manner, the European Commission publishes a central compiled list that includes the locations where the Trusted Lists are published and the certificate to be used to verify the authenticity and integrity of the MS trusted lists, as notified by Member States. This compiled List of the Trusted Lists (LOTL) is available publicly. The authenticity and integrity of the machine processable version of this compiled list is ensured through an electronic signature supported by a digital certificate. The certificate can be authenticated through one of the digests published on the Official Journal of the European Union.

  Similarly to the LOTL, a compiled **List of the Member States Art.15.1 Compliance Lists** could be published by the EC to allow access to the lists of all Member States in an easy manner and to enforce the trust model underlying the verification of the authenticity and integrity of the MS lists.

The Supervision Scheme assessment model relies on a common set of conformity criteria, a common assessment process based on a common conformity assessment guidance and on a common understanding of the responsibilities of the qualified trust service providers.

The **Conformity Criteria** (CRIT) for qualified trust service providers and the qualified trust services they provide refers to the criteria (incl. requirements) against which conformity assessment will be undertaken by EU MS supervisory bodies in the context of the Regulation. Those criteria take into account specificities of the type of trust service to be

assessed. They can be organised under the form of a check-list aiming to facilitate the tasks of both the assessors and the qualified trust service provider to be assessed. They are made publicly available and based on standards. The conformity criteria applicable in the context of the Supervision Scheme are provided in a companion document of the present document.

The **Conformity Assessment Guidance** (CAG) for European Union Member States supervisory bodies refers to the way conformity assessment bodies carry out an assessment in the context of the Supervision Scheme , i.e. to the way compliance of qualified trust service providers and the qualified trust services they provide is assessed against the requirements laid down in the Regulation [ref.1]. This covers:

- The conformity assessment process and the specific characteristics with regards to the conformity assessment process, including the frequency and depth of the assessments, the associated fees, the complaint related procedures, etc;
- The requirements on the conformity assessment bodies and the rules to be observed by such bodies when conducting assessments;
- The specifications for cross-border assessment and related mutual assistance; and
- The responsibilities of the parties.

The document entitled "Recommendations for a European Supervision Scheme: –Proposal for Conformity Assessment Guidance" (See Annex) focuses on the description of (i) the process flow for the supervision of qualified trust service providers and the qualified trust services they provide and (ii) on the Conformity Assessment Guidance (CAG) specifying how to assess compliance of those providers and their qualified trust services against the "Supervision Conformity Assessment Criteria". These latter "Supervision Criteria", against which the conformity of the qualified trust service providers and the qualified trust services they provide will be assessed, are suggested to be developed on the basis of the mapping between the proposal for Regulation COM(2012) 238 related delegated and implementing acts and the technical requirements and/or standards as provided in Section 6.

4.4 Conclusions

The current proposal for a 'Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market'[16] paves the way to the establishment of a single supervision scheme common to all EU MS supervisory bodies. We recommend delegated acts and implementing acts to be adopted in

[16] COM(2012) 238 of 04.06.2012.

the context of the supervision related articles of the future Regulation to effectively set up such a common basis for supervision of qualified trust service providers and the qualified trust services they provide.

Section 4.3 and "Annex C - Recommendations for a European Supervision Scheme: Proposal for Conformity Assessment Guidance" of the present document propose a concrete basis for such a common supervision scheme.

It is believed that the establishment of such a common basis for supervision of qualified trust service providers and the qualified trust services they provide will not only serve to raise the level of confidence in these providers and services within the EU boundaries but will also serve as a benchmarking reference for the mutual recognition between EU services and those "qualified" trust services from 3rd countries or international organisations. Recognition of "Qualified" trust services and trust service providers from 3rd country or international organisations that would be certified against the EU common supervision scheme or against an equivalent scheme by a conformity assessment body accredited by an accreditation body participating to IAF to carry out such assessments would be facilitated.

The proposed initiation phase in the current proposal for a Regulation creates some legal uncertainties, un-equality between relying parties and un-necessary complexity and should be simplified in a clear prior-authorisation model.

It is further recommended that Secondary EU wide legislation (e.g. delegated acts as per Art.13.5) should establish and maintain (incl. addition mechanism) an exhaustive list of EU wide, meaningful and precise categories of activities to be considered as trust services. Not having such a mechanism will not allow clear determination whether a service provider is to be considered as a trust service provider or not and may lead to discrimination between trust service providers.

5. IAS in the Cloud

5.1 IAS in the Cloud, opportunities and challenges.

Electronic Identification, Authentication and Signatures (IAS) is the expression that refers to the new legal framework proposed by the European Commission as successor to the eSignature directive (1999/93/EC). The "Digital Agenda for Europe" includes Key Action 3 to propose a revision of the eSignature Directive in 2011 with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems.

While the original Directive established a legal framework for electronic signatures and Certification Service Providers, the new version aims both at improving the signature aspects and at broadening the scope of the framework to include aspects of identification and authentication as well.

On the other hand we witness the arrival of Cloud computing, which is and will likely remain an evolving paradigm, going forward and gaining footprint. It can be informally defined as

"A 'Cloud' implementation is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service)."[17]

Its attractiveness stems from its characteristics to allow a consumer to unilaterally provision computing capabilities ("on demand self-service"), whilst allowing location independent resource pooling. This leads to rapid elasticity of services to align demand and supply, while supplied services are monitored and measured, so billing can be highly transparent. However, security and data privacy concerns are typically seen as the two critical barriers to adopting it.

The objective of this Position Paper is to briefly outline the potential for mutual positive enforcement between the IAS framework and Cloud computing. We argue that the Cloud's eminent need to achieve trust is greatly facilitated and supported by IAS. Furthermore, we equally argue that the Cloud's potential for delivering large-scale elastic and cost-effective services is a deployment model that is required by IAS to deliver what its users are expecting. This can lead to an IASaaS model

[17] European Commission, The future of cloud computing. Opportunities for European cloud computing beyond 2010, Expert Group Report, Public Version 1.0, 2010, page 8. See: http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf.

(Identification, Authentication and Signature as a Service). IAS in the Cloud may invoke legal challenges relating to applicable law, data protection and current e-Signature laws. A future legal framework on IAS should take into account the specificities of new models like IASaaS, ensuring that cloud based IAS services would be recognized as legally valid and compliant across the EU.

5.2 The Cloud's need for security is supported by IAS

5.2.1 Cloud service models

Cloud is embraced as a way to build more cost effective infrastructures. We briefly recall the Cloud Service Models that include SaaS, PaaS and IaaS. In the case of Software as a Service (SaaS) the consumer uses the provider's applications running on a cloud infrastructure. In the case of Platform as a Service (PaaS), the provided capability is to deploy onto the cloud infrastructure consumer-created or acquired applications. Programming languages, libraries, services, and tools are supported by the provider. Finally, in the case of Infrastructure as a Service (IaaS), processing, storage, networks, and other fundamental computing resources are provisioned where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. In each of those cases, the consumer does not manage or control the underlying cloud infrastructure but may have limited control over selected aspects.

We recall that the most common deployment models include Private Cloud, Community Cloud, Public Cloud and Hybrid Cloud. In the case of Private cloud, the infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). In the case of a Community cloud, the infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). In the case of Public cloud, provisioning is for open use by the general public. Finally, in the case of a Hybrid cloud, there is typically a mixture involved of public and private actors.

Cloud allows to optimize resource sharing in novel ways not found in a traditional datacentre. It is recognised in the Digital Agenda which states:

"Europe should also build its innovative advantage in key areas through reinforced eInfrastructures and through the targeted development of innovation clusters in key

fields. It should develop an EU-wide strategy on "cloud computing" notably for government and science."[18]

However, security and data privacy concerns are typically seen as the two critical barriers to adopting it. This is clearly expressed in messages such as those given last year by the Industry Working Group[19] to Vice President Kroes. Key aspects that need to be addressed include trust, multi-tenancy, encryption, and compliance. Different stakeholders emphasize different aspects though. When considering the barriers from a user perspective, the concepts of security, reliability, data privacy and legal concerns are commonly raised. When considering from a vendor perspective, mainly the different national regulatory frameworks are mentioned.

The IAS regulation holds great potential to lower those barriers for those two stakeholders and for many others alike.

To benefit from Cloud-based solutions, one is quickly forced to make choices with regard to many technical aspects.

5.2.2 End user perspective

Let us first consider the end user perspective. Imagine an organisation that decides to deploy its Human Resources ICT as *SaaS* (Software as a Service). This means the different HR modules (organisation planning, hiring, evaluation, retention, timesheets, payments, training, pension etc) will be available "in the cloud". Managing the Identity, Authentication and Signature (IAS) aspects of internal employees, contractors, service providers, candidates etc is fundamental to achieving the required trust, but it is also a complex challenge.

The most common approach is to call upon an Identity and Access Management (IAM) solution. Such an application supports the lifecycle of Identities (users and managers), which may include the management of attributes (that can be relevant for authentication purposes), as well as the accesses of these Identities once authenticated. In a Cloud context, userid/password authentication is mostly

[18] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 245, 23.

[19] Industry recommendations to Vice President Neelie Kroes on the orientation of a European cloud computing strategy, November 2011. See http://ec.europa.eu/information_society/activities/cloudcomputing/docs/industryrecommendations-ccstrategy-nov2011.pdf.

replaced by some form of strong authentication[20]. To pass authentication across organisational borders, Identity federation[21] concepts allow organisations to trust one another's identity assertions, e.g. using SSO (Single Sign-On). Entitlement management[22] then supports the lifecycle of the accesses of the managed identities. What consumers of cloud services can actually do is usually governed via a "group based" access policy. For such access control to function, Identification and Authentication are prerequisites.

In many Use Cases (e.g. the creation of a new employee within the organisation), the identities of the various actors as well as their activities needs to be authenticated. The most reliable way to do this is through electronic identification, authentication and signatures. In practise this is achieved through various Internet-style protocols[23].

Furthermore, for the purpose of confidentiality and data protection, Cloud solutions have a need to support data encryption (data-at-rest, data-in-flight) and corresponding key management[24].

5.2.3 Management perspective

Let us now consider a management perspective. Cloud Computing resources are handled through control interfaces. It is through these interfaces that the new machine images can be added, existing ones can be modified, and instances can be started or ceased. A successful attack on a Cloud control interface grants the attacker power over the victim's account, with all the stored data included. As a consequence, the protection of these control interfaces is paramount to the security of the Cloud resources. The business model of Cloud service providers includes a significant amount of "self-service", also for various management aspects. As the contractor/self-service manager of the Cloud service will by definition have to

[20] Strong authentication standards include e.g. OATH Event-based (HOTP), Time-based (TOTP) and Challenge-Response (OCRA) Software Tokens.

[21] A federated identity in information technology is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems For example using technologies such as SAML, WS-Federation, Liberty ID-FF.

[22] For example XACML.

[23] As Cloud solutions are typically based on SOAP or Web Services, such activities are modelled in protocols that are encoded in XML.

[24] Leading to approaches such as the OASIS Enterprise Key Management Infrastructure EKMI.

connect remotely, available and trusted IAS-components and services will contribute to his security[25].

5.3 Cloud as an effective IAS services deployment model

5.3.1 Need for trust

As Cloud computing is highly dependent on the trust a consumer has in his provider, IAS has a clear contribution to make to Cloud computing. Customers must trust their cloud providers with respect to the confidentiality and integrity of their data, as well as computation correctness. However, the other way around equally holds. For applications providing IAS functionality, the advantages of running in the Cloud can be significant.

Let us first consider a Certification Service Provider. While some aspects of his service such as his trustworthy core systems (e.g. those that manage his root key) cannot easily be ported into the cloud, directory services and services providing status information (OCSP/CRL) can.

Let us now re-imagine the organisation that decides to deploy its HR ICT as SaaS. Managing the IAS aspects of internal employees, contractors, service providers, candidates etc is fundamental to achieving the required trust, but it is also a complex challenge with regard to performance. A Cloud model can significantly contribute to the cost effective deployment of IAS services, potentially leading to an *IASaaS* model (Identification, Authentication and Signature as a Service).

5.3.2 Potential of an IASaaS model

If one considers what goes on behind the scenes when a user accesses a protected application, it is obvious to identify the potential of an *IASaaS* model.

---

[25] Technically, the cloud control interface are typically realized either as a SOAP-based Web Service, or as a Web application. If the interface is SOAP-based, then WS-Security can be applied. Security tokens such as X.509 certificates and XML Signature are commonly used. If the control interface is a Web application, security relies on SSL/TLS combined with some client authentication mechanisms. It is well known that username/password based client authentication are highly vulnerable to attacks such as XSS (Cross-Site Scripting), thus other methods should take preference (e.g.TLS client certificates). In either case, IAS will facilitate improved protection of the cloud management interfaces.

Assuming an unidentified/unauthenticated user presents himself at the application, the application invites the user to select his Identity Provider (IdP), by returning a list of acceptable IdP's. The user selects his IdP of choice, is redirected there, authenticates there and will then return to the target application with a "token", typically a signed XML data structure e.g. in the format of a SAML-token.

The selected IdP is solicited by many users, and as applications support a continuously broader range of users e.g. across borders, the importance of peaks such as on Monday mornings, or prior to a submission deadline will only increase. For such purpose, the IdP needs to be scalable and robust. This extends beyond the initial authentication exchange, since applications may later challenge the user on supplying particular attributes. The user will turn again to his IdP, or to separate Attribute Providers (AP's). These will equally be returned to the target application in the form of a "token" such as a signed XML data structure. So there is a clear need for scalable and cost-effective performance of authentication and attribute service provisions, which can be seen as Cloud candidates.

After the creation of such a signed XML data structure, there needs to be its validation by its consumer. For example an authentication token will be consumed by the application (or the security component protecting that application). This will include the validation of the electronic signature over the data structure (which may include sub-elements with their own signatures), and the logical evaluation whether the content provided convinces the security component to let the user perform his action on the application. The same peaks (e.g. Monday morning, prior to a submission deadline) are applicable here, but they are even more concentrated. Users may decide to rely upon different IdP's, but the application will most likely rely upon a single security component for processing the IAS tokens. This component has to handle those aggregated peaks. Again, a Cloud model has great potential here.

Obviously, given the sensitivity of the services provided, a private cloud seems a more logical model than a public cloud for the provision of such services.

5.4 Moving IAS into the cloud: legal issues

The legal issues linked to the deployment of cloud services have been studied in previous initiatives[26], and the primary challenges are well understood. Principally,

[26] See e.g. "The Cloud: Understanding the Security, Privacy and Trust Challenges", N. Robinson, L. Valeri.

they relate to ensuring compliance with data protection rules, obtaining acceptable guarantees with respect to security, availability, performance, transparency and contingency planning, as well as data portability (including exit modalities). When IAS services are applied through a cloud model, all of these challenges need to be appropriately addressed, and a number of additional complexities can present themselves as a result of the very specific nature and goals of IAS services. However, if these barriers can be overcome, the immediate consequence is that a fully compliant IAS service can be offered on a potentially very large scale. Clearly, the general benefits of cloud services also apply to IAS services.

5.4.1 Data protection

Arguably the most significant legal concern with respect to cloud computing is data protection, for service providers and customers alike. When IAS services are offered via a cloud model, this concern is further amplified, as legally protected personal data will almost inevitably[27] be entrusted to a cloud provider. This complicates legal compliance, as an IAS cloud provider offering its services in the EU will have to comply with all applicable data protection laws, even if they are established outside of the EU, in accordance with Article 4 of the Data Protection Directive. This places a significant burden on cloud service providers, who will need to comply with multiple national laws: as service providers to their customers, it will inevitably be the national data protection laws of their customers that govern their contracts, rather than the data protection laws of the countries in which the provider are established.

Each national data protection law may impose specific requirements or restrictions on cloud computing services, either directly via national legislation, or –more likely – through opinions issued by national data protection authorities, or even by opinions from Worker's Council or other organised labour representatives. Such requirements may relate to the location where data centres may be established, the contractual relationship that the cloud provider may have with its subcontractors, auditing rights, security guarantees and the possibility for data subjects to exercise their rights. The export of personal data to a destination outside of the European Economic Area – which is almost inevitable in a cloud computing model, given the necessity of operating multiple data centres in geographically spread out regions to ensure

---

J. Cave, T.Starkey, H. Graux, S. and P. Hopkins, ENISA, 2010; http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-privacy-trust-challenges-2010_en.pdf, p.53 and following

[27] With the exception of purely pseudonymous IAS services and IAS services that exclude natural persons from their scope, such as e.g. company seals in the cloud.

stability and scalability – is additionally subjected to strict legal requirements, and will often require the conclusion of very specific contracts that comply with EU data protection principles. In short, there is a significant compliance burden for cloud providers as a result of the current European regulatory approach to data protection.

However, it is worth noting that these compliance challenges are not unique to IAS services or even to cloud computing, and that some solutions have been developed over the past years. Notable examples include the Safe Harbour arrangements, which allow US based data processors to self-certify their compliance with European data protection principles[28], and the use of Standard Contractual Clauses which have the European Commission's formal approval[29]. By integrating these Clauses into cloud service contracts, international exchanges of personal data can be legitimized with a reasonable degree of assurance. Perhaps most importantly, the ongoing review of the Data Protection Directive points to a significant awareness with policy makers of certain impracticalities within the current legislation (such as the cumulative applicability of multiple national laws), and to a willingness to remedy these. Thus, improvements can be expected on this point in the future.

5.4.2 Applicable laws

As a second challenge, it is clear that IAS cloud services as a whole will not necessarily be subject to European laws. Under the current eSignatures Directive (as with the eCommerce Directive), CSPs are largely subject to the national laws of the countries in which they are established. This means that an IAS provider established in the EU will have to comply with the eSignatures/eCommerce legislation in its own country, next to the data protection laws of all of its customers. Providers established outside of the EU will typically apply their own national laws (again, next to potentially all European data protection laws), leading to a regulatory landscape which is fragmented. This reality further emphasizes the need for more strongly harmonised legislation, as e.g. proposed by the draft IAS Regulation and the draft Data Protection Regulation. In that respect, cloud computing (including cloud based IAS services) may prove to be a potent stimulus to these harmonization efforts, as the need for universally valid services will become ever clearer.

[28] See http://export.gov/safeharbor/

[29] See http://ec.europa.eu/justice/data-protection/document/international-transfers/index_en.htm

5.4.3 eSignature laws compliance

Finally, it is worth noting that IAS cloud providers are likely to have some difficulty in ensuring compliance with the current eSignatures Directive on a number of points, especially if they aspire to offering qualified service levels. Typical challenges will include the assurance of sole control over signing solutions, which is traditionally judged more harshly with respect to remotely controlled facilities than for locally kept devices, and obtaining an affirmative compliance decision of the secure-signature-creation device in countries that require this. Such issues will likely be alleviated by the upcoming update of the legal framework, and the accompanying revision of the standardisation framework and supervisory model. Clarifications on these aspects will ensure that cloud based IAS services would be recognized as legally valid and compliant across the EU.

6. Overview of delegating and implementing acts within the Regulation

The table below provides an overview of the provisions of the Proposal calling for delegated acts or implementing acts. It also contains recommendations of the IAS study team for the content of such acts, should the Commission consider moving forward in their preparation.

For each envisaged act, the table briefly describes its scope and content, and references any standards related to it. The table can be used as a first input for the drafting of the acts and for integrating the required links to standardisation efforts.

The following topics have been identified:

6.1 Notification

Article	Text within the Article and general context	Scope / Content / Standard to be included in the delegated / implementing act	Act number
Notification 7 (4)	Implementing act(s) defining the circumstances, formats and procedures of the notification referred to in art. 7.1 […]. 7.1: MS which notify an electronic identification scheme shall forward to EC the following information and without undue delay, any subsequent changes thereof: o a description of the notified electronic identification scheme; o the authorities responsible for the notified electronic identification scheme; o information on by whom the registration of the unambiguous person identifiers is managed; o a description of the authentication possibility; o arrangements for suspension or revocation of either the notified identification scheme or authentication possibility or the compromised parts concerned.	**Scope:** Notification of eID schemes **Content:** • Definition of a form (including template for art 7.1.a and 7.1.b), specifying: o Details on the notifying MS (administration, contact details); o Description on the scheme: nature, eID means currently covered, requirements and processes for the issuance and management of the eIDs under the scheme, governance (including management and maintenance) of the scheme itself; o Identification of any relevant entities in the scheme, including their role, competences, responsibilities and nature (governmental vs nongovernmental, not for profit or for	1 Priority: H Ease: M Scheduling: ASAP Iteration: 1

		profit); o Description of the current scope of the project in terms of user base (eID means holders) and use cases, along with plans and prognoses for future developments and changes; o Explanation/justification of how the scheme and means meet the requirements of the Regulation, including its link to the MS (issued by, on behalf of or under the responsibility of the MS). • Definition of a procedure: o Letter from PermRep to CONNECT Director-General o Review for completeness, including right to request additional information o Terms and timescales for responses o Updates and revisions measures, including an obligation for the notifying entity to keep the notified information accurate and up to date at all times. **Standard:** *Need for standard: N. Standards will be required to make notified data available in a useful format to the public (ex. via a Trust List), but this is a separate issue dealt with below.*	

6.2 Coordination

Coordination 8 (2)	act(s) establishing the necessary modalities to facilitate the cooperation between the MS referred to in §8.1 with a view to fostering a high level of trust	**Scope:** MS coordination on eID	2

	and security appropriate to the degree of risk. Those implementing acts shall concern, in particular, the exchange of information, experiences and good practice on electronic identification schemes, the peer review of notified electronic identification schemes and the examination of relevant developments arising in the electronic identification sector by the competent authorities of the MS. 8.1: MS shall cooperate in order to ensure the interoperability of electronic identification means falling under a notified scheme and to enhance their security.	**Content:** • Set-up of a formal "expert group" on eID (level: Directors-General of competent national administrations) • Mission of the group: exchange of information, experiences and good practice on e-identification schemes, the peer review of notified e-identification schemes and the examination of relevant developments arising in the e-identification **Standard:** *need for standard: N*	Priority: M Ease: E Scheduling: <12 Iteration: >1
Coordination 8 (3)	act(s) concerning the facilitation of cross border interoperability of electronic identification means by setting of minimum technical requirements.	**Scope:** Specification of min technical requirements for notified eID schemes cross-border interoperability **Content:** - (Set of) specifications - Interoperability requirements should also address security, either through a single minimum security threshold, or through a multilevel quality policy (such as the QAA in STORK) - Introducing the specification in formal standardisation process (via a standardisation mandate to ESOs). - Interoperability will require the Commission to communicate the notified schemes to the public. A Trusted List may be advisable; in this case, the basic approach and standards used with respect to eSignatures and (in the future) other Trust Services can be used. However, specific profiles of the applicable standards would be needed: - *EN 19 602 Trust Service Status Lists Format* - *EN 19 612 Trusted List Format*	3 Priority: L Ease: M Scheduling: >12 / av. STD Iteration: 2 (1: spec., 2: standard)

		Standard: *Need for standard: Y (low)* *Standard available: N, when: TBD* *Standard ref: ESO Technical Report (TR)* *Standard content:* same as specification(s)	

6.3 Supervisory body

Supervisory body **13 (5)**	act(s) concerning the definition of procedures applicable to the tasks referred to in art. 13.2. 13.2: The SB shall be responsible for the performance of the following tasks: o monitoring TSPs established in the territory of the designating MS to ensure that they fulfil the requirements laid down in Art. 15; o undertaking supervision of QTSPs established in the territory of the designating MS and of the QTSs they provide in order to ensure that they and the QTSs provided by them meet the applicable requirements laid down in this Regulation; o ensuring that relevant information and data referred to in §19.2.g, and recorded by QTSPs are preserved and kept accessible after the activities of a QTSP have ceased, for an appropriate time with a view to guaranteeing continuity of the service. 15: Security requirements applicable to TSPs 19.2.g: QTSPs providing QTSs shall record for an appropriate period of time all relevant information concerning data issued and received by the QTSP, in particular for the purpose of providing evidence in legal proceedings. Such recording	**Scope: Common supervision procedures** **Content:** • Compilation of the requirements related to or relevant for supervision and monitoring as established in the Regulation. • Supervision procedure • Specification on data preservation (§13.2.c) • Definition of “appropriate time” in §13.2.c **Standard:** *Need for standard:* Y (the supervision procedure should be standardised). *Standard available:* Y*:* • EN 19 403 General requirements and guidance for Conformity Assessment of TSPs Supporting Electronic Signatures • EN 19 413 Conformity Assessment for TSPs Issuing Certificates • EN 19 423 Conformity Assessment for TSPs providing Time-Stamping Services • EN 19 433 Conformity Assessment for TSPs providing Signature Generation Services • EN 19 513 Conformity Assessment of Registered Electronic Mail Service Providers	4 related: §13.6 Priority: H Ease: M Scheduling: ASAP Iteration: 2 (1: spec, 2: STD)

	may be done electronically.	• EN 19 523 Conformity Assessment of Data Preservation Service Providers • EN 19 613 Conformity Assessment of Trusted List Providers *Standard content:* - STD should build on TS 101456, Crobies Deliverable 1, IAS study deliverable D3.	
Supervisory body **13 (6)**	act(s) defining the circumstances, formats and procedures for the report referred to in §13.3. 13.3: Each SB shall submit a yearly report on the last calendar year's supervisory activities to EC and MSs by the end of the first quarter of the following year. It shall include at least: o information on its supervisory activities; o a summary of breach notifications received from TSPs in accordance with Art. 15(2); o statistics on the market and usage of QTSs, including information on QTSPs themselves, the QTSs they provide, the products they use and the general description of their customers. 15.2: TSPs shall […] notify the competent SB […] of any breach of security or loss of integrity that has a significant impact on the TS provided and on the personal data maintained therein. […]	**Scope: Common supervision procedure (c'td): yearly report** **Content:** • Template of the report to be submitted to EC under art 13.3 with all the relevant informational features the report should contain • Report content: (a) information on its supervisory activities; (b) a summary of breach notifications; (c) statistics on the market and usage • Submission procedure (delivery date, to who, how, format) **Standard:** *Need for standard:* N: *Standard available:* N, *when:* TBD; *Standard ref: TBD* *Standard content:* Preparatory work is currently underway under an ENISA public tender (ref. ENISA P/09/12/TCD). The resulting study will provide recommendations on breach notification formats, procedures, and reporting obligations, including specific templates. These should be the basis for legislative work in this area.	4 Related to: §13.5 Scheduling: ASAP Iteration: 2 (1: ENISA recommendation, 2: Implementing act)

6.4 Mutual assistance

Mutual assistance 14 (4)	act(s) specifying the formats and procedures for the mutual assistance provided for in Art. 14. 14.1: SBs shall cooperate with a view to exchange good practice and provide each other, within the shortest possible time, with relevant information and mutual assistance so that activities can be carried out in a consistent manner. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the security audits as referred to in Art. 15, 16 and 17. 14.2: A SB to which a request for assistance is addressed may not refuse to comply with it unless: o it is not competent to deal with the request; or o compliance with the request would be incompatible with this Regulation. 14.3: Where appropriate, SBs may carry out joint investigations in which staff from other MS' SBs is involved. The SB of the MS where the investigation is to take place, in compliance with its own national law, may devolve investigative tasks to the assisted SB's staff. Such powers may be exercised only under the guidance and in the presence of staff from the host SB. The assisted SB's staff shall be subject to the host SB's national law. The host SB shall assume responsibility for the assisted SB staff's actions. 15.1: Without prejudice to Art. 16(1), any TSP may submit the report of a security audit carried out by a recognised independent body to the SB to confirm that appropriate security measures have been taken.	**Scope: Procedure defining SB mutual assistance** **Content:** • Set-up of a formal "expert group" on trusted services, consisting of SB representatives from all MS; • Establishing coordination mechanisms, including periodic meetings and governance of the expert group; • Elaborating communication and response mechanisms, including assistance obligations through definition of incidents or issues where assistance is mandatory. Response conditions (response times and availability) should be defined. • Joint investigative procedures should be defined, including processes for the identification of a lead investigator, which should be based on the country of establishment of the investigated target, or of the largest/economically most significant target in case of targets in multiple countries; • Investigative powers must be further defined in case of emergencies, including auditing requirements and procedures (prior notice, duration, seizure, copying of equipment, including through collaboration with law enforcement authorities where necessary). **Standard:** *need for standard: N*	2 Related articles: Priority: M Ease: M Scheduling: <12 Iteration: 1

	16.1: QTSPs shall be audited by a recognised independent body once a year to confirm that they and the QTSs provided by them fulfil the requirements set out in this Regulation, and shall submit the resulting security audit report to the supervisory body. 17 (1) QTSPs shall notify the supervisory body of their intention to start providing a QTS and shall submit to the supervisory body a security audit report carried out by a recognised independent body, as provided for in Art. 16(1). QTSPs may start to provide the QTS after they have submitted the notification and security audit report to the supervisory body.		

6.5 Security requirements applicable to trust service providers

Security requirements applicable to trust service providers 15 (5)	act(s) concerning the further specification of the measures referred to in articles 15.1. §15.1: TSPs who are established in the territory of the Union shall take appropriate technical and organisational measures to manage the risks posed to the security of the TSs they provide. Having regard to state of the art, these measures shall ensure that the level of security is appropriate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of adverse effects of any incidents. Without prejudice to Art. 16.1, any TS provider may submit the report of a security audit carried out by a recognised independent body to the SB to confirm	**Scope:** Defining appropriate security requirements for TSPs. Note that any delegated act should take into account that 15(5) applies to trust services in general (including nonqualified ones). Thus, *if* the Commission adopts a delegated act, then this distinction should be made. **Content:** • Policy and security requirements can be based on the existing Directive for qualified service providers, as well as on existing standards. **Standard:** *Need for standard:* Y	5 Related articles: related: §13.5 (supervision criteria) Priority: optional Ease: M Scheduling: optional Iteration: 2

	that appropriate security measures have been taken. §16.1: QTSPs shall be audited by a recognised independent body once a year to confirm that they and the QTSs provided by them fulfil the requirements set out in this Regulation, and shall submit the resulting security audit report to the SB.	*Standard available:* Y, *when:* *Standard ref:* • EN 19 401 General Policy Requirements for TSPs Supporting Electronic Signatures • EN 19 431 Policy & Security Requirements for TSPs providing Signature Generation Services • EN 19 511 Policy & Security Requirements for Registered Electronic Mail (REM) Service Providers • EN 19 521 Policy & Security Requirements for Data Preservation Service Providers (DPSPs)	(1: spec., 2: standard)
Security requirements applicable to TS providers 15 (6)	act(s) defining the circumstances, formats and procedures, including deadlines, applicable for the purpose of articles 15.1 to 15.3. 15 (1) TSPs who are established in the territory of the Union shall take appropriate technical and organisational measures to manage the risks posed to the security of the TSs they provide. Having regard to state of the art, these measures shall ensure that the level of security is appropriate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of adverse effects of any incidents. Without prejudice to Art. 16(1), any TS provider may submit the report of a security audit carried out by a recognised independent body to the SB to confirm that appropriate security measures have been taken. 15 (2) TSPs shall, without undue delay and where feasible not later than 24 hours after having become aware of it, notify the competent SB, the competent national body for information security and other	Template of the summary of the breach notifications received to be submitted to the ENISA [template for submitting the information to EC is done under 13 (6) with reference to 13 (3) (b)] with all the relevant informational features the summary should contain **Content:** • Template of the report to be submitted to SB under art 15.2 with all the relevant informational features the report should contain • Report content: (a) identification of the service provider; (b) description of the nature of the breach; (c) description of the expected impact of the breach (potential victims, severity, potential costs); (d) potential measures that can be taken by the supervisory body, SB, other third parties and potential victims to mitigate the potential damage damage • Submission procedure (delivery timing requirements, template, communications channels) • Template of the reports to be used by SB in their	4 Related to: §15.5 and 13.3 Scheduling: <12 Iteration: 2 (1: ENISA recommendation, 2: Implementing act)

	relevant third parties such as data protection authorities of any breach of security or loss of integrity that has a significant impact on the TS provided and on the personal data maintained therein. Where appropriate, in particular if a breach of security or loss of integrity concerns two or more MS, the SB concerned shall inform SBs in other MS and the European Network and Information Security Agency (ENISA). The SB concerned may also inform the public or require the TS provider to do so, where it determines that disclosure of the breach is in the public interest. 15 (3) The SB shall provide to ENISA and to EC once a year with a summary of breach notifications received from TS providers. 16 (1) QTSPs shall be audited by a recognised independent body once a year to confirm that they and the QTSs provided by them fulfil the requirements set out in this Regulation, and shall submit the resulting security audit report to the supervisory body.	reporting to ENISA and EC cf art 15.3 (to be integrated under the art.13.3 implementation efforts) **Standard:** *Need for standard:* N: *Standard available:* N, *when:* TBD; *Standard ref: TBD* *Standard content:* Preparatory work is currently underway under an ENISA public tender (ref. ENISA P/09/12/TCD). The resulting study will provide recommendations on breach notification formats, procedures, and reporting obligations, including specific templates. These should be the basis for legislative work in this area.	

