EUROPEAN
COMMISSION

Brussels, 24.7.2019
COM(2019) 372 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts

1. Introduction

Article 32a of the Anti-Money Laundering Directive 2015/849/EU[1] requires Member States to put in place by 10 September 2020 national centralised automated mechanisms, such as central registries or central electronic data retrieval systems, which allow the identification of any natural or legal persons holding or controlling payments accounts, bank accounts and safe deposit boxes. The Anti-Money Laundering Directive defines a minimum set of information that should be included in such centralised mechanisms. It also provides that Financial Intelligence Units should have immediate and unfiltered access to them, while the other competent authorities should also have access for fulfilling their tasks obligations under the Anti-Money Laundering Directive. Directive 2019/1153 on facilitating access to financial and other information[2] obliges the Member States to designate the national authorities competent for the prevention, detection, investigation or prosecution of criminal offences that should have direct, immediate and unfiltered access to the minimum set of information of such centralised mechanisms. Those competent authorities shall include at least the Asset Recovery Offices.

Access by competent authorities to central bank account registers or retrieval systems will be an important component in the fight against money laundering; associate predicate offences and terrorist financing, as well as more generally in combatting serious crimes. Bearing in mind the objectives of the Anti-Money Laundering Directive and the Directive on facilitating access to financial and other information, a future EU-wide interconnection of bank account registries and data retrieval systems would facilitate the cross-border cooperation of the competent authorities involved in the fight against money laundering, terrorist financing and other serious crimes.

Article 32a(5) of the Anti-Money Laundering Directive requires the Commission to assess the conditions and the technical specifications and procedures for ensuring secure and efficient interconnection of the centralised automated mechanisms. Therefore, this report assesses the various IT solutions at EU level, already operational or being currently under

[1] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 0849, 09.07.2018, p.1.

[2] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, OJ L186 of 11.7.2019, pp. 122-137.

development, which may serve as models for a possible interconnection of the centralised mechanisms. For an interconnection to be achieved, a legislative instrument would be required.

This report should considered in conjunction with the Commission's Supranational Risk Assessment report[3], the Commission's report on Financial Intelligence Units[4] and the Commission's report on the assessment of recent alleged anti-money laundering cases involving EU credit institutions[5], which are presented in parallel.

2. State of play

2.1. Centralised registries or electronic data retrieval systems on bank accounts in the Member States

For the time being[6], centralised mechanisms containing bank account information are operational in 15 Member States[7]. From the replies received from the Member States, there is a slight preference in favour of the technical solution of the central registry: whereas 17 Member States are having or going to have central registries, 9 Member States declared to have or to envisage central data retrieval systems[8]. There is also a preference for the systems which contain data additionally to the minimum set of information relating to the account profile, provided for in Article 32a(5) of the 5th Anti-Money Laundering Directive (11 replies to 6)[9].

[3] Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities COM (2019) 370.

[4] Report from the Commission to the European Parliament and the Council assessing the framework for cooperation between Financial Intelligence Units COM(2019) 371.

[5] Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institutions COM(2019) 373.

[6] The information in this section is based on the replies from the Member States to a dedicated Questionnaire sent to them in March 2019, on the information received in the transposition workshop of 1 April 2019 held by the Commission and on Annex 7 of the Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing Council Decision 2000/642/JHA (SWD(2018) 114 final).

[7] Belgium, Bulgaria, Czechia, Germany, Greece, Spain, France, Croatia, Italy, Latvia, Lithuania, Austria, Portugal, Romania, Slovenia. Slovakia has in place a centralised electronic data retrieval system, which is, however, currently accessible only for judicial officers.

[8] Finland adds to both marks as it is about to deploy a system which uses both solution. A central register collects and contains the relevant information in one central database, whereas a central electronic data retrieval system consists of a central IT portal, retrieving information from different underlying databases (maintained e.g. by the financial institutions).

[9] From the replies received from the Member States such additional information might include information on financial contracts concluded by the owner of the account, or on transactions carried out in relation to the account.

