DURCHFÜHRUNGSBESCHLUSS (EU) 2015/1505 DER KOMMISSION

vom 8. September 2015

über technische Spezifikationen und Formate in Bezug auf Vertrauenslisten gemäß Artikel 22 Absatz 5 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG ([1]), insbesondere auf Artikel 22 Absatz 5,

in Erwägung nachstehender Gründe:

(1) Vertrauenslisten sind wesentlich für die Schaffung von Vertrauen unter den Marktteilnehmern, denn sie geben Auskunft über den Status des Diensteanbieters zum Zeitpunkt der Beaufsichtigung.

(2) Die grenzüberschreitende Verwendung elektronischer Signaturen wurde durch die Entscheidung 2009/767/EG der Kommission ([2]) erleichtert, mit der die Mitgliedstaaten erstmals zur Aufstellung, Führung und Veröffentlichung von Vertrauenslisten mit Angaben zu Zertifizierungsdiensteanbietern verpflichtet wurden, die gemäß der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates ([3]) öffentlich qualifizierte Zertifikate ausstellen und von den Mitgliedstaaten beaufsichtigt und akkreditiert werden.

(3) Artikel 22 der Verordnung (EU) Nr. 910/2014 verpflichtet die Mitgliedstaaten, auf gesicherte Weise elektronisch unterzeichnete oder besiegelte Vertrauenslisten in einer für die automatisierte Verarbeitung geeigneten Form zu erstellen, zu führen und zu veröffentlichen und der Kommission unverzüglich die für die Erstellung der nationalen Vertrauenslisten verantwortlichen Stellen zu melden.

(4) Vertrauensdiensteanbieter und die von ihnen erbrachten Leistungen sollten als qualifiziert angesehen werden, wenn dem Diensteanbieter auf der Vertrauensliste der qualifizierte Status zugeordnet ist. Damit gewährleistet ist, dass anderweitige Verpflichtungen aus der Verordnung (EU) Nr. 910/2014, insbesondere den Artikeln 27 und 37 von den Diensteanbietern leicht problemlos aus der Ferne und auf elektronischem Wege erfüllt werden können, und um den Vertrauensschutz anderer Zertifizierungsdiensteanbieter zu wahren, die keine qualifizierten Zertifikate ausstellen, aber Dienste im Zusammenhang mit elektronischen Signaturen gemäß der Richtlinie 1999/93/EG erbringen und bis zum 30. Juni 2016 in die Liste aufgenommen werden, sollte es den Mitgliedstaaten möglich sein, auf nationaler Ebene auf freiwilliger Basis andere Dienste als die qualifizierten Vertrauensdienste in die Vertrauenslisten aufzunehmen, sofern deutlich gekennzeichnet wird, dass diese Dienste nicht gemäß der Verordnung (EU) Nr. 910/2014 qualifiziert sind.

(5) Im Einklang mit Erwägungsgrund 25 der Verordnung (EU) Nr. 910/2014 können die Mitgliedstaaten auch andere, auf nationaler Ebene festgelegte Arten von Vertrauensdiensten zusätzlich zu jenen festlegen, die in Artikel 3 Absatz 16 der Verordnung (EU) Nr. 910/2014 definiert sind, sofern deutlich gekennzeichnet wird, dass diese Dienste nicht gemäß der Verordnung (EU) Nr. 910/2014 qualifiziert sind.

(6) Die in diesem Beschluss vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 48 der Verordnung (EU) Nr. 910/2014 eingesetzten Ausschusses —

HAT FOLGENDEN BESCHLUSS ERLASSEN:

Artikel 1

Jeder Mitgliedstaat sorgt für die Aufstellung, Veröffentlichung und Führung von Vertrauenslisten, die Angaben zu den qualifizierten Vertrauensdiensteanbietern, für deren Beaufsichtigung sie zuständig sind, und zu den von ihnen erbrachten qualifizierten Vertrauensdiensten enthalten. Diese Listen erfüllen die technischen Spezifikationen des Anhangs I.

([1]) ABl. L 257 vom 28.8.2014, S. 73.
([2]) Entscheidung 2009/767/EG der Kommission vom 16. Oktober 2009 über Maßnahmen zur Erleichterung der Nutzung elektronischer Verfahren über „einheitliche Ansprechpartner“ gemäß der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt (ABl. L 274 vom 20.10.2009, S. 36).
([3]) Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. L 13 vom 19.1.2000, S. 12).

Artikel 2

Die Mitgliedstaaten können in die Vertrauenslisten Angaben über nicht qualifizierte Vertrauensdiensteanbieter samt den von diesen erbrachten nicht qualifizierten Vertrauensdiensten aufnehmen. In der Liste muss deutlich gekennzeichnet sein, welche Vertrauensdiensteanbieter samt den von ihnen erbrachten Vertrauensdiensten nicht qualifiziert sind.

Artikel 3

(1) Nach Artikel 22 Absatz 2 der Verordnung (EU) Nr. 910/2014 müssen die Mitgliedstaaten die für die automatisierte Verarbeitung geeignete Fassung ihrer Vertrauensliste im Einklang mit den technischen Spezifikationen des Anhangs I elektronisch unterzeichnen oder besiegeln.

(2) Veröffentlicht ein Mitgliedstaat eine menschenlesbare Fassung der Vertrauensliste in elektronischer Form, so stellt er sicher, dass diese Fassung der Liste dieselben Angaben enthält wie die für die automatisierte Verarbeitung geeignete Fassung, und unterzeichnet oder besiegelt sie elektronisch im Einklang mit den technischen Spezifikationen des Anhangs I.