6.6 Supervision of QTSPs

Supervision of QTSPs **16 (5)**	act(s) concerning the specification of the conditions under which the independent body carrying out the audit referred to in Art. 16(1) and in Art. 15(1) and	**Scope:** definition of recognition requirements and procedures for recognised independent bodies	4 related:

	17(1) shall be recognised. 16 (1) QTSPs shall be audited by a recognised independent body once a year to confirm that they and the QTSs provided by them fulfil the requirements set out in this Regulation, and shall submit the resulting security audit report to the SB. 15 (1) TSPs who are established in the territory of the Union shall take appropriate technical and organisational measures to manage the risks posed to the security of the TSs they provide. Having regard to state of the art, these measures shall ensure that the level of security is appropriate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of adverse effects of any incidents. Without prejudice to Art. 16(1), any TSP may submit the report of a security audit carried out by a recognised independent body to the SB to confirm that appropriate security measures have been taken. 17 (1) QTSPs shall notify the SB of their intention to start providing a QTS and shall submit to the SB a security audit report carried out by a recognised independent body, as provided for in Art. 16(1). QTSPs may start to provide the QTS after they have submitted the notification and security audit report to the SB.	**Content:** • Required competences and assurances for independent bodies; • Requirements and procedures for the recognition of independent bodies; • To be aligned with IAF (International Accreditation Forum) membership requirements, to facilitate international cross border interoperability. **Standard:** *Need for standard:* N	§13.5 Priority: H Ease: M Scheduling: ASAP Iteration: 1
Supervision of QTSPs **16 (6)**	act(s) defining the circumstances, procedures and formats applicable for the purpose of paragraphs 1, 2 and 4. 16 (1) QTSPs shall be audited by a recognised independent body once a year to confirm that they and the QTSs provided by them fulfil the	**Scope:** Circumstances, procedures and formats for auditing QTSPs, including trusted list impacts **Content:** • Definition of processes for annual audits via	4 related: §13.5 Priority: H Ease: M

	requirements set out in this Regulation, and shall submit the resulting security audit report to the SB. 16 (2) Without prejudice to paragraph 1, the SB may at any time audit the QTSPs to confirm that they and the QTSs provided by them still meet the conditions set out in this Regulation, either on its own initiative or in response to a request from EC. The SB shall inform the data protection authorities of the results of its audits, in case personal data protection rules appear to have been breached. 16 (4) With reference to paragraph 3, if the QTSP does not remedy any such failure within a time limit set by the SB, it shall lose its qualified status and be informed by the SB that its status will be changed accordingly in the trusted lists referred to in Art. 18. 16 (3) The SB shall have the power to issue binding instructions to QTSPs to remedy any failure to fulfil the requirements indicated in the security audit report. 18 Trusted lists	references to standards; • Definition of reporting requirements including retention of reports; • Definition of conditions under which SBs may initiate or conduct audits, and circumstances under which data protection authorities must be informed, and to what extent; • Definition of impacts of all of the above on the publication status of the QTSP in the trusted list **Standard:** *Need for standard:* Y *Standard available:* Y*:* *Standard ref:* • EN 19 403 General requirements and guidance for Conformity Assessment of TSPs Supporting Electronic Signatures • EN 19 413 Conformity Assessment for TSPs Issuing Certificates • EN 19 423 Conformity Assessment for TSPs providing Time-Stamping Services • EN 19 433 Conformity Assessment for TSPs providing Signature Generation Services • EN 19 513 Conformity Assessment of Registered Electronic Mail Service Providers • EN 19 523 Conformity Assessment of Data Preservation Service Providers • EN 19 613 Conformity Assessment of Trusted List Providers	Scheduling: ASAP Iteration: 1

6.7 Initiation of a QTS

Initiation of a QTS **17 (5)**	act(s) defining the circumstances, formats and procedures for the purpose of paragraphs 1, 2 and 3. 17 (1) QTSPs shall notify the SB of their intention to start providing a QTS and shall submit to the SB a security audit report carried out by a recognised independent body, as provided for in Art. 16(1). QTSPs may start to provide the QTS after they have submitted the notification and security audit report to the SB. 17 (2) Once the relevant documents are submitted to the SB according to paragraph 1, the qualified service providers shall be included in the trusted lists referred to in Art. 18 indicating that the notification has been submitted. 17 (3) The SB shall verify the compliance of the QTSP and of the QTSs provided by it with the requirements of the Regulation. The SB shall indicate the qualified status of the qualified service providers and the QTSs they provide in the trusted lists after the positive conclusion of the verification, not later than one month after the notification has been done in accordance with paragraph 1. 16 (1) QTSPs shall be audited by a recognised independent body once a year to confirm that they and the QTSs provided by them fulfil the requirements set out in this Regulation, and shall submit the resulting security audit report to the SB. 18 Trusted lists	**Scope:** Circumstances, procedures and formats for initiating QTSP services **Content:** • Definition of a template with information to be notified to SB, including identification, contact details, scope of services, requested inclusion in trusted list, chosen independent body, and full report of the independent body along with the date of the assessment (report may not be older than 1 month); • Definition of processes to be followed by SBs for the verification of the notification prior to the inclusion in the trusted lists, including specifically further investigation and auditing rights prior to inclusion, and the right to obtain further information from the recognised independent body; • Consequences of delays should be clearly specified. **Standard:** *Need for standard:* N	4 related: §13.5 Priority: H Ease: M Scheduling: ASAP Iteration: 1

6.8 Trusted lists

Trusted lists 18 (5)	act(s) concerning the definition of the information referred to in paragraph 1. 18 (1) Each MS shall establish, maintain and publish trusted lists with information related to the QTSPs for which it is competent together with information related to the QTSs provided by them.	**Scope:** Definition of the content of trusted lists, based on the existing work of Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC **Content:** • As per Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC (although generalised to cover other types of TSPs; minor changes can be expected); **Standard:** • *See below*	4 related: §13.5 Priority: H Ease: E Scheduling: ASAP Iteration: 1
Trusted lists 18 (6)	act(s) defining the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. 18 (1) Each MS shall establish, maintain and publish trusted lists with information related to the QTSPs for which it is competent together with information related to the QTSs provided by them. 18 (2) MS shall establish, maintain and publish, in a secure manner, electronically signed or sealed trusted lists provided for in paragraph 1 in a form suitable for automated processing. 18 (3) MS shall notify to EC, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and	**Scope:** Definition of the technical specs, formats and maintenance obligations of national trusted lists, based on the existing work of Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC **Content:** • As per Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC (although generalised to cover other types of TSPs; minor changes can be expected). **Standard:** *Need for standard:* Y	4 related: §13.5 Priority: H Ease: E Scheduling: ASAP Iteration: 1

	details of where such lists are published, the certificate used to sign or seal the trusted lists and any changes thereto. 18 (4) The Commission shall make available to the public, through a secure channel, the information, referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing.	*Standard available:* Y, *when:* *Standard ref:* • *EN 19 602 Trust Service Status Lists Format* • *EN 19 612 Trusted List Format* • *For historical reference: ETSI TS 102 231, implemented as through the Decisions above (deprecated by the new ENs)*	

6.9 Requirements for QTSPs

Requirements for QTSPs 19 (5)	act(s) establishing reference numbers of standards for trustworthy systems and products (compliance with Art. 19). 19 (2) QTSPs providing QTSs shall: o use trustworthy systems and products which are protected against modification and guarantee the technical security and reliability of the process supported by them; o use trustworthy systems to store data provided to them, in a verifiable form so that: – they are publicly available for retrieval only where the consent of the person to whom the data has been issued has been obtained, – only authorised persons can make entries and changes, – information can be checked for authenticity;	**Scope:** References to applicable standards, as per the approach under the eSignatures Directive **Content:** • As per 2003/511/EC of 14 July 2003 (although generalised to cover other types of TSPs; minor changes can be expected). **Standards**: • EN 19 401 General Policy Requirements for TSPs Supporting Electronic Signatures • EN 19 411 Policy & Security Requirements for TSPs Issuing Certificates	5 Related articles: related: §13.5 (supervision criteria) Priority: H Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

6.10 Legal effects and acceptance of electronic signatures

Legal effects and acceptance of electronic signatures 20 (6)	act(s) concerning the definition of the different security levels of electronic signature referred to in paragraph 4. 20 (4) If an electronic signature with a security assurance level below QeS is required, in particular by a MS for accessing a service online offered by a public sector body on the basis of an appropriate assessment of the risks involved in such a service, all electronic signatures matching at least the same security assurance level shall be recognised and accepted.	**Scope:** Definition of security levels **Content:** • Definition of security levels, in general terms of criteria; • Should be linked back to trusted lists, to ensure that security levels can be validated by relying parties. **Standards**: See below	6 Related articles: related: - Priority: L Ease: E Scheduling: optional Iteration: 2 (1: spec., 2: standard)
Legal effects and acceptance of electronic signatures 20 (7)	act(s) establishing reference numbers of standards for the security levels of electronic signature (compliance with paragraph 6). 20 (6) The Commission shall be empowered to adopt delegated acts in accordance with Art. 38 concerning the definition of the different security levels of electronic signature referred to in paragraph 4. 20 (4) If an electronic signature with a security assurance level below QeS is required, in particular by a MS for accessing a service online offered by a public sector body on the basis of an appropriate assessment of the risks involved in such a service, all electronic signatures matching at least the same security assurance level shall be recognised and accepted.	**Scope:** References to applicable standard specifying security levels **Content:** • Definition of security levels; • Should be linked back to trusted lists, to ensure that security levels can be validated by relying parties. **Standards**: Not available yet; should be developed under the M460	6 Related articles: related: - Priority: L Ease: E Scheduling: optional Iteration: 2 (1: spec., 2: standard)

6.11 QCs for electronic signature

QCs for electronic signature 21 (4)	act(s) concerning the further specification of the requirements laid down in Annex I. Annex I QCs for electronic signatures shall contain: o an indication, at least in a form suitable for automated processing, that the certificate has been issued as a QC for electronic signature; o a set of data unambiguously representing the QTSP issuing the QCs including at least, the MS in which that provider is established and – for a legal person: the name and registration number as stated in the official records, – for a natural person: the person's name; o a set of data unambiguously representing the signatory to whom the certificate is issued including at least the name of the signatory or a pseudonym, which shall be identified as such; o electronic signature validation data which correspond to the electronic signature creation data; o details of the beginning and end of the certificate's period of validity; o the certificate identity code which must be unique for the QTSP; o the AeS or advanced electronic seal of the issuing QTSP; o the location where the certificate supporting the AeS or advanced electronic seal referred to in point (g) is available free of charge; o the location of the certificate validity status services that can be used to enquire about the validity status of the QC; o where the electronic signature creation data related to the electronic signature validation data are located in a QSCD, an appropriate indication of	**Scope:** Definition of requirements through references to standards updated through M460 **Content:** • Definition of requirements, in general terms of criteria; cf Decision 2003/511/EC. **Standards**: See below	6 Related articles: related: - Priority: H Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

	this, at least in a form suitable for automated processing.		
QCs for electronic signature 21 (5)	act(s) establishing reference numbers of standards for QCs for electronic signature (compliance with Annex I). Annex I QCs for electronic signatures shall contain: o an indication, at least in a form suitable for automated processing, that the certificate has been issued as a QC for electronic signature; o a set of data unambiguously representing the QTSP issuing the QCs including at least, the MS in which that provider is established and – for a legal person: the name and registration number as stated in the official records, – for a natural person: the person's name; o a set of data unambiguously representing the signatory to whom the certificate is issued including at least the name of the signatory or a pseudonym, which shall be identified as such; o electronic signature validation data which correspond to the electronic signature creation data; o details of the beginning and end of the certificate's period of validity; o the certificate identity code which must be unique for the QTSP; o the AeS or advanced electronic seal of the issuing QTSP; o the location where the certificate supporting the AeS or advanced electronic seal referred to in point (g) is available free of charge; o the location of the certificate validity status services that can be used to enquire about the validity status of the QC; o where the electronic signature creation data related to the electronic signature validation data are located in a QSCD, an appropriate indication of	**Scope:** Reference numbers for QCs **Content:** • Following the template of Decision 2003/511/EC. **Standard:** *Need for standard:* Y *Standard available:* Y, *when:* *Standard ref:* • *EN 19 411 Policy & Security Requirements for TSPs Issuing Certificates* • *EN 19 412 Profiles for TSPs issuing Certificates* • *EN 19 432 Profiles for TSPs providing Signature Generation Services*	6 Related articles: related: - Priority: H Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

	this, at least in a form suitable for automated processing.		

6.12 Requirements for QSCDs

Requirements for QSCDs 22 (2)	act(s) establishing reference numbers of standards for QSCDs (compliance with Annex II). Annex II (1) QeS creation devices shall ensure, by appropriate technical and procedural means, that at least: o the secrecy of the electronic signature creation data used for electronic signature generation is assured; o the electronic signature creation data used for electronic signature generation can occur only once; o the electronic signature creation data used for electronic signature generation cannot, with reasonable assurance, be derived and the electronic signature is protected against forgery using currently available technology; o the electronic signature creation data used for electronic signature generation can be reliably protected by the legitimate signatory against use by others. Annex II (2) QeS creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing. Annex II (3) Generating or managing electronic signature creation data on behalf of the signatory shall be done by a QTSP.	**Scope:** Reference numbers for QCs **Content:** • Following the template of Decision 2003/511/EC. **Standard:** *Need for standard:* Y *Standard available:* Y, *when:* *Standard ref:* • *EN 19 211 Protection Profiles for Secure Signature Creation Devices* • *EN 19 212 Application Interfaces for Secure Signature Creation Devices* • *EN 19 221 Security Requirements for Trustworthy Systems Managing Certificates for Electronic SignaturesEN 19 241: Security requirements for trustworthy systems supporting Server Signing (Signature Generation services)*	6 Related articles: related: - Priority: H Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

	Annex II (4) QTSPs managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data for back-up purposes provided the following requirements are met: o the security of the duplicated datasets must be at the same level as for the original datasets; o the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.		

6.13 Certification of QSCDs

Certification of QSCDs **23 (1)**	QeS creation devices may be certified by appropriate public or private bodies designated by MS provided that they have been submitted to a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in a list that shall be established by EC by means of implementing acts.	**Scope:** identification of standards for security evaluation of QSCDs **Content:** • Following the template of Decision 2003/511/EC. **Standard:** *See below*	6 Related articles: related: - Priority: H Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)
Certification of QSCDs **23 (3)**	act(s) concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1. 23 (1) QeS creation devices may be certified by appropriate public or private bodies designated by MS provided that they have been submitted to a	**Scope:** references to standards for security evaluation of QSCDs **Content:** • Following the template of Decision 2003/511/EC.	6 Related articles: related: -

	security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in a list that shall be established by EC by means of implementing acts.	**Standard:** *Need for standard:* Y *Standard available:* Y, *when:* *Standard ref:* • EN 19 203: Conformity Assessment of Secure Devices and Trustworthy systems	Priority: H Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

6.14 Publication of a list of certified QSCDs

Publication of a list of certified QSCDs **24 (3)**	act(s) defining circumstances, formats and procedures applicable for the purpose of paragraph 1. 24 (1) MS shall notify to EC without undue delay, information on QSCDs which have been certified by the bodies referred to in Art. 23. They shall also notify to EC, without undue delay, information on electronic signature creation devices that would no longer be certified. 23 (1) QeS creation devices may be certified by appropriate public or private bodies designated by MS provided that they have been submitted to a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in a list that shall be established by EC by means of implementing acts.	**Scope:** circumstances, formats and procedures for the publication of lists of certified QSCDs. **Content:** • As per Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC, modified to be applied to QSCDs, rather than TSPs; **Standard:** *Need for standard:* Y, if machine processable lists are desired (as recommended by CROBIES) *Standard available:* N. The basic trusted list standard can be used, but a specific profile for QSCDs would need to be developed under M460. CROBIES inputs can be used as a starting point for this work, building on: • *EN 19 602 Trust Service Status Lists Format* • *EN 19 612 Trusted List Format* • *For historical reference: ETSI TS 102 231,*	4 related: §13.5 Priority: H Ease: E Scheduling: ASAP Iteration: 1

		implemented as through the Decisions above	

6.15 Requirements for the validation of QeSs

Requirements for the validation of QeSs **25 (2)**	act(s) concerning the further specification of the requirements laid in down in paragraph 1. 25 (1) A QeS shall be considered as valid provided that it can be established with a high level of certainty, that at the time of signing: o the certificate, that supports the signature, is a QeS certificate complying with the provisions laid down in Annex I; o the QC required is authentic and valid; o the signature validation data correspond to the data provided to the relying party; o the set of data unambiguously representing the signatory is correctly provided to the relying party; o the use of any pseudonym is clearly indicated to the relying party if a pseudonym is used; o the electronic signature was created by a QSCD; o the integrity of the signed data has not been compromised; o the requirements provided for in Art. 3 point 7 are met; o the system used for validating the signature provides to the relying party the correct result of the validation process and allows the relying party to detect any security relevant issues. Annex I QCs for electronic signatures shall contain: o an indication, at least in a form suitable for automated processing, that the certificate has been issued as a QC for electronic signature;	**Scope:** Definition of validation requirements, including references to applicable standards. **Content:** • Primarily reference to eligible standards. **Standard:** *See below*	6 Related articles: related: - Priority: M Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

	o a set of data unambiguously representing the QTSP issuing the QCs including at least, the MS in which that provider is established and – for a legal person: the name and registration number as stated in the official records, – for a natural person: the person's name; o a set of data unambiguously representing the signatory to whom the certificate is issued including at least the name of the signatory or a pseudonym, which shall be identified as such; o electronic signature validation data which correspond to the electronic signature creation data; o details of the beginning and end of the certificate's period of validity; o the certificate identity code which must be unique for the QTSP; o the AeS or advanced electronic seal of the issuing QTSP; o the location where the certificate supporting the AeS or advanced electronic seal referred to in point (g) is available free of charge; o the location of the certificate validity status services that can be used to enquire about the validity status of the QC; o where the electronic signature creation data related to the electronic signature validation data are located in a QSCD, an appropriate indication of this, at least in a form suitable for automated processing. 3 (7) 'AeS' means an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with high level of confidence, use under his sole		

	control; and (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable;		
Requirements for the validation of QeSs **25 (3)**	act(s) establishing reference numbers of standards for the validation of QeSs (compliance with paragraph 1). 25 (1) A QeS shall be considered as valid provided that it can be established with a high level of certainty, that at the time of signing: o the certificate, that supports the signature, is a QeS certificate complying with the provisions laid down in Annex I; o the QC required is authentic and valid; o the signature validation data correspond to the data provided to the relying party; o the set of data unambiguously representing the signatory is correctly provided to the relying party; o the use of any pseudonym is clearly indicated to the relying party if a pseudonym is used; o the electronic signature was created by a QSCD; o the integrity of the signed data has not been compromised; o the requirements provided for in Art. 3 point 7 are met; o the system used for validating the signature provides to the relying party the correct result of the validation process and allows the relying party to detect any security relevant issues. Annex I QCs for electronic signatures shall contain: o an indication, at least in a form suitable for automated processing, that the certificate has been issued as a QC for electronic signature; o a set of data unambiguously representing the QTSP issuing the QCs including at least, the MS in which that provider is established and	**Scope:** Reference to applicable standards **Content:** • Reference to eligible standards. **Standard:** • *EN 19 101: Policy and Security Requirements for Electronic Signature Creation and Validation* *EN 19 102: Procedures for Signature Creation and Validation* • *EN 19 111:Protection Profiles for Signature Creation & Validation Applications*	6 Related articles: related: - Priority: M Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

	– for a legal person: the name and registration number as stated in the official records, – for a natural person: the person's name; o a set of data unambiguously representing the signatory to whom the certificate is issued including at least the name of the signatory or a pseudonym, which shall be identified as such; o electronic signature validation data which correspond to the electronic signature creation data; o details of the beginning and end of the certificate's period of validity; o the certificate identity code which must be unique for the QTSP; o the AeS or advanced electronic seal of the issuing QTSP; o the location where the certificate supporting the AeS or advanced electronic seal referred to in point (g) is available free of charge; o the location of the certificate validity status services that can be used to enquire about the validity status of the QC; o where the electronic signature creation data related to the electronic signature validation data are located in a QSCD, an appropriate indication of this, at least in a form suitable for automated processing. 3 (7) 'AeS' means an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with high level of confidence, use under his sole control; and (d) it is linked to the data to which it relates in such a way that any subsequent change in		

	the data is detectable;		

6.16 Qualified validation service for QeSs

Qualified validation service for QeSs 26 (2)	act(s) establishing reference numbers of standards for qualified validation service referred to in paragraph 1 (compliance with point (b) of paragraph 1). 26 (1) (b) A qualified validation service for QeSs shall be provided by a QTSP who: allows relying parties to receive the result of the validation process in an automated manner which is reliable, efficient and bearing the AeS or advanced electronic seal of the provider of the qualified validation service.	**Scope:** Reference to applicable standards **Content:** • Reference to eligible standards. **Standard:** • *EN 19 441 Policy & Security Requirements for TSPs providing Signature Validation Services* *EN 19 442 Profiles for TSPs providing Signature Validation Services* • *EN 19 111:Protection Profiles for Signature Creation & Validation Applications*	6 Related articles: related: - Priority: M Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

6.17 Preservation of QeSs

Preservation of QeSs 27 (2)	act(s) concerning the further specification of the requirements laid down in paragraph 1. 27 (1) A QeS preservation service shall be provided by a QTSP who uses procedures and technologies capable of extending the trustworthiness of the QeS validation data beyond the technological validity period.	**Scope:** Definition of preservation requirements, including references to applicable standards. **Content:** • Primarily reference to eligible standards. **Standard:**	6 Related articles: related: - Priority: M Ease: M Scheduling:

		See below	<12 Iteration: 2 (1: spec., 2: standard)
Preservation of QeSs **27 (3)**	act(s) establishing reference numbers of standards for the preservation of QeSs (compliance with paragraph 1). 27 (1) A QeS preservation service shall be provided by a QTSP who uses procedures and technologies capable of extending the trustworthiness of the QeS validation data beyond the technological validity period.	**Scope:** Reference to applicable standards **Content:** • Reference to eligible standards. **Standard:** • *SR 19 522 Data Preservation Services through signing*	6 Related articles: related: - Priority: M Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

6.18 Legal effects of electronic seals

Legal effects of electronic seals **28 (6)**	act(s) concerning the definition of different security assurance levels of electronic seals referred to in paragraph 4. 28 (4) If an electronic seal security assurance level below the qualified electronic seal is required, in particular by a MS for accessing a service online offered by a public sector body on the basis of an appropriate assessment of the risks involved in such a service, all electronic seals matching at a	**Scope:** Definition of security levels **Content:** • Definition of security levels, in general terms of criteria; • Should be linked back to trusted lists, to ensure that security levels can be validated by relying parties.	6 Related articles: related: - Priority: L Ease: E Scheduling:

	minimum the same security assurance level shall be accepted.	**Standards**: See below	optional Iteration: 2 (1: spec., 2: standard)
Legal effects of electronic seal 28 (7)	act(s) establishing reference numbers of standards for the security assurance levels of electronic seals (compliance with paragraph 6). 28 (6) The Commission shall be empowered to adopt delegated acts in accordance with Art. 38 concerning the definition of different security assurance levels of electronic seals referred to in paragraph 4. 28 (4) If an electronic seal security assurance level below the qualified electronic seal is required, in particular by a MS for accessing a service online offered by a public sector body on the basis of an appropriate assessment of the risks involved in such a service, all electronic seals matching at a minimum the same security assurance level shall be accepted.	**Scope:** References to applicable standard specifying security levels **Content:** • Definition of security levels; • Should be linked back to trusted lists, to ensure that security levels can be validated by relying parties. **Standards**: Not available yet; should be developed under the M460	6 Related articles: related: - Priority: L Ease: E Scheduling: optional Iteration: 2 (1: spec., 2: standard)

6.19 Requirements for QCs for electronic seal

Requirements for QCs for electronic seal 29 (4)	act(s) concerning the further specification of the requirements laid down in Annex III. Annex III QCs for electronic seals shall contain: o an indication, at least in a form suitable for automated processing, that the certificate has been issued as a QC for electronic seal; o a set of data unambiguously representing the	**Scope:** Definition of requirements through references to standards updated through M460 **Content:** • Definition of requirements, in general terms of criteria; cf Decision 2003/511/EC.	6 Related articles: related: 21.4 Priority: H

	QTSP issuing the QCs including at least the MS in which that provider is established and – for a legal person: the name and registration number as stated in the official records, – for a natural person: person's name; o a set of data unambiguously representing the legal person to whom the certificate is issued, including at least name and registration number as stated in the official records; o electronic seal validation data which correspond to the electronic seal creation data; o details of the beginning and end of the certificate's period of validity; o the certificate identity code which must be unique for the QTSP; o the AeS or advanced electronic seal of the issuing QTSP; o the location where the certificate supporting the AeS or advanced electronic seal referred to in point (g) is available free of charge; o the location of the certificate validity status services that can be used to enquire the validity status of the QC; o where the electronic seal creation data related to the electronic seal validation data are located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.	**Standards**: See below	Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)
Requirements for QCs for electronic seal 29 (5)	act(s) establishing reference numbers of standards for QCs for electronic seal (compliance with Annex III). Annex III QCs for electronic seals shall contain: o an indication, at least in a form suitable for automated processing, that the certificate has been issued as a QC for electronic seal; o a set of data unambiguously representing the QTSP issuing the QCs including at least the MS in	**Scope:** Reference numbers for QCs for electronic seal **Content:** • Following the template of Decision 2003/511/EC. **Standard:** *Need for standard:* Y *Standard available:* N, *when:*	6 Related articles: related: 21.4. Priority: H Ease: M Scheduling:

	which that provider is established and – for a legal person: the name and registration number as stated in the official records, – for a natural person: person's name; o a set of data unambiguously representing the legal person to whom the certificate is issued, including at least name and registration number as stated in the official records; o electronic seal validation data which correspond to the electronic seal creation data; o details of the beginning and end of the certificate's period of validity; o the certificate identity code which must be unique for the QTSP; o the AeS or advanced electronic seal of the issuing QTSP; o the location where the certificate supporting the AeS or advanced electronic seal referred to in point (g) is available free of charge; o the location of the certificate validity status services that can be used to enquire the validity status of the QC; o where the electronic seal creation data related to the electronic seal validation data are located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.	*Standard ref:* • *EN 19 411 Policy & Security Requirements for TSPs Issuing Certificates; a profile for seals is needed* • *EN 19 412 Profiles for TSPs issuing Certificates; a profile for seals is needed*	<12 Iteration: 2 (1: spec., 2: standard)

6.20 Qualified electronic seal creation devices

Qualified electronic seal creation devices **30 (1)**	act(s) establishing reference numbers of standards for qualified electronic seal creation devices (compliance with Annex II). Annex II (1) QeS creation devices shall ensure, by	**Scope:** Reference numbers for QCs **Content:** • Following the template of Decision 2003/511/EC.	6 Related articles: related: -

- mutatis mutandis 22 (2)	appropriate technical and procedural means, that at least: o the secrecy of the electronic signature creation data used for electronic signature generation is assured; o the electronic signature creation data used for electronic signature generation can occur only once; o the electronic signature creation data used for electronic signature generation cannot, with reasonable assurance, be derived and the electronic signature is protected against forgery using currently available technology; o the electronic signature creation data used for electronic signature generation can be reliably protected by the legitimate signatory against use by others. Annex II (2) QeS creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing. Annex II (3) Generating or managing electronic signature creation data on behalf of the signatory shall be done by a QTSP. Annex II (4) QTSPs managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data for back-up purposes provided the following requirements are met: o the security of the duplicated datasets must be at the same level as for the original datasets; o the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.	**Standard:** *Need for standard:* Y *Standard available:* Y*; QSCD standards have been drafted to also cover QSealCD*; however, a specific profile will be needed. *Standard ref:* • *EN 19 211 Protection Profiles for Secure Signature Creation Devices* • *EN 19 221 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures* • *EN 19 212 Application Interfaces for Secure Signature Creation Devices*	Priority: H Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)
Qualified electronic seal	Qualified electronic seal creation devices may be certified by appropriate public or private bodies	**Scope:** identification of standards for security evaluation of QSealCDs	6

creation devices 30 (2) - *mutatis mutandis 23 (1)*	designated by MS provided that they have been submitted to a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in a list that shall be established by EC by means of implementing acts.	**Content:** • Following the template of Decision 2003/511/EC. **Standard:** *See below*	Related articles: related: - Priority: H Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)
Qualified electronic seal creation devices 30 (2) - *mutatis mutandis 23 (3)*	act(s) concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1. 23 (1) QeS creation devices may be certified by appropriate public or private bodies designated by MS provided that they have been submitted to a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in a list that shall be established by EC by means of implementing acts.	**Scope:** references to standards for security evaluation of QSealCDs **Content:** • Following the template of Decision 2003/511/EC. **Standard:** *Need for standard:* Y *Standard available:* Y. *QSCD standards have been drafted to also cover QSealCD:* *Standard ref:* • EN 19 203: Conformity Assessment of Secure Devices and Trustworthy systems	6 Related articles: related: - Priority: H Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)
Qualified electronic seal creation devices 30 (3) - *mutatis mutandis 24 (3)*	act(s) defining circumstances, formats and procedures applicable for the purpose of paragraph 1. 24 (1) MS shall notify to EC without undue delay, information on QSCDs which have been certified by the bodies referred to in Art. 23. They shall also notify to EC, without undue delay, information on electronic signature creation devices that would no	**Scope:** circumstances, formats and procedures for the publication of lists of certified QSealCDs. **Content:** • As per Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC, modified to be applied to QSealCDs, rather than	4 related: §13.5 Priority: H Ease: E Scheduling:

	longer be certified. 23 (1) QSCDs may be certified by appropriate public or private bodies designated by MS provided that they have been submitted to a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in a list that shall be established by EC by means of implementing acts.	TSPs; **Standard:** *Need for standard:* Y, if machine processable lists are desired (as recommended by CROBIES) *Standard available:* N. The basic trusted list standard can be used, but a specific profile for QSealCDs would need to be developed under M460. CROBIES inputs can be used as a starting point for this work, building on: • *EN 19 602 Trust Service Status Lists Format* • *EN 19 612 Trusted List Format* • *For historical reference: ETSI TS 102 231, implemented as through the Decisions above*	ASAP Iteration: 1

6.21 Validation and preservation of qualified electronic seals

Validation and preservation of qualified electronic seals 31 ***- mutatis mutandis 25 (2)***	act(s) concerning the further specification of the requirements laid in down in paragraph 1. 25 (1) A QeS shall be considered as valid provided that it can be established with a high level of certainty, that at the time of signing: o the certificate, that supports the signature, is a QeS certificate complying with the provisions laid down in Annex III; o the QC required is authentic and valid; o the signature validation data correspond to the data provided to the relying party; o the set of data unambiguously representing the signatory is correctly provided to the relying party; o the use of any pseudonym is clearly indicated to	**Scope:** Definition of validation requirements, including references to applicable standards. **Content:** • Primarily reference to eligible standards. **Standard:** *See below*	6 Related articles: related: 25.2 Priority: M Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

	the relying party if a pseudonym is used; o the electronic signature was created by a QSCD; o the integrity of the signed data has not been compromised; o the requirements provided for in Art. 3 point 21 are met; o the system used for validating the signature provides to the relying party the correct result of the validation process and allows the relying party to detect any security relevant issues. Annex III QCs for electronic seals shall contain: o an indication, at least in a form suitable for automated processing, that the certificate has been issued as a QC for electronic seal; o a set of data unambiguously representing the QTSP issuing the QCs including at least the MS in which that provider is established and – for a legal person: the name and registration number as stated in the official records, – for a natural person: person's name; o a set of data unambiguously representing the legal person to whom the certificate is issued, including at least name and registration number as stated in the official records; o electronic seal validation data which correspond to the electronic seal creation data; o details of the beginning and end of the certificate's period of validity; o the certificate identity code which must be unique for the QTSP; o the AeS or advanced electronic seal of the issuing QTSP; o the location where the certificate supporting the AeS or advanced electronic seal referred to in point (g) is available free of charge; o the location of the certificate validity status services that can be used to enquire the validity status of		

	the QC; o where the electronic seal creation data related to the electronic seal validation data are located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing. 3 (21) 'advanced electronic seal' means an electronic seal which meets the following requirements: (a) it is uniquely linked to the creator of the seal; (b) it is capable of identifying the creator of the seal; (c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable;		
Validation and preservation of qualified electronic seals 31 ***- mutatis mutandis 25 (3)***	act(s) establishing reference numbers of standards for the validation of qualified electronic seals (compliance with paragraph 1). 25 (1) A QeS shall be considered as valid provided that it can be established with a high level of certainty, that at the time of signing: o the certificate, that supports the signature, is a QeS certificate complying with the provisions laid down in Annex III; o the QC required is authentic and valid; o the signature validation data correspond to the data provided to the relying party; o the set of data unambiguously representing the signatory is correctly provided to the relying party; o the use of any pseudonym is clearly indicated to the relying party if a pseudonym is used; o the electronic signature was created by a QSCD;	**Scope:** Reference to applicable standards **Content:** • Reference to eligible standards. **Standard:** *QS standards have been drafted to also cover QSeals:* • *EN 19 101: Policy and Security Requirements for Electronic Signature Creation and Validation* • *EN 19 102: Procedures for Signature Creation and Validation* • *EN 19 111:Protection Profiles for Signature Creation & Validation Applications*	6 Related articles: related: 25.3 Priority: M Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

	o the integrity of the signed data has not been compromised; o the requirements provided for in Art. 3 point 21 are met; o the system used for validating the signature provides to the relying party the correct result of the validation process and allows the relying party to detect any security relevant issues. Annex III QCs for electronic seals shall contain: o an indication, at least in a form suitable for automated processing, that the certificate has been issued as a QC for electronic seal; o a set of data unambiguously representing the QTSP issuing the QCs including at least the MS in which that provider is established and – for a legal person: the name and registration number as stated in the official records, – for a natural person: person's name; o a set of data unambiguously representing the legal person to whom the certificate is issued, including at least name and registration number as stated in the official records; o electronic seal validation data which correspond to the electronic seal creation data; o details of the beginning and end of the certificate's period of validity; o the certificate identity code which must be unique for the QTSP; o the AeS or advanced electronic seal of the issuing QTSP; o the location where the certificate supporting the AeS or advanced electronic seal referred to in point (g) is available free of charge; o the location of the certificate validity status services that can be used to enquire the validity status of the QC; o where the electronic seal creation data related to		

	the electronic seal validation data are located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing. 3 (21) 'advanced electronic seal' means an electronic seal which meets the following requirements: (a) it is uniquely linked to the creator of the seal; (b) it is capable of identifying the creator of the seal; (c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable;		
Validation and preservation of qualified electronic seals 31 ***- mutatis mutandis 26 (2)***	act(s) establishing reference numbers of standards for qualified validation service referred to in paragraph 1 (compliance with point (b) of paragraph 1). 26 (1) (b) A qualified validation service for qualified electronic seals shall be provided by a QTSP who: allows relying parties to receive the result of the validation process in an automated manner which is reliable, efficient and bearing the AeS or advanced electronic seal of the provider of the qualified validation service.	**Scope:** Reference to applicable standards **Content:** • Reference to eligible standards. **Standard:** *QS standards have been drafted to also cover QSeals:* • *EN 19 441 Policy & Security Requirements for TSPs providing Signature Validation Services* *EN 19 442 Profiles for TSPs providing Signature Validation Services* • *EN 19 111:Protection Profiles for Signature Creation & Validation Applications*	6 Related articles: related: 26.2 Priority: M Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

Validation and preservation of qualified electronic seals 31 ***- mutatis mutandis 27 (2)***	act(s) concerning the further specification of the requirements laid down in paragraph 1. 27 (1) A qualified electronic seal preservation service shall be provided by a QTSP who uses procedures and technologies capable of extending the trustworthiness of the qualified electronic seal validation data beyond the technological validity period.	**Scope:** Definition of preservation requirements, including references to applicable standards. **Content:** • Primarily reference to eligible standards. **Standard:** *See above*	6 Related articles: related: 27.2 Priority: M Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)
Validation and preservation of qualified electronic seals 31 ***- mutatis mutandis 27 (3)***	act(s) establishing reference numbers of standards for the preservation of qualified electronic seals (compliance with paragraph 1). 27 (1) A QeS preservation service shall be provided by a QTSP who uses procedures and technologies capable of extending the trustworthiness of the QeS validation data beyond the technological validity period.	**Scope:** Reference to applicable standards **Content:** • Reference to eligible standards. **Standard:** • *SR 19 522 Data Preservation Services through signing*	6 --- Related articles: related: 27.3 --- Priority: M Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

6.22 Requirements for qualified electronic time stamps

Requirements for qualified electronic time stamps **33 (2)**	act(s) establishing reference numbers of standards for the accurate linkage of time to data and an accurate time source (compliance with paragraph 1). 33 (1) A qualified electronic time stamp shall meet the following requirements: o it is accurately linked to Coordinated Universal Time (UTC) in such a manner as to preclude any possibility of the data being changed undetectably; o it is based on an accurate time source; o it is issued by a QTSP; o it is signed using an AeS or an advanced electronic seal of the QTSP, or by some equivalent method.	**Scope:** Reference numbers for qualified time stamps **Content:** • Following the template of Decision 2003/511/EC. **Standard:** *Need for standard:* Y *Standard available:* Y, *when:* *Standard ref:* • *EN 19 231 Security requirements for trustworthy systems supporting time-stamping* • *EN 19 421 Policy & Security Requirements for TSPs providing Time-Stamping Services* • *EN 19 422 Profiles for TSPs providing Time-Stamping Services*	6 Related articles: related: 22.2 Priority: H Ease: M Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

6.23 Legal effects and acceptance of the electronic documents

Legal effects and acceptance of the electronic documents **34 (4)**	act(s) defining formats of electronic signatures and seals that shall be accepted whenever a signed or sealed document is requested by a MS for the provision of a service online offered by a public sector body referred to in paragraph 2. 34 (2) A document bearing a QeS or a qualified electronic seal of the person who is competent to issue the relevant document, shall enjoy legal	**Scope:** Definition of signature formats and seals that should mandatorily be accepted by public services, comparable to the Decision of 25 February 2011 2011/130/EU establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities	6 Related articles: related: - Priority: H

	presumption of its authenticity and integrity provided the document does not contain any dynamic features capable of automatically changing the document.	**Content:** • Can be large reprised from Decision 2011/130/EU, i.e. mainly a reference to the acceptable formats **Standard:** *Need for standard:* Y *Standard available:* Y *Standard ref:* • EN 19 132: XML Advanced Electronic Signatures (XAdES) • EN 19 122: CMS Advanced Electronic Signatures (CAdES) • EN 19 142: PDF Advanced Electronic Signatures (PAdES) • EN 19 152: Advanced Electronic Signatures in Mobile Environments • EN 19 162: Associated Signature Containers (ASiC)	Ease: E Scheduling: <12 Iteration: 2 (1: spec., 2: standard)

6.24 Legal effect of an electronic delivery service

Legal effect of an electronic delivery service 35 (3)	act(s) concerning the specification of mechanisms for sending or receiving data using electronic delivery services, which shall be used with a view to fostering interoperability between electronic delivery services.	**Scope:** Definition of mechanisms applicable to electronic delivery services (EDS). Note that this paragraph refers to all EDS, not only to QEDS **Content:** Can be based on art. 36 (which relates to QEDS),	7 Related articles: related: - Priority: optional

		but should be technology neutral • Procedural requirements with respect to the confirmation of the identity of the sender and recipient • Procedural requirements with respect to the confirmation of the time of sending and receipt of the payload • Logging/retention obligations in relation to the communication stream • Data protection compliance (data minimization, privacy by design, no logging of payload) • High level requirements Responsibilities/liabilities of EDS • Legal effect/value, likely in terms of validity as proof of sending/receipt **Standard:** *Need for standard:* N, unless the delegated act wants to create interoperability between a specific implementation of EDSes in accordance with a specific standard/format choice (e.g. certain signatures, timestamps, communication protocals, etc.); in this case, references to applicable standards may be inevitable.	Ease: D Scheduling: optional Iteration: 2 (1:act, 2:standard, if any)

6.25 Requirements for qualified electronic delivery services

Requirements for qualified electronic delivery	act(s) establishing reference numbers of standards for processes for sending and receiving data (compliance with paragraph 1).	**Scope:** Reference numbers for QEDS **Content:**	7 Related articles:

services 36 (2)	36 (1) Qualified electronic delivery services shall meet the following requirements: o they must be provided by one or more QTSP(s); o they must allow the unambiguous identification of the sender and if appropriate, the addressee; o the process of sending or receiving of data must be secured by an AeS or an advanced electronic seal of QTSP in such a manner as to preclude the possibility of the data being changed undetectably; o any change of the data needed for the purpose of sending or receiving the data must be clearly indicated to the sender and addressee of the data; o the date of sending, receipt and any change of data must be indicated by a qualified electronic time stamp; o in the event of the data being transferred between two or more QTSPs, the requirements in points (a) to (e) shall apply to all the QTSPs.	• Reference to applicable standards. **Standard:** *Need for standard:* Y *Standard available:* Y. Further study is currently on-going via SR 19 530 Study on standardisation requirements for e-Delivery services applying e-Signatures *Standard ref:* • EN 19 511 Policy & Security Requirements for Registered Electronic Mail (REM) Service Providers	related: 35 Priority: optional Ease: D Scheduling: optional Iteration: 2 (1: spec., 2: standard)

6.26 Requirements for QCs for website authentication

Requirements for QCs for website authentication 37 (3)	act(s) concerning the further specification of the requirements laid down in Annex IV. Annex IV QCs for website authentication shall contain: o an indication, at least in a form suitable for automated processing, that the certificate has been issued as a QC for website authentication; o a set of data unambiguously representing the QTSP issuing the QCs including at least the MS in which that provider is established and – for a legal person: the name and registration number as stated in the official records,	**Scope:** Further details of QC for website authentication **Content:** • If adopted, the primary clarifications relate to the contents of the QC, notably specifying more explicitly which data should be used to unambiguously represent the QTSP and the holder of the QC (name and registration number, address info, etc). **Standard:**	7 Related articles: related: Priority: optional Ease: M Scheduling: optional Iteration: 2

	– for a natural person: person's name; o a set of data unambiguously representing the legal person to whom the certificate is issued, including at least name and registration number as stated in the official records; o elements of the address, including at least city and MS, of the legal person to whom the certificate is issued as stated in the official records; o the domain name(s) operated by the legal person to whom the certificate is issued; o details of the beginning and end of the certificate's period of validity; o the certificate identity code which must be unique for the QTSP; o the AeS or advanced electronic seal of the issuing QTSP; o the location where the certificate supporting the AeS or advanced electronic seal referred to in point (h) is available free of charge; o the location of the certificate validity status services that can be used to enquire the validity status of the QC.	*Need for standard:* see below	(1: spec., 2: standard)
Requirements for QCs for website authentication 37 (4)	act(s) establishing reference numbers of standards for QCs for website authentication (compliance with Annex IV). Annex IV QCs for website authentication shall contain: o an indication, at least in a form suitable for automated processing, that the certificate has been issued as a QC for website authentication; o a set of data unambiguously representing the QTSP issuing the QCs including at least the MS in which that provider is established and – for a legal person: the name and registration number as stated in the official records, – for a natural person: person's name; o a set of data unambiguously representing the legal	**Scope:** Reference numbers for QC for website authentication **Content:** • Reference to applicable standards. **Standard:** *Need for standard:* Y *Standard available:* Y, although further work might be required; cf. below. *Standard ref:* • EN 19 411 Policy & Security Requirements for TSPs Issuing Certificates	7 Related articles: related: 37.3 Priority: optional Ease: D Scheduling: optional Iteration: 2 (1: spec., 2: standard)

	person to whom the certificate is issued, including at least name and registration number as stated in the official records; o elements of the address, including at least city and MS, of the legal person to whom the certificate is issued as stated in the official records; o the domain name(s) operated by the legal person to whom the certificate is issued; o details of the beginning and end of the certificate's period of validity; o the certificate identity code which must be unique for the QTSP; o the AeS or advanced electronic seal of the issuing QTSP; o the location where the certificate supporting the AeS or advanced electronic seal referred to in point (h) is available free of charge; o the location of the certificate validity status services that can be used to enquire the validity status of the QC.	• EN 19 412 Profiles for TSPs issuing Certificates; however, a specific profile for website authentication under this standard would need to be developed	

Acronyms:

AeS Advanced electronic Signature
EC European Commission
MS Member State
QC Qualified Certificate
QeS Qualified electronic Signature
QSCD Qualified electronic Signature Creation Device
QTS Qualified Electronic Trust Service
QTSP Qualified Electronic Trust Service Provider
SB Supervisory Body
SCD Electronic Signature Creation Device
STD Standard
TS Electronic Trust Service
TSP Electronic Trust Service Provider

7. Economic, social and environmental impact of a European framework for ancillary services

7.1 Introduction

7.1.1 Context and objectives of the study

Electronic communication and electronic services, such as e-commerce and e-delivery, necessitate ancillary trust services allowing data authentication and information security. Network and information security should be understood as one of the crucial elements of the information society enabling smooth development and deployment of new systems, applications and electronic services. However, security problems persist. The increasing use of the Internet and electronic services are linked with fraud issues and cybercrime.