2.2. EU systems interconnecting national decentralised electronic databases

There are several EU projects ensuring the EU-wide decentralised interconnection of national electronic databases.[10] The IT systems that are considered relevant for this report are the following:

The European Criminal Records Information System (ECRIS) became operational in April 2012 in order to improve the exchange of information on criminal records throughout the EU.[11] All Member States are currently connected to ECRIS. ECRIS ensures that information on convictions is exchanged between Member States in a uniform, fast and compatible way and provides judges and prosecutors with easy access to comprehensive information on the criminal history of persons concerned.[12]

The European c and driving licence information system (EUCARIS) connects countries so they can share vehicle and driving licence information and other transport related data. EUCARIS is a mechanism that connects the Vehicle and Driving Licence Registration Authorities in the Union through which vehicle owner and vehicle insurance can be exchanged between National Contact Points of Member States.[13]

The EU-wide interconnection of insolvency registers (IRI), which includes two different projects. The first version of the system (IRI 1.0) has been available on the European e-Justice Portal[14] since July 2014. It was developed as a pilot-project[15] with the voluntary participation of certain Member States[16]. The second version (IRI 2.0) is based on Regulation (EU) 2015/848 on insolvency proceedings, and will interconnect the national insolvency registries of all Member States (with the exception of Denmark). All Member States should be compliant with the interconnection by June 2021. IRI 1.0 is based on a standardised secure

[10] Centralised IT systems with single databases at EU level, such as the Schengen Information System or the Visa Information System, are excluded from the assessment, as such systems are irreconcilable with the pre-existence of nationally centralised databases.

[11] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of criminal records between Member States and Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA - currently modified by Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS).

[12] In April 2019 a new legislative framework was adopted in order to supplement ECRIS with a mechanism allowing for efficient exchange of criminal records information on third country nationals convicted on the EU territory. The European Criminal Records Information System for Third Country Nationals (ECRIS-TCN) will be a centralised hit/no hit system containing only identity information of convicted TCN and indication of the Member State where he/she had been previously convicted. Upon the hit, the requesting Member State will have to request the conviction information via existing ECRIS from the Member State(s) indicated by the ECRIS-TCN.

[13] Legal bases for the Prüm service are the - Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA.

[14] https://beta.e-justice.europa.eu/246/EN/bankruptcy_amp_insolvency_registers__search_for_insolvent_firms_in_the_eu

[15] The pilot project was implemented on the basis of and executed further to the Multiannual European e-Justice Action Plan 2009-2013, OJ C 75, 31.3.2009, p. 1-12 and the Multiannual European e-Justice Action Plan 2014-2018, OJ C 182, 14.6.2014, p. 2-13.

[16] Currently Czechia, Germany, Estonia, Italy, Latvia, the Netherlands, Austria, Romania and Slovenia participate.

web service messages (SOAP over HTTPS), while IRI 2.0 additionally supports data exchanges leveraging the Connecting Europe Facility (CEF) eDelivery building block[17].

The Business Registers Interconnection System (BRIS) is the interconnection of business registers, allowing business registers to exchange cross-border messages on mergers and branches, and the users of the e-Justice portal to obtain multilingual information on EU companies. The system has been operational since June 2017, in accordance with Directive (EU) 2012/17 as regards the interconnection of central, commercial and companies registers[18]. BRIS uses the Connecting Europe Facility eDelivery building block for exchanges of standardised messages. The system is decentralised with a central component (the European Central Platform) storing and indexing company names and registration numbers.

The Land Registers Interconnection (LRI) is an on-going voluntary project[19], which aims to provide a single access point within the European e-Justice Portal to the land registers of participating EU countries. It is planned to become operational in the second quarter of 2020.

The European Business Ownership and Control Structures (EBOCS) is a project carried out by European Business Registries Association with the financial support of the Internal Security Fund (ISF) Police (Annual Work Programmes 2016 and 2018). The EBOCS platform provides simplified and unified access to business register data on business ownership and control structures for financial analysis and investigation purposes. It also provides for the aggregation of the results of the queries in a visualisation map. It is noted that the EU does not own the intellectual property rights of this system.

The e-CODEX system (e-Justice Communication via Online Data Exchange) facilitates secure communication in civil and criminal proceedings by providing a decentralised system for cross-border electronic messages exchange in the justice area.[20] e-CODEX is currently facilitating the electronic communication between citizens and courts, and between Member State administrations in piloting the European Order for Payment and the European Small Claims Procedure. In the criminal justice field, e-CODEX is also the solution of choice for the e-Evidence Digital Exchange System[21], for electronic exchanges in the context of the European Investigation Order (EIO) and Mutual Legal Assistance Treaties (MLATs).

[17] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery

[18] Directive (EU) 2012/17 of the European Parliament and of the Council of 13 June 2012 amending Council Directive (EEC) 89/666 and Directive (EC) 2005/56 and Directive 2009/101 of the European Parliament and of the Council as regards the interconnection of central, commercial and companies registers, OJ L 156, 16.6.2012.

[19] There is no legal basis for the interconnection but this functions as voluntary system where Member States can opt-in.

[20] The e-CODEX system consists of a package of software products (CEF eDelivery and the e-CODEX connector), which can be used to set up an access point at national level for the purpose of such secure communication. It is not a system interconnecting national databases or registries, but a communication infrastructure ensuring secure communication and exchange of information between national IT systems and as such it is considered relevant for the assessment in this report. e-CODEX was developed between 2010 and 2016 by 21 Member States with the participation of other countries/territories and organisations.

[21] Established further to the Council conclusions on improving criminal justice in cyberspace from 9 June 2016.

3. Main parameters

3.1. Condition for access by users

Looking at the existing systems, it is apparent that the accessibility of the user-facing system interacting with the interconnected IT system is determined by the purpose it is established for. Where the interconnection was established with the aim to enhance the transparency of information for businesses in the internal market (BRIS, IRI), the system is publicly accessible. Where the objective of the interconnection is to improve cross-border cooperation between competent authorities for law enforcement or public administrative purposes, such as in the case of ECRIS or the Prüm service of EUCARIS[22], the access is restricted.

The "find a company" functionality of BRIS is available in the e-Justice Portal for everyone, while the messaging infrastructure is currently restricted by law for national business registers. With regard to IRI, the information through the search interface is publicly accessible and a possibility for Member States to restrict the access to requestors with a legitimate interest is only given in the context of "consumer insolvency proceedings". ECRIS is accessible only to designated central authorities of the Member States. Similarly, the access to the services of EUCARIS is open to public authorities via the designated national contact points. For EBOCS, access is restricted to the participating Counter Crime Agencies.

System	Public access	Restricted access	comments
BRIS	Yes		The "find a company" functionality of BRIS is available in the e-Justice Portal for everyone, while the messaging infrastructure is currently restricted by law for national business registers.
IRI	Yes		
ECRIS		Yes	for central authorities of the Member States especially nominated for this function
EUCARIS		Yes	for the EUCARIS National Contact Points, through which public authorities can get access, depending on the legal basis of the cooperation
EBOCS		Yes	For the Counter Crime Agencies participating in the project
LRI	Yes*		advanced features will be only available for authenticated legal professionals

Table 1: Accessibility of the user-facing system interacting with the interconnected IT system

Under the Anti-Money Laundering Directive, the purpose of the centralised mechanisms on bank accounts is to improve the fight against money laundering and terrorist financing and access is limited to certain public authorities. The Directive on facilitating access to financial and other information extends the purpose of the use of the information in the central mechanisms to serious crime and the access rights to designated competent authorities. Finally, the scope of the domestic authorities having direct access to the national registries

[22] While several authorities can access EUCARIS, the Prüm service of EUCARIS regulates access by law enforcement authorities.

* not yet operational

lies with the Member States operating the registries. This might lead to a discrepancy, as certain types of authorities might get access in one Member State but not in another. In a cross-border exchange through the EU-wide interconnection system this could lead to a situation where an authority is requesting information from the registry of another Member State, where that search is denied to a similar authority.

One option could be that the same authorities, which will be provided with direct access to the centralised mechanisms in accordance with the Anti-Money Laundering Directive and the Directive on facilitating access to financial and other information, will be provided with access to the interconnection platform. Another option would be that access rights to the interconnection system are given to the same types of authorities in all Member States, which could be achieved by a harmonised and closed list at EU level of the types of authorities specified in accordance with the purpose of the access to the information.