At the moment, eSignatures are recognised through the EU Directive 19999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures, which aims to harmonise the internal market for eSignature services. The identification, authentication and signature (IAS) components related to identity and the ancillary services (time stamping, long term preservation of signatures, e-seal, admissibility of e-documents, registered e-delivery, legal persons' website authentication and the "I accept" button) as such, have not received the same treatment at the European Union level.

Divergent rules with respect to legal recognition of the ancillary services and the accreditation of certification service providers in the EU Member States may create a significant barrier to the use of electronic communication and other electronic services. A clear European framework regarding the conditions applying to these ancillary services could strengthen confidence in, and general acceptance of, new technologies. Promotion of interoperability is seen as an essential requirement for acceptance within the market.

Against this background, the European Commission has asked the IAS Study Team in a meeting on Thursday 23 February 2012 to assess the potential impact of the inclusion of the seven ancillary services in EU Directive 19999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures (hereafter "the Directive"). This assignment is part of the IAS study work.

This document presents the results of our work.

7.1.2 Overview of ancillary services

We present a short overview of the seven ancillary services that are in scope of this study.

a. Time stamping

An "electronic time stamp" is data in electronic form which indicate the time when such data was created.

A "qualified electronic time stamp" is an electronic time stamp, signed using an advanced electronic signature or other equivalent methods of authentication, linked to e.g. the Greenwich time in such a manner as to preclude the possibility of changing the data undetectably.

b. Long term preservation of signatures

Long term preservation of signatures is the transformation of the signature and if required the signed document in such a way that it can be validated after expiration of original signature algorithms or certificates. This is required because electronic signatures are often used to sign documents such as contracts that have an expiry date after the expiry date of the key with which the document is signed. Without long term preservation of signatures, any attempt to validate the signatures after the expiry date of the key would not be guaranteed.

c. E-seals

An "electronic seal" is data in electronic form which are attached to or logically associated with other electronic data and which ensure the integrity of a document and link the legal person to which the seal is issued to the document.

A "qualified electronic seal" is an electronic seal which is based on a qualified certificate which is solely dedicated to the support of electronic seal.

d. Admissibility of native e-documents/ admissibility of e-documents resulting from the scanning of paper documents

There should be no discrimination in the admissibility of native e-documents or e-documents resulting from the scanning of documents that were originally paper-based. In order to permit such admissibility, it should be possible to guarantee that the original document is functionally and semantically identical to the document submitted.

e. Certified electronic delivery

A "certified electronic delivery" is a service that enables to transmit data by electronic means and provides evidence relating to the handling of the data including proof of submission and delivery and protects transferred data against the risk of loss, theft, damage or any alterations.

f. Legal persons' website authentication

A legal person's website authentication, or "web authentication certificate" implies a certificate which allows a website user to instantly ascertain that such website is secure and linked to a certain legal person.

We position ancillary services in the value chain of eSignatures on the Supply Side, as illustrated in the figure below.

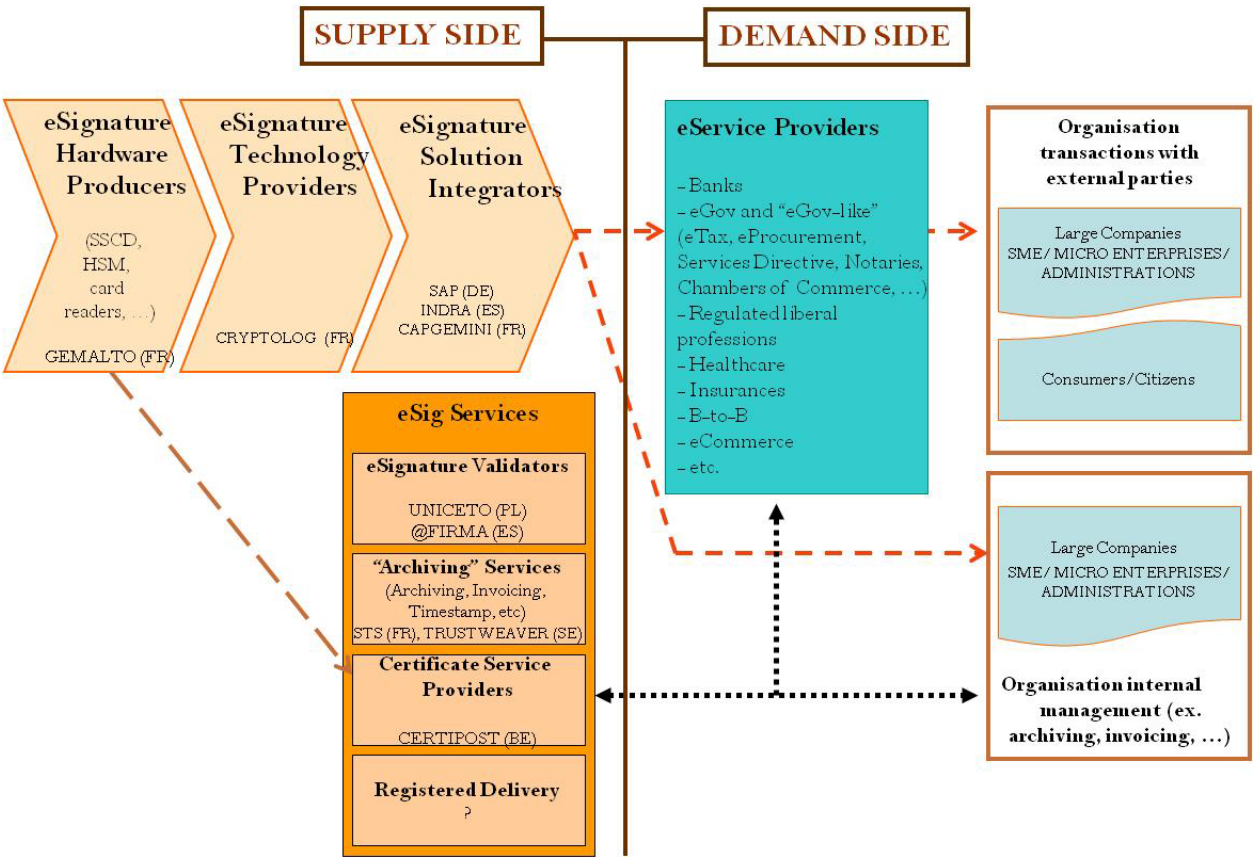


Figure 1 - Supply and Demand Side of eSignatures (source: EC DG INFSO)

In the following sections of this document, we first present the methodology and protocols that have guided our research. Next, we present the results of our research.

7.2 Drawing up the conceptual framework for REA

7.2.1 REA-question

We used the so-called "PICO" acronym to confirm the research question that guides the REA.

1. **Population**
   - o Businesses
   - o Public authorities
   - o Citizens

2. **Intervention**
   The inclusion of each of the seven ancillary services (time stamping, long term preservation of signatures, e-seal, admissibility of e-documents, registered e-delivery and legal persons' website authentication) in EU Directive 19999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures.

3. **Comparison**
   "As is" situation: no inclusion of ancillary services in EU Directive 19999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures.

4. **Outcome**
   - o Economic impact, e.g. compliance cost and simplification potential, fraud prevention, economic growth (including the fostering of innovation and R&D)
   - o Social impact, e.g. safety and security
   - o Environmental impact, e.g. raw materials (paper)

Based on the PICO acronym and the original briefing we received from the European Commission, the following REA question was established:

> *What is the economic, social and environmental impact of an increased use of ancillary services on businesses, public authorities and citizens, as a consequence of the inclusion of such ancillary services in the successor regulation of the EU Directive 19999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures?*

7.2.2 Search process

a. Criteria for excluding and including studies

- o Geographic scope: All developed countries (OECD countries with focus on European Member States (27), the United States and Australia)

- Date of publication: Published after 2006
- Language of publication: Focus on English documentation which is publicly available
- Research methods: All methods with equal attention to empirical (academic) studies and policy evaluation / impact studies

b. Terms for searching for relevant literature

A list of search terms was developed in order to search the relevant databases in an efficient manner:

- Ancillary services: time stamping, long term preservation of signatures, e-seal, admissibility of e-documents, registered e-delivery and legal persons' website authentication; and different variants for each of the 7 services
- Digital signature(s)
- Security software
- ICT security
- Internet fraud
- Cybercrime
- Dematerialization
- Digital economy
- Economic/social/environmental impact, effectiveness, efficiency, evaluation

c. Sources that will be searched

We included a number of important electronic databases and other sources:

- Large scale pilot projects: These projects are largely run with and/or by EU Member States. The pilot projects typically develop practical solutions for cross-border government services, which are tested in real government service cases across Europe.
- European Commission Impact Assessments.
- Publications of Agoria (the technology federation of Belgium).
- Academic library and electronic databases (through University of Ghent)
  - LibHub, the search interface to most e-articles available at Ghent University. It contains articles of the most important scholarly journal publishers (Elsevier, Wiley, Taylor&Francis, ...), aggregators (Highwire, Jstor, Project Muse, ...) and several open access repositories (arxiv, Citeseer, UGent biblio, ...).
  - Electronic databases:
  - IEEE Xplore: Database of technical literature in engineering and technology
  - Elsevier: Provider of science and health information
  - Citeseer: Scientific literature digital library
  - Springer: International publisher of science, technology and medicine
  - Sociological Abstracts: Database with international literature in sociology and related disciplines in the social and behavioural sciences
  - EconLit: Source of references to economic literature
  - Web of Science – Web of Knowledge: Research platform for information in the sciences, social sciences, arts and humanities
  - OECD: Database with information in the environment, human health and safety

- World bank documentation and reports: Database with operational documents (project documents, analytical and advisory work, and evaluations), formal and informal research papers and most World Bank publications.
- Social Science Research Network (SSRN): Devoted to the rapid worldwide dissemination of social science research and is composed of a number of specialized research networks in each of the social sciences.

- PwC knowledge exchange: Internal, global PwC knowledge database for information requests.

d. Terms for sorting/describing literature

The findings will be described and sorted, using the following structure:

- Title/ Author/ Date/ Publication;
- Population (businesses, public authorities, citizens);
- Purpose of the study;
- Main findings;
- Critical role of ancillary services.

7.2.3 Research findings

a. Large Scale Pilots (LSPs)

LSP	Peppol (Pan European Public Procurement Online)
Consortium	The PEPPOL consortium is comprised of seventeen partners (mostly leading public eProcurement agencies) within 11 countries: Austria, Denmark, Finland, France, Germany, Greece, Italy, Norway, Portugal, Sweden and the United Kingdom.
Date	2008 – currently running
Source	PEPPOL website[30] and additional documents such as technical specifications about WebNotarius and factsheets for economic operators, contracting authorities and ICT-industry
Purpose of study	Initiated in 2008, the Pan-European Public Procurement Online (PEPPOL) project has been developing and implementing the technology standards to align business processes for electronic procurement across all governments within Europe, aiming to expand market connectivity and interoperability between eProcurement communities.
Main findings	**Benefits for contracting authorities** o Improved market access, particularly for SMEs (small and medium enterprises), increases competition and lowers costs o Greater transparency increases public accountability and reduces potential for corruption o Automated procurement speeds up administrative activities and reduces costs o Streamlined processes facilitate faster transition to green, sustainable purchasing o Enhanced exports by national businesses increase the tax base **Benefits for economic operators** By breaking down barriers to allow seamless electronic communication across borders and communities, PEPPOL offers significant benefits to suppliers wishing to trade with the public sector: o Improved access to tenders across borders increases business potential

[30] http://www.peppol.eu/

- Greater transparency increases public accountability
- Automated procurement speeds up administrative activities and reduces costs
- Electronic communication results in immediate processing of invoices and improved cash flow
- Once connected to PEPPOL's network, suppliers can communicate easily to everyone within the PEPPOL community – thereby enhancing efficiency and business prospects

Benefits for IT industry

As the sector most likely to use eProcurement for public tenders today, ICT solutions and service providers (and other industry sectors in future) will realise further efficiency gains and cost savings as more contracting authorities move to eProcurement. Those firms working with PEPPOL will also be presented with a number of business opportunities:

- Widespread PEPPOL adoption will create significant additional demand for more advanced IT services and more service transactions.
- First movers will gain valuable experience with PEPPOL standards and will have an advantage in securing early implementation contracts.
- Expertise in PEPPOL standards will add capabilities to their portfolio of offerings.

The PEPPOL eSignature Validation Infrastructure provides contracting authorities with the ability to validate digital signature certificates cross border.

Electronic signatures based on electronic certificates are in common use already. They allow the secure identification of the sender of a document and ensure that a document has not been modified. PEPPOL aims to create interoperability between the different national schemes, so that in practice a public sector entity can validate certificates issued in other member states, allowing for electronic submission of tenders cross borders.

Government purchases in the European Union account for an estimated 19% of GDP, or €2.2B annually. Currently, less than 5% of total procurement budgets are awarded electronically, and only 1.6% of contracts are supplied by an entity in another Member State. It is estimated that if eProcurement is adopted by all European contracting authorities, annual savings could exceed €50B.

Critical role of ancillary services	The PEPPOL components support the eProcurement process from eSourcing to ePayment.

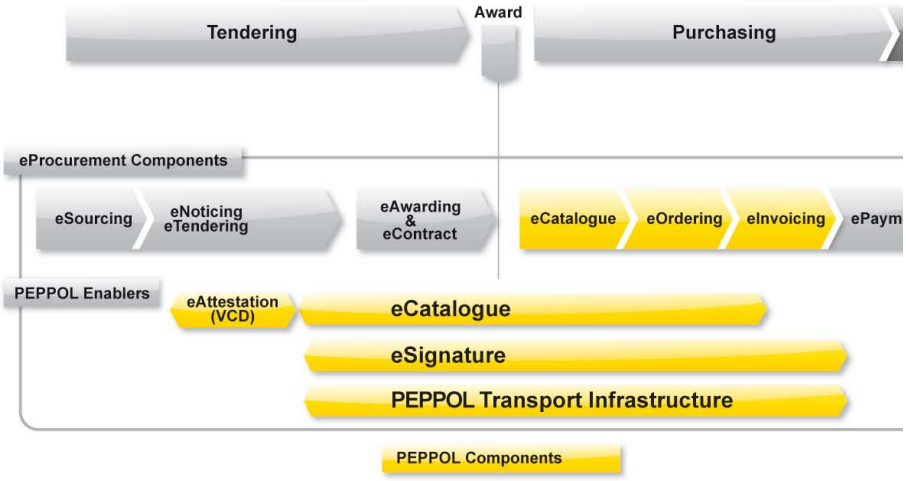


Figure 2 - PEPPOL components

eSignature is a core component in the scheme. eSignatures identify companies or single persons, allowing the receiver of a document to confirm the identification of the sender (authenticity) and provide assurance that the document has not been modified in transit (integrity). PEPPOL's vision is to create interoperability between the different national schemes, so that a contracting authority can validate certificates issued in other EU member states, enabling electronic submission of tenders across borders. This means that an economic operator (supplier) can use the eSignature of its choice when submitting an offer to any public sector awarding entity.

PEPPOL addresses specific problems relating to the creation, verification and acceptance of eSignatures accompanying eProcurement documents, to enable cross border signature validation. The PEPPOL validation infrastructure consists of a network of federated validation services, able to validate qualified signature certificates from trusted certification authorities according to the national 'Trusted Services List' (TSL) and also non-qualified certificates as long as they are accepted in certain procurement domains.

Use of the eSignature validation software is not mandatory for organisations piloting PEPPOL components. However, it is a valuable add-on service and has application beyond PEPPOL to any 'trust model' that comprises various certification authorities. The eSignature verification service is also independent of the PEPPOL transport infrastructure. To realise this vision, the PEPPOL project deliverables include a.o. XKMS and OASIS DSS interface specifications, architecture and trust models, and a trans-national verification system (prototype).

For validation, PEPPOL makes a.o. use of WebNotarius for an electronically signed and time stamped confirmation. WebNotarius supports all popular signature standards (PKCS 7, CMS, Sig, S/MIME, XML dsig, CAdES, Xades, PAdes), and uses the de-facto standards for validation (TSL, OCSP, CRL, deltaCRL, ARL, DVCS, LDAP, SCVP, XKMS).

The following Information is provided during the eSignature verification process: verification result, the date and time of verification, name of the document under which the signature was verified, signatures related to the particular electronic document, certificate or certificates verifying given electronic signature, reason, in case of incorrect verification and reason for signature/signatures verified as negative .

As such it is obvious that ancillary services (time stamping, long time preservation) play a critical role in the delivery of PEPPOL services and scenarios.

LSP	e-Codex (e-Justice Communication via Online Data Exchange)
Consortium	Austria, Belgium, Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Malta, The Netherlands, Portugal, Romania, Spain, Turkey, CCBE and CNUE
Date	December 2010 - December 2013
Source	E-CODEX website[31] and additional documents such as deliverable 4.1 and e-Codex newsletter[32]
Purpose of study	Improving the cross-border access of citizens and businesses to legal means in Europe as well as improving the interoperability between legal authorities within the EU
Main findings	**Benefits for citizens** The project will result in a smoother cross-border operation of several judicial services. **Benefits for legal community** A strong future collaboration between the legal community and the e-CODEX project will empower the legal community in relation to both judicial authorities as well as EU citizens. By implementing the e-CODEX project, the legal community will facilitate the spread and usage of the instruments adopted in the European judicial area for all of Europe's citizens. This way the judicial services will not be limited to a national level, but instead be able to operate all over Europe. This will reinforced the administrative and judicial cooperation in the field of Justice and Internal Affairs. Increasing claims by e-Justice Nowadays not very often citizens and companies take small cross-border claims to court for the complexity and the inaccessibility. By digitalizing the legal cross-border process, the way to file a claim will be simplified. **Benefits for IT industry** The IT industry is an important reference group to consult for e-CODEX in this Large Scale Project. The IT industry is invited to support e-CODEX. This support can range from business advice to helping to improve processes or providing technical support in delivering technology. **Benefits for standard bodies**

[31] www.e-codex.eu/

[32] http://www.e-codex.eu/index.php/component/acymailing/archive/view/mailid-12/key-62868e9b0ad4fae911bc6bc640716d87/subid-3-47a0d68e35df6545004013ae54cedd52/tmpl-component#e-Signature

	There will be opportunities for both parties to become engaged in sharing experiences and developing different categories of services - including, but not necessarily limited to, potential e-Justice services. More than that, the contribution of the Standard Bodies will be seen as valuable since they will add legitimacy in setting up policies in a specific field of activity.
Critical role of ancillary services	The broader vision of the project is that any citizen and/or legal professional in the EU can communicate electronically with any legal authority, including communication of legal authorities with each other. Services which will need to be developed are the ones which allow data exchange in the area of eJustice between the Member States. Time stamping is clearly indicated as a requirement, as specified in the e-CODEX deliverable “D 4.1 e-Identity: Inventory and requirements”. As specified on the e-CODEX website, Security and privacy are of serious concern for the project. To ensure these aspects and to prevent identity theft, e-CODEX does not only rely on and follow the developments within the currently known security- and transportation standards but involves studies commissioned by the European Commission and the experience of approved large scale projects like STORK, SPOCS and PEPPOL. The observed standards could for example be ebXML in case of transportation and WS-* and SAML in case of different security aspects. As such it is eminent that ancillary services (particularly time stamping, long term preservation and e-seals) are important for e-CODEX.

LSP	SPOCS (Simple Procedures for Online Cross-Border Services)
Consortium	Austria, France, Germany, Greece, Italy, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Sweden, United Kingdom
Date	2009-2012
Source	SPOCS website[33] and additional documents such as factsheets
Purpose of study	Businesses seeking to expand into other countries often struggle to comply with all the regulations they need to follow. Applying for licences, permits and completing other administrative procedures in another country can be complicated. SPOCS is a project that aims to overcome those obstacles
Main findings	**Added value for citizens** SPOCS will contribute to: o Fostering competitiveness o Achieving greater interoperability o Streamlining electronic procedures o Gaining efficiency in administrative simplification and modernisation o Improving usability and attractiveness of PSCs o Increasing transparency and user-friendliness of procedures for service providers and service recipients o Increasing cross-border activities o Stimulating cross-border cooperation between Member States o Reducing misuse/ fraud **Added value for public administrations** o Administrative simplification and modernisation will enable you to save money and use your resources more efficiently o Improve efficiency of cross border cooperation between Member States o Increase cross border activities o Increase user friendliness of public administration and improve administrative processes

[33] www.eu-spocs.eu/

- Improve usability and attractiveness of PSC in your country
- Promote growth and competitiveness of EU services and industry
- Achieve interoperability

Added value for IT

- Creates demand for IT Products and services by public authorities and opportunities for businesses.
- Provides jointly developed, tested, scalable and quality assured software that can be re-used by everyone a free of license costs.
- Allows to create new software products or add value to existing ones by re-using SPOCS modules without license fees.
- Is stimulating the demand for next generation PSC solutions in a potentially large market of 16 countries that participate in SPOCS.
- Will motivate public authorities to invite private businesses to support them. This may range from business advice like improving processes and organisations to technical support e.g. delivering technology.
- Will encourage member states to improve the e-government capabilities of Points of Single Contact and competent authorities thus increasing the demand for IT products and services
- Supports product development as it produces specifications and software components that private companies can turn into commercial products, add value to and offer customers in the public sector.
- All results of SPOCS are open and available under EU Public License without license fees. gives you access to the latest information about building blocks for interoperable e-government services.
- Has set up a number of groups that bring potential buyers and suppliers of ICT products and services together.
- Can create spill-over effects that create additional demand for products and services beyond SPOCS.

Added value for business representatives

SPOCS will provide solutions that, among others, will allow:

- Information to be provided to the service provider that will combine information gathered from different Member States i.e. processes in one Member State related with documents from another.
- Submission of electronic documents from different Member States that can be easily checked for their validity and their suitability.
- Automatic retrieval of documents from a source of authentic documents in another Member State.

- Provision of a secure communication channel from the Point of Single Contact of one Member
- State to the service provider of another Member State with all the acknowledgment receipts required by law.

Availability of e-Services from your own country's online portal through the destination country's portal.

Critical role of ancillary services

The building blocks of SPOCS are syndication, eDocumentation, eDelivery, eSafe and eService. For each of these building blocks, identification, authentication and signature will be important. Ancillary services, such as time stamping, will contribute to this.

Project deliverables such as "Specifications for interoperable access to eDelivery and eSafe systems - Appendix 1: Security Architecture Development Process" clearly indicate that timestamps are required for making it obvious when the document was signed, as well as for indicating the timing of events in audit logs. Audit records should also have reliable timestamps to make chronological reconstruction reliable.

This is further supported by "Specifications for interoperable access to e-Delivery and e-Safe systems – Appendix 2 Trust Service Status List Profiling ("SPOCS-TSL"), as well as "Appendix 6 Security Model".

Furthermore, eDelivery is explicitly specified as a building block.

As such it is obvious that ancillary services (particularly time stamping, certified electronic delivery) are required for continuing the successful deployment of SPOCS.

LSP	STORK
Consortium	The project includes 18 countries, with a total of 35 consortium partners. The consortium is a mix of public and private sector organisations.
Date	Currently running
Source	STORK website[34]
Purpose of study	The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. Cross-border user authentication for such e-relations will be applied and tested by the project by means of five pilot projects that will use existing government services in EU Member States. In time however, additional service providers will also become connected to the platform thereby increasing the number of cross-border services available to European users.
Main findings	STORK has tested cross-border services in six areas such as Cross-border Electronic Services, SaferChat, Student Mobility, Electronic Delivery (secure online delivery of documents), Change of Address and European Commission Authentication Service (ECAS). **Benefits for citizens** The STORK project makes it easier for citizens to access online public services across borders by implementing Europe-wide interoperable cross border platforms for the mutual recognition of national electronic identity (eID) between participating countries **Benefits for e-government** o People will be able to authenticate themselves securely and easily to access online Government services across Europe, using their national eID system. o The secure access to administrative formalities will make easier to move, live and work in different EU countries. o People will be able to use cross-border services over the Internet without the need to visit the country in advance. o The security of on-line transactions will be strengthened through increased use of eID services to authenticate users. o Secure interoperable eID authentication will encourage the growth of online services. o Common specifications at EU level will reduce the costs of

[34] www.eid-stork.eu

implementing eID services.

- Interoperable eID authentication is a key enabler for the EU Services Directive and Digital Agenda, helping Member States to set up single points of contact for access to Government services.

Critical role of ancillary services

Today, the European Commission provides various A2A services with restricted access rights. Currently, these are often handled by a rather insecure system using e-mails, usernames and PIN/passwords. With the Service Directive in particular, Europe is facing a major eID challenge.

A2A services of common interest that could benefit from an improved IAS solution include:

- Internal Market Information System (IMI)
- Communication and information resource centre for administrations
- Business and Citizens (CIRCABC)
- Electronic exchange of social security information (EESSI)
- DG SANCO Reference Database System (SANREF)
- Consumer Protection Cooperation System (CPCS)
- LISFLOOD-Alert
- European Competition Network – Electronic Transmission (ECN-ET)
- European Database for Medical Devices (EUDAMED)
- Secure Exchange and Storage of Agricultural Data (SESAD)

This list of services does of course not pretend to be exhaustive.

It is obvious that having an EU-wide STORK or STORK-like deployed solution, would help address the Europen eID challenge, particularly with regard to Identification and Authentication.

For the implementation, at the protocol level, communication will make use of protocols such as the SAML (Security Assertions Mark-up Language) protocol. SAML requests and responses may be signed and encrypted. As per the SAML protocol specifications, time stamping is a required service (e.g. to help fight attacks such as replay). Furthermore, reliable identification of a company website and e-Seals are also contributors to STORK's services.

LSP	epSOS (European patients smart open services)
Consortium	The project team consists of 47 beneficiaries from 20 European Union (EU) member states and 3 non-EU member states
Date	2008-2013
Source	epSOS website[35]
Purpose of study	epSOS aims to design, build and evaluate a service infrastructure that demonstrates cross-border interoperability between electronic health record systems in Europe
Main findings	**Benefits for patients** The goal of the epSOS large scale pilot project is to develop and test ("pilot") services that**:** o Enable you as a patient to receive medication (ePrescriptions) when you are in another participating epSOS pilot country (the medication must initially be electronically prescribed in your home country). o Provide health professionals access to the relevant, translated clinical information stored in your home country ("Patient Summary"). This data can only be accessed by the health professional where you are seeking care and only after you have provided your explicit consent. **Benefits for health professionals** o As a health professional, epSOS helps you to provide better healthcare to foreign patients by giving you access to the necessary electronic patient data. o Access to a Patient Summary and the patient's currently active prescriptions to improve the decision making process in diagnosis, based on the relevant clinical data from the patient's home country. o Ability to identify the patient in the country of origin and consult the essential healthcare data using tools integrated in your existing work station or via the internet at the epSOS portal. All this is subject to strict security rules. o Assistance in obtaining patient consent for healthcare services. o Access to a leading service supported by the European Commission, while using your familiar technical environment or the epSOS portal. o Access to patient data and eHealth information in your own language with an original copy.

[35] www.epsos.eu

- Better patient care through cross-border healthcare data exchange.
- Improved use of resources when providing healthcare to foreign patients.
- Increase of security by using a paperless electronic patient data system.

Critical role of ancillary services

For EPSOS, identification, authentication and signatures are important requirements to guarantee the security of the healthcare data processing. Ancillary services are required to achieve this environment of trust.

EPSOS uses a trust architecture that combines elements from PKI and IdP models. It can be illustrated as:

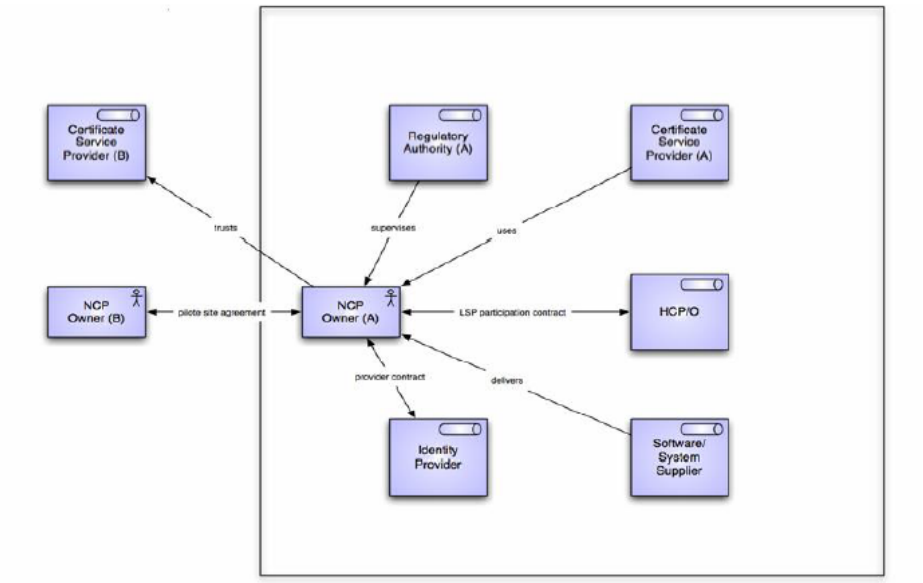


Figure 3 - EPSOS Trust Model Architecture - business view (source: Smart Open Services for European Patients - Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription - Deliverable: Work Package Document WP3.7 D.3.7.2. Final Security Services Specification Definition - Section II - Security Services)

EPSOS specifies access control security, data integrity, data confidentiality, data exchange, auditing and accounting security, non-repudiation, and PKI security as domains.

It is obvious that time stamping, long term preservation, e-seals, and certified e-delivery could contribute significantly to the efficiency and effectiveness of the electronic services proposed in EPSOS.

b. European Commission Impact Assessments

Title	**Proposal for a regulation of the EU parliament and of the council - Amending Council Regulation No 3821/85 on recording equipment in road transport and amending Regulation No 561/2006 of the European Parliament and the Council**
Author	Commission Staff Working Paper
Date	2011
Publication	European Commission - 2011 impact assessment (IA) reports
Purpose of study	Impact Assessment of measures enhancing the effectiveness and efficiency of the tachograph system that accompanies the forthcoming revision of Council Regulation No 3821/85
Methodology of study and analysis performed	Executed in accordance with EU Impact assessment guidelines o Cost/benefit analysis but not complete. o Data collection from stakeholders, Member States and literature.
Main findings	Regulation will make fraud more difficult and reduce the administrative burden, which is expected to save companies €515 million per year. By ensuring better compliance with rules on driving times and rest periods, drivers will be better protected, road safety will increase and fair competition will be assured.
Critical role of ancillary services	The digital tachograph is a device (referred to as VU - vehicle unit or OBU - on-board unit) that is built-in into the vehicle by an accredited workshop using a workshop card. A cable connects it with a motion-sensor that captures the movements of the vehicle. The motion-sensor and the digital tachograph are cryptographically authenticated. To lawfully operate the vehicle, a driver needs to use his driver card. The digital tachograph card is a smartcard, replacing the older paper-based cards. There are four card types: driver (logging all important driver and vehicle events), controller (to allow compliance checks), transport company (information retrieval), and workplace (calibration of the tachograph device in the vehicle in an accredited workshop). In every Member State, a MSA (Member State Authority) has been created for its deployment. The MSA takes responsibility for the three core components in the Member State: o CIA or Card Issuing Authority, the formal body issuing the cards; o CP or Card Personaliser, the producer and personaliser of the cards;

- CA or Certification Authority, the producer of cryptographic certificates.

The system is typically linked to a Member State driving license register, to a national identity register, and to the EU-wide Tachonet. Tachonet has been created as the European network for interconnecting the MSA's. XML messages are used for information exchange between the CIA's. Connectivity is via TESTA. Security is achieved via a Public Key Infrastructure. A European PKI has been set-up with the ERCA (European Root Certification Authority) as its root-CA. In the case of the Digital Tachograph, the benefits come from the combination of dematerialisation and trust. This would not be possible without eSignatures.

While the system which is currently in production does not rely on trusted timestamps or similar ancillary services, the announcements that have been made for the next generation make it clear that ancillary services will be required. To facilitate secure communications between the stakeholders and actors are involved in the transportation landscape, particularly time stamping and certified delivery (e.g. for automatic batch reporting of the actual driving times from transport companies to the controllers) are the most likely candidates.

Title	**Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience**
Author	European staff working document
Date	2009
Publication	European Commission - 2009 impact assessment (IA) reports
Purpose of study	Impact assessment of EU legislation to enhance the level of preparedness and response across Europe against cyber attacks
Methodology of study and analysis performed	Executed in accordance with EU Impact assessment guidelines o In summary, the methodology used throughout the Study is based on proven approaches for similar highly consequential advisory undertakings regarding critical infrastructures. The framework, range of experience and expertise, personal interaction and recommendation process enabled the Study team to delve deeply into the issues facing Europe's future networks, draw upon the knowledge of those most familiar with it, and establish a model for future interaction and sharing. o Qualitative analysis of policy options based on impact indicators magnitude and likelihood
Main findings	The vulnerability of CII exposes society to high economic cost once incidents occur. For example, the World Economic Forum estimated in 2008 that there is a 10 to 20% probability of a major CII (Critical Information Infrastructure) breakdown in the next 10 years, with a potential global economic cost of approximately $250 billion. Research conducted for Business Roundtable by Keybridge Associates suggests that the economic costs of a month-long Internet disruption to the United States alone could be more than $200 billion. A UK payment association estimated that the direct losses caused by malware to its member organisations grew from £12.2 million in 2004 to £33.5 million in 2006. According to the UK information security breaches survey, the worst security incidents caused disruption of service to small businesses for 1-2 days at an average cost of £8,000-£15,000 each, whereas large businesses suffered average interruptions of 1-2 days at an average cost of £80,000-£130,000 each. The average total cost of the worst incident (including direct financial cost and reputation damage) for large business is £90,000-£170,000 and for very large business is £1-£2 million. Rationale for EU action: o National approach to tackle the problems may not be sufficient; o EU-wide approach can complement and bring added value to national programs.
Critical role of ancillary services	In order to withstand cyber-attacks, various Ancillary Services have a potential for significant contribution. Most cyber-attacks are based on the creation and subsequent use of a botnet against a victim or victims. Such attacks start by seducing innocent Internet users to install some form of malware, turning them into an instrument of attack. Installing this malware will force them to share their identity or computer platform with the "Command and Control" server of

the attacker.

As the seduction of the innocent users is often based on or includes some form of phishing, e-seals, certified electronic delivery and web authentication certificates all contribute to providing the end user trust mechanisms that will allow him to judge whether the information or transaction presented to him is genuine or not.

E-seals can be used to ensure the authenticity of the origin of communications or documents. Certified electronic delivery (assuming the sender needs to be registered) can equally be used to ensure the authenticity of the origin of communications or documents.

And a legal person’s website authentication (a " web authentication certificate”) will allow a website user to instantly ascertain that such website is secure and linked to a certain legal person.

c. Other documentation

Title	E-invoicing: Final step of an efficient invoicing process
Author	Heike Mai, Thomas Meyer
Date	2010
Publication	Deutsche Bank Research
Purpose of study	Report about the current state of e-invoicing
Methodology of study and analysis performed	No information about the methodology used.
Main findings	E-invoicing is creating great expectations. Only integrated processes can yield cost savings however. The legal situation and the lack of interoperability are holding back the rollout.
Critical role of ancillary services	Confidence in e-invoicing can be increased by eSignatures. The confidence in such eSignatures can be increased by using Ancillary Services such as time stamping (terms of payment usually contain a reference to the moment the invoice was sent) and certified e-delivery (so a supplier can be sure his customer did receive the invoice).

Title	Young People and Emerging Digital Services - An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks
Author	Wainer Lusoli, Caroline Miltgen
Date	2009
Publication	Institute for Prospective Technological Studies
Purpose of study	The study aims to remedy the almost complete lack of EU evidence on eID services perceptions.
Methodology of study and analysis performed	The study comprises desk research, focus groups in four countries, an expert workshop, a survey pre-test and an online survey in four countries (France, UK, Germany and Spain)
Main findings	Most young people are sceptical of the Internet as an environment for the exchange of personal data. Major doubts exist in relation to the protection of personal data, whereas views are more balanced on infrastructure safety. Young Europeans are significantly concerned about a range of possible privacy consequences of the spreading of personal data. They are mostly concerned about stealth use, improper sharing and financial misuse of their personal information. Only 27% of young people feels that their personal information on the Internet is kept private (compared with 52% when asked to adults). Several elements would encourage the use of eID systems, such as assurance of respect of laws on data protection and information on the use of data. The overall message is that young people want some degree of assurance that their online transactions are technically safe and preserve their personal data privacy.
Critical role of ancillary services	In order to provide a degree of assurance that online transactions are technically safe and preserve personal data privacy, Ancillary Services could contribute. E-seals can be used to ensure the authenticity of the origin of communications or documents. Certified electronic delivery (assuming the sender needs to be registered) can equally be used to ensure the authenticity of the origin of communications or documents. A legal person’s website authentication, or a " web authentication certificate” will allow a website user to instantly ascertain that such website is secure and linked to a certain legal person.

Title	Long-term verifiability of the electronic healthcare records' authenticity
Author	Dimitrios Lekkas, Dimitris Gritzalis
Date	2007
Publication	International journal of medical informatics 76 (2007) 441-448
Purpose of study	To investigate whether the long-term preservation of the authenticity of electronic healthcare records (EHR) is possible
Methodology of study and analysis performed	Analysis of requirements and restrictions for long-term digital signatures and development and analysis of solution framework (assumptions, requirements and implementation).
Main findings	Data authenticity is defined as the preservation of the integrity of the data (i.e. data is not modified during storage or transmission) plus the possibility of origin verification (i.e. the secure identification of the creator or the owner of the data). Both properties are assured by means of digitally signing. Authenticity of EHR is crucial for the trustworthiness of a HIS, especially in distributed environments where data is transmitted over insecure channels and stakeholders have never physically met. Summary points: What was known before the study: o Digital signatures have short lifespan. o Time-stamping and single notarization partially solve the problem. o The longevity of healthcare records is crucial. What the study has added to the body of knowledge: o Trust can be successively transited to new entities, data and technologies. o The initial signature of the EHR is not required to remain valid in the future. o Cumulative notarization adds important security strengths and longevity to a signed EHR. o The proposed open, practical, XML-based framework gives an efficient solution to the problem of long-term verifiability of healthcare records' authenticity.
Critical role of ancillary services	In the case of preservation of the authenticity of electronic healthcare records, Ancillary Services such as Time Stamping and long term preservation are explicitly mentioned as contributing factors.

Title	The web identity prevention: factors to consider in the anti-phishing design
Author	Vijay Chaudhari, Mohd. Ilyas Khan, Bhupendra Verma
Date	2010
Publication	International Journal of Engineering Science and Technology Vol. 2(7), 2010, 2807-2812
Purpose of study	A few factors that can be used to the web identity theft prevention are discussed, such as evaluation of user psychology & educational efforts; source identification, URLs, certification authority, Mutual Authentication, Client & Server Side Security, recognition of phishing messages etc.
Methodology of study and analysis performed	The study is based on existing literature.
Main findings	Some particulars of the Phishing Attack: o Number of unique phishing email reports received by APWG from consumers in the year 2009: October -33254, November - 30490 and December - 28897. o Number of unique phishing web site detected in the year 2009: October - 46522, November - 44907 and December - 46190. o Number of brand hijacked by phishing campaigns in year 2009: October - 356, November 306 - and December – 249. o In the United Kingdom losses from web banking fraud—mostly from phishing—almost doubled to £23.2m in 2005, from £12.2m in 2004. o United States businesses lose an estimated US$2 billion per year as their clients become victims. In 2007 phishing attacks escalated. 3.6 million Citizens lost US $ 3.2 billion in the 12 months ending in August 2007. Some approaches that are supposed to be practical to moderate phishing attacks are discussed: 1. Public-key infrastructure: 2. Digital Signature 3. Authentications 4. HTTPS 5. Education & Training to Client
Critical role of ancillary	In the context of fighting off phishing attacks, Ancillary Services can play a role.

services	E-seals can be used to ensure the authenticity of the origin of communications or documents. Certified electronic delivery (assuming the sender needs to be registered) can equally be used to ensure the authenticity of the origin of communications or documents. A legal person's website authentication, or a " web authentication certificate" will allow a website user to instantly ascertain that such website is secure and linked to a certain legal person.

Title	**Phishing Secrets: History, Effects, and Countermeasures**
Author	Antonio San Martino, Xavier Perramon
Date	2010
Publication	International Journal of Network Security, Vol.11, No.3, PP.163–171, Nov. 2010
Purpose of study	This paper presents the results of a study performed over phishing threats and vulnerabilities present in nowadays authentication environments. The main goal of this paper is to present our solution, the anti-phishing model which can be applied to any web environment, and not just to e-banking or the financial sector, without limitations nor additional requirements.
Methodology of study and analysis performed	Assessment of phishing history and proposition and assessment of new authentication method resistant to phishing attacks.
Main findings	From data reported for years 2006, 2007 and 2008 we can estimate an average of 15000 submissions reported to PhishTank and around 10000 valid phishing attempts. If the cost for each phishing incident is around 900$, as reported by Gartner, we can calculate a direct monetary loss of 90 million dollars per month just considering only those reported to PhishTank. By addressing phishing threats it is possible to save a loss of money and in addition new businesses will be made thanks to the increment in the customer trust and confidence and a consequent increment in the service demand. As presented in the previous paragraph, a huge number of phishing attempts exist, this implies a social and economical impact . The social impact is reported by Bajaj: "Phishing has already taken its toll. Consumer confidence in email is at an all time low. Sixty-seven percent, or 150 million, U.S. consumers don't use banking online today. And, over 88 million online banking customers would switch bank, or reduce online banking usage". In addition to the indirect losses produced by the low demand and usage of the e-banking services, there are direct losses. The Computer Crime Research Centre (CCRC) is a non-profit, non-governmental and scientific research organization. CCRC reported on 2004 an article entitled: "The financial losses of Russian businesses caused by "carder" reached $20,000,000". Carders are illegal organizations specialized on counterfeiting plastic cards and to use Internet for receiving information on card holders and card numbers. Gartner reports that the average dollar loss per incident in 2007 was $886 and the cost of phishing attacks is calculated on 3.2 billion dollars for 2007 in US only.

	Virus Bulletin, on 2007, reports that Malware and Phishing cost more than 7 billion dollars in two years. In order to show an example of personal losses we report the case between the Bank of Ireland and a group of customers that fell victim to a phishing scam that drained 160,000 Euros ($202,000) from their accounts.
Critical role of ancillary services	In the context of fighting off phishing attacks, Ancillary Services can play a role. E-seals can be used to ensure the authenticity of the origin of communications or documents. Certified electronic delivery (assuming the sender needs to be registered) can equally be used to ensure the authenticity of the origin of communications or documents. A legal person's website authentication, or a " web authentication certificate" will allow a website user to instantly ascertain that such website is secure and linked to a certain legal person.

Title	**Information security and cybercrime**
Author	Ian Brown, Lilian Edwards, Chris Mardsen
Date	2009
Publication	Social Science Research Network (SSRN)
Purpose of study	This paper gives an overview of some tools for crime such as malware and botnets. It also gives a summary of national legislation and European law implementing Network Information Security (NIS). Some specific legal problem areas are discussed (e.g. phishing, buying zero day exploits)
Methodology of study and analysis performed	This study is more a literature overview.
Main findings	Legislation, policy, government spending and corporate response in the field of information security have been examined by for instance the Organisation for Economic Cooperation and Development (OECD) and the European Commission, which has identified three key risks for Internet security: 1. Attackers are increasingly motivated by profit rather than the technical interest that drove earlier "hackers" – with growing interest from organised crime and a sophisticated underground economy in stolen information and hacking tools 2. Mobile devices and networks present a significant new threat landscape, where security is so far less developed than on the personal computer 3. Ubiquitous computing will move computation and networking into the fabric of buildings and everyday things (e.g. through RFID and sensor networks), presenting new vulnerabilities.

	Security incentives of organisations, ISPs and users should be better aligned. End users rarely have the time or technical background to shoulder the responsibility pushed onto them by the government for securing their own online activities. Financial services institutions, ISPs and software vendors in particular are in a better position to manage some security risks. The best way to encourage them to do this would be to carefully reallocate to them some of the liability for fraudulent payments, traffic from infected machines and insecure software.
Critical role of ancillary services	In the context of fighting cybercrime, Ancillary Services can play a role. E-seals can be used to ensure the authenticity of the origin of communications or documents. Certified electronic delivery (assuming the sender needs to be registered) can equally be used to ensure the authenticity of the origin of communications or documents. A legal person's website authentication, or a " web authentication certificate" will allow a website user to instantly ascertain that such website is secure and linked to a certain legal person.

7.3 Discussion

- This REA has been undertaken in order to collect evidence on the relevance to include (some of) the ancillary services in scope of this study, in the new European IAS regulation.
- Qualitative evidence on potential impacts of particular ancillary services is available, but robust quantitative evidence has not been found and probably does not exist at this time. Against this background, it presents a considerable challenge to assess in a precise manner the potential contribution / impact of ancillary services. However, the qualitative evidence we retrieved, suggests there are good arguments (in the absence of hard data) why some of the ancillary services should be considered for inclusion in the European regulation.
- We want to mention that Identification and Authentication are prerequisites for the implementation of the Large Scale Pilot Projects. These are not further elaborated since they are not Ancillary Services.
- We summarize the relationship between selected research findings and ancillary services as per the table below:

	Time stamping	Long term preservation of eSignature	e-Seals	Admissibility Of native e-docs	Certified electronic delivery	Legal person's website authentication
PEPPOL	Y	Y				
e-Codex	Y	Y	Y			
SPOCS	Y				Y	
STORK	Y		Y			Y
epSOS	Y	Y	Y		Y	
EC impact assessment 2011 Digitach	Y				Y	
EC impact assessment large scale cyberattacks			Y		Y	Y
e-invoicing	Y				Y	

Young people			Y		Y	Y
LTV of EHR	Y	Y				
Web identity prevention			Y			Y
Phising secrets			Y		Y	Y
Information security and cybercrime			Y		Y	Y

Table 1 - The relationship between selected research findings and ancillary services

- Ancillary Services can be positive contributors to achieve wider deployment of electronic IAS services. As such, inclusion of these Ancillary Services in the European regulation may therefore help buttress the legal value and interoperability of the LSP's outcomes, and of other Use Cases of technology. This will result in benefits for citizens, public authorities and businesses.
- A first set of Ancillary Services that appears to have a potential to contribute to the value of eSignatures includes:
  - time stamping, and
  - long-term preservation of signatures.
- We observe these two services are both close to the typical services involved when using eSignatures in a basic way.
- A second set of Ancillary Services clusters around their added value in the context of fighting Cybercrime. Cybercrime and fraud are economically important issues. An EU-wide approach is needed to tackle these problems. The number of phishing attacks is high and growing. United States businesses have lost an estimated US$2 billion per year overtime. There is no reason to think the situation would be different in Europe.
  - E-seals can be used to ensure the authenticity of the origin of communications or documents.
  - Certified electronic delivery (assuming the sender needs to be registered) can equally be used to ensure the authenticity of the origin of communications or documents.
  - A legal person's website authentication, (or a web authentication certificate) will allow a website user to instantly ascertain that a website is linked to a certain legal person.

7.4 References

7.4.1 Studies included in the Rapid Evidence Assessment

- European Commission (2011) Proposal for a regulation of the EU parliament and of the council - Amending Council Regulation No 3821/85 on recording equipment in road transport and amending Regulation No 561/2006 of the European Parliament and the Council
- European Commission (2010) Impact assessment - Regulation of the European parliament and the council concerning the European Network and Information Security Agency
- European Commission (2006) Impact assessment - A strategy for a Secure Information Society - "Dialogue, partnership and empowerment"
- European Commission (2009) Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience
- Joseph J. Cordes, Anthony Yezer, Garry Young, Mary Catherine Foreman,Charlotte Kirschner (2006) Estimating economic impacts of homeland security measures
- Daniel Plohmann, Elmar Gerhards-Padilla, Felix Leder (2011) Botnets: Detection, Measurement, Disinfection and Defence
- Heike Mai, Thomas Meyer (2011) E-invoicing: Final step of an efficient invoicing process
- Wainer Lusoli, Caroline Miltgen (2009) Young People and Emerging Digital Services - An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks
- Ralf Cimancer, Meik Hansen, Prof. Dr. Herbert Kubicek (2009) Electronic Signatures as Obstacle for Cross-Border E-Procurement in Europe
- Committee for information, computer and communications policy (2009) The role of digital identity management in the internet economy: a primer for policymakers
- Dimitrios Lekkas, Dimitris Gritzalis (2007) Long-term verifiability of the electronic healthcare records' authenticity
- Tamas Szadeczky (2010) Problems of digital sustainability
- Vijay Chaudhari, Mohd. Ilyas Khan, Bhupendra Verma (2010) The web identity prevention: factors to consider in the anti-phishing design
- Antonio San Martino, Xavier Perramon (2010) Phishing Secrets: History, Effects, and Countermeasures
- Aashish Srvastava (2011) Resistance to change: six reasons why businesses don’t use eSignatures
- I-Chiu Chang, Hsin-Ginn Hwang, Ming-Chien Hung, Ming-Hui Lin, David C. Yen (2007) Factors affecting the adoption of electronic signature: Executives’ perspective of hospital information department
- Ian Brown, Lilian Edwards, Chris Mardsen (2009) Information security and cybercrime
- Robert D. Atkinson and Andrew S. McKay (2007) Understanding the Economic Benefit of the Information Technology Revolution

- Toby Stevens, John Elliott, Anssi Hoikkanen, Ioannis Maghiros, Wainer Lusoli (2011) The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies
- WebNotarius Service Communications technical specification ver. 2.0.

7.4.2 Other references

- Davies P. (2003) The Magenta Book. Guidance Notes for Policy Evaluation and Analysis. Chapter 2: What Do We Already Know? London: Cabinet Office
- Butler G.,Hodgkinson J., Holmes E. and Marshall S.(2004) Evidence Based Approaches to Reducing Gang Violence, A Rapid Evidence Assessment for Aston and Handsworth Operational Group

8. Discussion on a pan-European eID system, challenges and opportunities

8.1 Introduction

The purposes of this chapter are twofold: first, it tries to briefly asses the current state of the European legal framework relating to electronic Identification, Authentication and Signatures (hereinafter IAS) mechanisms in an online environment. We will identify the main rationale behind the need for these mechanisms in electronic transactions and communication. We will also examine the main European legislation in place and we will try to identify the main requirements a successful IAS system should include.

Second, the chapter outlines a possible solution for a functional pan-European electronic identification (eID) model, drawing inspiration from existing legal frameworks. We will argue that it could be possible to set up a pan-European eID system, without a direct need to engage in wide-scale harmonization and without a comprehensive legal framework in place. We will examine an existing pan-European system and we will try to apply the same principles to a European eID system. Lastly, we will identify some basic features the proposed system should offer, in order to offer additional benefits compared to existing solutions, as well as possible risks and obstacles associated with such system.

8.1.1 Why do we need IAS for the information society – trusted communication and transactions

Internet has always been built on trust and self-regulation. But as is the case in an offline world, with growing number of entities in the community the level of trust starts to dissolve quickly. Today the internet is no longer an online village, where you knew 'everyone', with only 16 million users in 1995, nor a small town with 500 million 'inhabitants' in 2001. Today the internet is a vast system of 2 billion users (nearly a third of world population), growing with several millions of users each month.[36] It comes as no surprise that in such enormous community, the level of trust is considerably lower than it used to be. At the same time, the growing size of the World Wide Web and 'Internet of things' provides growing possibilities for stakeholders and brings an increasing demand for reliable verification of information origin and identification of the entity 'on the other side'. More and more sensitive transactions are being concluded online. "*The development of ubiquitous networks of electronic communications, and the general trends of globalization and increasing human mobility give*

[36] Statistics at: http://www.internetworldstats.com

rise to the need to ascertain 'who is who' on the internet, in the street, in the usage of services and in commercial transactions."[37]

Without sufficient trust in electronic communication, consumers will be reluctant to conclude transactions over the internet and enterprises will be reluctant to move services online. Digital confidence was identified as one of the main obstacles for further expansion of electronic services. Among the top reasons why people do not order goods and services online are concerns about payment security, privacy and trust. "*Consumers will not shop online if they do not feel their rights are clear and protected.*"[38] Thus, the lack of trust in the online environment is seriously hampering European's economic development.

The problem is that the internet's original infrastructure by design lacks reliable means of identification. The communication originator and its recipient can be identified (in the internet's default infrastructure) only through an IP address, the information designated to a device through which the transaction is concluded, rather than to any entity behind the transaction. In many, if not most, of the internet 'transactions' this will not present any problem, since there is no need for stronger means of identification. In fact, anonymity is still one of the most prominent beneficial features of the internet as a place of free speech and free expression, which is extremely hard to control and can even support a change of political regime, as witnessed in the recent events often referred to as the 'Arab spring'.

On the other hand, the lack of an identification infrastructure also implies that it is not possible to reliably identify an entity behind a transaction even in cases where all the parties would wish to do so. Paradoxically, this often leads to a situation where individuals are 'forced' to provide more information than would be inherently necessary to successfully conclude a given transaction. A typical example would be an online shop, where customers are usually requested to provide an extensive set of personal details before concluding a simple sale of goods contract, whereas the same contract happens in an anonymous fashion in real-world situations. Service providers often use a 'take it or leave it' approach to push potential customers to provide all the information they want.[39] Thus, not only 'insufficient-identification', but also 'over-identification' are associated with the lack of appropriate IAS infrastructure. A proper eID system should seek to address both issues - reliability in terms of identification and privacy.[40]

---

[37] Andrade, N. N. G. d., Towards a European eID regulatory framework. The Legal Gaps, Barriers and Challenges of constructing a legal framework for the protection and management of electronic identities, (2012 - forthcoming) European Commission, Joint Research Center, p.4.

[38] Ibid., p.12.

[39] See: Rooy, D.v., Bus, J., *Trust and privacy in the future internet—a research perspective*, Identity in the Information Society (2010) Vol. 3, No.2, p.398. (available at: Springerlink.com)

[40] Andrade, *op.cit.,* p.8.

With a growing number of online service providers and 'official' communication transferred online, a reliable identification is a prerequisite for concluding contracts at a distance with electronic means of communication. As the Commission recognized in its' Digital Agenda for Europe: *"Electronic identity (eID) technologies and authentication services are essential for transactions on the internet both in the private and public sectors. Today the most common way to authenticate is the use of passwords. For many applications this may be sufficient, but more secure solutions are increasingly needed."*[41] Reliable eID systems will help to provide necessary trust value for online communication, transactions and electronic documents.

These systems could even improve standards we are used to rely on in an offline world. A digital signature which is linked to a specific eID will be far more reliable than a traditional hand written signature - the method of authentication which is trusted more for the reasons of long customary practice than its actual reliability. Moreover, a reliable eID system would open possibilities for certain (traditionally offline) services to be offered online (e.g., government services, legal proceedings, healthcare services, etc.) and therefore easily accessible, on demand and with 24/7 availability. Furthermore, a functional eID system could provide new opportunities for new types of services (e.g., 'safe-chat' for minors, or reliable dating services - in a sense of personal identification, not the desired outcome). Today, "*when a large scale EU or global enterprise wants to manage the IAS aspects of employees, contractors and partners, it faces a highly diversified landscape in both legal and technical terms. This is highly inefficient and costly.*"[42] Consequently, the system would cut expenses, while preserving and even enhancing productivity - the objective that enterprises, governments and individuals are desperately trying to achieve in times of economic stagnation.

After all, trustworthy eID systems already exist, as will be discussed further in this chapter. However, these are usually not based as much on legal foundations, but more often on technological ones. The legal framework is outdated and generally cannot keep up with the rapid technological developments. As a result, stakeholders are trying to fill the legal gap with more or less improvised solutions, building rather on practical measures than on legal policies. With an emergence of new authentication systems, such as various social network sites, and their extensive implementation with other services, the need to 'set up new standards' and corresponding legal framework is even more pressing, since these systems may soon become a de-facto standard in an online community. In order to realize the goals set up in the Digital Agenda for Europe - "*a flourishing digital economy by 2020*" - Europe will certainly need a predictable and reliable legal framework for information society.

---

[41] European Commission, *A Digital Agenda for Europe*, COM(2010) 245 final/2 (Digital Agenda).

[42] Quoted from: IAS Deliverable D1, page 30.

8.1.2 Current European legal framework

There are three key legal texts on European level regarding identity management: the e-Signature Directive,[43] the Privacy Directive[44] and the Services Directive.[45] The current framework is therefore based on a combination of different directives, implementing laws at national level and technological standards. It is not the purpose of this chapter, nor in its scope, to examine these instruments in much detail,[46] but it is necessary to briefly mention their role in an IAS framework.

The **Privacy Directive** established rules concerning processing and handling of personal data within the Union and possible transfer of these data outside the Union. The Directive was successfully implemented in all Member States and today the basic principles are the same throughout the Union. In the process of implementation, some important issues for interoperability were left in the competence of the Member States. In this regard, it is worth mentioning that the Privacy Directive expressly states that the "*Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed*".[47] Consequently, although the Directive harmonized conditions that have to be met when handling personal data within the Union, it also left some interoperability for IAS systems unresolved.

The **Service Directive** sought to remove barriers within the internal market and, strictly speaking, is not directly relevant for the IAS framework. Nevertheless, it provides an important obligation for Member States to make all procedures and formalities, relating to access to a service activity, available through electronic means.[48] This implies a *de-facto* obligation for a functional cross-border authentication system.

---

[43] Directive 1999/93/EC on a community framework for electronic signatures; OJ L 13 (2000), p.12.

[44] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ L 281 (1995), p.31.

[45] Directive 2006/123/EC on services in the internal market; OJ L 376 (2006), p.36.

[46] For a more comprehensive overview of European as well as national legal frameworks in place, see e.g.: Leenes et al., *Stork - Towards Pan-European Recognition of Electronic IDs (eIDs) - D2.2 - Report on Legal Interoperability*, (2010) STORK, available at: https://www.eid-stork.eu/; or Graux, H., Majava, J., and Meyvis, E., *Study on eID Interoperability for PEGS - Update of Country Profiles - Analysis & Assessment Report*, (2009) IDABC programme (available at: http://ec.europa.eu/idabc/servlets/ Docb482.pdf?id=32522, accessed on 26.September 2011).

[47] Article 8.7 of the Privacy Directive.

[48] Art.8.1 of the Service Directive provides: "Member States shall ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant point of single contact and with the relevant competent authorities."

The **e-Signature Directive** is the main source of rules concerning electronic certificates and certification services. The Directive seems to address only one aspect of the IAS, but as Public Key Infrastructure (PKI) systems are becoming a standard for identity management systems in general, the Directive provides an important basis also for remaining IAS aspects. The exact scope of the e-Signature Directive is a subject of constant debate. It is either seen as providing a legal basis only for electronic signatures to be used in the same manner and with the same legal value as hand written signatures; or more broadly as providing a general set of rules for using electronic signatures as a technology in general, covering any possible use of such technology and thus also entity identification and authentication.[49] The first position is supported by the fact that the e-Signature Directive does not provide a material legal framework for the use of e-signatures in different situations than as an alternative to a hand written signature. The latter position builds on the wording of the Directive, where the electronic signature is defined as "a method of authentication"; and where a "certification-service-provider" is broadly characterized as "an entity or a legal or natural person who issues certificates or provides *other services related to* electronic signatures"[emphasis added].[50]

Moreover, important issues for a functional IAS framework remain unresolved in the Directive. The e-Signature Directive took as one of its building blocks the concept of identification. It described certificate as "an electronic attestation which links signature-verification data to a person and confirms the identity of that person".[51] It also imposed on CSPs the obligation to "verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued".[52] But without a necessary policy framework for identification and authentication procedures on EU level, Member States and CSPs were left to choose appropriate measures according to their local traditions and business/policy preferences. Rules and procedures for establishing an identity are thus subject to national legislation and differ throughout the Union. While this may seem reasonable, taking into account the sensitive nature of Member States' competence in this area, it creates further obstacles for cross-border recognition and implementation of a common European IAS framework.

Overall, e-signatures have been in the centre of legislative attention for several years. They were supposed to provide electronic documents with the same legal value as the paper versions enjoy in an offline world. The e-Signature Directive partially achieved the said goal,

---

[49] Graux, Majava, and Meyvis, *op.cit.*, pp.107-110.

[50] Art. 2.1 and 2.11 of the e-Signature Directive. See: Graux, H., *Rethinking the e-signatures Directive: Moving towards a comprehensive legal framework for eID*, (2011) IPTS workshop - Electronic identity for Europe, pp.3-6.

[51] Article 2.9 of the e-Signature Directive.

[52] Anex II, Ibid.

but e-signatures are still not a common tool for an average user in day-to-day electronic communications and transactions. Though the e-Signature Directive provided an important kick-start for the Union's policy in the area of IAS, its ambitious goals ("facilitate the use of electronic signatures and contribute to their legal recognition"[53]), seem today somehow incomplete and insufficient. The Commission is aware of this and proposed a revision of the e-Signature Directive in its Digital Agenda for Europe. It is interesting to note here the phrasing chosen by the Commission in its proposal: the revision of the Directive should result in a legal framework for 'secure *eAuthentication* systems'.[54] This might suggest, that the interest of Union's legislator is finally shifting from just 'signature' aspect to the whole picture of IAS framework. Issues of Identification, Authentication and Signatures are interconnected and cannot fully operate without addressing all of them. As noted by the Commission: "*Electronic Identity Management is a key element for the delivery of any e-services.*"[55]

8.1.3 Existing IAS systems

There are of course a number of electronic IAS systems already in place and we all use at least some of these on a regular basis (e.g., email, mobile phones using a SIM card, eBanking, etc.). For an easier explanation, we will divide these models into four main categories: Governmentally controlled, Open private, Closed Private and Hybrid private model. We will examine each model's strengths, weaknesses and suitable applications. Finally we will conclude, that there is a place for a different system that would accommodate some of the features missing in existing models.

a. Governmentally Controlled Model (national eID)

Various eID authentication systems have been built and deployed across the Member States and more are under way. Today, all Member States either already have some kind of governmentally controlled IAS system (or at least part of it) in place, or are currently preparing to introduce one in the near future.[56] These systems enjoy the highest trust value from the security and legal certainty point of view (within the given Member State), and they are usually built on a local implementation of the e-Signature Directive. Government authorities generally act as trust issuers and systems thus enjoy a high trust value.

---

[53] Art.1 of the e-Signature Directive.

[54] Key action 3 of the Digital Agenda, p.11.

[55] Commission, Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, COM (2008) 798 final, p.10.

[56] See e.g.: Graux, H., Majava, J., and Meyvis, E., *op.cit.*

The identification process is based on two-factor or three-factor authentication, ensuring a high level of security. Systems are typically designed primarily for communication directly with the trust issuer (government) and are based on a centralised identity model.[57] Although they might be opened also for other relying parties, they usually act as closed systems. Typically, PKI certificates are issued on a smart card (as a part of a national ID card or on a separate card) and additional device (a card reader) is usually required in order to use the system. Systems enjoy full legal recognition within their (local) legal framework. The use of the system is often however very limited, since governments are being cautious about wider deployment. Systems are also geographically limited and designed for domestic use only.

Depending on the point of view, the geographic limitations of a governmentally controlled model can be considered its main strength or weakness. From a Member States' perspective, the limited scope of the system ensures its full legal recognition within the local jurisdiction, since it fully complies with relevant local legislation (registration, eligibility, privacy policy, identity requirements, etc.). Furthermore, since these systems may offer an equivalent to traditional identification documents (paper-based ID cards, passports, drivers licence, etc.), governments are not eager to 'share' these systems with the private sector, and even less with any kind of 'foreign' entity in cross-border situations. Governments want to be in full control over the system, since they include sensitive personal data about their citizens and 'sharing' such information with other states could hinder the states' traditional sovereignty in this field.

From the users' point of view, the system will be sufficient as far as they only deal with domestic services (be it in the public or private sector). This might very well be the case for the majority of individual users, but it will most likely prove insufficient when it comes to middle-sized businesses and large enterprises, which are active in cross-border trade in the internal market. For these entities (as well as for an increasing number of individuals who benefit from the free movement within the Union for purposes of work, study or simply travel), the strict geographic scope of these systems will constitute the greatest disadvantage, since they will only be able to use the system, after they fulfil local criteria and undergo a (more or less) burdensome process of registration; or worse, they might not be eligible to use the system at all.

An evident solution would be to make these existing local systems interoperable. A number of initiatives were launched in this respect,[58] which have identified a number of obstacles

---

[57] For comparison of different identity management models, see e.g.: OECD, *The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers*, DSTI/ICCP/REG(2008) 10/FINAL, Annex 1, p.16 (available at: http://www.oecd.org/dataoecd/23/38/43195291.pdf, accessed on 26.September 2011).

[58] To name but a few: STORK, PRIME, CROBIES, SPOCS; for a more complete list of research initiatives and projects devoted to eID and interoperability see: Andrade, *op.cit.*, p.7; see also a list of currently

and are trying to find ways to overcome them.[59] But this process may prove to be too difficult, taking into account the fact that these systems are established through national legislation and their interoperability often requires a complicated process of legislative changes and amendments.

b. Open Private Model (CertiPost, OpenID, Entrust, DigiNotar)

In the Open Private Model, trusted credentials are issued by a private organization - a professional identity provider. Usually, the identity provider does not act itself as a relying party. The employed technology mostly applies high security standards, and the identification process involves two-factor or three-factor identification. Typically, the identity provider has to be accredited as the Certification Authority (CA) according to its domestic legislation and will have a (higher or lower) level of liability towards its clients. The interoperability of identity management systems in this model is based on a 'federated identity model'[60] (linking various and even previously created accounts together), or on a 'centralised' identity system. Services are usually provided in exchange for remuneration.

Contrary to the governmentally controlled systems, identity providers in the Open Private Model are competing with other providers in a free market. Therefore, identity providers will be trying to connect as many services and relying parties to their system as possible. Users are free to choose an identity provider and can decide between a variety of services, trust levels, security levels, etc. There are no geographic limitations, and the scope will depend on provider's business model and ability to engage relying parties in its system. Thus, the use of the system is limited to the provider's network of relying parties and will be mainly used for transactions in the private sector, although the public sector may also take part in the system. An Open Private Model may offer legal recognition and liability assurance, but these will depend on local legislation and any contractual limitations imposed by the service provider, and may not be sufficiently clear for an average user. However, the systems are often suitable only for enterprises, or individual users with above average technical skills and knowledge.

The lack of a legal framework requires identity providers to compensate legal certainty with contractual terms, which might not be sufficiently clear and relevant for an average user.

---

running projects funded by ICT Policy Support Programme in the area of e-government, available at: http://ec.europa.eu/information_society/

[59] See e.g.: Hartmann, D., Körting, S., *Security issues in cross-border electronic* authentication, (2010) The European Network and Information Security Agency; or Leenes et al., *op.cit.*

[60] See e.g.: Smedinghoff, T.J., *Federated Identity Management: Balancing Privacy Rights, Liability Risks, and the Duty to Authenticate*, (2009) available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1471599 (accessed on 23.September 2011).

Systems might be too cumbersome to be deployed in more common transactions and will therefore have only a limited scope of use.

c. Closed Private Model (e-banking, mobile operators, e-shop account, AppleID, email)

The closed private model is by far the most commonly used identification system online. Every internet user owns at least one account within some kind of a closed private network. These range from e-mail accounts or e-banking services, through mobile operators, to simple e-shop accounts and various online profiles (e.g., AppleID, NikeID), but include also small-scale solutions such as corporate ID systems. In this model, identity providers are private organizations but, unlike in the open private model, they do not act as professional identity service providers. Instead, they use authentication system for one purpose only - communication between provider and user. The identity provider thus also acts as the only relying party of the system. The closed private model is designed to operate independently, with no formal connections to other systems. Therefore, the term 'silo model' is often used, since each such system represents a closed silo of identities that can be used only inside the silo.[61] From a security point of view, these systems range from very elaborated and strong ones with two or three-factor authentication (e-banking), to systems with relatively low security standards and one-factor identification (e-mail, e-shop account).

As already noted, it is not possible to interconnect 'siloed' systems and link one profile to different services. Hence, users have to create a new account with each service provider. Soon, users will end up with multiple accounts with many different providers. This could theoretically bring a security benefit for the user in case of security breach. While one system may be compromised and user's data stolen, the compromised system will have no inherent links with other systems (silos), and consequently, user's profiles stored in other systems will remain unaffected. On the other hand, with multiple accounts, users have to manage multiple accounts, login names and passwords. Typically, this will not lead to a higher level of security, as users are confronted with too much information to remember, they usually decide to use the same login details (name and password) for most, if not all, their accounts. Combined with lower authentication standards in most of these systems (one-factor authentication), after acquiring user's password for one system, potential cyber-criminals will most likely gain access to several remaining accounts.

The legal predictability of these systems is diverse. While some systems (like e-banking) may offer similar legal effects as traditional face-to-face transactions; most of these systems will be governed by contractual terms and conditions and might therefore offer different levels of legal certainty and liability limitations. Taking into account the known fact that users

[61] See: OECD, *op.cit.*, Annex 1, p.16.

hardly ever read through these terms, their awareness about possible risks will be moderate at best.

d. Hybrid Private Model (social connect – Facebook, Google, Twitter)

Recently, this new type of authentication model is gaining popularity on the web. With the rapid growth and success of social networking sites (namely Facebook, Twitter and the recently publicly lunched Google+), users are creating more and more detailed electronic identities and fill their social network profiles with more and more personal information. Users may not be aware of the fact that their social networking site can, over time, acquire a much more detailed profile of their identity, than they intended to share. The information individuals would not be willing to share even with trusted parties in the real world (such as our location, relationship status, health concerns, etc.) are being uploaded to their electronic identities and made (more or less) publically available on a daily basis. All this with a 'voluntary' consent of the data subject. Not only individuals, but also businesses and organizations are increasingly making use of social networking profiles. With more than 800 million active users,[62] Facebook is by far the largest publicly accessible eID database in the world.

Hence, social networking sites soon recognized an opportunity to act as *quasi*-professional identity providers. The system lies between closed and open private models and could therefore be called a 'Hybrid Private Model'. The eID is issued by a private organization, which is not a professional identity provider. The identity provider is then also a primary relying party of the system (unlike in the open private model), but makes it also possible for other relying parties to use its authentication system and link users' profiles with other service providers (unlike the closed private model). The system thus basically works as a federated identity model.[63]

For users, this is a convenient way of setting up an account with different service providers. Time management certainly plays a part in the popularity of this authentication model. The user simply logs in to her social network profile and confirms that a third party can access information stored in that profile. To comply with data protection regulations, the information accessed by a third party is indicated to users, who must give their prior consent. The system has practically no geographical boundaries and can be used across a variety of websites and services, as long as all parties are comfortable with such use. The legal aspects of this authentication method are however very limited. Since the 'original' identity provider (social network) does not require any kind of reliable identity authentication prior to

[62] http://www.facebook.com/press/info.php?statistics

[63] See: Smedinghoff, T.J., *op.cit.*

setting up users profile, the factual identity of a user cannot be determined.[64] A Hybrid Private Model may therefore only be suitable for transactions and communication with a relatively low-trust value. The legal recognition and certainty of such eID is practically non-existent. It will be governed by the contractual terms agreed upon between user, identity provider and third parties. Applicable law is also selected in the agreement.[65]

While this kind of identity management system is convenient for many users and may be the best solution in certain situations, it is important to acknowledge that this method will not be perceived as a standard by individual users. In case a dispute will arise between two parties relying on such system, the legal means available will soon prove insufficient, because the system does not provide for any guarantees. Moreover, individuals may not be fully aware of possible trade-offs with their privacy when using such system. The privacy concerns are a frequent source of criticism when it comes to social networking sites. Privacy setting possibilities may be constantly developing, but an average user usually relies on the default values set by the identity provider. Users' 'informed consent'[66] that is needed in order to transfer information to a third party can theoretically be legally valid, but actual 'informed' value of such consent is normally disputable. In practice, the information that users are about to make available is described in vague and general terms, rather than simply displaying all the information to be shared with the third party. In addition, it is not only a third party which acquires information about the user. The identity provider (social network) also gains additional information about user's behaviour vis-à-vis third party services. Consequently, users may end up with more personal information stored with an identity provider than they intended to.

8.1.4 Preliminary conclusion

All the above mentioned systems are successfully deployed in an online environment. They are more suitable in certain situations and less in others. More importantly, users know how to use them and are used to relying on these methods in their electronic communication and transactions. It should therefore not be our aim to supplant or replace these systems with some kind of new state-of-the-art authentication system. The existing systems all have their ideal way of use and they will provide the best solution in certain situations, therefore they all certainly have a place in an IAS framework. As in the real world situations, "*[t]he need to*

---

[64] It should be noted, that Terms and Conditions of a service usually require users to provide only real, accurate, correct and up to date information necessary for registration (although this is not always the case, e.g., Twitter). See e.g.: http://www.facebook.com/terms.php; or http://www.google.com/accounts/TOS. However, this cannot be considered a reliable identity authentication method.

[65] Most likely, the agreement will provide for the laws of the State of California.

[66] Article 2(h) of the Privacy Directive.

identify someone differs and has different aims, when it is done by the immigration control, by the highway patrol, by the bartender, by the bank clerk etc."[67] The same is valid for an online world. Various means of identification should therefore be preserved.

However, the existing framework leaves many gaps open. The evolving technology tries to answer the demand for some kind of a solution and is naturally trying to fill in these gaps. "*As a result, technology seems to be providing the values of certainty and predictability in the regulation of relationships that law should provide."*[68] This might be practical and effective, but will not bring a solution in the long term. Thus, there is clearly a space, and moreover a need, for a better alternative to existing systems. The necessary preconditions for this alternative will be discussed in the next section.

8.2 Requirements for a pan-European eAuthentication system

In the section below, we will briefly examine the high level requirements that would need to be met by a pan-European eAuthentication system, irrespective of technical implementation choices.

8.2.1 User friendliness

If we want to create a system that will be accepted by an average user, it must be above all user-friendly, easy-to-use and understandable. Users should embrace the system, rather than be required to use the system. It should be recognized as an advantageous solution compared to traditional systems. However, it is necessary to strike a right balance between user friendliness and security requirements. On the one hand, identification based on a single-factor authentication will certainly provide a higher level of 'friendliness', but will be much vulnerable to security attacks. On the other hand, system with a perfect security infrastructure and three-factor authentication will by definition require number of steps to complete the process and will clearly be more inconvenient. Hence, it would seem reasonable to provide multi-level authentication within the same system. While a 'basic' single-factor authentication could be used in ordinary transactions and communication, a second more complex 'advanced' authentication could be employed whenever there would be a need for a higher trust value, even within the transaction that started with a 'basic' authentication. The idea is not new and the method of two-stage identification is often being

[67] Myhr, T., Regulating a European eID: A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID, (2005) The Porvoo e-ID Group, p. 8.

[68] Andrade, *op.cit.*, p.15.

used with e-banking services, where an account information can be accessed with a 'basic' two-factor authentication (e.g., certificate and password), whereas payment has to be completed with an 'advanced' three-factor authentication (e.g., certificate, password and code received via mobile phone).

While the final solution and technical implementation of the system might be considered premature in the stage of merely drafting a legal framework, it should also be born in mind, that these are the factors which may influence end-users' decisions the most. The system's interface as well as the practical solutions regarding the authentication tokens (smart card, certificate on USB memory stick, mobile phone implementation, etc.) will have a major impact on the system's utilisation. Without these criteria in mind already in the stage of preparing a legal framework, the system may very well turn up as yet another solution suitable only for specific user groups (e.g., lawyers, healthcare practitioners or accountants, who are by the nature of their profession required to interact frequently with the public sector and other parties in a formal way) or large enterprises with specialized IT departments.[69] Notwithstanding results and progress achieved in these sectors, "*the usability of authentication solutions in private sector applications is considered to be of key importance*".[70]

8.2.2 Technologically neutral, interoperable, cross-applicable

In an ever developing field of technology, it is extremely difficult to create a system that would be able to keep up with innovation requirements and a user's needs. The legal framework must not pose further obstacles. Basic rules must therefore be technology-neutral. That is not to say that technical standards should not be addressed at all. On the contrary, legal rules should ensure that a technical infrastructure will not hamper interoperability and cross-application of the system. Minimal technical standards should be regulated on a central level by the means of functional criteria for all stakeholders. These standards have to be easily 'upgradable' to match with the current state of technology and, therefore, should not depend directly on the legal framework.