In case the interconnection is extended to all authorities currently granted access under the national laws, detailed provisions on the conditions for access and searches by the competent national authorities would be necessary. In this regard, it is important to highlight that the Directive on the use of financial information and other information lays down strict conditions for the access and for searches of bank account information, contained in the centralised automated mechanisms by competent authorities, designated at national level. Such conditions include, for example, the provision of access to the registries and data retrieval systems only to specifically designated and authorised persons of each competent authority. Another measure mitigating the risks posed by the enlarged access rights by the designated national authorities could be the restriction of the scope of the available information in the interconnection system to the minimum set of information relating to the account profile as set out in Article 32a(3) of the Anti-Money Laundering Directive.

As regards the scope, Article 32a(3) Anti-Money Laundering Directive defines the information which all centralised systems have to contain, such as the account holder, bank accounts identified by IBAN and safe deposit boxes held by a credit institution within the national territory. However. Article 32a(4) of the Directive provides for the possibility that Member States include other information in the registries deemed essential for Financial Intelligence Unis and competent authorities for fulfilling their obligations under the Directive. From a perspective of protection of personal data, it appears necessary to restrict the scope of the information accessible through the interconnection platform to the minimum mandatory set of information defined in Article 32a(3) of the Anti-Money Laundering Directive. In line with data protection rules, the access to personal data should be proportionate to what is necessary for the objectives defined in Anti-Money Laundering Directive. A similar approach is taken by the Directive on the use of financial and other information. Article 4(2) of this Directive clarifies that the additional information that Member States include in the centralised mechanisms shall not be accessible and searchable by competent authorities.

3.2. Search functionality

The applicable search criteria are of key importance to ensure that the interconnection of the automated centralised mechanisms brings added value for the users. The search criteria should be designed in a way that reinforces the relevant authorities' capacity to carry out their tasks and conduct investigations more effectively while ensuring proportionality and respecting the applicable data protection requirements.

Consideration should be given to who will be entitled to perform the search (private parties or public parties) and to the data which can or cannot be expected to be known to the person carrying out the search. Imposing a requirement that the search should contain data that is unlikely to be known to the person conducting the query may render effective searches difficult or impossible. It is also noted that there are cases where a Financial Intelligence Unit or a law enforcement authority from one Member State will not be aware of the date of birth or national identification number of a citizen of another Member State. If the interconnection is made available to such additional information in the centralised systems, it will be important to determine whether it will also be possible to carry out searches on the basis of such additional information.

The types of information constituting the harmonised minimum set of information in Article 32a(3) of the Anti-Money Laundering Directive could be envisaged as search criteria. This would make the interconnection system fit for original purposes of the centralised mechanisms. Additional safeguards in allowing to verify hits (in particular in cases where search results in several replies) would be needed.

The conditions on the modalities of searches applicable are decisive on the effectiveness of the use of the interconnected databases. The option to run "fuzzy searches", i.e. searches that will deliver broader results even if a word is misspelled or incomplete, will broaden the hit results, thereby increasing the probability that the requested information is accessed through the search, but might raise data protection concerns, as it might expose personal data that were not actually concerned by the search. On the contrary, an "exact match" requirement mitigates the risks of unnecessary exposure of personal data, but will increase the probability that the requested information is overlooked by the search engine (in case of difference in the spelling of the entry or of using different transliteration rules).

The possibility of carrying out "fuzzy searches" would reduce the use of automatic validation procedures and therefore avoid or reduce the volume of erroneous hits, but would also reduce the operational value of the system. In case of using "fuzzy searches" other tools to mitigate the risk of fishing expeditions should be considered, for example as in IRI where there is a maximum limit of the number of displayed results.

3.3. Governance structure, responsibility for maintenance

In the case of BRIS, IRI, LRI and ECRIS the various services of the European Commission are *responsible for maintaining the IT system*, i.e. they have to ensure the availability of the interconnection component and they bear the costs of setting up and maintaining it. For the time being e-CODEX is maintained by a consortium of Member States (the CEF eDelivery

component is within the European Commission's remit). In EUCARIS, the responsibility is borne by the 28 Member States and the participating third States, while in EBOCS, the system is owned by the European Business Registers' Association (EBRA). Since these IT systems are interconnecting national databases, the responsibility to maintain the national databases and to ensure their availability is for the Member States.

For the *governance structure* of a system interconnecting databases, the competences in decision making in policy and operational issues should be constructed in a way in which it serves the interests of the national components.

In BRIS, the BRIS Steering Committee acts as the Commission's internal forum for the policy decisions, oversight and management of BRIS, while the Company Law Expert Group – Business Registers (CLEG-BRIS) acts as the forum for the policy level collaboration between the actors involved. A similar distinction between policymaking and operative structures can be seen with regard to EUCARIS where the General Assembly consisting of high representatives of the government agencies determines the policy to be pursued, endorses the budget and annual contributions and makes arrangements for system management.

3.4. Data controllership

The responsibility for maintaining the IT system is different from the issue of *responsibility from the perspective of data protection*. According to the General Data Protection Regulation[23], the data controller is the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data, and bears the responsibility for the processing of personal data. The issue of controllership is complex and many factors are relevant for the assessment of controller, including but not limited to the question who stores the data and where).

With regard to IRI, the EU platform is only interconnecting the decentralised national databases and all the data displayed in the central platform are simply "transient data", they are not stored in the EU component, nor are logs from the queries run by the users through the web-service recorded or kept at the centre. The situation is somewhat different with regard to BRIS, which introduced a particular feature of storing the core profile data of the businesses in a central component at Commission level, which the national registries keep updating in regular intervals. The initial query is run against this central database, resulting in a hit-list with the names of the entities. The requestor can get detailed data on a particular entity by choosing the name of that entity from the hit-list, which action generates a direct interconnection to the information in the national database.

With regard to a possible interconnection of centralised mechanisms, consideration should be given to developing an IT system, where the central routing component does not store any personal data, and where all decisions on the means and purposes of data processing are taken

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

at national level. The objective of the interconnection service would be simply to facilitate data processing on behalf of the centralised mechanisms that would remain the controllers of their respective data sets.

3.5. Costs of establishment and maintenance

Setting up a system interconnecting the national central mechanisms will generate costs both in terms of establishment and in terms of maintenance of the system, which costs would have to be shared between the EU and its Member States. Looking at the sharing of costs in the model examples, as a rule, the costs related to the EU component (central routing component, EU platform) were financed from the general budget of the EU, whereas Member States bore the costs needed for the adjustment of their national systems making them interoperable with the EU system of interconnection. In the case of BRIS, the development of the first version, that went live on June 2017, which included the European Central Platform, required around EUR 1,7 million. As to IRI which has a more simple architecture, the costs for the development of the central search pilot system (IRI 1.0) were approximately EUR 280 000, whereas the adaptation of the central search application towards the establishment of IRI 2.0 will cost approximately EUR 170 000. With regard to ECRIS, the total cost of the deployment of the "Reference Implementation", which is the software to exchange data concerning criminal records between Member States, reached EUR 2 050 000. The yearly cost of maintenance of the system amounted to EUR 150 000. With regard to EUCARIS, a general fee of around EUR 20 000 is asked from each participating countries for maintenance purposes.

From the figures above, it appears that the costs of establishment and maintenance of an EU-wide interconnection system are relatively low, compared to the benefits such a project brings to the EU. Cost efficiency could be improved by reusing existing capacities (such as eDelivery access points, Connecting Europe Facility building blocks, core vocabularies of the European Commission's Directorate-General for Informatics, etc.).

4. Technical specifications of the systems, including data security

4.1. Network used and data security

The Prüm service of EUCARIS and ECRIS use the Trans European Services for Telematics between Administrations (TESTA), which is a private network completely separate from the public internet. The designated national contact points have access to this private network. The TESTA network service is run by the Commission, and provides guaranteed performance and a high level of security. As to EUCARIS, use via public internet is possible, but currently not used. It has connections with all the EU institutions and national networks and is preferred in the context of law enforcement cooperation which involves sensitive information. Other secure networks have also been developed by the EU institutions, for example the Common Communications Network and Common Systems Interface (CCN/CSI) which is in use in the area of customs policy and taxation.