The system should be suitable for a wide scale utilisation and cross-applicable over broad range of services. Relying parties should be able to implement the system easily with their services. Likewise, the system must be able to communicate with multiple end-user platforms and devices.

---

[69] Today, already more than 50% of enterprises in the Union are making use of e-government services by sending filled forms electronically, whereas for individuals the number is only 13%. (Eurostat - http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/E-government_statistics)

[70] Graux, Majava, and Meyvis, *op.cit.*, p.121.

8.2.3 Secure and reliable

An increasing number of online possibilities, brings about an equivalent increase in potential misuse and cybercrime. "*Europeans will not engage in ever more sophisticated online activities, unless they feel that they, or their children, can fully rely upon their networks*."[71] A reliable eID system has to prevent possible security threats and take appropriate steps to prevent any kind of misuse.

A system has to be able to function 24/7, so that users and relying parties know that the system will be available whenever they will need it. Reliable communication between different parts of the system has to be secured. Inaccurate information or loss of data could have severe consequences and must be prevented. A system should provide a technical-support centre to help resolve difficulties of any party using the system.

8.2.4 Legally predictable

Mutual recognition and legal acceptance throughout the Member States should be considered as the main benefit of the system compared to existing systems. Users could finally rely on one system throughout the Union, with clear and predictable legal consequences in all Member States. This central feature is also the major obstacle for setting up such a system, since EU is lacking the necessary harmonization in this field. Nevertheless, it is not necessary in order for a system to work to be entrusted with the same legal value in every Member State. As a start, it would be sufficient to assign at least certain minimal legal value to the system and provide users with a clear guidance over applicability and possible use in each Member State. Notwithstanding these assumptions, the final objective of the system should be full legal recognition as a valid means of identification throughout all Member States.

The legal predictability could attract a number of stakeholders to take part in the system. Without this feature, the system will not be much different from already existing solutions. Legal acceptance and mutual recognition would bring a necessary trust level, and would enable utilisation of the system in wide areas, since parties relying on such system would have a similar legal certainty in their transactions as if dealing face-to-face.

8.2.5 Scalability

The system must be able to accommodate the growing demand and its own growth. It should be 'simple' enough to enable swift communication and functioning throughout its

[71] Digital Agenda, *op.cit.*, p.5.

infrastructure, yet it must be secure enough to prevent misuse and avert security threats. This is a rather technical issue which can be solved with the system's implementation, but the important constraints should be born in mind when drafting necessary framework.

The system's additional services, other than identification, should also be taken into account. Identity authentication is only one feature of functional IAS system. Other services like e-signing, time stamping or e-archiving could also be included in the same system.

8.2.6 Trust

All of the aforementioned requirements should contribute to the most important prerequisite of the system - trust. As already mentioned above, insufficient trust has been identified as one of the main rationales for individuals not to get involved in electronic transactions. "*In a transformation to digital functions, it is vital to understand how the mechanisms of trust and identification can be maintained. Trust effectively facilitates human transactions and economic activities by reducing risks.*"[72] It is therefore essential to overcome this obstacle. A stakeholders' engagement in the process of drafting and implementing necessary legal framework could help to address main issues and facilitate a successful start of the system. It should be remembered, that the system will be offered on voluntary basis and that it should not replace on-going initiatives and existing solutions, but rather offer a better alternative or possibility to make these systems interoperable. Therefore, sufficient trust in the system will be crucial for stakeholders to take part in the system.

The level of trust will be directly connected with the identity providers. The more strict criteria will be set up for the identity authentication of an entity before issuance of its eID, the higher trust will be enjoyed within the system. On the other hand, criteria set up too strictly could hamper stakeholders ability to participate in the system. Conversely, an open system without trusted mechanisms for establishing eID's would not be useful either, since parties would not have a sufficient trust in issued identity credentials. A proper balance has to be achieved between these principles.

Users must have sufficient trust in the ability of identity providers to keep their personal data safe and will not reveal more than necessary. Similarly, relying parties must have sufficient trust in issued eIDs, processes employed to establish these eIDs, as well as an assurance of liability in case 'things go wrong'. An important role of supervising mechanisms should be observed in this respect. Impartial authorities at local, as well as Union's level should be entrusted with supervising powers over relevant parts of the system. Compliance with

[72] Van Rooy, D., Bus, J., *Trust and privacy in the future internet—a research perspective*, Identity in the Information Society (2010) Vol. 3, No.2, p.398. (available at: Springerlink.com)

applicable legislation and policy in the fields of privacy and data protection should be under close scrutiny by existing Member States' authorities.[73]

8.2.7 Obstacles

The creation of a pan-European IAS system with characteristics outlined above will be faced with many challenges and obstacles. The main issues are briefly identified in this section.

a. No offline legal framework for IAS

The complexity of the current European legal framework and the absence of clear rules concerning entity authentication at the European level were already discussed in the chapter above. In addition, there is the lack of any legal framework at the domestic level. A study carried out within the "eID Interoperability for PEGS"[74] showed, that in 25 Member States there is no "*legal definition of the concept of an identity, and more importantly, how an identity can be established in an electronic environment*".[75] Only two Member States (namely Austria and Finland) have the concept of identification legally defined. Having said that, it is only natural that the common taxonomy is also absent at European level. This might be quite striking, but considering the traditional way of entity authentication in real world situations (physical appearance and demonstration of official documents), and the fact that "*in a historic perspective up until not very long ago a person had no need for an identity card*";[76] the conclusion is not that surprising. Consequently, it might be even harder to set up an appropriate legal framework for IAS in electronic environment, when there is no express legal basis neither in an offline environment, and procedures used in a real world derive mainly from customary practice.

Furthermore, this 'customary practice' differs throughout the Member States and the attributes necessary for establishing one's identity are diverse. Whereas the majority of Member States issues their citizens with some kind of physical ID document (such as paper-based ID card) and associated identity number, there are some exceptions to this rule.[77] Besides, attributes contained in these documents differ greatly, which can be demonstrated

---

[73] According to Article 3.3 of the e-Signatures directive, Member States already have an obligation to set up an "appropriate system that allows for supervision of certification-service-providers which are established on its territory (…)"

[74] Graux, Majava, and Meyvis, *op.cit.*

[75] Ibid., p.118.

[76] Myhr, *op.cit.*, p.7.

[77] United Kingdom and Ireland do not issue any generally applicable ID cards nor general identity numbers. The introduction of identity cards in UK was reversed by the Identity Documents Act 2010 (c. 40).

with the information contained within various eID cards issued by Member States. These range from a single identifier to an exhaustive list of identity attributes.[78] Finally, in some Member States legal persons can be issued with their own eID, whereas in other Member States only natural persons can obtain an eID and a legal person has to act through its 'natural' representatives. Taking all of this into account, one can easily conclude that some kind of common standard has to be found in order to set up an interoperable and cross-border applicable IAS system.

b. Political issues and sensitive nature of national and European competence

Managing citizens' identity and corresponding databases is a field of traditionally national competence which touches sensitive issues of state sovereignty. Issuance of unique identifiers usually has to deal with constitutional restrictions and privacy policy regulations at national level. In some countries (notably Germany and Hungary), the constitutional courts already declared issuance of generalised unique identifiers to be in contradiction with their respective constitutions, and multiple 'sectoral' identifiers had to be used instead.[79]

National governments may be reluctant to submit information about their citizens outside their (national) control and jurisdiction. Important privacy issues will be at stake, since the concept of privacy and accompanying standards will differ for each Member State, and the level of protection can be set up higher or lower. Authentication requirements are defined at national level and hold a little relevance in cross-border situations.[80] Furthermore, with an introduction of a European-wide eID system a number of 'big-brother' conspiracy theories will certainly emerge. The security and reliability of the system will thus be ever more crucial. This will be hard to control, given that the system will be spread throughout the Member States with different infrastructure and security standards.

Finally, the Union's competence in the given field is somehow unclear. Since the potential use of eID ranges across different fields, from 'internal market' (shared competence) to

---

[78] As noted in the STORK report: "The eID's in the various Member States differ in the amount and nature of the attributes they contain. On the one extreme we have the Dutch DigiD, which only contains the identifier BSN. On the other extreme we have eIDs, such as the Portuguese Cartão de Cidadão which contains name, date and place of birth, date and place of issuance of the card, validity period of the card, parents, marital status, title and number of the card, picture and handwritten signature, residence, and National register number, the holder's address and two digital certificates, one for identification and authentication and one for a qualified electronic signature." (Leenes et al., *op.cit.* p.41)

[79] Graux, Majava, and Meyvis, *op.cit.*, pp.122-123.

[80] Although it should be noted, that the e-Signature Directive created an exception for CSPs issuing PKI based certificates, since even foreign entities can be accredited after meeting requirements, which are the same for national and foreign providers.

administrative cooperation (supporting action) it will be difficult to choose (and sustain) the most suitable area of Union's action. In this regard, the already mentioned paragraph 7 of article 8 of the Privacy Directive should be born in mind.[81] With the Lisbon Treaty, through Article 77 (3) TFEU,[82] the Union was granted new competence in the field of identity cards, but the heading of this article - border checks and immigration policies - suggests that it would not provide an appropriate legal basis for a fully functional eID.

Having said that, one might wonder, whether we should even try to establish a pan-European eID system, before we first resolve all the mentioned issues at the national level? The answer is quite optimistic: yes we should, because we have done it before! Earlier examples show that pan-European initiatives may prove to be successful alternatives living side by side with local initiatives. In the next section we will explore one of these initiatives a bit further in detail, the .EU TLD system and make an analogy with a possible introduction of a .EU ID system.

8.3 Lessons learnt from .euTLD

In this section, we will explain the basic characteristics of the .eu domain name system and outline the way it works. We will further try to apply principles identified within this system to outline a similar way for establishing a pan-European eID system. We will only consider features which might be relevant for such an eID system and we will therefore not go into much detail on other features.

The .eu Top Level Domain (TLD) was established as a voluntary domain name system (DNS), with the aim to promote the use of and access to the Internet networks and virtual markets, and consequently increase choice and competition.[83] On the basis of Art.171 TFEU two regulations were adopted. First, Regulation 733/2002 on the implementation of the .eu Top Level Domain, and second, Regulation 874/2004[84] which laid down more specific public

---

[81] Article 8.7 of the Privacy Directive: "Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed"

[82] Article 77 (3) TFEU: “If action by the Union should prove necessary to facilitate the exercise of the right referred to in Article 20(2)(a), and if the Treaties have not provided the necessary powers, the Council, acting in accordance with a special legislative procedure, may adopt provisions concerning passports, identity cards, residence permits or any other such document. The Council shall act unanimously after consulting the European Parliament.”

[83] Recital (4) of the Regulation (EC) No 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain, OJ L 113, 30.4.2002, p.1 (Regulation 733/2002).

[84] Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration, OJ L 162, 30.4.2004, p.40 (Regulation 874/2004).

policy rules and principles governing registration. The registration was opened to the public in April 2006 and since then the .euTLD grow quickly to the present number of nearly 3.5 million registered domains.[85]

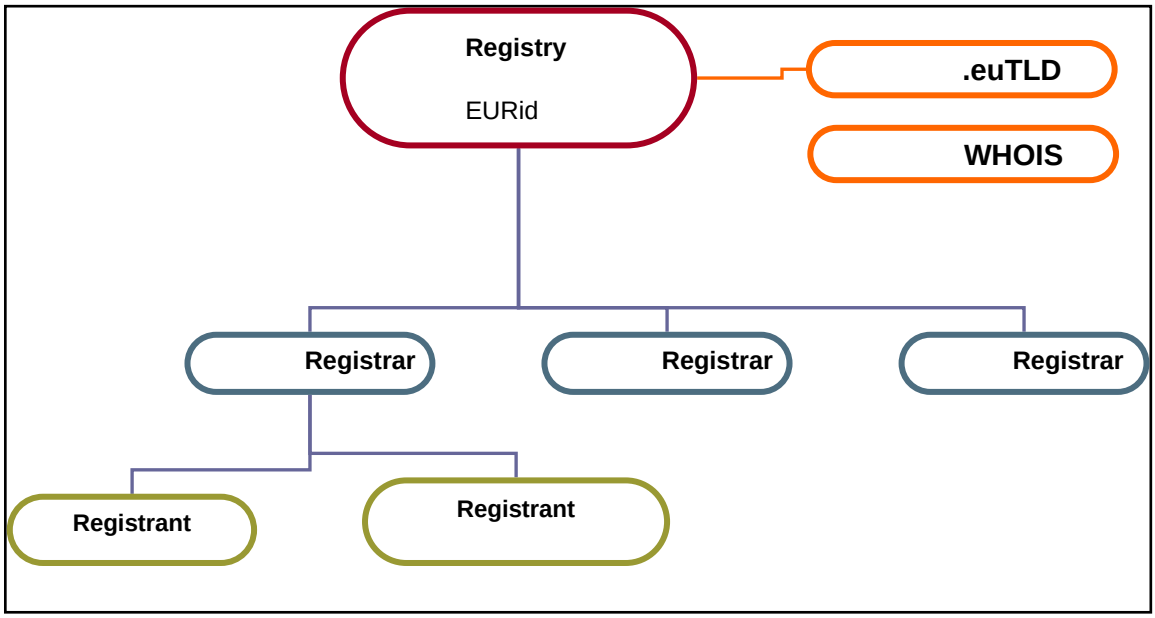


Figure 1: .euTLD system

The whole system is organized in a rather simple way (see figure 1). On the basis of Regulation 733/2002 a central **Registry** was selected through public procurement. The Registry had to be "a non-profit organization, formed in accordance with the law of a Member State and having its registered office, central administration and principal place of business within the Community"[86]. The *'call for expressions of interest*' was published in the Official Journal and subsequently the Commission entered into contract with the selected organization - EURid. The contract specifies the conditions of administration and management of the .euTLD by the Registry, and provides the Commission with supervising powers.[87] The Registry is responsible for the accreditation of registrars and is not itself involved in registering domain names with the registrants, instead it merely approves or rejects registration requests submitted by registrars. This is an important feature of the system, since it resolves any potential language requirements and local identification issues. The process of accreditation "should be objective, transparent, and non-discriminatory", and

[85] http://www.eurid.eu/ (accessed on 23.September 2011).

[86] Art. 3.2, Regulation 733/2002.

[87] Ibid., Art.3.1(c).

"only parties who meet certain basic technical requirements to be determined by the Registry should be eligible for accreditation".[88]

A **Registrar** is "a person or entity that, via contract with the Registry, provides domain name registration services to registrants"[89]. It is important to point out, that the term 'entity' means *any* entity and not only European based natural or legal persons. Hence, the system is open to free competition of registrars that comply with relevant domestic legislation and additional minimum requirements. These requirements are stipulated in the model agreement[90] that the Registry concludes with registrars and include mainly minimum technical requirements[91] and privacy policy concerns[92]. The agreement is concluded for a period of one year and is automatically renewable, but the Registry can terminate the agreement in case the registrar breaches its obligations.

In addition, registrars may voluntarily choose to subscribe to the **Code of Conduct**,[93] in order to distinguish themselves from other competitors and to gain a possible market advantage. The Code of Conduct is a voluntary instrument of self-regulation, which promotes accountability within the registrar community and regulates issues that would be difficult to address through a legal framework. It provides for a complaint procedure to deal with customers complaints and thus creates an additional layer of supervision.

A **Registrant** eligible for .euTLD is an entity (undertaking, organisation or natural person)[94] *residing* within the Union. Registrants are free to choose (and change) registrars which they enter into contract with. At the same time, registrants have to agree to general Terms and Conditions[95] issued by the Registry, and provide the registrar with certain necessary information.[96] The registration of domain names is governed by the first-come, first-served principle.

---

[88] Recital 3, Regulation 874/2004.

[89] Art.2(b), Regulation 733/2002.

[90] Available at: http://www.eurid.eu/en/become-registrar (accessed on 23.September 2011).

[91] As also required under recital 3 of the Regulation 874/2004, and in more concrete terms in Article 2.5 of the EURid Agreement.

[92] These are expressed in Art.9 of the EURid Agreement and basically refer to relevant European rules (especially directive 95/46/EC - Data Protection Directive, Commission Decision 2002/16/EC and Safe Harbour Privacy Principles).

[93] Available at: http://www.coc.eu/ (accessed on 23.September 2011).

[94] Art.4.2(b), Regulation 733/2002.

[95] Available at: http://www.eurid.eu/en/eu-domain-names (accessed on 23.September 2011)

[96] Art.3, Regulation 874/2004.

The .euTLD system provides also for a central WHOIS database[97] and an Alternative Dispute Resolution (ADR) mechanism, conducted by an independent body selected by the Registry.[98]

8.3.1 Application to eID

Applying the .euTLD system outlined above to the European eID context, one should in the first place stress the importance of the chosen regulatory instrument. The successful establishment and swift implementation of .euTLD system was (partly) caused by the decision to employ a Regulation as a basis for its legal framework. It allowed the creation of a system that relies in its operation on local legislation (through registrars); nevertheless its main infrastructure is independent from Member States' diverse legal environments. There was no need for extensive harmonization, since the system only imposed some minimum standards for interoperability and left all the practical issues with Member States. The same approach will be crucial for setting up a European eID system with a similar simplicity.

Drawing inspiration from .euTLD system, it is possible to imagine the whole system as a kind of federated identity management system,[99] where the eID (IP address of the website) is stored in a central database (Domain Name Server) and provided upon request to a competent party.

A European eID framework could be based on the same TFEU articles as .euTLD regulations (Art.170-172), since the scope of these articles provides the necessary legal basis, as already suggested in their Title - 'Trans-European networks'.

Art.170 provides:

"To help achieve the objectives referred to in Articles 26 [internal market] and 174 [economic, social and territorial cohesion] and to enable citizens of the Union, economic operators and regional and local communities to derive full benefit from the setting-up of an area without internal frontiers, the Union shall contribute to the ***establishment and development of trans-European networks*** *in the areas of transport,* ***telecommunications*** *and energy infrastructures." [emphasis added]*

Art.171 further provides that in achieving these objectives, the Union:

---

[97] WHOIS database features information about the registered domain names owners (registrants) and about managing registrars. This information is submitted by the registrars and the obligation to provide necessary data is provided for in the contract with the Registry. Anyone can access the WHOIS database through EURid website and check the status, the owner and the registrant of any .eu domain. See also: Art.16, Regulation 874/2004.

[98] Art.22, Ibid.; ADRs are currently handled only by the Czech Arbitration Court (http://eu.adr.eu/).

[99] See: Smedinghoff, *op.cit.*

*"(...) — shall implement any measures that may prove necessary **to ensure the interoperability** of the networks, in particular in the field of technical standardisation, (…)"*

8.3.2 The principles of a possible eID legal framework

The **eID Registry** would be selected through public procurement after publishing a *'call for expressions of interest*' in the Official Journal. The Registry would have to be a non-profit organisation, formed in accordance with the law of a Member State, and have its registered office, central administration and principal place of business within the Union. In this way, an impartial and most suitable choice could be made, and entities from all Member States could take part in the tender. After the Registry is established, it would authorise all registrars (identity providers or certification service providers [CSP]) through the conclusion of a model agreement and act as a supervising authority. Therefore, it could not itself act as an identity provider or a certification authority. The Registry would further establish the central database of the system, manage the information submitted by registrars and ensure the interoperability of the system, through designating necessary standards with a regular review according to evolving technological standards.

The **Registrars** would act as identity providers or Certification Service Providers (hereinafter referred to as **identity providers**). They would have to comply with domestic legal rules, and, if outside the Union, with relevant European legislation (Data Protection, etc.). Identity providers would apply local registration requirements. This would be an important feature of the system, since it solves the conflict between different national frameworks. In addition, there would be no need to address language requirements in the regulation, since all procedures regarding end-users' registration would be conducted at domestic levels, according to domestic rules and through identity providers registered with competent domestic authorities. On the other hand, identity providers would have to adhere to common rules and comply with minimum standards set up by the Registry. This would solve the problem of interoperability and diverse technical standards. Finally, identity providers would have a possibility to accede to voluntary self-regulation instruments (e.g. Code of Conduct), demonstrating their commitment to provide services of a higher standard.

The key feature of the above outlined system is, that in order to work it does not require a comprehensive IAS European framework to be put in place. First, the process of identification and establishment of eID is left with local identity providers, who must ensure compliance with local legislation. In this way, sensitive issues of national identification policy are left with the Member States. The Registry thus acts as a mere recipient of standardised eID credentials, after the identity provider carried out a process of identification at local level and according to local rules. Second, by delegating identification process to local identity providers, the language requirements and local identification issues will be solved on the domestic level and will not create cumbersome barriers for the whole system. This is

certainly not to say, that there is no need for an elaborated IAS framework at European level, but the proposed system could provide an important kick-start for further development, as well as fill-in the gap in the current framework.

Moreover, the system would ensure supervision on multiple levels. First on domestic level, competent authorities would carry out supervision over identity providers operating within their jurisdiction, the same identity provider would further be under supervision of the Registry, which would ensure that common standards are complied with in all Member States. Finally, the Registry itself would be under scrutiny of competent European authorities (the Commission), which are also already monitoring Member States' authorities. To close the circle, European authorities are reviewed by European citizens through European Parliament and by Member States through the Council.

The system would operate as a '**user-centric**' identity management model. In user-centric systems users have greater control over their personal information. As noted above, users will be free to choose their identity provider, independently from service providers (relying party) in order to receive their services. Users thus do not communicate their personal details directly with the relying party, instead identity providers act as trusted third parties that authenticate and store user's information. The relying party then simply accepts identity assertion provided by identity providers. "*In this model, users choose what information to disclose when dealing with service providers in particular transactions – although service providers may still require certain information for the transaction to take place.*"[100] Identity providers in user-centric model are separated from relying parties and should therefore operate in the interest of users (their customers) rather than relying parties. This should gain consumers a greater 'bargaining' power in determining what information is necessary to disclose in each type of transaction. Moreover, users may choose several identity providers so that the information is not stored all in one place.[101]

Since the system will operate with a number of identity providers acting as trusted third parties, it must be based on the *Circle of Trust* principle. This means that each participating identity provider is trusted to accurately document the processes used to identify an entity, the type of authentication system used, and any policies associated with the resulting authentication credentials.[102] The 'model agreement' with the Registry could serve as a necessary prerequisite for the principle, since the agreement would be the same for all

---

[100] OECD, *op.cit.*, p. 17.

[101] Ibid.

[102] For more detailed explanation of Circle of Trust concept, see e.g.: The Liberty Alliance Project, *Liberty Alliance Contractual Framework Outline for Circles of Trust*, available at: http://projectliberty.org/liberty/files/whitepapers/liberty_alliance_contractual_framework_outline_for_circles_of_trust

identity providers. The rights and responsibilities relating to identification requirements could be defined as a separate set of standards maintained by the Registry and easily modifiable in case of technological progress or any other need.

Instead of a central WHOIS database featured in the .euTLD system,[103] the eID system would provide a **central database** with a list of trusted certificates. In this way, relying parties would be able to simply (and even automatically) check the validity of a certificate provided by a third party. The database would operate on the basis of established Online Certificate Status Protocol (OCSP),[104] and would therefore enable simple, fast and for the end-user fully automatic verification of the certificate employed.

To complete the comparison with the .euTLD system the need for **Alternative Dispute Resolution** (ADR) mechanism in the presented eID system is not evident. The ADR could prove useful in disputes between the Registry, registrars (identity providers) and relying parties, since these would otherwise be governed by different local jurisdictions. The ADR could therefore facilitate a uniform procedure for all identity providers involved in the system, creating an additional layer of trust in relying party vis-à-vis identity provider situations. As for the disputes between identity providers and users (their customers), the ADR would probably not be a suitable solution, since possible disputes would have to deal with local legislation concerning registration, privacy policy and data protection rules.

To conclude, drawing inspiration from the .euTLD system, a possible legal framework for eID would be based on three main regulating instruments: (i) EU regulation, (ii) contractual agreements, and (iii) self-regulating instruments. (i) The regulation would set up the basic legal framework, the system's central infrastructure, harmonize definitions and provide a clear level-playing field for stakeholders. (ii) Contractual agreements would provide more detailed rules for day-to-day operation and would harmonize requirements for stakeholders to take part in the system, consequently creating a circle of trusted parties. A contractual basis would also allow for further, relatively easy, changes to the system. Technical as well as policy amendments could be made easily, without a need for a lengthy and cumbersome legislative process. (iii) Lastly, (voluntary) self-regulating instruments such as Codes of Conduct (together with appropriate rules and procedures for their enforcement), could positively influence a competition on the market, help end-users to make an informed decision and overall higher the level of services offered.

---

[103] See No.62 *supra.*

[104] For a basic explanation, see e.g.: Wikipedia, or SearchSecurity.

8.4 Characteristics of a possible pan-European eAuthentication system

8.4.1 Inherent dilemma

The system, as outlined in the section above, holds an inherent dilemma: the more legal consequences will be linked to the model, the more difficult it will be to have it accepted by the Member States. This is quite important to realize, since we are trying to establish a functional IAS model on the basis of only very limited European legal foundations in this area. We should keep in mind, that while some Member States are in favour of such systems and will probably support its wide utilisation and legal acceptance, others might be much more cautious and restricted in their approach.

We will therefore set aside a discussion about precise legal effects and services to be offered within the system. Instead, we will only examine the general requirements the proposed model should have, in order to distinguish itself from already existing systems and thus offer new benefits for its users. The list is in no way fully comprehensive nor exhaustive. It is recalled, that it will be firstly the Member States who will determine the final outcome of the system outlined in this chapter. Their willingness to embrace the system and their ability to implement it within the national rules will be crucial for its success, or failure.

8.4.2 Voluntary

The proposed system should be an alternative to already existing systems. It should be able to attract 'customers' by providing an added value, which other services cannot offer (mutual recognition, legal acceptance in cross-border situations, easy and secure way to identify oneself and others, etc.). As already stressed above, existing systems will be without doubt more suitable for many online activities and the proposed system will not therefore aim to replace these. Clearly, some users will not even make use of the system and they should therefore not be forced to embrace it. Existing systems and initiatives could cooperate with the system and provide additional services.

Hence, the main rationale for a European eID system is offering a missing service that could facilitate new opportunities for internal market and make free movement of goods, services, capital as well as persons within the Union even more possible. Once necessary rules and infrastructure will be in place, businesses, governments, service providers and individuals will be encouraged to implement the system on a voluntary basis. They should perceive the system as a reliable way to conclude transactions and deal with communication they were used to carry out only in an offline fashion, due to the high trust-value requirements and need for authentication of the claims.

Identity providers could participate in the system after fulfilling some minimal requirements and after acceding to the agreement with the Registry. Users will benefit from the free competition on the market, since they will be able to choose the provider that will be most suitable for their profile. New as well as existing organizations can participate in the system as identity providers - many entities already provide similar services and this could be additional 'product' in their portfolio (e.g. banks, eSignature CAs, governments, 'regional' administrations, etc.). Moreover, the competing environment should encourage new research and development, to provide potential customers with the best solution. In this way, stakeholders engaged in the system would be encouraged to keep up with the current technological development in the area, which is a very desirable feature in constantly developing area of technology.

8.4.3 User friendly

For an average end-user, the easy-to-use interface and convenience will be crucial factors for her decision to participate in the system. The existing possibilities should be explored and existing end-user devices used as much as possible. In first instance, the system should work with already widely employed PKI certification systems. This would enable identity providers to 'install' necessary tokens for users' eIDs on devices they already possess (e.g. smart card, USB, mobile phone, etc.). Accordingly, users would have a possibility to choose solutions they prefer the most. An additional benefit of this approach would be that users could apply procedures they are already familiar with.

8.4.4 Secure

Security should be another crucial aspect of the system. Apart from technological requirements and the need to keep up with the latest development in the field, further obligations would be imposed on participating parties. A strict compliance with relevant rules and especially data protection and privacy policy must be observed at all levels. The competent national authorities should carry out a rigorous supervision over identity providers under their jurisdiction. Likewise, competent European authorities would review the operation of the Registry and make sure that uniform rules apply to all identity providers. Users would also have a certain level of responsibility. They would be required to employ reasonable precautionary measures to prevent misuse of their eID, the same obligation which they already have with regard to their bank cards.

Through agreement with the Registry, the identity providers would be authorised to use the system and users could be sure that these entities have to comply with relevant EU and

national legislation. The system would therefore enhance the level of trust in online services connected to the system, because users would know that the entity behind the website was reviewed and authorized by competent authorities.

8.4.5 Privacy

Often an eID includes more information than will usually be necessary for most transactions, therefore, the system should treat each authentication request on a case-by-case basis, or rather create categories of requests necessary for a given transaction type. In this way, users would gain additional privacy benefits when using the system. The users would no longer be pushed to 'over-identify' themselves in order to gain access to a certain service. Only specific attributes related to the transaction should be corroborated (e.g., to the question: "Is the user older than 18?" the system would provide only "yes/no" answer, and not the user's whole birth date). Relying parties could not argue that users have to provide them with extensive personal information, so they can be sure they will be able to identify the user in case there is a legal need. Instead, the system would provide them with only limited information necessary for the given transaction and more complete information would be revealed only in case there is a legitimate need (e.g., in case of legal dispute). *Attribute authentication* would therefore be a key feature in bringing more privacy to users, who could be sure that they only provide information which is necessary.

8.4.6 Custom made

The system could also provide for certain adjustments to accommodate individual needs. There could be a possibility to enable only certain services (e.g., eGovernment services and document signing) and to disable others (e.g., eBanking, online shopping). The issued eID's could therefore offer a wide variety of authentication 'levels' and functions. For example: minors could be issued with an eID that could be used only to authenticate themselves for 'safe-chat' services; whereas their parents could use their eID for the whole range of services. This is certainly not a new concept (since even bank cards offer a variety of options and associated services), but having the possibility to enable/disable a wide range of services using a simple system would bring more convenience for users, open new possibilities for service providers and businesses, as well as provide solution for some unresolved issues like safe-chat and safe online activities for children.

8.4.7 Portability

It has become a growing trend to base trust in some online situations mainly on reputation acquired over the time in a certain online community. A typical example would be the user's

profile on a discussion forum, where she, over time, builds up a certain reputation as a natural consequence of her activities. Thus, members of the forum will soon be divided in different categories associated with different experience and trust levels. When a new user joins the forum, she will be able to immediately recognize 'experienced commentators' and ascribe a higher trust value to their posts. Accordingly, even users with high level of experience or trust from an offline world will have to firstly build up their reputation within the given community, before their comments will be taken seriously.[105]

Increasingly, other online services are starting to apply the same model. The prominent example being online auction sites (such as eBay), where the necessary trust-level in individual-to-individual transactions is based on the individual's reputation, built up on reviews provided by other users of the system. Online reputation is thus becoming an increasingly important factor even in the course of trade and commercial transactions. It is however difficult, if not impossible, to transfer one's reputation across different websites and services, and users are required to start from scratch each time they change a service provider.

The proposed system could provide a solution for this problem. The service provider, with whom the user had already established his reputation, would simply issue the user with a credential that could be attached to the user's eID and could then be used with other service providers. Moreover, as suggested in the PRIME white paper,[106] the whole process could still be conducted in an anonymous fashion, so users would be able to use their pseudonyms and their real identity would remain hidden. The credential's validity could be checked with the issuing service provider, without disclosing a link between user's pseudonym and identity; unless there would be a legitimate reason for disclosing it, e.g., in case a user would breach her contractual obligations.[107] In such case, under strict conditions, the user's identity could be revealed by linking the given credential with a specific pseudonym and the user's real identity.

8.4.8 Drawbacks of the proposed system

Even though the proposed system would be relatively simple and based on an existing example (.euTLD), the possible drawbacks and weaknesses should also be noted.

---

[105] This will not always be the case, but the example provides a clear explanation of the issue. For a practical example, see e.g.: Leenes, R., Schallaböck, J., and Hansen, M., *Prime (Privacy and Identity Management for Europe) White Paper*, (2008) Prime White paper, pp.10.

[106] Ibid.

[107] Ibid., pp.10-11.

The main disadvantage of the eID system based on the example of .euTLD is, that it would not provide a comprehensive IAS framework. The issues identified in the above sections, such as the lack of common taxonomy and identification standards, would remain mostly unresolved. The system would be a simple way to interconnect national legal frameworks and make them more or less interoperable, but taking DNS as an inspiration for an IAS system may prove an inadequate choice, as the DNS system is far less complex. Further actions on European level would certainly be required to set up a fully operational IAS system for the future.

Furthermore, as already noted, the final result would be heavily dependent of the Member States' willingness to associate the use with specific legal consequences and provide for a mutual recognition in cross-border situations. This will not be an easy process, since the legal position of similar systems at national level is also quite complicated. Some minimum legal effects could be prescribed by the regulation introducing the proposed system, however, these will have to be rather low requirements in order to gain sufficient support for the legislative process. In the same time, without at least minimum legal requirements, the system would not provide many additional benefits compared to already existing mechanisms and could therefore turn up useless.

Besides, once the necessary legislation would be agreed upon, more 'practical' risks associated with the system should not be underestimated. As the proposed model would possibly include a considerable amount of personal information, the consequences in case of security breach might be quite severe. Therefore, a high technical reliability and security standards would have to be employed inside the system. This might not be a great challenge at the beginning, but with a growing size and utilisation of the system the possibility of security attacks would also be growing. A vast amount of personal data in the system would be an invitation for hackers to 'test their skills' and would represent an attractive target.

Moreover, the independent and impartial supervision must ensure that the system would not be abused by any stakeholder, be it in the private or public sector. Since the proposed model could be used as a powerful source of information by both enterprises and governments, users have to be sure that their data would only be accessible when there is a legitimate need and under strict conditions. The control mechanisms would have to be arranged in a way that would be most beneficial for users and would limit access to the information not only for private parties, but also for public bodies.

Lastly, it is not guaranteed that end-users would spontaneously embrace the new model, once it would be available. It should be remembered, that an average internet user might not be aware of risks (and benefits) associated with the different types of IAS systems they use. For an average user, the main concern is simply whether the system they are currently using works easily or not. Issues of privacy and legal certainty might not come to their

attention. For advanced users, on the other hand, existing systems might provide sufficient means to conclude transactions they need to.

Thus, before the introduction of the system proposed in this chapter, it might first be necessary to persuade users that these are qualities that actually matter. In this respect it is essential to raise users' awareness about important issues of privacy, legal certainty and accountability in currently employed IAS systems. As with any other product offered on a voluntary basis, the producer should first make sure, that there would be a sufficient demand for its product. This chapter tried to make clear, that there is a *need* for a more reliable and legally predictable IAS model. Whether there is also a sufficient *demand* for this new model, might be a different question.

8.5 Conclusion

It was not the purpose of this chapter to design a definitive and detailed solution for a complete and fully functional pan-European eAuthentication system. Instead, it merely tries to pinpoint a possible direction on our way to establishing a comprehensive IAS legal framework. Like many others, this chapter calls for further harmonization and comprehensive legal instruments on the European level. However, it also tried to argue that there might be an easier and faster way to set up a functional pan-European eAuthentication and even eIAS system.

We tried to show that Europe has already succeeded before in establishing a similar system, in an area with different national policies, definitions and legal frameworks. Drawing inspiration from the .euTLD, we tried to demonstrate, that it is not always necessary to employ wide-ranging and comprehensive legal instruments to set up a pan-European system. Instead, the same aim might be realized with relatively simple regulations, interconnecting, rather than adapting, existing national frameworks.

Notwithstanding the fact, that a functional pan-European eAuthentication system, as proposed in this chapter encompasses much more difficulties than the relatively simple .euTLD domain name system, we could still draw an important inspiration from its organization and arrangement. This could enable a swift and (compared to a more comprehensive approach through harmonization and directives) rather easy establishment of a European eAuthentication system. In this regard, it should be pointed out, that Europe indeed has to act without much delay. With emerging *quasi*-identification systems, such as Facebook, Twitter or Google, the need to act quickly in this field is ever more pressing, since these services may soon gain a status of *de-facto* standards in the information society, and it will become difficult to subsequently replace them with a meaningful solution based on a clearer and more reliable legal foundation.

The main responsibility will thus lie with the Member States, who must decide how fast they want to act (whether they want to act at all) and how far they want to go. The solution outlined in this chapter will not be complete, nor permanent, but it could provide an important kick-start for further discussion in the IAS field and as a first patch to address some gaps in the current legal framework. At any rate, Europe cannot afford to wait for long, if it wants to keep up with the constant development in the information society.

8.6 References

a. Publications

- Andrade, N. N. G. d., *Towards a European eID regulatory framework. The Legal Gaps, Barriers and Challenges of constructing a legal framework for the protection and management of electronic identities*, (2012 - forthcoming) European Commission, Joint Research Center.

- Graux, H., *Rethinking the e-signatures Directive: Moving towards a comprehensive legal framework for eID*, (2011) IPTS workshop - Electronic identity for Europe.

- Graux, H., Majava, J., and Meyvis, E., Study on eID Interoperability for PEGS - Update of Country Profiles - Analysis & Assessment Report, (2009) IDABC programme (available at: http://ec.europa.eu/idabc/servlets/ Docb482.pdf?id=32522, accessed on 26.September 2011).

- Hartmann, D., Körting, S., Security issues in cross-border electronic authentication, (2010) The European Network and Information Security Agency.

- Leenes et al., Stork - Towards Pan-European Recognition of Electronic IDs (eIDs) - D2.2 - Report on Legal Interoperability, (2010) STORK, available at: https://www.eid-stork.eu/.

- Leenes, R., Schallaböck, J., and Hansen, M., Prime (Privacy and Identity Management for Europe) White Paper, (2008) Prime White paper.

- Myhr, T., Regulating a European eID: A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID, (2005) The Porvoo e-ID Group.

- OECD, The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers, DSTI/ICCP/REG(2008) 10/FINAL. (available at: http://www.oecd.org/dataoecd/23/ 38/43195291.pdf, accessed on 26.September 2011).

- Rooy, D.v., Bus, J., Trust and privacy in the future internet—a research perspective, Identity in the Information Society (2010) Vol. 3, No.2, (available at: Springerlink.com).