BRIS, IRI, LRI and EBOCS use the public internet (with appropriate encryption technology for data flowing through the web). When it comes to the secure exchange of information over the public internet, the eDelivery building block enables businesses and public administrations to exchange electronic data and documents in digital format in an interoperable, secure, reliable and trusted way with other organisations. This is aligned with the definition of Electronic Registered Delivery Services (known as 'ERDS') in article 3(36) of the eIDAS Regulation.[24]

For the possible interconnection of centralised systems which arguably includes sensitive information, the use of TESTA could be envisaged. Nevertheless, public internet solutions could also be considered. Almost all national centralised systems use the public internet. From the perspective of data security and integrity, the fact that the system will consist of decentralised databases will mitigate possible risks, as decentralisation and distributed technologies are *per se* more resilient to cyber-attacks, since it is much more difficult to corrupt data to a general scale and much more easier to recover data after incidents.

4.2. Central routing component

There are two main types of architectures of IT systems, i.e. the purely decentralised systems and those that have a central platform or routing component deployed at EU level, which serves as "connector" between the decentralised national databases.

In “purely distributed systems”, there is no EU platform or component, but all countries communicate directly to each other, with the help of commonly agreed standards which allow for direct peer-to-peer exchanges between the connected points of the Member States. Therefore, when a query is launched, this is dispatched individually to each other national system, and the replies received are collected and displayed trough the web-client surface of the requestor. EUCARIS, ECRIS and e-CODEX implement this technology (relying on a jointly developed application).

In "distributed systems with a central routing component" there is a centralised platform at EU level: a single, central web-service, maintained and operated at the EU level, which is connected to all national systems. Users run queries through the central web-service, which collects the information from the national databases. BRIS, EBOCS and IRI use this technology.[25]

A solution with a central routing component might be easier to implement from a connectivity point of view. Where there is one single platform, each Member State has to establish and maintain only one connection between the national system and this centralised

[24] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114.

[25] There are alternatives to a central component. For example, the CEF eDelivery Service Metadata Publisher (SMP) enables the participants of a messaging infrastructure to dynamically discover each other's capabilities (legal, organisational, and technical). Because of this distributed architecture, each participant has to have a unique ID. A central component, called Service Metadata Locator (SML), uses these IDs to create URLs that, when resolved, direct the eDelivery Access Points towards the specific information about the participant.

platform. In absence of a 'real' centralised platform, however, each Member State will need to establish, test and maintain connections to all other national systems of the Member States (e.g. the Prüm service of EUCARIS currently counts almost 756 connections). A purely distributed system has to deal with the challenge of the multiplied number of connections, which may increase the problems in terms of management, control and audit. Nevertheless, there are technological solutions to the challenge of managing large number of possible connections. At the same time, the fact that in a central routing system the central component may become a single point of failure for the whole system deserves due consideration.

4.3. Data exchange protocol

The BRIS and e-CODEX use the CEF eDelivery solution, whereas the IRI 2,0 will use both the CEF eDelivery and SOAP[26] communication. The Prüm service of EUCARIS and the EBOCS use SOAP based interfaces. The LRI applies RESTful Web Sevices[27].

The CEF eDelivery Building Block helps users to exchange electronic data with one another in a secure, reliable and trusted way. The CEF eDelivery solution is based on a distributed model called the "4-corner model" where the back-end systems of the users do not exchange data directly with each other but through Access Points. These Access Points are conformant to the same technical specifications and therefore capable of communicating with each other. Another benefit of eDelivery is that it caters for the security of the data exchanged between the different access points, without the need for bespoke development. As a result of this, users adopting CEF eDelivery can easily and safely exchange data even if their IT systems were developed independently from each other. The eDelivery model – very useful for interfacing with multiple back-end systems – various functionalities can be centralised instead. When using this technology solution, the Member States (and optionally the Commission in the case of a central routing component) would have to deploy an eDelivery gateway at their respective level. They can reuse their existing gateways developed for other services (which contributes to the cost effectiveness of the solution). There is a compatible software solution developed by the European Commission's Directorate-General for Informatics and provided free of charge under a European Union Public Licence (EUPL). However, some customisation and development is usually required. The eDelivery model follows asynchronous communication, which implicitly generates certain latencies in performance (typically of 3-10 seconds). There is a general EU policy with regard to CEF building blocks aiming at the convergence of the various systems developed under the different EU policy areas.