- Smedinghoff, T.J., Federated Identity Management: Balancing Privacy Rights, Liability Risks, and the Duty to Authenticate, (2009) available at: http://papers.ssrn.com/sol3/papers. cfm?abstract_id=1471599 (accessed on 23.September 2011).

- Commission, European, *A Digital Agenda for Europe*, COM(2010) 245 final/2.

- Commission, European, Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, COM (2008) 798 final.
- Commission, European, *A Roadmap for a pan-European eIDM Framework by 2010*, Information Society and Media Directorate-General, eGovernment unit, v1.0.
- Commission, European, Towards interoperability for European public services, COM(2010) 744 final.
- The Liberty Alliance Project, Liberty Alliance Contractual Framework Outline for Circles of Trust, available at: http://projectliberty.org/liberty/files/whitepapers/liberty_alliance_contractual_framework_outline_for_circles_of_trust (accessed on 23.September 2011).
- Van Rooy, D., Bus, J., Trust and privacy in the future internet—a research perspective, Identity in the Information Society (2010) Vol. 3, No.2, (available at: Springerlink.com).

b. Legislation

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ L 281 (1995).
- Directive 1999/93/EC on a community framework for electronic signatures; OJ L 13 (2000).
- Directive 2006/123/EC on services in the internal market; OJ L 376 (2006).
- Regulation (EC) No 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the .eu Top Level Domain, OJ L 113, 30.4.2002.
- Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration, OJ L 162, 30.4.2004.

c. Other sources:

- http://www.facebook.com/press/info.php?statistics
- http://www.facebook.com/terms.php
- http://www.google.com/accounts/TOS
- http://twitter.com/tos
- http://epp.eurostat.ec.europa.eu/

- http://www.eurid.eu/

9. Annex A – Recommendations for an IAS Regulation

This Annex details a series of inputs, including definitions, basic principles, obligations for service providers and a supervision mechanism, which were offered by the study team as an input to the European Commission's legislative work on the IAS Regulation. Some of the inputs of this deliverable have been taken into account by the Commission, whereas others have been superseded by further policy developments since their production.

9.1 Building blocks for General Provisions

9.1.1 Possible provisions for scope

1. This Regulation applies to the following trust data:

- electronic signatures
- electronic seals
- electronic time stamps
- electronic identity attestations, and
- electronic attribute attestations

within the meaning of this Regulation

2. This Regulation applies to trust services supporting the creation, validation and preservation of trust data[108], and the following ancillary services:

- electronic document delivery services
- electronic archiving services
- digitalization services

within the meaning of this Regulation

3. This Regulation does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by

[108] Examples of supporting services: Certification Authority, Signature Validation Authority, Time Stamping Authorities, Registration Authority, Identity Providers (official/non-official), Identity Attestation Service Providers

national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

4. This Regulation does not impose any obligations nor restrictions on the Member States in relation to the issuance of identity documents, travel documents or any other identifying documents issued to their citizens by public administrations or under their authority.

5. No part of this Regulation shall affect the rights of citizens, business or public administrations to conclude contractual arrangements governing the issuance, validation and legal effect of electronic transactions.

9.1.2 Possible provisions for definitions

- "trust data" means data in electronic form which are attached to or logically associated with other electronic data and which corroborates [*confirms*] the origin and the integrity of the associated data[109]
- "qualified trust data" means trust data meeting the applicable quality requirements as laid down in this Regulation.
- "trust services" means services supporting the creation, validation and preservation of trust data, as well as ancillary services, specifically designed to enable the use of trust data.[110]
- "qualified trust services" means trust services meeting the applicable quality requirements as laid down in this Regulation.
- "trust service provider" means the natural or legal person, public authority, agency or any other body which provides one or more electronic trust services.
- "electronic signature" means trust data added by a signatory to the associated data with the intent to sign on his own behalf, on behalf of a legal person or a public sector body. [111]
- "electronic seal" means trust data added by an entity to the associated data on behalf of a legal person or a public sector body with the intent to seal or stamp.

---

[109] Such trust data could be created by an individual (eg signature) or by TTP (time stamp). The main objective of this definition is to create an equivalent to the concept of 'authentication', which is not stricter then the current definition of anelectronic signature in the eSignatures Directive

[110] Generic telecommunication and ISP services are excluded from this scope

[111] Note that this does not exclude simple "I agree" buttons, (PIN) codes, scanned signatures, etc/

- "electronic time stamp" means trust data establishing that associated data existed at a particular time.
- "electronic identity attestation" means trust data establishing that associated data is a collection of an entity's identity attributes uniquely representing that entity.
- "entity" means any natural or legal person or any information system.
- "signatory" means any natural person creating an electronic signature
- "identity attribute" means a distinct, measurable, physical or abstract named property belonging to an entity.
- "electronic identity attribute attestation" means trust data establishing that associated data is a collection of an entity's identity attributes.
- "qualified electronic certificate" means a qualified electronic identity attestation linking an entity to unique data, such as codes or private cryptographic keys.[112]
- "trust data product" means hardware or software, or relevant components thereof, which are intended to be used for the creation, validation or preservation of trust data or are intended to be used by a trust service provider for the provision of trust services.
- "qualified trust data product" means a trust data product meeting the applicable quality requirements as laid down in this Regulation.
- "conformity assessment body" means a body that performs conformity assessment activities within the meaning of article 2.13 of Regulation 765/2008.
- "registered electronic mail service" means any service provided by a trust service provider regarding the transfer of data whereby the sender upon his request, receives an acknowledgement of the submission and/or of the delivery to the addressee.

9.2 Building blocks for Basic Principles

9.2.1 Possible provisions for market access

[112] The definition relates to both non-repudiation (signature) certificates and authentication certificates. difference between identity attestation and certificate is that certificate is linked to key (PKI based).

1. Member States shall not make the provision of trust services and trust data products subject to prior authorisation. Member States shall not limit the number of trust service providers or trust data products.

2. Each Member State shall ensure the establishment of an appropriate system for the supervision of qualified trust services provided by trust service providers which are established on its territory and qualified trust data products that have undergone a conformity assessment by an entity established on their territory.

3. The conformity of qualified trust data products shall be assessed against the requirements laid down in this Regulation by conformity assessment bodies.

4. Without prejudice to the provisions of paragraph 1, 2 and 3, Member States may extend the scope of their supervision system to non-qualified trust services provided by trust service providers established on its territory. All supervision criteria related to such systems must be objective, transparent, proportionate and non-discriminatory.

9.2.2 Possible provisions for Internal market principles

1. Member States may not restrict the provision of trust services originating in another Member State in the fields covered by this Regulation.

2. Member States shall ensure that trust data products which comply with this Regulation are permitted to circulate freely in the internal market.

9.2.3 Possible provisions for non-discrimination principle

Member States shall ensure that trust data is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form or it is not qualified trust data.

9.2.4 Possible provisions for generic quality requirements for trust service providers providing qualified trust services

Trust service providers providing qualified trust services must demonstrate the reliability necessary for providing trust services, by at least

- employing personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in relevant technology and familiarity with proper security

procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;

- maintaining sufficient financial resources to operate in conformity with the requirements laid down in the Regulation, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
- before entering into a contractual relationship with a person seeking to use a trust service informing that person by a durable means of communication of the precise terms and conditions regarding the use of the trust service, including any limitations on its use, the existence of a supervision system and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the trust service;
- using trustworthy systems and trust products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
- taking measures against forgery of trust data provided by the trust service provider
- record all relevant information concerning trust data issued by the trust service provider for an appropriate period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings. Such recording may be done electronically;
- use trustworthy systems to store trust data provided by the trust service provider in a verifiable form so that:
    - they are publicly available for retrieval in only those cases for which the consent of the person to whom the trust data has been issued, has been obtained,
    - only authorised persons can make entries and changes,
    - information can be checked for authenticity, and
    - any technical changes compromising these security requirements are apparent to the trust service provider.

9.2.5 Possible provisions for liability of qualified trust service providers

1. As a minimum, by issuing qualified trust data or by guaranteeing such data a trust service provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that trust data

- as regards the accuracy at the time of issuance of all information contained in the trust data, and
- as regards the fact that the trust data contains all the details prescribed for being qualified trust data

unless the trust service provider proves that he has not acted negligently.

2. A trust service provider may indicate in qualified trust data it issues limitations on the use of that trust data provided that the limitations are recognisable to third parties. The trust service provider shall not be liable for damage arising from use of that trust data which exceeds the limitations placed on it.

3. The provisions of paragraphs 1 to 2 shall be without prejudice to Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

9.2.6 Possible provisions for data protection

1. Trust service providers and national bodies responsible for supervision shall comply with the requirements laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2. A trust service provider which issues trust data may collect personal data only directly from the data subject, or after the explicit consent of the data subject, and only insofar as it is necessary for the purposes of issuing and maintaining the trust data. The data may not be collected or processed for any other purposes without the explicit consent of the data subject.

9.2.7 Possible provisions for international aspects

Trust data which are issued as qualified trust data by a trust service provider established in a third country shall be recognised as legally equivalent to trust data issued by a trust service provider established within the Community

a) if the trust service provider is supervised, or

b) if the trust service provider is recognised as providing qualified trust services under a bilateral or multilateral agreement between the Community and third countries or international organisations.

9.2.8 Possible provisions for standardisation and presumption of conformity

The Commission may, after consultation of the European trust services committee or on its recommendation, establish and publish reference numbers of standards or similar normative documents for qualified trust data products in the Official Journal of the European Communities. Compliance with the requirements laid down in this Regulation shall be presumed for trust data products meeting those standards.

9.3 Building blocks for the Supervision of qualified services

9.3.1 Possible provisions for Supervisory authorities

1. Each Member State shall provide that one public authority is responsible for the supervision of qualified trust services as laid down in article …[113] Member States may provide that the supervision of one or more categories of qualified trust services is delegated to the European supervisory authority.

2. A European supervisory authority shall be designated by the European Commission through delegated acts. The European supervisory authority shall be responsible for

- supervising trust service providers established in a third country providing qualified trust services towards natural or legal persons residing or established in the European Union;
- supervising trust service providers established in a third country providing qualified trust services, at their request;
- supervising trust service providers established in the European Union for which a Member State delegated the supervision.

3. A supervisory authority shall adopt its own rules of procedure and organise its own operational arrangements, including to provide for the continuation of exercising duties when a member's term of office expires or a member resigns, the establishment of subgroups for specific issues or sectors and the appointment of a chair and secretariat.

[113] This should reference the internal market article, and be aligned with it.

9.3.2 Possible provisions for independence and confidentiality

1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it.

2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.

3. Members of the supervisory authority shall refrain from any action incompatible with the duties of the office and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.

5. Each supervisory authority shall be provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers, including those to be carried out in the context of mutual assistance, co-operation and active participation in the European trust services committee.

6. Each supervisory authority shall be provided with its own staff which shall be appointed by and be subject to the direction of the head of the supervisory authority.

7. The supervisory authority shall not be subject to financial control which might affect its independence. The supervisory authority shall have separate annual budgets. The budgets shall be made public.

8 The members and the staff of the supervisory authority shall be subject, both during and after their term of office, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.

9.3.3 Possible provisions for duties

1. The supervisory authority shall:[114]

- appropriately supervise the provision of qualified trust services
- ensure the appropriateness of conformity assessments of qualified trust data products

[114] Details on the exact competences should be addressed by delegated acts, including notably the power to manage/establish list of qualified service providers, dealing with market complaints, sanctions, etc.

- publish the outcome of the supervision activities in a harmonised way

2. The Commission shall be empowered to adopt delegated acts in accordance with Article ... for the purpose of further specifying the procedures, requirements and formalities for performing these duties.

9.4 Building blocks for the establishment of a European Trust Services Committee / EU level governance framework

9.4.1 Possible provisions for European trust services committee

1. A European trust services committee is hereby set up.

2. The European trust services committee shall be composed of the head of the supervisory authority of each Member State and the head of the European supervisory authority.

3. The Commission shall have the right to participate in the activities and meetings of the European trust services committee and shall designate a representative. The chair of the European trust services committee shall, without delay, inform the Commission on all activities of the European trust services committee.

9.4.2 Possible provisions for independence

1. The European trust services committee shall act independently when exercising its tasks within the meaning of this Regulation.

2. Without prejudice to requests by the Commission referred to in Articles [*the commission's right to ask for standards, recommendations, etc*]….., the European trust services committee shall, in the performance of its tasks, neither seek nor take instructions from anybody.

9.4.3 Recommendation on the possible tasks of the European trust services committee

1. The European trust services committee shall ensure the consistent application of this Regulation. To this effect, the European trust services committee shall, on its own initiative or at the request of the Commission, in particular:

- advise the Commission on any issue related to the provision of trust services in the Union, including
    - on any contemplated amendment of this Regulation, or
    - on the adoption of delegated acts and implementing acts within the framework of this Regulation and the conclusion of agreements with third countries, or
    - with respect to standards and similar normative documents, or
    - policies with respect to levels of assurance of trust services and trust data products[115];
- examine, on request of the Commission or on its own initiative or of one of its members, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;
- review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;
- promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;
- promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;
- promote the exchange of knowledge and documentation on trust services legislation and practices worldwide;

2. The European trust services committee shall forward its opinions, guidelines, recommendations, and best practices to the Commission and make them public.

3. The Commission shall inform the European trust services committee of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European trust services committee.

[115] This relates to multilevel quality and assurance levels, such as the STORK QAA policy levels

9.4.4 Recommendation for international co-operation

1. In order to facilitate cross-border trust services with third countries and legal recognition of trust data originating in third countries, the European trust services committee shall engage in discussions in view of facilitating the conclusion of bilateral and multilateral agreements with third countries and international organisations.

2. Whenever the European trust services committee is informed of any difficulties encountered by Community undertakings with respect to market access in third countries, it may, if necessary, submit proposals to the Commission for an appropriate mandate for the negotiation of comparable rights for Community undertakings in these third countries.

9.4.5 Possible provisions for procedure

1. The European trust services committee shall take decisions by a simple majority of its members.

2. The European trust services committee shall adopt its own rules of procedure and organise its own operational arrangements, including to provide for the continuation of exercising duties when a member's term of office expires or a member resigns, the establishment of subgroups for specific issues or sectors and the appointment of a chair and secretariat.

9.4.6 Possible provisions for reports

1. The European trust services committee shall regularly and timely inform the Commission about the outcome of its activities. It shall draw up an annual report on the situation regarding the provision of trust services and trust products in the Union and in third countries.

The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article ….

2. The report shall be made public and transmitted to the European Parliament, the Council and the Commission.

9.5 Building blocks for the regulation of Qualified trust services

9.5.1 Possible provisions for legal effects of electronic signatures

1. Where the law requires a signature, that requirement is met in relation to associated data if an electronic signature is used which is as reliable as is appropriate for the purpose for which the associated data was generated or communicated, in the light of all the circumstances.

2. A qualified electronic signature shall satisfy the legal requirements of a signature in relation to associated data in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data and be admissible as evidence in legal proceedings.

3. Paragraph (2) does not limit the ability of any person: (a) to establish in any other way, for the purpose of satisfying the requirement referred to in paragraph (1), the reliability of an electronic signature; or (b) to adduce evidence of the non-reliability of an electronic signature.

9.5.2 Possible provisions for legal effects of electronic seals

1. Where the law requires a seal or stamp, that requirement is met in relation to associated data if an electronic seal is used which is as reliable as is appropriate for the purpose for which the associated data was generated or communicated, in the light of all the circumstances.

2. A qualified electronic seal shall satisfy the legal requirements of a seal or stamp in relation to associated data in the same manner as a seal or stamp satisfies those requirements in relation to paper-based data and be admissible as evidence in legal proceedings.

3. Paragraph (2) does not limit the ability of any person: (a) to establish in any other way, for the purpose of satisfying the requirement referred to in paragraph (1), the reliability of an electronic seal; or (b) to adduce evidence of the non-reliability of an electronic seal.

9.5.3 Possible provisions for quality requirements for qualified electronic signatures and qualified electronic seals

A qualified electronic signature is an electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;[116]

b) it is capable of identifying the signatory;

c) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

d) it is created [117]

   a. using means [*and/or processes*] that the signatory can reasonably maintain under his sole control[118];

   b. using one or more qualified trust data products and/or services configured and used to implement unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature[119], and meeting the requirements of

   c. ensuring, by appropriate technical and procedural means, that at the least:

- the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
- the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
- the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

   d. not altering the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

e) it can be validated for a period of time that is required [applicable, appropriate] by the circumstances to which the electronic signature applies.[120]

---

[116] a) and b) should still be included because they refer to the whole signature process and not only the identity attestation (cfr. these requirements are also default requirements for identity attestations)

[117] Standards mapping to be introduced through eg. delegated acts.

[118] [Recitals should clarify and emphasise that sole control is not limited to hardware devices like smart cards but can also be achieved by procedures, contracts, etc

[119] Alternatively, the proposal could also reintroduce the definition of "signature creation data", which would achieve the same result.

[120] This can be done by means of an appropriate combination of Trust Data and/or Trust Services and/or procedural means supporting the validation and preservation of electronic signatures (e.g. very short term (before revocation of QC) by AdES-ST form, short term (before expiration of QC) by AdES-T, long term

f) it is supported by a qualified electronic certificate, which is compliant with article … and which is solely dedicated to the support of qualified electronic signatures.

9.5.4 Possible provisions for legal effects of electronic identity attestations

1. Where the law requires the validation of the identity of an entity, that requirement is met in relation to associated data if an electronic identity attestation is used which is as reliable as is appropriate for the purpose for which the associated data was generated or communicated, in the light of all the circumstances.

2. A qualified electronic identity attestation shall satisfy the legal requirements of an entity's identity validation in the same manner as a physical identity document that would satisfy the legal requirements for the validation of the identity of the entity and be admissible as evidence in legal proceedings.

3. Paragraph (2) does not limit the ability of any person: (a) to establish in any other way, for the purpose of satisfying the requirement referred to in paragraph (1), the reliability of an electronic identity attestation; or (b) to adduce evidence of the non-reliability of an electronic identity attestation.

4. Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent trust service providers from indicating in the trust data a pseudonym instead of the entity's name

9.5.5 Possible provisions for Quality requirements for qualified electronic identity attestations

A qualified electronic identity attestation is an electronic identity attestation which meets the following requirements:

1. The identity attestation relies on evidence stemming from trusted sources, such as:

- for identity related information issued by the [Member States'] public administrations or under their responsibility: identity documents, travel documents or any other identifying documents issued to the citizens by these public administrations or under their authority.

AdES-LT, very long term AdES-LTA). Making use of trustworthy (qualified) Trust data or Trust services will increase assurance of meeting this requirement.

- for any other identity attribute: information issued and guaranteed by or under the authority of the entitled entity[121].

2. The attestation has been trustworthy[122] verified by the trust service provider, for example by physical appearance of the entity and/or by validation of the information by/with the entitled entity.[123]

3. The trust service provider issuing the qualified identity attestation, must:

- ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
- ensure that the date and time when the qualified electronic identity attestation is issued or revoked can be determined precisely;
- in case of issuance of a qualified electronic certificate,
- ensure that the certificate meets the requirements laid down in [Annex I] ;
- guarantee confidentiality of the unique data, such as codes or private cryptographic keys, during the process of generating such data;
- not store or copy the unique data, such as codes or private cryptographic keys of the person to whom the trust service provider provided key management services.

9.5.6 Possible provisions for additional liability

1. Trust service providers issuing qualified identity attestations are, as a minimum, liable for damage caused to any entity or legal or natural person who reasonably relies on that qualified electronic identity attestation for assurance that at the time of the issuance of the electronic identity attestation, the accuracy of the identity attributes has been appropriately verified;

2. Trust service providers issuing qualified electronic certificates are, as a minimum, liable for damage caused to any entity or legal or natural person who reasonably relies on that qualified electronic certificate

---

[121] We should find good wording for ensuring that this covers professional organisations (eg. Ordre des Medicins), private entities (eg. supermarket for customers or company for employees).

[122] "trustworthy verification" to be further specified by the Committee.

[123] Alternative wording: verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which the qualified electronic identity attestation is issued;

(a) for assurance that at the time of the issuance of the qualified electronic certificate, the signatory identified in the qualified electronic certificate held the signature-creation data corresponding to the signature-verification data given or identified in the electronic certificate;

(b) for assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the trust services provider generates them both;

3. As a minimum, a trust service provider issuing qualified electronic identity attestations, is liable for damage caused to any entity or legal or natural person who reasonably relies on the qualified electronic identity attestation for failure to register revocation of the qualified electronic identity attestation unless the trust service provider proves that he has not acted negligently.

9.5.7 Possible provisions for legal effects of electronic time stamps

1. Where the law requires proof that data existed at a particular time, including the requirement for dating a document, that requirement is met in relation to associated data if an electronic time stamp is used which is as reliable as is appropriate for the purpose for which the associated data was generated or communicated, in the light of all the circumstances.

2. A qualified electronic time stamp shall satisfy the legal requirements of a time stamp in relation to associated data in the same manner as a time stamp satisfies those requirements in relation to paper-based data and be admissible as evidence in legal proceedings.

3. Paragraph (2) does not limit the ability of any person: (a) to establish in any other way, for the purpose of satisfying the requirement referred to in paragraph (1), the reliability of an electronic time stamp; or (b) to adduce evidence of the non-reliability of an electronic time stamp.

9.5.8 Possible provisions for quality requirements for qualified electronic time stamps

A qualified electronic time stamp is an electronic time stamp which meets the following requirements:

- the verification of the date and/or time attribute based on the coordinated universal time each time the date and/or time must be determined;

- the electronic time stamp is signed using a qualified electronic signature or qualified electronic seal [or any other business controls achieving the same level of trustworthiness[124]].

9.5.9 Possible provisions for additional liability

In addition to the generic liability provisions as laid down in article …, trust service providers within the meaning of article … , are, as a minimum, liable for damage caused to any entity or legal or natural person who reasonably relies on the accuracy of the time and date specified in the qualified time stamp. [125]

9.6 Building blocks for the Regulation of Ancillary services

9.6.1 Possible provisions for legal effects of registered electronic mail

1. The explicit or implicit requirement of a registered mail can be met provided that the sender used an electronic registered mail service[***126***].

2. Subject to the application of specific legal or regulatory requirements regarding registered mail, a qualified electronic registered mail is considered to meet the explicit or implicit requirement of a registered mail.

3. Paragraph (2) does not limit the ability of any person: (a) to establish in any other way, for the purpose of satisfying the requirement referred to in paragraph (1), the reliability of a registered electronic mail; or (b) to adduce evidence of the non-reliability of a registered electronic mail.

9.6.2 Possible provisions for quality requirements for qualified registered electronic mail

A qualified registered electronic mail is a registered electronic mail which meets the following requirements:

The electronic registered mail service is being delivered by a trust service provider who must:

---

[124] Committee will decide (publish) on trustworthy business controls.

[125] No need to include second paragraph on minimum liability as time stamp is just a signature.

[126] Alternative (broader) wording: "electronic document delivery services"

1. Demonstrate impartiality towards the recipients of their services.
2. At the time of deposit of the message, provide the properly identified sender with an acknowledgement of deposit,
    a. signed by the trust service provider with a qualified electronic signature or a qualified electronic seal,
    b. indicating the identification of the trust service provider, the name of the addressee as reported by the sender[127], and
    c. timestamped using a qualified time stamp.
3. Prior to the sending being delivered, with or without proof of sending, appropriately verify the identity of the addressee of the electronic registered mail, or where appropriate the identity of the proxy.
4. Upon request of the sender, deliver the acknowledgement of receipt or refusal of the message by the addressee, or the acknowledgment of non-delivery,
    a. signed by the trust service provider with a qualified electronic signature or a qualified electronic seal,[128]
    b. indicating the identification of the trust service provider, the name of the addressee as reported by the sender or the proxy[129], and
    c. timestamped using a qualified time stamp.
5. The acknowledgment of receipt, refusal or non-delivery must be provided after expiration of a term of [fifteen days], starting from the date of deposit of the message

9.6.3 Possible provisions for requirements for qualified certificates

Qualified certificates must contain:

(a) an indication that the certificate is issued as a qualified certificate;

(b) the identification of the certification-service-provider and the State in which it is established;

(c) the name of the signatory or a pseudonym, which shall be identified as such;

---

[127] Include requirement for "identification number of the message"?

[128] To be discussed if signature also required from recipient.

[129] Include requirement for "identification number of the message"?

(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

(e) signature-verification data which correspond to signature-creation data under the control of the signatory;

(f) an indication of the beginning and end of the period of validity of the certificate;

(g) the identity code of the certificate;

(h) the advanced electronic signature of the certification-service-provider issuing it;

(i) limitations on the scope of use of the certificate, if applicable; and

(j) limits on the value of transactions for which the certificate can be used, if applicable.

9.6.4 Possible provisions for secure signature verification

During the signature-verification process it should be ensured with reasonable certainty that:

(a) the data used for verifying the signature correspond to the data displayed to the verifier;

(b) the signature is reliably verified and the result of that verification is correctly displayed;

(c) the verifier can, as necessary, reliably establish the contents of the signed data;

(d) the authenticity and validity of the certificate required at the time of signature verification are reliably verified;

(e) the result of verification and the signatory's identity are correctly displayed;

(f) the use of a pseudonym is clearly indicated; and

(g) any security-relevant changes can be detected.

10. Annex B – Annexes to Chapter Economic, social and environmental impact of a European framework for ancillary services

10.1 Section A – Methodology used for Systematic Review/REA

Introduction to Systematic Reviews

In order to establish effective practices in dealing with a specific problem, it is important to determine what is known about the issue in question from the full range of existing evidence. Traditionally, a narrative or literature review would be undertaken to search this evidence; however, there are limitations with this approach. Principally, they are susceptible to selection and/or publication biases as literature reviews are often opportunistic in that they review only literature and evidence that is readily available to the researcher.

Systematic reviews of existing literature are increasingly being used as a valid and reliable means of harnessing existing research evidence. They differ from literature reviews by (Davies, 2003:4):

- Being more systematic and rigorous in the ways in which they search and find existing evidence.
- Having explicit and transparent criteria for appraising the quality of existing research evidence, especially identifying and controlling for different types of bias in existing studies.
- Having explicit ways of establishing the comparability (or incomparability) of different studies and, thereby, of combining and establishing a cumulative effect of what the existing evidence is telling us.

Systematic reviews involve a systematic, rigorous and exhaustive search of all the relevant literature. Searches are conducted using electronic and print sources, hand searching and relevant 'grey' literature (i.e. unpublished studies or work in progress) is identified. This approach helps to remove the problems of bias associated with traditional literature reviews. The search criteria used in undertaking a systematic review and the criteria by which the literature is appraised and interpreted are clearly defined. This leads to greater transparency and allows future studies to be added to the review, enabling an interactive and cumulative body of sound evidence to be developed on a subject area. (Butler, 2004)

Background to Rapid Evidence Assessments

Undertaking a systematic review takes time, typically around six months to a year. Users of research and evaluation evidence often need quicker access to what the existing evidence is telling them. To this end, Rapid Evidence Assessments (REAs) have been developed for use in public policy research and impact evaluation. REAs are based on the principles of a systematic review. The functions of a REA are to (Davies, 2003):

- Search the electronic and print literature as comprehensively as possible within the constraints of a policy or practice timetable.
- Collate descriptive outlines of the available evidence on a topic.
- Critically appraise the evidence (including an economic appraisal).
- Sift out studies of poor quality.
- Provide an overview of what the evidence is saying.

Like systematic reviews, they are based on comprehensive electronic searches of appropriate databases and some searching of print materials, but in order to complete them in a shorter time frame concessions are made. As a result, exhaustive database searching, hand searching of journals and textbooks, or searches of 'grey' literature is not immediately undertaken. However, searching may be continued beyond the time available for a REA until a comprehensive search of the available research literature has been completed and a full-blown systematic review is achieved. In such cases, a REA would be better described as an interim evidence assessment. (Butler, 2004)

All REAs carry the caveat that their conclusions may be subject to revision once more systematic and comprehensive reviews of the evidence base have been completed. This is consistent with the important principle that systematic reviews are only as good as their most recent updating and revision allows (Davies, 2003).

10.2 Section B: Sources with indirect bearing on impact of Ancillary Services

This section lists a number of sources which were retrieved and considered relevant, but only have an indirect bearing upon the impact of ancillary services.

Title	The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies
Author	Toby Stevens, John Elliott, Anssi Hoikkanen, Ioannis Maghiros, Wainer Lusoli
Date	2010
Publication	JRC scientific and technical reports
Purpose of study	This study gathers knowledge about the strategies, product portfolios, financial information, dynamics between players and about other relevant factors of eID market stakeholders in Europe. This knowledge contributes to the overall analysis of the eID market and to a better understanding of the economic factors affecting the eID markets national level, the drivers and barriers that affect the uptake of electronic identities, the business models likely to prevail and the other factors that contribute to generating innovation in the market. The focus of the study includes privacy, security, and new business models enabled by development in eID. It is expected to reveal: o the nature, structure, developments and dynamics for today's European eID markets o the key trends in the markets o who the key stakeholders in that market are o the key differences between the European eID markets in terms of size, relative o development and key drivers and barriers o on what information companies base their eID-related business decisions o what external data sources they have at their disposal
Methodology of study and analysis performed	The scope of work includes an accurate but not exhaustive analysis of the eID market, of the key stakeholders within that market, and the data sources that are available. A number of European countries were chosen in light of their eID infrastructure: Belgium, Finland, France, Germany, Spain and Turkey. The project methodology was light weight and exploratory but theoretically informed; it is sufficiently robust to provide the foundation for a possible larger future project. Specifically, it compromised:

- A review of past pan-European analyses in the public and private sectors
- An analysis of findings in view of modelling the eID landscape
- An assessment of market and innovation dynamics

Main findings	A number of general conclusions were drawn: 1. The portability of credentials, both amongst and between public and business players, and the development of a wide choice of channels for delivering eID would facilitate the embedding of eID into the existing infrastructure. 2. Further development of biometrics would enable 3-factor authentication, which in turn could a) ease the evolution from security-driven to citizen-centric eID and b) enhance trust so as to facilitate the transition to eID as a service. 3. As market stakeholders are in stand-by mode in relation to what infrastructure eID would be embedded in, much more should be done to try-out federating processes and embedding eID into applications using open standards. More information on successful business cases should be circulated freely to enable the use of eID across contexts and public/private sectors. 4. While we cannot predict the future evolution towards an eID-enabled centrally overseen, public infrastructure and/or an affordable and trusted private sector eID-enabled, cloud infrastructure, the role of Government both as a legislator and as a promoter of open standards, (including its power as a first buyer of eID services), should be further explored. 5. Finally, in all circumstances, more needs to be done to promote the wider use of existing standards and to oversee the implementation of the embedding of eID in the infrastructure, as well as to offer a solution to the problem of user enrolment, currently a costly and safety dependent procedure.

Title	**Impact assessment - Regulation of the European parliament and the council concerning the European Network and Information Security Agency.**
Author	European staff working document
Date	2010
Publication	European Commission - 2010 impact assessment (IA) reports
Purpose of study	Impact of different policy options for Network Information Security

Methodology of study and analysis performed	Executed in accordance with EU Impact assessment guidelines o Qualitative analysis of policy options o Cost effectiveness analysis
Main findings	The following problem drivers have been identified, amongst others, which make stakeholders vulnerable to Network Information Security (NIS) threats and NIS incidents. They all show that there is a need for a reliable structure at EU level to tackle the problem and to be up to speed, throughout Europe, with the constantly changing technology and market conditions around NIS. o The diversity and fragmentation of national approaches. NIS problems are not constrained by national boundaries and therefore cannot be effectively addressed at national level only. At the same time, the problem is dealt with in many different ways by public authorities in different Member States. The multiple security requirements in different Member States imposes a cost burden on businesses which operate EU-wide, leading to fragmentation and a lack of competitiveness in the European internal market. o The need for more efficient action against cyber crime. NIS efforts have been predominantly organised under the former first pillar, i.e. matters discussed among the institutions. However, with the entry into force of the Lisbon Treaty, it is necessary to take into account a broader task package for an NIS agency, also covering 'second and third pillar' areas, i.e. matters that were formerly decided by the council alone.

Title	**Impact assessment - A strategy for a Secure Information Society - "Dialogue, partnership and empowerment"**
Author	European staff working document
Date	2006
Publication	European Commission - 2006 impact assessment (IA) reports
Purpose of study	Economic and social impact of different policy options for a Secure Information Society
Methodology of study and analysis performed	Executed in accordance with EU Impact assessment guidelines o Qualitative impact assessment of policy options
Main findings	Economic and social impact of different policy options. Moreover the importance of ICT and e-communication services is assessed in quantitative terms. Information and Communications Technologies play a vital role in Europe's continuing modernisation. The e-communications services sector continues to represent the largest segment of the overall ICT sector, accounting for 44,4% of the total value, up from 43% last year. The sector was worth €640 billion in 2005, €273 billion of which derived from e-communication

services. The production and use of ICT account for around 40% of productivity growth and one quarter of overall growth in Europe.

Title	Estimating economic impacts of homeland security measures
Author	Joseph J. Cordes, Anthony Yezer, Garry Young, Mary Catherine Foreman,Charlotte Kirschner
Date	2006
Publication	George Washington Institue of Public Policy (GWIPP)
Purpose of study	Economic analysis of a homeland security measures
Methodology of study and analysis performed	Different models and measures of impacts are used to assess the impact of an increased level of homeland security: Calculation of gross and net costs of homeland security, Cost/benefit analysis, Regulatory Impact Analysis, Computer General equilibrium models, Game theory
Main findings	A city's decision to increase their Homeland Security Advisory System implies a direct weighing of costs and benefits. For the city, costs include the price of increasing a security presence in areas of critical locations, increased waiting time at airports and on highways, and other social costs such as private industry costs for securing their facilities, and any possible decrease in tourism. The primary benefit from a city's decision is the possibility of preventing a terrorist attack and reduction in crime as a result of the increased police presence.

Title	Botnets: Detection, Measurement, Disinfection & Defence
Author	Daniel Plohmann, Elmar Gerhards-Padilla, Felix Leder
Date	2011
Publication	ENISA
Purpose of	Discussion on the threat of botnets and best practices.

study	
Methodology of study and analysis performed	For this study, a distinction has been made between detection and measurement on the one hand and countermeasures on the other. However, accurate detection and measurement can be interpreted as a prerequisite to efficient application of countermeasures. Where possible, interdependencies of the techniques examined have been outlined.
Main findings	The total annual global economic loss attributed to malicious software activities is estimated at more than US$ 10 billion. The current legal frameworks of various EU Member States and their national diversity in the context of cybercrime are a key factor in the efficiency of the fight against botnets. The applicability of promising detection and mitigation approaches is also limited through certain conflicts between data protection laws and laws that ensure a secure operation of IT services. Finally, working processes increase the reaction time to the extent that they can be evaded with little effort by criminal individuals, capitalising on the ease with which botnets can be configured. The global botnet threat is best countered by close international cooperation between governments and technically-oriented and legislative institutions. For an efficient supranational mitigation strategy to work, cooperation between stakeholders must be intensified and strengthened by political will and support.

Title	**Problems of Digital Sustainability**
Author	Tamas Szadeczky
Date	2010
Publication	Acta Polytchnica Hungarica
Purpose of study	The aim of this research is to investigate the difference between conventional and digital communication, especially as regards to the long-term storage and usage of electronic documents.
Methodology of study and analysis performed	The research question was analysed via observation, information gathering and empirical statements based on the personal professional practice of the author.
Main findings	Problems of digital sustainability 1. Excessive Velocity

2. Diversity of Formats

3. On-Line Data Security

4. Offline Data Security

5. Authenticity of an Electronic Signature

During storage and processing of electronic documents, an organization faces serious difficulties. The risk stemming from the outlined problems is diverging in different countries. The faster that digital communication develops, the harder it is to find time to solve problems. Therefore the chance of a later escalating of troubles increases.

Digital preservation deals with the dangers stemming from the above-mentioned problems and with the protection against them.

Title	**Resistance to change: Six reasons why businesses don't use eSignatures**
Author	Aashish Srivastava
Date	2011
Publication	Springer Science+Business Media, LCC 2011
Purpose of study	This paper presents the findings of an empirical study that examined factors that have contributed to the low acceptance of electronic signatures, in particular the digital signature, by the business community for effecting contracts and commercial transactions between each other. The paper also makes some useful suggestions that may encourage businesses to use electronic signatures in order to facilitate the growth of e-commerce
Methodology of study and analysis performed	The research was confined only to Australian businesses that had access to the Internet. A sampling list of 400 companies was developed. A total of 27 face-to-face or telephonic interviews were conducted. A five-stage 'framework for analysis' approach designed by Ritchie and Spencer was adopted for analysing the interview data (Familiarisation, identifying a thematic framework, indexing, charting, mapping and interpretation)
Main findings	Six main factors that have been identified 1. The prevailing culture and customs associated with manuscript signatures 2. Ignorance about the electronic signature technology 3. Legal concerns 4. Security issues

5. The cost of using the technology
6. The complexity associated with its setting up and usage.

Most importantly, there appears to be an overwhelming ignorance in the business community with regard to electronic signatures and the legislation governing the technology. It is important that the business community be adequately informed and educated about the technology and the relevant legislation. The business community has also expressed important legal concerns, including the absence of evidentiary rules and guidelines. Unless these issues are addressed in the legislation, businesses would be fearful of the legal implications of using electronic signatures.

Businesses' reluctance to integrate electronic signatures into their business environment seems to be also driven by concerns regarding their perceived lack of security. If electronic signatures are properly secured, their misuse can be minimised. Electronic signatures stored on a PISD secured through biometric sensors are likely to be a secure option. Note that with recent advancements in the smart card technology it is now possible to have a fingerprint sensor on the smart card itself.

.

Title	**Factors affecting the adoption of electronic signature: Executives' perspective of hospital information department**
Author	I-Chiu Chang, Hsin-Ginn Hwang, Ming-Chien Hung, Ming-Hui Lin, David C. Yen
Date	2007
Publication	Elsevier
Purpose of study	The healthcare industry is experiencing a major transformation towards e-healthcare, which delivers and enhances related information through the Internet among healthcare stakeholders and makes the electronic signature (eSignature) more and more important. This paper identifies factors that affect hospitals in adopting eSignature. Based on the research findings, implications and limitations are discussed.
Methodology of study and analysis performed	This paper uses a mature framework, Technology–Organization–Environment (TEO), in information system discipline to identify factors that affect hospitals in adopting eSignature. A survey was conducted on regional hospitals and medical centres in Taiwan to verify the validity of the research framework. The results showed that TEO framework is useful in distinguishing hospitals as adopters and non-adopters of eSignature. An expert panel helped to determine the appropriateness of the research framework, check the completeness and suitability of the questionnaire, and offered guidance for the research progress whenever there was a need. Discriminant analysis was conducted to distinguish between those hospitals that adopted

	eSignature and those that did not. A literature review was performed.
Main findings	By the completion time of this research, 70% of the research hospitals in Taiwan are delaying their adoption of eSignature, which further delays the development of computerized medical records as planned by the Taiwan government under its digital hospital project. The future functions of a digital hospital can be listed as long distance treatments, Internet virtual hospitals, and medical e-commerce. Without eSignature, the above future function may not be easily achieved. The four significant factors in distinguishing signature adopters from non-adopters are hospital size, adequate resources, vendor support, and government policy. This study suggests the government take a stronger position to provide financial aid and educate the non-adopters. Reducing uncertainty of policies, not only regulations for eSignature but also the reimbursement related to the promotion of eSignature, is needed.
Quality appraisal	o Findings: Findings are credible and have a coherent logic. o Design: Research design is clearly explained. An expert panel was involved. o Sample composition: Questionnaires were mailed out to the executives and directors of the information departments of 86 hospitals to collect the needed information. o Analysis: Discriminant analysis was conducted to distinguish between those hospitals that adopted eSignature and those that did not. o Reporting: Clear reporting, clear summary of results

Title	**Understanding the Economic Benefit of the Information Technology Revolution**
Author	Robert D. Atkinson and Andrew S. McKay
Date	March 2007
Publication	The Information Technology & Innovation Foundation (ITIF)
Purpose of study	Notwithstanding the centrality of IT to economic growth, there have been surprisingly few attempts to catalogue what is known about IT's impacts on the economy. It is the aim of this study to do so.
Methodology of study and analysis	The objective of the study is reached by collecting, organizing, and surveying studies and examples of IT's impact in five key areas:

performed

1. Productivity
2. Employment
3. More efficient markets
4. Higher quality goods and services
5. Innovation and new products services

Main findings

Five key principles policymakers around the globe should follow if their nations are to fully benefit from the digital revolution:

1. Give the Digital Economy Its Due: Economic policymakers need to view IT issues not just as narrow IT policy, but as the centerpiece of economic policy. This means putting issues of digital transformation at the front and center of economic policy.

2. Actively Encourage Digital Innovation and Transformation of Economic Sectors: The private sector will drive much of digital transformation, but government can play a supportive role. Government should support research in emerging IT areas. IT should also use a wide array of policy levers, including tax, regulatory, and procurement policies, to spur greater IT innovation and transformation, particularly in key sectors like health care, education, transportation, and others influenced by public policy. Moreover, government should lead by example by leveraging their own IT efforts to achieve more effective and productive public sector management and administration.

3. Use the Tax Code to Spur IT Investment: Investment is how IT innovations are diffused throughout the economy. Because IT seems have a much larger impact on productivity, tax policies should focus on spurring additional investment in newer generations of IT.

4. Encourage Universal Digital Literacy and Digital Technology Adoption: Ensuring that societies take full advantage of the IT revolution will require that the large majority of citizens participate in the digital economy. National governments need to work in partnership with the for-profit, non-profit, and state and local government sectors to help citizens use and access technology.

5. Do No Harm: Making digital transformation the centre of economic policy means not just supporting IT, just as importantly it means avoiding harming the digital engine of growth. All too often well-intentioned policymakers consider laws and regulations that would slow digital transformation.

Both benefits and downsides of IT are broadly discussed.

Benefits:

- It drives productivity and growth
- IT boosts growth indirectly
- IT ensures that the economy runs at full capacity
- IT enables goods and services to be allocated more efficiently
- IT enables higher quality products and services
- IT drives innovation

Downsides:

- Economic costs
- Risks to privacy and community
- IT-enable dislocations

Quality appraisal

- Findings: Findings are credible and have a coherent logic
- Design: Literature overview
- Sample composition: Not applicable, this is a literature overview
- Analysis: No real analysis. Overview of existing information
- Reporting: clear and structured reporting

11. Annex C – Recommendations for a European Supervision Scheme: Proposal for Conformity Assessment Guidance

The current proposal for a 'Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market' paves the way to the establishment of a single supervision scheme common to all EU MS supervisory bodies. We recommend delegated acts and implementing acts to be adopted in the context of the supervision related articles of the future Regulation to effectively set up such a common basis for supervision of qualified trust service providers and the qualified trust services they provide.

The present document proposes a concrete proposal for such a common "European Scheme for supervision of qualified trust service providers and the qualified trust services they provide", in accordance with the relevant articles from COM(2012) 238[130]. From the way the COM(2012) 238

[130] Those relevant articles are the following:

- COM(2012) 238, Art. 13.5 referring to delegated acts concerning the definition of procedures applicable to the supervisory tasks referred to in Art.15.2;
- COM(2012) 238, Art. 13.6 referring to implementing acts concerning the definition of the circumstances, formats and procedures for the report on the last calendar year's supervisory activities of each supervisory body, as referred to in Art.15.3;
- COM(2012) 238, Art. 14.4 referring to implementing acts concerning the specification of the formats and procedures for the mutual assistance provide in Art.14;
- COM(2012) 238, Art. 15.5 referring to delegated acts concerning the further specification of the appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide as referred to in Art.15.1;
- COM(2012) 238, Art. 15.6 referring to implementing acts concerning the definition of the circumstances, formats and procedures, including deadlines, applicable for the purpose of Art.15.1 to 3;
- COM(2012) 238, Art. 16.5 referring to delegated acts concerning the specification of the conditions under which the independent body carrying out the audit referred to in Art.15.1 and in Art.16.1, and in Art.17.1 shall be recognised;
- COM(2012) 238, Art. 16.6 referring to implementing acts concerning the definition of the circumstances, formats and procedures applicable for the purpose of Art.15.1, Art.15.2 and Art.15.4;
- COM(2012) 238, Art. 17.5 referring to implementing acts concerning the definition of the circumstances, formats and procedures applicable for the purpose of Art.15.1 to 3;
- COM(2012) 238, Art. 18.5 referring to delegated acts concerning the definition of the information referred to in Art.18.1;
- COM(2012) 238, Art. 18.6 referring to implementing acts concerning the definition of the technical specifications and formats for trusted lists applicable for the purpose of Art.18.1 to 4; COM(2012) 238, Art. 19.5 referred implementing acts concerning the establishment of reference numbers of standards for trustworthy systems and

proposal for Regulation is proposing to organise those delegated acts and implementing acts, it is possible to establish a common European Scheme for supervision of qualified trust service providers and the qualified trust services they provide.

The present document focuses on the description of (i) the process flow for the supervision of qualified trust service providers and the qualified trust services they provide and (ii) on the Conformity Assessment Guidance (CAG) specifying how to assess compliance of those providers and their qualified trust services against the "Supervision Conformity Assessment Criteria". These latter "Supervision Criteria", against which the conformity of the qualified trust service providers and the qualified trust services they provide will be assessed, will be the topic of a document that will be referenced by the present document.

The proposed complete scheme for such a common "European Scheme for supervision of qualified trust service providers and the qualified trust services they provide" builds upon work done in ETSI ESI with regards to general requirements and guidance for conformity assessment of trust service providers (ETSI TS 119 403), national supervision schemes, the COM(2012) 238 proposal for Regulation. The proposed complete scheme may be integrated as such in an appropriate delegated or implementing act, or be included in the ETSI standardisation framework as an instantiation of ETSI TS 119 403[131].

It is believed that the establishment of such a common basis for supervision of qualified trust service providers and the qualified trust services they provide will not only serve to raise the level of confidence in these providers and services within the EU boundaries but will also serve as a benchmarking reference for the mutual recognition between EU services and those "qualified" trust services from 3rd countries or international organisations. Recognition of "qualified" trust services and trust service providers from 3rd country or international organisations that would be certified against the EU common supervision scheme or against an equivalent scheme by a conformity assessment body accredited by a national accreditation body participating to the European cooperation for Accreditation (and/or the International Accreditation Forum (IAF)[132]) to carry out such assessments would be facilitated.

---

products enabling presumption of compliance with requirements laid down in Art.19 where trustworthy systems and products meet those standards.

[131] ETSI TS 119 403 provides a general framework for the establishment of trust service provider assessment scheme whatever type of trust service and trust service provider, qualified or not, and not limited to the one covered by COM(2012) 238 proposal for Regulation. The proposed "European scheme for the supervision of qualified trust service providers and the qualified trust services they provide" is (as) compliant (as possible) with ETSI TS 119 403.

[132] The IAF is the world association of National (Conformance Assessment) Accreditation Bodies and other bodies interested in conformance assessment in the fields of management systems, products, services, personnel and other similar programs of conformance assessment.

It should be highlighted that the proposed "initiation phase" in the current proposal for a Regulation creates some legal uncertainties, un-equality between relying parties and un-necessary complexity and should be simplified in a clear prior-authorisation model. In this case, the supervision scheme flow can be simplified. Such simplifications are depicted in Annex 1.

It is further recommended that Secondary EU wide legislation (e.g. delegated acts as per Art.13.5) should establish and maintain (incl. addition mechanism) an exhaustive list of EU wide, meaningful and precise categories of activities to be considered as trust services. Not having such a mechanism will not allow clear determination whether a service provider is to be considered as a trust service provider or not and may lead to discrimination between trust service providers.

11.1 Introduction

The "European Scheme for supervision of qualified trust service providers and the qualified trust services they provide", hereafter referred to as the Supervision Scheme, provides:

- Common **Conformity Assessment Guidance** for European Union Member States supervisory bodies on how to assess compliance of qualified trust service providers and the qualified trust services they provide against the requirements laid down in the Regulation 2013/xxx/EU of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [ref.1] hereafter referred to as the Regulation;

- Common **Conformity Criteria for qualified trust service providers and the qualified trust services they provide**, against which conformity assessment will be undertaken by EU MS supervisory bodies or their designated assessors in the context of the Regulation.

The present document is the **Conformity Assessment Guidance** document of the Supervision Scheme.

11.2 Principles of the Supervision Scheme

The following principles underlie the Supervision Scheme:

- **Transparency**: As the present document and the document on the conformity assessment criteria are made publicly available, this will make the EU Supervision Scheme and its related processes transparent.

- **Equality**: As the main goal is to prove/ensure that the EU Regulation is abided by, the Supervision Scheme, including the Conformity Criteria, the Conformity Assessment Guidance and assessment process, is identical to every qualified trust service provider, regardless the goals of the trust service providers and regardless the assessor.

- **Minimum level of security assurance**: This is reached through the introduction of minimal criteria that need to be met.

- **Better preparation of qualified trust service providers**: By making public the Supervision Scheme, including the (minimum) conformity criteria, assessment guidance and process, qualified trust service providers have the opportunity to better understand the content and

purpose of the supervision, prepare themselves in advance to make wise decisions and investments when designing their systems to meet the criteria and pass the supervision.

- **EU wide trust establishment**: The European dimension of the Supervision Scheme is a sound basis to assure stakeholders and relying parties that supervised qualified trust service providers comply with it and that their supervised qualified trust services are trustworthy.

- **Facilitate international recognition**: The above goals and principles will facilitate international recognition of the EU Supervision Scheme and hence the recognition and acceptance of the qualified trust service providers and the qualified trust services they provide.

- **Dissemination of qualified (supervision) status information of qualified trust service providers and their qualified trust services**: The actual qualified status of any supervised qualified trust service provider and of the qualified trust services it provides shall be disclosed in the Trusted List of the Member State in which the qualified trust service provider is established or for which it is competent.

11.3 Terminology, definitions and abbreviations

11.3.1 Terminology and definitions

Term	Definition
assessor	Person who assesses conformity to requirements as specified in a given policy requirements document.
accreditation	An attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity [ref.2].
competence	Ability to apply knowledge and skills to achieve intended results.
conformity assessment	The process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled [ref.2].
conformity assessment body	An independent body of assessors accredited by a National Accreditation Body as having the competence to carry out a conformity assessment activities, including calibration, testing, certification and inspection, in line with the present European Supervision Scheme.
national accreditation body	The sole body in a Member State that performs accreditation with authority derived from the State [ref.2].
control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature. [ref.5]
control objective	Statement describing what is to be achieved as a result of implementing controls. [ref.5]
information security management system	Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information

Term	Definition
	security. [ref.5]
guideline	Recommendation of what is expected to be done to achieve an objective. [ref.5]
policy	Overall intention and direction as formally expressed by management. [ref.5]
process	Set of interrelated or interacting activities which transforms inputs into outputs. [ref.5]
trust service policy	Set of rules that indicate the applicability of the output of a trust service to a particular community and/or class of application with common security requirements.
trust service full practice statement	The entire set of statements of the practices (together with the entire set of related documentation, public and non-public) that a trust service provider employs in providing one or more trust services.
technical expert	Person who provides specific knowledge or expertise to the assessor
trust service policy	Set of rules that indicate the applicability of the output of a trust service to a particular community and/or class of application with common security requirements.
trust service full practice statement	The entire set of statement of the practices (together with the entire set of related documentation, public and non-public) that a trust service provider employs in providing one or more trust services.
risk analysis	Systematic use of information to identify sources and to estimate risk (i.e. the combination of the probability of the occurrence of a particular set of circumstances and its consequence). [ref.5]
risk treatment	Process of selection and implementation of measures to modify risk. [ref.5]
statement of applicability	Documented statement describing the control objectives and controls that are relevant and applicable to the organization's information security management system. [ref.5]
trust service	Any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals [ref.1 - Art.3.12]
trust service output	A physical or binary (logical) object generated or issued as a result of the use of a trust service. *Examples of binary trust service outputs are certificates, electronic time-stamps [ref.1 - Art.3.25], CRLs, OCSP responses, electronic signatures, electronic seals, electronic documents, electronic delivery, etc.*
qualified trust service	A trust service that meets the applicable requirements provided for in this Regulation [ref.1 - Art.3.13]
trust service provider	A natural or a legal person who provides one or more trust services [ref.1 - Art.3.14]
qualified trust service provider	A trust service provider who meets the requirements laid down in this Regulation [ref.1 - Art.13.15]
trusted list	Refers to a European Union Member State's "Supervision/Accreditation Status

Term	Definition
	List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC". Updated: Refers to a European Union Member State's "supervision status list of qualified trust service providers and of the qualified trust services they provide which are supervised by the referenced Member State for compliance with the relevant provisions laid down in Regulation 201x/xxx/EU.
certificate	An electronic attestation which links electronic signature or seal validation data of a natural or a legal person respectively to the certificate and confirms those data of that person [ref.1 - Art.3.10].
qualified certificate for electronic signature	A certificate which is used to support electronic signatures, is issued by a qualified trust service provider and meets the requirements laid down in [ref.1 - Annex I].
qualified certificate for electronic seal	A certificate which is used to support an electronic seal, is issued by a qualified trust service provider and meet the requirements laid down in [ref.1 - Annex III].
qualified certificate for website authentication	A certificate which makes it possible to authenticate a website and links the website to the person to whom the certificate is issued, which is issued by a qualified trust service provider and meets the requirements laid down in [ref.1 - Annex IV].

All other definitions from the Regulation are included by reference [ref.1].

11.3.2 Abbreviations

CAB	Conformity Assessment Body
CAG	Conformity Assessment Guidance
CRIT	Conformity Assessment Criteria
EA	European cooperation for Accreditation
EC	European Commission
IAF	International Accreditation Forum
ISMS	Information Security Management System
LOTL	List Of the Trusted Lists
MLA	Multi Lateral recognition Agreement
MS	Member State
NAB	National Accreditation Body
PKI	Public Key Infrastructure
SOA	Statement Of Applicability
TL	Trusted List

11.4 References

[ref.1] COM(2012) 238 Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[ref.2] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93. OJ L 218, 13/08/2008 p.30-47.

[ref.3] IAF Mandatory Document for the Certification of Multiple Sites Based on Sampling.

[ref.4] ISO/IEC 17021:2011: "Conformity assessment - Requirements for bodies providing audit and certification of management systems".

[ref.5] ISO/IEC 27000:2009: "Information technology - Security techniques - Information security management systems - Overview and vocabulary".

[ref.6] ISO/IEC 27005:2011: "Information technology - Security techniques - Information security risk management".

[ref.7] ISO/IEC 27006:2007 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems.

[ref.8] ISO/FDIS 19011:2011(E) Guidelines for auditing management systems.

11.5 Conformity assessment model

11.5.1 Context

The conformity assessments of qualified trust service provider and of the qualified trust services they provide are to be carried out in the context of the Regulation [ref.1] conferring EU wide recognition and acceptance of the assessments and with the additional aim to provide a basis for international cross-recognition of the assessments.

This lies within pan European regulations provided for the international framework for the accreditation of conformity assessment bodies through the European Cooperation for Accreditation (EA) and beyond through the International Accreditation Forum (IAF).

11.5.2 Description of the Assessment model

Figure 1 illustrates the model for the European Supervision Scheme for the conformity assessment of qualified trust service providers and the qualified trust service they provide against the provisions and requirements laid down in the Regulation [ref.1].

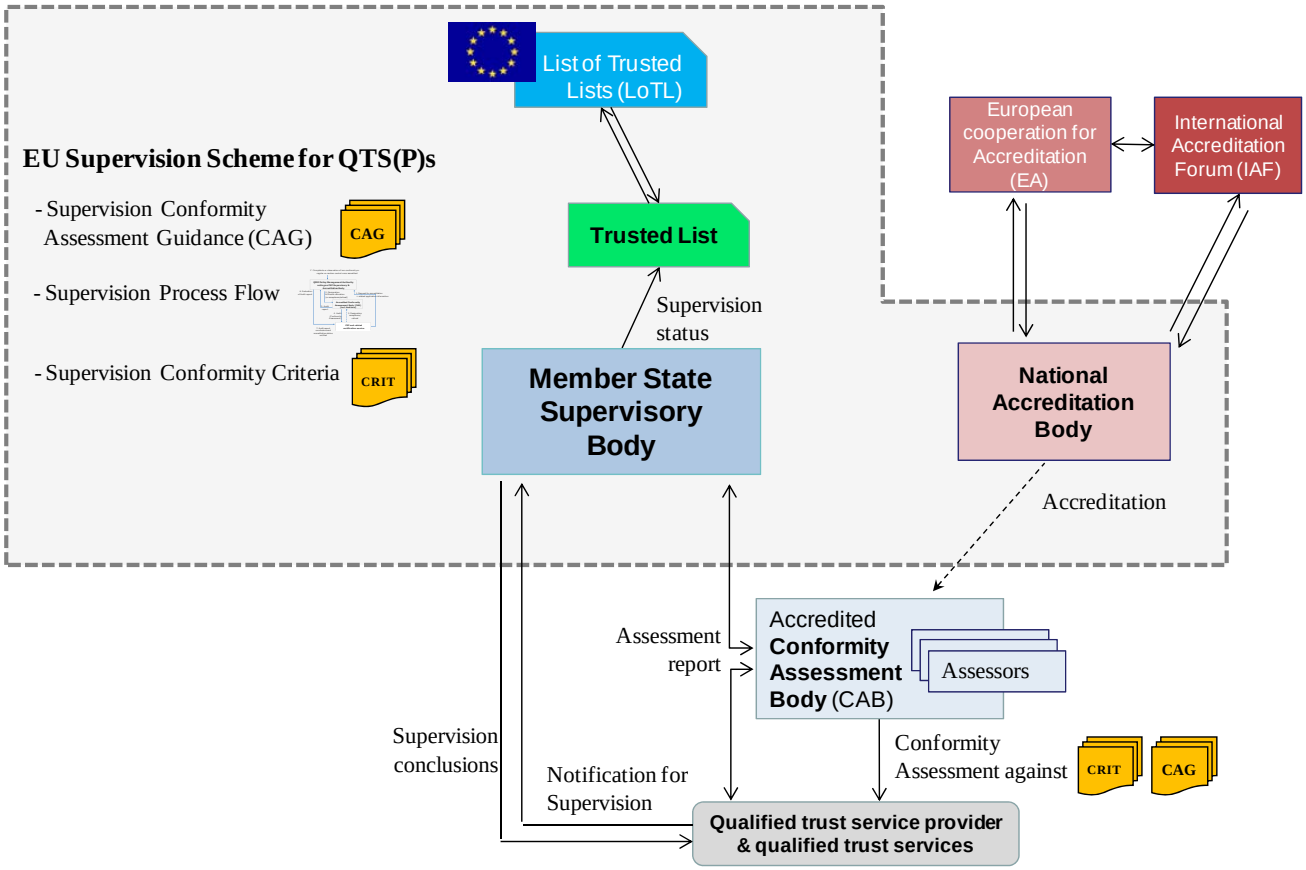


Figure 1: Model for European Supervision Scheme and related assessments for QTS(P)s

Within the above described context and within each EU Member State, the European Supervision Scheme rely on the following elements:

- The **National Accreditation Body** (NAB): This is the sole body in a Member State that shall perform, with authority derived from the State, accreditation of conformity assessment bodies in the context of the Supervision Scheme. Such accreditation shall assess the competency of the accredited conformity assessment bodies to carry out assessments under the requirements identified in the Supervision Scheme.[133]

- **Conformity Assessment Bodies** (CAB): A conformity assessment body is an independent body of assessors which carries out the assessment of a qualified trust service provider and of the qualified trust services it provides against the requirements established in the Supervision Scheme, in particular against its conformity criteria and in accordance with its conformity assessment guidance. The competence of Conformity Assessment Body to carry out such an assessment is accredited by a National Accreditation Body. One or more Conformity Assessment Bodies may be accredited and hence recognised under the Supervision Scheme. The results of a conformity assessment executed by a conformity assessment body is notified to the Supervisory Body of the Member State in which the assessed qualified trust service provider is established. Conformity assessment bodies refer to recognised independent bodies as referred to in Art.15.1, Art.16.1 and Art.17.1 of the Regulation [ref.1].

- The **Supervisory Body**: This is the body established in accordance with Art.13.1 of the Regulation and that are given all supervisory and investigatory powers that are necessary for the exercise of their task in

[133] The option has been made here to not allow, in the context of the present Supervision Scheme, Supervisory Bodies to play the equivalent role of the national accreditation body for evaluating the competence of a conformity assessment body to carry out a conformity assessment in line with the present European Supervision Scheme.

accordance with the Regulation [ref.1]. With regards to qualified trust services and qualified trust service providers, the supervisory body shall be responsible for undertaking supervision of those qualified trust service providers established in their territory, and/or in the MS having designated this body to undertake supervision of qualified trust service providers established in the designating MS under the responsibility of the designating MS, and of the qualified trust services those qualified trust service providers provide. This supervision shall ensure that those qualified trust service providers and the qualified trust services they provide meet the applicable requirements laid down in the Regulation. All supervisory bodies from the EU shall abide by the Supervision Scheme for this purpose.

- **Trusted Lists**: The supervisory body shall also be the body responsible for the notification of the qualified status of the qualified trust service providers and the qualified trust services they provide in their national Trusted List in accordance with the Regulation [ref.1 - Art.18] and the present document. Qualified status result from the verification by the supervisory body of the compliance of the qualified trust service providers and the qualified trust services they provide with the requirements of the Regulation, such a verification being based on, e.g., the results of a conformity assessment performed by an accredited conformity assessment body.

The **List of the Trusted Lists** (LOTL) is an additional important element in the Supervision Scheme. In order to allow access to the trusted lists of all Member States in an easy manner, the European Commission publishes a central compiled list that includes the locations where the Trusted Lists are published and the certificate to be used to verify the authenticity and integrity of the MS trusted lists, as notified by Member States. This compiled List of the Trusted Lists (LOTL) is available publicly. The authenticity and integrity of the machine processable version of this compiled list is ensured through an electronic signature supported by a digital certificate. The certificate can be authenticated through one of the digests published on the Official Journal of the European Union.

The Supervision Scheme assessment model relies on a common set of conformity criteria, a common assessment process based on a common conformity assessment guidance and on a common understanding of the responsibilities of the qualified trust service providers.

The **Conformity Criteria** (CRIT) for qualified trust service providers and the qualified trust services they provide refers to the criteria (incl. requirements) against which conformity assessment will be undertaken by EU MS supervisory bodies in the context of the Regulation. Those criteria take into account specificities of the type of trust service to be assessed. They can be organised under the form of a check-list aiming to facilitate the tasks of both the assessors and the qualified trust service provider to be assessed. They are made publicly available and based on standards. The conformity criteria applicable in the context of the Supervision Scheme are provided in a companion document of the present document.

The **Conformity Assessment Guidance** (CAG) for European Union Member States supervisory bodies refers to the way conformity assessment bodies carry out an assessment in the context of the Supervision Scheme , i.e. to the way compliance of qualified trust service providers and the qualified trust services they provide is assessed against the requirements laid down in the Regulation [ref.1].

This covers:

- The conformity assessment process and the specific characteristics with regards to the conformity assessment process, including the frequency and depth of the assessments, the associated fees, the complaint related procedures, etc.
- The requirements on the conformity assessment bodies and the rules to be observed by such bodies when conducting assessments.
- The specifications for cross-border assessment and related mutual assistance.
- and the responsibilities of the parties.

11.6 Responsibilities of the parties

Member States, through the supervisory body they have designated in accordance with the Regulation [ref.1 - Art.13.1], shall ensure that conformity assessment bodies conducting assessments in the context of the Supervision Scheme are accredited by a national accreditation body for its competency to carry out assessments for the type of qualified trust services and qualified trust service provider being assessed, where verifying the

compliance of such qualified trust services and qualified trust service provider with the provision laid down in the Regulation on the basis of assessment reports provided by conformity assessment bodies.

The national accreditation body shall ensure, through appropriate accreditation process, that the conformity assessment body is competent to carry out conformity assessment for the type of qualified trust services and qualified trust service provider being assessed.

The conformity assessment body shall carry out assessment of the qualified trust service provider and of the qualified trust services they provide using conformity criteria relevant to the type of qualified trust service(s) being assessed.

The qualified trust service provider shall ensure that the qualified trust service it provides is conformant to the relevant conformity criteria and assist the conformity assessment body in carrying out the assessment.

The supervisory body shall ensure that a trusted list is made available to interested parties which reflects the latest qualified status of the qualified trust service provider and of the qualified trust services they provide, based on the latest conformity assessment, within the scope of the assessment scheme. The supervisory body shall also ensure that authenticity and integrity of the trusted list is maintained.

11.7 Supervision process

11.7.1 Supervision process flow at a glance

The supervision process flow is depicted in Figure 2.

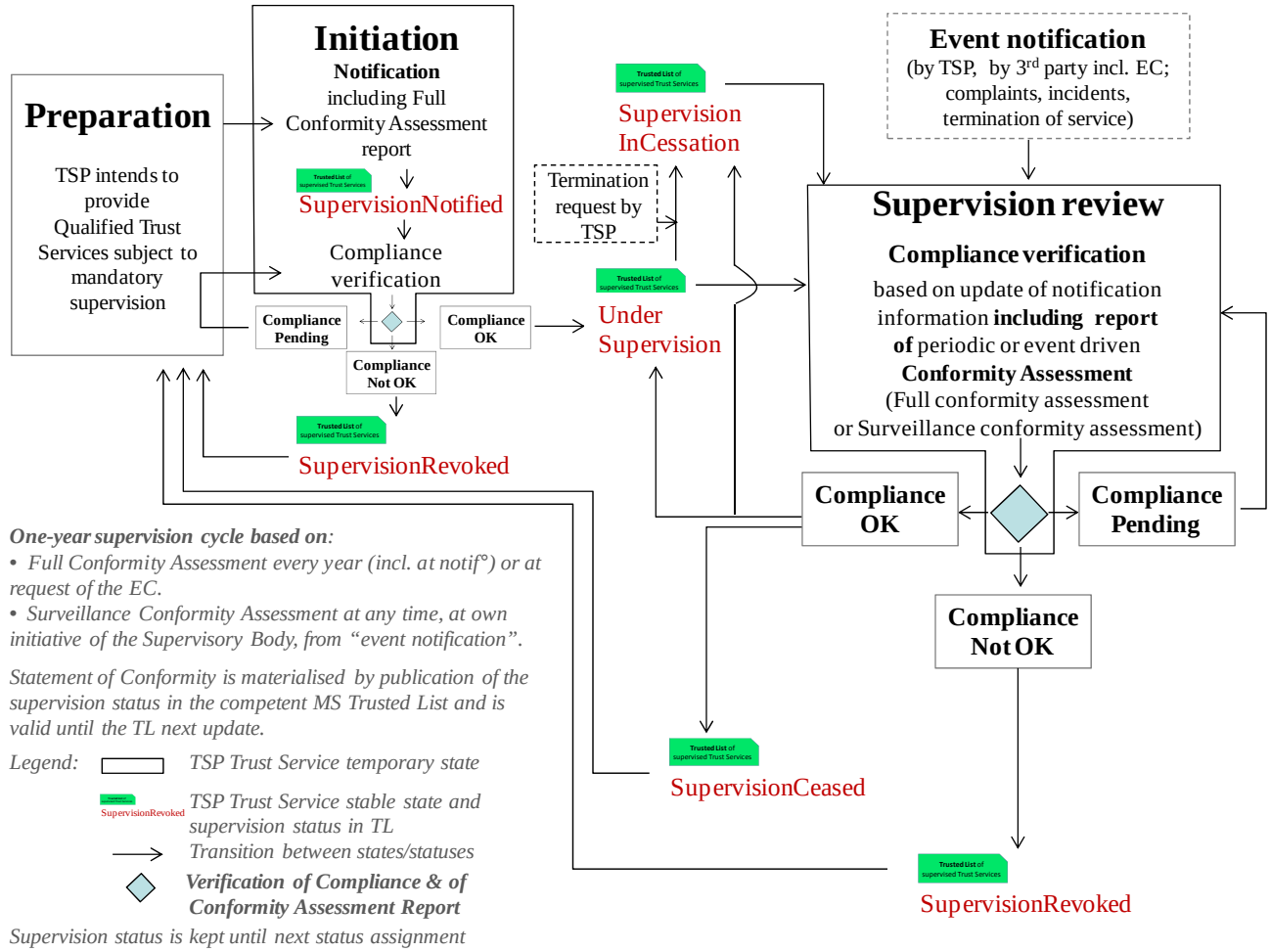


Figure 2: Supervision process flow of the European Supervision Scheme - QTS(P)s

The supervision process of the European Supervision Scheme is based on a [one-year][134] (re)assessment cycle with a Full Conformity Assessment (FCA) to be performed at the initiation of the process and to be renewed within one year after the previous FCA. Additional Surveillance Conformity Assessments (SCA) may or are to be performed on the basis of triggering events as specified in Section 11.9 of the present Annex C.

State transitions are associated to the publication or updates in trusted lists of the actual qualified status of the qualified trust service that materialises the compliance of the qualified trust service and of the qualified trust service provider as based on the compliance resulting from the latest conformity assessment by the CAB and the compliance verification by the Supervisory Body.[135]

The following activities can trigger the state transitions:

- **Preparation**: This is a set of activities during which the qualified trust service provider prepares himself to provide qualified trust services and to comply with the applicable requirements of the Regulation and in particular of the Supervision Scheme. During initial preparation, there is not yet a state assigned.

- **Initiation**: The supervision is initiated by the qualified trust service provider notifying the competent supervisory body of its intention to start providing one or more qualified trust services in accordance with the Regulation [ref.1 - Art.17.1]. This notification includes a Full Conformity Assessment report that is verified together with other notified information to verify the compliance of the qualified trust service provider and the qualified trust services it provides against the requirements of the Regulation. This verification leads to one of the "compliance ok", compliance not ok" or compliance pending" compliance verification outcomes.

- **Conformity Assessment**: These activities can be performed respectively:

    - During the initial assessment in the context of the initiation phase;

    - During the yearly (re)assessment following the latest conformity assessment (starting with the one following the initial assessment);

    - During the conformity assessments triggered by the notification of specific events as specified in Section 11.9

  Depending of the actual state of the supervised qualified trust service provider and of the qualified trust services it provides, the level of the conformity assessment may be identified as being either a full conformity assessment or a surveillance conformity assessment as specified in Section 11.7.1.a.

- **Supervision Review**: The supervision review is initiated by the yearly expiration of the previous conformity assessment or upon notification of an event as specified in Section 11.9. This requires the notification by the qualified trust service provider of the update of the notification information, including the report of a Full or Surveillance Conformity Assessment (*Full Conformity Assessment every year and depending on the nature of the event notification as per Section11.9, a Surveillance Conformity Assessment may be*

[134] COM(2012) 238 proposal for Regulation [ref.1] establishes a one-year based (re)assessment cycle. This is to be balanced against a cycle of a full (re)assessment every three years including a yearly surveillance assessment as being defined in ETSI TS 119 403, and to a benchmarking of other relevant (re)assessment cycles the European Supervision Scheme would be cross-evaluated against in the context of mutual recognition with 3rd countries or international organisations in accordance with the Regulation [ref.1 - Art.10].

[135] The here proposed process flow is compliant with the proposal for Regulation [ref.1] and is compliant and backward compatible with the current Trusted Lists model as defined in CD 2009/767/EC as amended by CD 2010/425/EU. Note that the CD's description of the "undersupervision" status could be updated as referring not only to being "currently under supervision, for compliance with the provisions laid down in [the Regulation]" but to being "currently supervised as compliant with the provisions laid down in [the Regulation] and under supervision for such compliance".

requested at any time, at own initiative of the Supervisory Body or from "event notification"). This updated notified information is evaluated to verify the compliance of the qualified trust service provider and the qualified trust services it provides against the requirements of the Regulation. This verification leads to one of the "compliance ok", compliance not ok" or compliance pending" outcomes:

- **Compliance OK**: This compliance verification outcome expresses successful passing of the verification of the supervision and of the compliance of the qualified trust service provider and of the qualified trust services it provides against the provisions laid down in the Regulation, including the successful passing of the conformity assessment.

  Following the verification of compliance of the qualified trust service provider and of the qualified trust services it provides, based on the result of the latest conformity assessment and associated report established by a conformity assessment body, and if no non-conformities are outstanding, the Supervisory Body has confirmed the conformity and decided that qualified trust service provider and of the qualified trust services it provides will gain the qualified status ("undersupervision") or keep their actual "qualified status" ("undersupervision" or "supervisionincessation") and can continue to provide those qualified services.

  This confirmation and the associated qualified status shall be reflected or respectively maintained in the applicable trusted list. This will be in principle valid for one year unless changed otherwise in accordance to surveillance or full conformity assessment triggered upon specific circumstances as specified in Section 11.9. A full conformity (re)assessment shall be planned for execution one calendar year after the last executed planned full conformity assessment.[136]

  In case of a limited number minor non-conformities, the supervisory body may confirm compliance with the provisions laid down in the Regulation and allow the qualified trust service provider to take corrective actions which shall be verified at the next (periodic) surveillance conformity assessment.

  The qualified trust service provider can still decide to notify its intention to cease or terminate one or more of its supervised qualified trust services or its activities as qualified trust service provider.

- **Compliance Pending**: Following the verification of compliance of the qualified trust service provider and of the qualified trust services it provides, based on the result of the latest conformity assessment and associated report established by a conformity assessment body, the Supervisory Body has decided that the qualified trust service provider and the qualified trust services it provides will keep their actual "qualified status" and that the qualified trust service provider can continue to provide such qualified trust services **but** needs to address the findings, including minor / major[137] non-conformities within a specified timeframe, as communicated by the supervisory body. Withdrawal of the qualified status (i.e. being moved to "supervisionrevoked" or "supervisionceased") and/or sanctions are possible as per the applicable law, in particular in case those non-conformities are not addressed satisfactorily or not addressed in due time.

  The supervisory body shall require an additional review to be executed in order to make sure the findings are adequately addressed in the applicable timeframe. The supervisory body shall inform the qualified trust service provider of the nature of the additional conformity assessment (being a full conformity assessment, a limited conformity assessment or a document evidence) that will be needed to verify effective correction and corrective actions.

- **Compliance Not OK**: As a consequence of the qualified trust service provider and/or the qualified trust services it provides failing to comply with the provision laid down in the Regulation, or failing to remedy to non-conformities notified from a previous conformity assessment and supervision compliance verification, or based on major / critical non-conformities identified in the latest conformity assessment or the latest supervision compliance verification by the supervisory body, the qualified trust service

---

[136] May be alternatively specified as "after the latest full conformity assessment".

[137] Only major non-conformities for which a (significant) improvement or correction has been identified and associated to a reasonable implementation deadline may lead to a "compliance pending" outcome; other major non-conformities will lead to a "compliance not ok" outcome. A more strict approach would here consist in allowing only minor non-conformities in the context of "compliance pending".

provider and/or its concerned qualified trust services shall lose their qualified status (moving to "supervisionceased" or "supervisionrevoked").

The supervisory body shall notify and demand the qualified trust service provider:

- to immediately stop the provision of any new output of the concerned qualified trust services, and
- to terminate the concerned qualified trust services in accordance to a termination plan validated by the supervisory body,
- to stop any advertisement about the previous qualified status of the concerned qualified trust services, and if applicable of its own qualified status, and
- to communicate adequately towards its stakeholders with regards to the loss of the qualified status of the concerned qualified trust services and, when applicable, the loss of its own qualified status.

A non-conformity can be defined as a[138]:

- minor non-conformity which is an imperfection or weakness in fulfilling a specified requirement or criteria;
- major non-conformity which can be defined as a non-fulfilment of a specified requirement or criteria;
- critical non-conformity which can be defined as a non-fulfilment of a specified requirement or criteria, such non-fulfilment implying by itself the need for the concerned qualified trust service provider to immediately stop such activities and/or for the concerned qualified trust services to be stopped immediately.

Notification of the assessment conclusions and qualified status notification: based on the results and recommendations in the latest conformity assessment report, and of its supervision compliance verification the supervisory body will notify the qualified trust service provider of its decisions and update, when applicable, the qualified status of the qualified trust service provider and/or of the concerned qualified trust services it provides.

Event notifications as specified in Section 11.9 may result in the conduction of a conformity assessment.

Requests from qualified trust service providers may also result in the change of the "qualified status" of the qualified trust services provider and/or of the qualified trust services they provide.

The flow between the various supervision states is defined as illustrated in Figure 3 below.[139]

[138] Classification of non-conformities could also be defined/refined according to another model (e.g. non-conformance, deficiency, observation on a per requirement basis).

[139] This updates the "supervision/accreditation status flow" defined in CD 2009/767/EC as amended by CD 2010/425/EU.