Where synchronous SOAP – allowing for communication over a secure layer – is used, most often a more simple architecture is chosen, aiming at best performance. RESTful architectural style represents a newer solution compared to SOAP, and there is a trend emerging, whereby SOAP is supplanted by REST technology. In both eDelivery and SOAP or REST based approaches trust is usually digital certificate-based and various checks are done.

[26] Simple Object Access Protocol.

[27] Representational State Transfer is a software architectural style that defines a set of constraints to be used for creating Web services.

As for future interconnection of the centralised mechanisms, it is noted that in CEF eDelivery is used where bilateral exchanges between the decentralised national databases are taking place, whereas in the systems where the communication takes place only vis-à-vis a national database and the central platform, the SOAP based interface (or RESTful) is sufficient.

4.4. Working in a multilingual environment and semantic interoperability

All assessed systems work in multilingual environment, apart from EBOCS which currently works in three languages with the plan to work in all languages in the long-term. In BRIS, transliteration is carried out at EU level, whereas in IRI, LRI and EUCARIS at national level. With regard to semantic interoperability (glossaries), a future interconnection of centralised mechanisms not require a specific vocabulary as the minimum set of information consists not of national concepts, but personal data, such as name, unique identifier (e.g. national ID numbers) and IBAN number. A common understanding in all national systems is essential, in particular because the national centralised mechanisms do not information on EU and third country entities. The transliteration rules of the Schengen Information System (SIS) could serve as a useful example in this context.

According to the European Interoperability Framework (EIF), the semantic aspect refers to the meaning of data elements and the relationships between them. It includes developing vocabularies and schemata to describe data exchanges, and ensures that data elements are understood in the same way by all communicating parties.

The system to interconnect banking registries will need to exchange data between different databases, each with its own data models and semantic standards. Common semantic standards will need to be set up, either natively in the systems or as a mapping layer between the different standards in the Member States. However, before creating any new semantic standard, reuse of already existing standards needs to be considered.

The Core Vocabularies (Business, Location, Person, as well as others) created by the ISA2 Programme are simplified, reusable, and extensible data models that can be used for this purpose. The different solutions for the interconnections of base registries, such as BRIS already reuse some of the standards (for example the Core Business Vocabulary).

5. Next steps

This reports sets out a number of elements to be considered for a possible interconnection of bank account registries and data retrieval systems and illustrates that the interconnection of those centralised mechanisms is technically feasible. Such a system could possibly be a decentralised system with a common platform at EU level. Technology already developed by the European Commission in the context of the various analysed models could be used.

Over the last years different systems have followed the reuse of common building blocks. These building blocks are essentially a set of well-known standards and technical specifications that can be applied to recurrent challenges such as the secure exchange of information. Consistently resorting to these building blocks is an approach advocated by

current digital policy of the Commission, to which the Member States have committed themselves in the Tallinn Declaration on eGovernment[28]. A future interconnection of national centralised automated mechanisms could leverage the use of the same building blocks to accelerate its creation and alignment to relevant EU regulations such as eIDAS.

Given that a future EU-wide interconnection of the centralised mechanisms would speed up access to financial information and facilitate the cross-border cooperation of the competent authorities, the Commission intends to further consult with the relevant stakeholders, governments, as well as the Financial Intelligence Units, law enforcement authorities and Asset Recovery Offices as potential "end-users" of a possible interconnection system.

[28] All the European Union Member States and EFTA countries signed the 'eGovernment Declaration' in Tallinn on 6 October 2017. The text of the Declaration is available at http://ec.europa.eu/newsroom/document.cfm?doc_id=47559