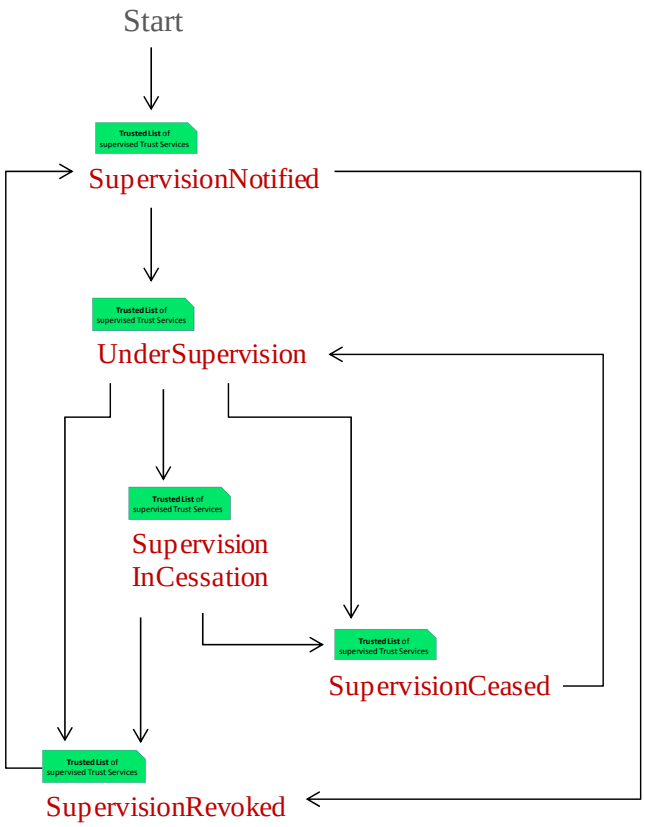


Figure 3: Qualified (supervision) status flow in the context of the European Supervision Scheme.

11.7.2 Preparation

This corresponds to the activities the qualified trust service provider undertakes to provide qualified trust services and to comply with the applicable requirements of the Regulation and in particular with the requirements of the Supervision Scheme.

The activities and their results are to be documented and stored in an internal repository, managed by the qualified trust service provider. During a supervision review (compliance verification) or a conformity assessment, the qualified trust service provider will be required to make the contents of this internal repository available to the reviewers/assessors.

The following activities are **required**:

- Gain sufficient knowledge with regard to the applicable criteria (CRIT) to the qualified trust service provider and to the qualified trust services it provides.
- Formulate a qualified trust service policy and qualified trust service full practice statement as applicable with regards to the type of qualified trust service that is intended to be provided. These may cover both qualified and non-qualified trust services. It is mandatory to make a clear distinction between those two types of trust services for any matter addressed in the qualified trust service policy and qualified trust service practice statement or similar documents.
- Execute a high-level risk analysis and formulate a draft statement of applicability (SOA). The high-level risk analysis will identify the most important assets, threats and risks, as well as the required safeguards. The SOA will identify the safeguards chosen for the qualified trust service provider environment and for any other environment used for the provision of the qualified trust services, and explains how and why they are appropriate. The SOA is derived from the output of the risk assessment/ risk treatment plan. It is required that the SOA directly relates the selected safeguards to the original risks they are intended to mitigate. The SOA should make reference to the policies, procedures or other documentation or systems through which

the selected control will actually manifest. It is also good practice to document the justification of why those controls not selected were excluded.

- Formulate detailed internal and external processes and procedures. This should focus particularly on all aspects of the lifecycle of the qualified trust services offered by the qualified trust service provider and of the related qualified trust service outputs.
- Draw up management system documentation for those processes and procedures.
- Implement those processes and procedures.
- Perform an internal audit. This should include processes and procedures as well the organisational and technology (application, infrastructure) aspects. The qualified trust service provider is free to choose his audit criteria but these should at least include or be equivalent to those listed in the Supervision Scheme criteria (CRIT).
- Execute a detailed Risk Analysis. This should be based on a well-established approach such as defined in ISO 27005 [ref.6] or equivalent.
- Elaborate, implement and execute a Security Policy and a Risk Treatment Plan. The latter should implement the selected safeguards. Those risks not mitigated but rather accepted as residual risk should also be documented formally.
- Formulate the final Statement of Applicability. This final SOA should include all elements and aspects of the qualified trust service provider relevant to qualified trust service outputs and the delivery of the qualified trust services related to them. It will serve as guidance to determine the scope of the qualified trust services offered, as well as the scope of supervision reviews and/or conformity assessments.
- Execute a self-assessment against the Supervision Scheme criteria and documents the outcomes.
- Implement both operational and risk monitoring of the safeguards. This should include both day-to-day monitoring and an annual internal review. The annual internal review should evaluate whether there are any significant changes in the risk environment, whether such changes can be envisaged, as well as whether the selected and implemented safeguards operate satisfactory.

The following activities are **required** as mandated for notification towards the competent supervisory body of the intention to provide qualified trust services:

- Undertake the execution, by an accredited conformity assessment body (independent of the qualified trust service provider) of a full conformity assessment against the Supervision Scheme (incl. criteria and conformity assessment guidance). The conformity assessment body shall be accredited by a national accreditation body member of the European cooperation for Accreditation (EA) to carry out assessment against the Supervision Scheme. The resulting assessment report shall be documented and result in a formal assessment report, explicitly listing any elements of non-conformity if applicable

11.7.3 Initiation

This corresponds to the notification of the qualified trust service provider to the competent supervisory body of its intention to start providing a qualified trust service and to the submission to the competent supervisory body of the required information.

The qualified trust service provider shall submit the following notification information to the competent supervisory body:

- The administrative and identification information related to the qualified trust service provider being either a public entity or a legal or natural person, when it is established in accordance with the national law. This includes but may not be limited to the name of the qualified trust service provider, company information as registered in accordance with national laws, organisation and company structure, capital, balance sheet and annual reports, contact information, etc.
- The identification and the type of qualified trust services to be assessed.

- A summary of the preparation documentation resulting from the expected and required preparation activities as described in section 11.7.1 (this information shall be documented and stored in an internal repository of the qualified trust service provider).

  Note: This is deemed to include the "security audit reports carried out by a recognised independent body" as per Art.15.1, 16.1 and 17.1 of the Regulation.

- Any other relevant information supporting the supervision compliance verification.

The above notification information must be submitted to the competent supervisory body at least one (1) month before the effective notification to the supervisory body of their intention to start the qualified trust service activities.[140]

Upon notification of the above listed documents, the supervisory body shall include the qualified trust service provider and/or the applicable qualified trust services in the trusted list with a status indicating that the notification has been submitted [ref.. Art.17.2], i.e. with the "SupervisionNotified" status.

Upon notification of the qualified trust services the qualified trust service provider intends to start, the supervisory body shall verify the compliance of the qualified trust service provider and the qualified trust services it provides against the requirements of the Regulation [ref.1], on the basis of the notified information.

The supervisory body is entitled to request additional information deemed to support the verification of such a compliance and will inform the qualified trust service provider promptly of the reasons for such a request and the delay for receiving such information.

This initial supervision compliance verification process may lead to one of the following outcomes:

- **Compliance Pending**: In such a case the Supervisory Body has decided that qualified trust service provider and of the qualified trust services it provides will keep their actual "SupervisionNotified" and that the qualified trust service provider can continue to provide such qualified trust services **but** needs to address the findings, including minor / major[141] non-conformities, as communicated by the supervisory body within the specified timeframe.

  The supervisory body shall require an additional review to be executed in order to make sure the findings are adequately addressed in the applicable timeframe. The supervisory body shall inform the qualified trust service provider of the nature of the additional conformity assessment (being a full conformity assessment, a limited conformity assessment or a document evidence) that will be needed to verify effective correction and corrective actions.

  The "SupervisionNotified" status may be moved to "supervisionrevoked" and/or sanctions possible as per the applicable law, in particular when those non-conformities are not addressed satisfactorily or not addressed in due time.

- **Compliance Not OK**: As a consequence of the qualified trust service provider and/or the qualified trust services it provides failing to comply with the provision laid down in the Regulation, or failing to remedy to non-conformities notified from a previous conformity assessment and supervision compliance verification (resulting from a Conformity Pending outcome obtained after notification), or based on major / critical non-

[140] It should be highlighted that the proposed "initiation phase" in the current proposal for a Regulation creates some legal uncertainties, un-equality between relying parties and un-necessary complexity and should be simplified in a clear prior-authorisation model. In this case, the supervision scheme flow described in Figures 2 & 3 of Section 11.7.1 can be simplified as depicted in Annex 1, this sentence may be removed, and the present document updated in consequence.

[141] Only major non-conformities for which a (significant) improvement or correction has been identified and associated to a reasonable implementation deadline may lead to a "compliance pending" outcome; other major non-conformities will lead to a "compliance not ok" outcome. A more strict approach would here consist in allowing only minor non-conformities in the context of "compliance pending".

conformities identified in the latest conformity assessment or the latest supervision compliance verification by the supervisory body, the qualified trust service provider and/or its concerned qualified trust services shall see its "supervisionnotified" status moved to "supervisionrevoked".

The supervisory body shall notify and demand the qualified trust service provider:

- to immediately stop the provision of any new output of the concerned qualified trust services, and
- to terminate the concerned qualified trust services in accordance to a termination plan validated by the supervisory body,
- to stop any advertisement about the previous qualified status of the concerned qualified trust services, and if applicable of its own qualified status, and
- to communicate adequately towards its stakeholders with regards to the loss of the qualified status of the concerned qualified trust services and, when applicable, the loss of its own qualified status.

- **Compliance OK**: The Supervisory Body has confirmed the conformity and decided that the qualified trust service provider and the qualified trust services it provides will gain the qualified status "undersupervision" and that it can continue to provide those qualified services.

  This confirmation and this associated qualified status shall be reflected in the applicable trusted list. This will be in principle valid for one year unless changed otherwise in accordance to surveillance or full conformity assessment triggered upon specific circumstances as specified in Section 11.9. A full conformity (re)assessment shall be planned for execution one calendar year after the last executed planned full conformity assessment.

  In case of a limited number of minor non-conformities, the supervisory body may confirm compliance with the provisions laid down in the Regulation and allow the qualified trust service provider to take corrective actions which shall be verified at the next (periodic) surveillance conformity assessment or the next full conformity assessment.

11.7.4 Supervision Review

Once under the "UnderSupervison" status, the qualified trust service provider and the qualified trust services it provides are under continuous supervision and will enter into a "supervision review" state as the result of an event notification as specified in Section 11.9 and on a yearly basis implying a full conformity assessment.

The qualified trust service provider shall review the outcome of the activities he was required to execute in "preparation" and, where it considers relevant, he should complement or refine its documentation. It shall consequently submit such updated notification information to the competent supervisory body.

The supervisory body shall verify the compliance of the qualified trust service provider and the qualified trust services it provides against the requirements of the Regulation [ref.1], on the basis of the notified updated information.

The supervisory body is entitled to request additional information deemed to support the verification of such a compliance and will inform the qualified trust service provider promptly of the reasons for such a request and the delay for receiving such information.

This supervision compliance review process may lead to one of the following outcomes:

- **Compliance Pending**: In such a case the Supervisory Body has decided that the qualified trust service provider and the qualified trust services it provides will keep their actual qualified status and that the qualified trust service provider can continue to provide such qualified trust services **but** needs to address the findings, including minor / major non-conformities, as communicated to them by the supervisory body within the specified timeframe.

  The supervisory body shall require an additional review to be executed in order to make sure the findings are adequately addressed in the applicable timeframe. The supervisory body shall inform the qualified trust service provider of the nature of the additional conformity assessment (being a full conformity assessment, a limited conformity assessment or a document evidence that will be needed to verify effective correction and corrective actions.

The actual qualified status may be moved to "supervisionrevoked" and/or sanctions possible as per the applicable law, in particular when those non-conformities are not addressed satisfactorily or not in due time,

- **Compliance Not OK**: As a consequence of the qualified trust service provider and/or the qualified trust services it provide failing to comply with the provision laid down in the Regulation, or failing to remedy to non-conformities notified from a previous conformity assessment and supervision compliance verification (resulting from a Conformity Pending state), or based on major / critical non-conformities identified in the latest conformity assessment or the latest supervision compliance verification by the supervisory body, the qualified trust service provider and/or its concerned qualified trust services shall see its actual qualified status moved to "supervisionrevoked".

  The supervisory body shall notify and demand the qualified trust service provider:

  - to immediately stop the provision of any new output of the concerned qualified trust service, and
  - to terminate the concerned qualified trust services in accordance to a termination plan validated by the supervisory body,
  - to stop any advertisement about the previous qualified status of the concerned qualified trust services, and if applicable of its own qualified status, and
  - to communicate adequately towards its stakeholders with regards to the loss of the qualified status of the concerned qualified trust services and, when applicable, the loss of its own qualified status.

- **Compliance OK**: The Supervisory Body has confirmed the conformity and decided that the qualified trust service provider and the qualified trust services it provides will keep its actual qualified status and that it can continue to provide those qualified trust services.

  This confirmation and the associated qualified status shall be (kept) reflected in the applicable trusted list. This will be in principle valid for one year unless changed otherwise in accordance to surveillance or full conformity assessment triggered upon specific circumstances as specified in Section 11.9. A full conformity (re)assessment shall be planned for execution one calendar year after the last executed planned full conformity assessment.

  In case of a limited number minor non-conformities, the supervisory body may confirm compliance with the provisions laid down in the Regulation and allow the qualified trust service provider to take corrective actions which shall be verified at the next (periodic) surveillance conformity assessment.

11.8 Requirements on Conformity Assessments

11.8.1 Conformity Assessment types

We can distinguish between two types of conformity assessments: full conformity assessments and surveillance conformity assessments.

a. Full Conformity Assessment (incl. initial assessment and re-assessment)

A full conformity assessment is required on a yearly basis. A full conformity assessment may also be initiated as a result of the notification of a specific event as specified in Section 11.9.

Depending on the criticality, the implications and nature of the notified event, the MS Supervisory Body shall initiate either a full conformity assessment or a surveillance assessment. A full conformity assessment shall occur whenever the notified event includes the following circumstances:

- whenever there is a major change of the scope;
- whenever there is a major change on the qualified trust services provided under the scope;

- whenever there is a new service included in the scope;
- when there is a major change of IT systems or business processes used by the qualified trust service provider to provide its qualified trust services; or
- when there has been a significant event, incident or complaint requiring such a full re-assessment of a qualified trust service subject to supervision.

At each full conformity assessment (visit), the implementation of the whole of the qualified trust service provider's management system should be verified in each of the areas addressed by the Supervision Criteria.

In addition, a representative sample of records relating to the operation of qualified trust service providers over the historical period since the previous assessment should be examined by the assessor.

Conformity assessment reports should contain assessment information on clearing of non-conformities reported previously.

b. Surveillance Conformity Assessment

The supervisory body shall define a programme of periodic surveillance and reassessment at sufficiently close intervals to verify that qualified trust service providers and the qualified trust service they provide continue to comply with the requirements. There shall be a period of no greater than [six] months for periodic surveillance.

Surveillance conformity assessment may also be initiated as a result of the notification of a specific event as specified in Section 11.9.

At each surveillance conformity assessment (visit), the implementation of a part of the qualified trust service provider's management system should be verified in each of the areas addressed in the Supervision Criteria (e.g. for qualified trust services issuing qualified certificates, the applicable standard(s) and/or requirements regarding Certification Practice Statement, key management life cycle, public key certificate management life cycle, CSP management and operation, insurance coverage and organisational requirements).

In addition, a sample of records relating to the operation of qualified trust service providers over the historical period since the previous assessment should be examined by the assessor.

The reports arising from surveillance during the period between the initial assessment and the reassessment should build up to cover in totality that the qualified trust service provider and the qualified trust services it provides meet the requirements of the applicable conformity assessment criteria (CRIT).

Surveillance conformity assessment reports should contain assessment information on clearing of non-conformities revealed previously.

11.8.2 Conformity Assessment process

Once having been designated and accepted by the qualified trust service provider, the assessors team performs the conformity assessment in accordance to the qualified trust services to be assessed.

The objective of the assessment is to confirm that the qualified trust service provider and the qualified trust services it provides conform to the applicable assessment criteria. This includes confirmation that the implemented qualified trust service provider system conforms to the requirements of the applicable legal provisions, technical standard(s) and is achieving the qualified trust service provider's policy objectives in compliance with the assessment criteria.

This assessment must include visits to the site(s) the qualified trust service provider is making use to provide its qualified trust services, in accordance with Section 11.8.3 on multi-site sampling.

The conformity assessment body and the qualified trust service provider shall agree when and where assessment process is conducted.

The supervised qualified trust service provider shall notify the competent supervisory body about the fact that a conformity assessment is to be conducted, its date and location, and on the identity of the conformity assessment body at least [15] calendar days in advance.

Assessors should review, prior to commencement of the assessment that the qualified trust service provider's (assessed qualified services) system is documented, implemented, and operational and can be shown to be operational.

Assessors should perform their conformity assessment of the qualified trust service provider's system in at least two stages:

- **Assessment stage 1**: This stage focuses on the review of the qualified trust service provider and its assessed qualified services system documentation as it has been documented through the assessment initiation notification and potentially augmented by a specific set of elements specifically required at this stage. On the basis of the observations made at the qualified trust service provider's site in this stage, assessors shall draft a preliminary assessment report and a plan for conducting stage 2 (on-site) assessment.

- **Assessment stage 2**: This stage consists in an on-site assessment that aims to validate the preliminary assessment report findings and to complete the evaluation/audit assessment of the qualified trust service provider and its assessed qualified trust services against the assessment criteria.

Assessment stage 1

In this stage of the assessment, assessors should obtain and review the documentation including the self-assessment and risk analysis with regard to the qualified trust service provider and its assessed qualified trust services system as notified to the supervisory body (respectively during initiation phase or as an update of such information once under supervision) and potentially augmented with specific types of information as part of stage 1 initiation. Assessors should make the qualified trust service provider aware of the further types of information and records that may be additionally required for verification during assessment stage 1.

The objectives of assessment stage 1 are to provide a focus for planning of assessment stage 2 by gaining an understanding of the structure and extent of the qualified trust service provider and its assessed qualified trust services system. Assessment stage 1 includes but should not be restricted to document review, review of the self-assessment, and review of the risk analysis. Other elements that could be included in assessment stage 1 are verification of records regarding legal entity, arrangements to cover liability, contractual relationships between the qualified trust service provider and potential contractors operating or providing sub-component services, internal/external audits or certifications, management review, and further investigations with regards to the preliminary assessment of the self-declared partial conformance or non conformance.

Assessors and the qualified trust service provider should agree when and where assessment stage 1 is conducted.

In order to provide a basis for the decision to confirm that the qualified trust service provider meets the requirements of the applicable conformity criteria (CRIT) for providing the assessed qualified trust services, assessors should require clear reports that provide sufficient information to make that decision.

Reports from the assessment team to the supervisory body are required at stage 1 in the assessment process. In combination with information held on file, these reports should at least contain:

a. A description of work performed, including scope and objectives, as well as the organisation of the assessor team and the timing.

b. A description of the organisational structure of the qualified trust service provider, including the use made and organisational structure of other parties (subcontractors) that provide parts of the assessed qualified trust services.

c. An account of the assessment including a summary of the document review, as well as the review of the self-assessment.

d. An account of the assessment of the qualified trust service provider's information security risk analysis.

e. An account of the assessment of the qualified trust service provider's organisational reliability.

f. Assessment time used and detailed specification of time spent on document review and assessment of the implementation of the qualified trust service provider's management system.

g. A conclusion with regards to conformance/non-conformance, and a description of non-conformities (if any), including a clarification of them.

h. Assessment enquiries that have been followed, rationale for their selection, and the methodology employed.

i. Recommendation by the assessment team concerning the confirmation on whether the qualified trust service provider meets the requirements of the applicable conformity criteria (CRIT) for providing its qualified trust services.

Qualified trust service providers should review prior to the assessment what records are considered as confidential or sensitive by them such that the assessment team could not examine these records during their assessment. The qualified trust service providers should consult with the assessors to judge and jointly conclude whether the records that can be examined are sufficient to perform an effective assessment. If the assessors conclude that an effective assessment is not possible, they should inform the qualified trust service provider that the assessment could take place only when the qualified trust service provider has accepted appropriate access arrangements to confidential or sensitive information.

In every case, the document review should be completed prior to the commencement of assessment stage 2.

The results of assessment stage 1 should be documented in a written report including the detailed plan and planning for conduction of assessment stage 2. This report is submitted by the conformity assessment body to the competent supervisory body for review, validation and decision on proceeding with assessment stage 2 and for selecting assessment team members with the necessary competence based on a proposal from the conformity assessment body. Once validated by the supervisory body, assessors should make the qualified trust service provider aware of assessment stage 2 plan and planning, as well as of the further types of information and records that may be required for detailed verification during assessment stage 2. [142]

Assessment stage 2

This stage always takes place at the site(s) of the qualified trust service provider (including sites of potential sub-contractors). On the basis of observations documented in the report on assessment stage 1, assessors execute the validated plan and planning for the conduction of assessment stage 2.

The objectives of assessment stage 2 are:

(a) To confirm that the qualified trust service provider adheres to its own policies, objectives and procedures.

(b) To confirm that the implemented qualified trust service provider's management system conforms to the requirements of the applicable conformity criteria (CRIT) and is achieving the qualified trust service provider 's policy objectives.

Assessment report to the supervisory body

[142] With regards to the conduction of a conformity assessment prior to the notification to the supervisory body, i.e. prior its involvement, the prior validation by the supervisory body of stage 2 of the assessment may not be required but will occur a posteriori when validating the notified information and compliance of the qualified trust service provider and the qualified trust services it aims to provide.

After having offered the qualified trust service provider the possibility to include his comments (clearly marked as 'management's comments'), the conformity assessment report produced by the assessors is passed to the supervisory body. The assessment conclusions can be of three natures:

- Passed: the assessed trust service is "certified conformant".
- Failed with severe non-conformities: the assessed trust service is not certified conformant.
- Passed with pending non-conformities: successful assessment status is conditioned to the implementation of corrective actions within a determined delay in function of the type and criticality of the correction(s).

The conformity assessment body that assesses whether the qualified trust service provider and the qualified trust services it provides meet the requirements of the applicable conformity assessment criteria (CRIT) should incorporate a level of knowledge and experience in all areas that is sufficient to evaluate the assessment processes and associated recommendations made by the assessment team. Confirmation that the qualified trust service provider and the qualified trust services it provides meet the requirements should not be given in cases where unresolved non-conformities remain.

The conformity assessment body should have clear procedures laying down the circumstances and conditions in which the confirmation that the qualified trust service provider and the qualified trust services it provides meet the requirements will be maintained. If on surveillance or reassessment non-conformities are found to exist, the qualified trust service provider should effectively correct such non-conformities within a time agreed. If correction is not made within the time agreed, confirmation of compliance with the requirements should be reduced, suspended or withdrawn. The time allowed to implement corrective action should be consistent with the severity of the non-conformity and the risk to the assurance of products or services meeting specified requirements.

The documented statement confirming that the qualified trust service provider and the qualified trust services it provides meet the requirements should be confined to declared scopes, activities and locations and should provide a short description of the qualified trust service provider's organisation including identification of the legal entity and, if applicable, identification of the part of the legal entity that provides the qualified trust services. In addition, identification and locations should be provided and scope and activities should be described of other parties (subcontractors) that provide parts of the services.

Assessment conclusions and assessment status notification

Assessment conclusions and potential recommendations and/or requests for corrective actions are communicated by the conformity assessment body to the qualified trust service provider for implementation.

Assessed qualified trust service providers may be permitted to keep details of their internal processes and information security measures confidential when applicable.

11.8.3 Requirements on multisite sampling

The organisational structure of the qualified trust service provider, for the provision of its qualified trust services, could be such that the same activity is performed at a number of sites or that similar or different activities are performed at a number of sites operated by different legal entities. Assessors undertaking the conformity assessment may opt for assessing a sample of these sites. In this case, assessors should maintain procedures that include the full range of issues below in the building of their sampling programme.

The requirements from the IAF Mandatory Document for the Certification of Multiple Sites Based on Sampling [ref.3] shall apply.

Prior to undertaking their first assessment based on sampling, assessors should publish the sampling methodology that they employ. The procedures of assessors should ensure that the initial review of the conformity assessment contract with or mission against the qualified trust service provider and the qualified trust services it provides, identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined in accordance with the provisions below.

Where a qualified trust service provider has a number of similar sites that support the provision of the qualified trust services it provides, the following requirements should be fulfilled:

a) All sites of the qualified trust service provider are operating under the same or similar qualified trust service provider's management system that is centrally administered and audited and subject to central management review.

b) All sites have undergone internal auditing in accordance with the qualified trust service provider's internal auditing procedures.

c) A representative number of sites have been sampled by assessors, taking into account the requirements below:

   i) the results of internal audits of head office and the sites;

   ii) the results of management review;

   iii) variations in the size of the sites;

   iv) variations in the business purpose of the sites;

   v) complexity of the qualified trust service provider's management system;

   vi) complexity of the information systems at the different sites;

   vii) variations in working practices;

   viii) variations in activities undertaken;

   ix) potential interaction with critical information systems or information systems processing sensitive information;

   x) differing legal requirements.

d) The sample should be partly selective based on the above in point c) and partly non-selective and should result in a range of different sites being selected, without excluding the random element of site selection.

e) Every site of the qualified trust service provider that is subject to significant threats to assets, vulnerabilities or impacts should be included in the sampling programme.

f) The surveillance programme should be designed in the light of the above requirements and should, within a reasonable time, cover all sites of the qualified trust service provider.

g) In the case of a non-conformity being observed either at the head office or at a single site, the corrective action procedure should apply to the head office and all sites of the qualified trust service provider organisation.

The conformity assessment process must address the qualified trust service provider 's head office activities to ensure that a single management system applies to all sites and delivers central management at the operational level.

The conformity assessment must address all the issues outlined above.

11.9 Events triggering assessments (incl. notification of changes, termination, incidents, complaints, at supervisory body sole's discretion, EC request)

The notification of the following events shall lead to a supervision review requiring either a full conformity assessment or a surveillance conformity assessment depending on the criticality, the implications and the nature of the notified event:

- Notification of a security breach or any incident with regards to the qualified trust service provider and/or the qualified trust services it provides;
- Complaints by third parties;
- On request by the European Commission;
- On notification of a change in the policy(ies) and/or practices of the qualified trust service provider and/or the qualified trust services it provides;
- Notification of the qualified trust service provider of its intention to cease one or more of the qualified trust services it provides (note that such a notification will lead to the change of the actual qualified status into "supervisionincessation" in the trusted list of the competent supervisory body);
- Notification of the, expected or un-expected, termination of the qualified trust service provider and/or the qualified trust services it provides.

The supervisory body can initiate a supervision review at any time on its sole discretion.

11.10 Conformity Assessment Bodies

11.10.1 Recognition of Conformity Assessment Bodies - Requirements on NABs

Conformity assessment bodies shall be accredited, in the sense of Regulation 765/2008 [ref.2], by a National Accreditation Body (NAB) for carrying out assessments against the Supervision Scheme.

National Accreditation Body shall comply with ISO/IEC 17011 [ref.6] when assessing and accrediting conformity assessment bodies (CABs).

11.10.2 Requirements on Conformity Assessment Bodies

Principles regarding impartiality, competence, responsibility, openness, confidentiality and responsiveness to complaints as per ISO 17021:2011 [ref.4] apply.

Requirements from ISO 17021:2011 [ref.4], clauses 5 to 8 (included) apply with the following additions.

CABs shall comply with ISO/IEC 27006 [ref.7].

CABs shall comply with ISO/FDIS 19011 [ref.8].

a. Assessor's code of conduct

Assessors deployed for performing assessments in the context of the Supervision Scheme must observe a Code of Conduct fulfilling at least the following:

(a) To act in a trustworthy and unbiased manner in relation to both the body by which the assessor is employed, contracted or otherwise engaged and any other organisation involved in an assessment performed by him/her or by personnel directly under his/her control.

(b) To act independently and impartially; to disclose to the body deploying him/her any relationships he/she may have or may have had with the organisation to be assessed and to decline any assignment that could cause or could be perceived as causing conflict of interest.

(c) Not to accept any inducement, gift, commission, discount or any other profit from organisations assessed, from their representatives, or from any other interested person, nor knowingly allow personnel for whom he/she is responsible to do so.

(d) Not to disclose the observations, or any part of them, of the assessment team for which he/she is or was responsible or of which he/she is or was part, or any other information obtained in the course of an assessment, to any third party unless authorised in writing by both the assessed organisation and the body by which the assessor is or was deployed.

(e) Not to act in any way prejudicial to the reputation or interest of the body by which the assessor is or was deployed.

(f) To identify, evaluate the significance and take safeguards with regard to threats that can be attributed to one or more of the following categories:

(i) Self-interest;

(ii) Self-review;

(iii) Advocacy;

(iv) Familiarity; and

(v) Intimidation;

(g) In the event of any alleged breach of the code of conduct, to co-operate fully in any formal enquiry procedure

b. Competence criteria and requirements for assessors

Each individual assessor deployed by an independent conformity assessment body for performing conformity assessment must be qualified based on the following criteria:

(a) Academic qualifications must have been gained by a programme of studies consisting of a range of inter-related topics in which understanding is achieved by a predefined progression or route. It should be expected that where the assessor has accrued extensive experience and supplementary professional education and training, the requirement for academic qualifications would be significantly outweighed by their practical experience in the field.

(b) Having at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to Public Key Infrastructure and Information Security Management.

(c) Having demonstrated understanding of the applicable standards.

(d) Having demonstrated understanding of the concepts of management systems in general.

(e) Having demonstrated understanding of the issues related to various areas of qualified trust services related techniques and technologies, cryptology, Public Key Infrastructure, Information Security Management, and organisational reliability.

(f) Having demonstrated understanding of the principles and processes related to risk assessment and risk management.

(g) Having successfully followed a training course of at least five days on the subject of management system assessment and the management of assessment processes.

(h) Having the following personal attributes: objective, mature, discerning, analytical, persistent, and realistic. The candidate should be able to put complex operations in a broad perspective and should be able to understand the role of individual units in larger organisations.

(i) Having knowledge and attributes to manage the assessment process.

(j) Having the ability and processes to maintain own knowledge and skills of qualified trust services related techniques and technologies, cryptology, Public Key Infrastructure, Information Security Management, and management system assessment.

(k) Prior to assuming responsibility for performing as an assessor, the candidate must have gained experience in the entire process of qualified trust service providers and trust services assessment. This experience should have been gained by participation under supervision of qualified (lead) assessors in a minimum of four assessments for a total of at least 20 days, including documentation review, implementation assessment and assessment reporting.

(l) All relevant experience must be current.

An assessor performing as assessment team leader (Lead Assessor) must additionally fulfil the following requirements:

(m) Having acted as qualified assessor in at least three complete qualified trust service providers and qualified trust services assessments.

(n) Having demonstrated to possess adequate knowledge and attributes to manage the assessment process.

(o) Having demonstrated the capability to communicate effectively, both orally and in writing.

Satisfaction of these criteria must be demonstrated.

Assessors must maintain professional liability/errors and omissions insurance enough to cover liabilities.

c. Requirement on assessment teams

Assessment teams shall be competent for the duties assigned to them. The following requirements apply to the assessment team as a whole.

In each of the following areas at least one assessor in the team must satisfy assessors' criteria for taking responsibility within the assessment team:

1) managing the team (Lead Assessor);

2) demonstrated knowledge of the legislative and regulatory requirements and of legal compliance in the particular field of certification service and information security;

3) demonstrated knowledge of the current technical state-of-art regarding qualified trust services related techniques and technologies, cryptology and Public Key Infrastructure;

4) demonstrated knowledge in technologies applicable to the qualified trust services being assessed;

5) demonstrated knowledge of performing information security related risk assessments so as to identify assets, threats and the vulnerabilities of the qualified trust service provider and the qualified trust services it provides and understanding their impact and their mitigation and control;

6) demonstrated knowledge of organisational reliability issues.

The assessment team must be competent to trace indications of security incidents in the qualified trust service provider operations back to the appropriate elements of the qualified trust service provider management system.

An assessment team may consist of one person provided that the person meets all criteria set out above.

d. Guidance on the use of technical experts

In order to ensure that the assessment team has at its disposal all necessary expertise, assistance of Technical Experts with specific knowledge regarding the following subjects should be used:

(a) knowledge of the legislative and regulatory requirements and of legal compliance in the particular field of certification service and information security;

(b) knowledge of the current technical state-of-art regarding qualified trust services related techniques and technologies, cryptology and Public Key Infrastructure;

(c) knowledge in technologies applicable to the qualified trust service being assessed; and

(d) knowledge of performing information security related risk assessments so as to identify assets, threats and the vulnerabilities of the qualified trust service provider and its qualified trust services and understanding their impact and their mitigation and control.

Those not satisfying all qualification criteria for individual assessors, may be used to assist the assessment team. Such Technical Experts must at all times be responsible to the Lead Assessor and not function independently of Assessors in the team.

11.11 Cross-border Assessment and Mutual Assistance

Requirements from the Regulation shall apply [ref.1 - Art.14].

Annex 1 - Simplified Supervision Scheme based on prior-authorisation

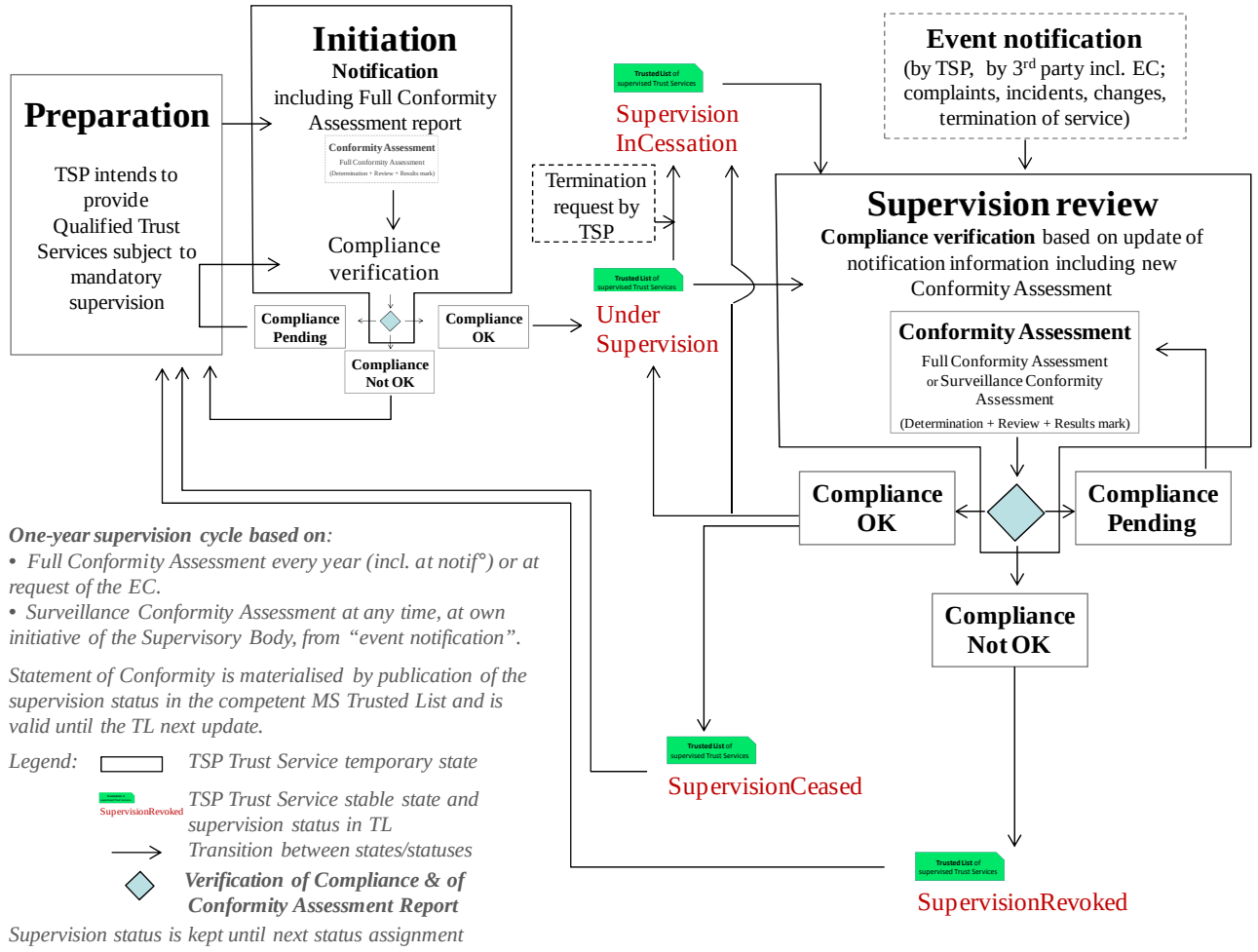


Figure A.1: Supervision process flow of the European Supervision Scheme (simplified).

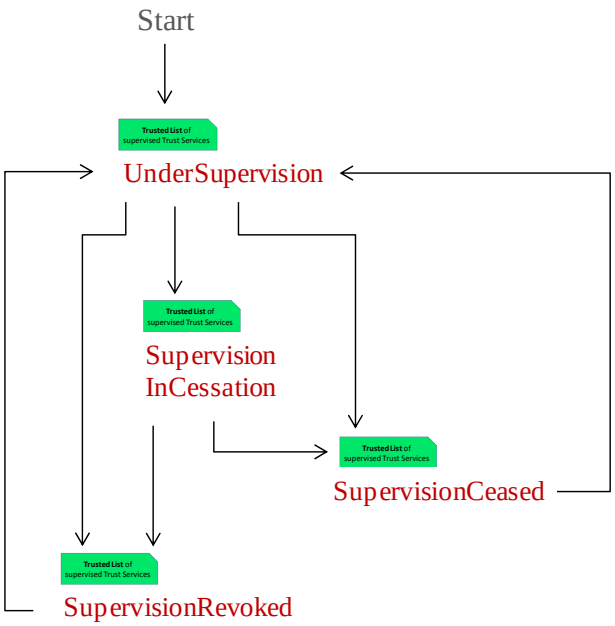
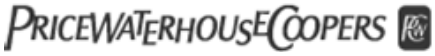


Figure A.2: Qualified (supervision) status flow in the context of the European Supervision Scheme (simplified).


DLA PIPER


SEALED
Trust Services Architects


time.lex


PRICEWATERHOUSECOOPERS



European Commission

Feasibility study on an electronic identification, authentication and signature policy (IAS)

Final Report

Luxembourg, Publications Office of the European Union

2013 – 415 pages

ISBN 978-92-79-31151-2
DOI: 10.2759/25928

KK-03-13-324-EN-N



DOI: 10.2759/25928 ISBN 978-92-79-31151-2