Artikel 4

(1) Die Mitgliedstaaten melden der Kommission die in Artikel 22 Absatz 3 der Verordnung (EU) Nr. 910/2014 genannten Angaben unter Verwendung des Musters in Anhang II.

(2) Zu den in Absatz 1 genannten Angaben gehören auch zwei oder mehr Public-Key-Zertifikate eines Systembetreibers mit einer um mindestens drei Monate zeitversetzten Gültigkeitsdauer, die den privaten Schlüsseln entsprechen, die verwendet werden können, um die für die automatisierte Verarbeitung geeignete Fassung sowie die menschenlesbare Fassung der Vertrauensliste elektronisch zu unterzeichnen oder zu besiegeln, wenn diese veröffentlicht werden.

(3) Nach Artikel 22 Absatz 4 der Verordnung (EU) Nr. 910/2014 macht die Kommission die in den Absätzen 1 und 2 genannten Angaben in der von den Mitgliedstaaten gemeldeten Fassung in signierter oder besiegelter und für die automatisierte Verarbeitung geeigneter Form über einen sicheren Kanal auf einem authentifizierten Web-Server öffentlich zugänglich.

(4) Die Kommission macht die in den Absätzen 1 und 2 genannten Angaben in der von den Mitgliedstaaten gemeldeten Fassung in signierter oder besiegelter menschenlesbarer Form über einen sicheren Kanal auf einem authentifizierten Web-Server öffentlich zugänglich.

Artikel 5

Dieser Beschluss tritt am zwanzigsten Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Dieser Beschluss ist in allen seinen Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 8. September 2015

Für die Kommission

Der Präsident

Jean-Claude JUNCKER

ANHANG I

TECHNISCHE SPEZIFIKATIONEN FÜR EINE GEMEINSAME VORLAGE FÜR VERTRAUENSLISTEN

KAPITEL I

ALLGEMEINE ANFORDERUNGEN

Vertrauenslisten müssen sowohl die aktuellen als auch alle historischen Daten über den Status der gelisteten Vertrauensdienste ab dem Zeitpunkt der Aufnahme eines Vertrauensdiensteanbieters in die Vertrauenslisten enthalten.

Die in diesen Spezifikationen verwendeten Begriffe „genehmigt", „akkreditiert" und/oder „beaufsichtigt" gelten auch für die einzelstaatlichen Genehmigungssysteme, doch müssen die Mitgliedstaaten in ihrer Vertrauensliste Zusatzinformationen zu diesen einzelstaatlichen Regelungen geben, einschließlich präziser Angaben zu den etwaigen Unterschieden gegenüber den Aufsichtssystemen, denen qualifizierte Vertrauensdiensteanbieter und die von ihnen angebotenen qualifizierten Vertrauensdienste unterliegen.

Die in der Vertrauensliste zur Verfügung gestellten Informationen sollen der besseren Validierung qualifizierter Vertrauensdienst-Tokens, d. h. physischer oder binärer (logischer) Objekte, dienen, die von qualifizierten Vertrauensdiensten erzeugt oder ausgestellt werden (z. B. qualifizierte elektronische Signaturen/Siegel, fortgeschrittene elektronische Signaturen/Siegel, die auf einem qualifizierten Zertifikat beruhen, qualifizierte Zeitstempel oder qualifizierte Zustellbelege).

KAPITEL II

DETAILLIERTE SPEZIFIKATIONEN FÜR EINE GEMEINSAME VORLAGE FÜR VERTRAUENSLISTEN

Die vorliegenden Spezifikationen beruhen auf den in ETSI TS 119 612 Version 2.1.1 (im Folgenden „ETSI TS 119 612") festgelegten Spezifikationen und Anforderungen.

Soweit in den vorliegenden Spezifikationen keine besonderen Anforderungen festgelegt sind, müssen die Anforderungen aus ETSI TS 119 612 Abschnitte 5 und 6 in ihrer Gesamtheit erfüllt werden. Soweit in den vorliegenden Spezifikationen besondere Anforderungen festgelegt sind, haben diese Vorrang vor den entsprechenden Anforderungen aus ETSI TS 119 612. Bei Unterschieden zwischen den vorliegenden Spezifikationen und den Spezifikationen laut ETSI TS 119 612 haben die vorliegenden Spezifikationen Vorrang.

Name des Systembetreibers (Abschnitt 5.3.6)

Dieses Feld muss vorhanden sein und den Spezifikationen laut TS 119 612 Abschnitt 5.3.6 entsprechen. Dabei muss der Systemname wie folgt lauten:

„EN_name_value" = „Vertrauensliste mit Angaben zu den qualifizierten Vertrauensdiensteanbietern, die vom ausstellenden Mitgliedstaat beaufsichtigt werden, sowie Angaben zu den von ihnen angebotenen qualifizierten Vertrauensdiensten gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG."

URI zu den Systeminformationen (Abschnitt 5.3.7)

Dieses Feld muss vorhanden sein und den Spezifikationen gemäß TS 119 612 Abschnitt 5.3.7 entsprechen. Dabei müssen die „angemessenen Informationen" über das System mindestens Folgendes enthalten:

a) Für alle Mitgliedstaaten identische einleitende Informationen über den Umfang und Hintergrund der Vertrauensliste, das zugrunde liegende Aufsichtssystem und gegebenenfalls die nationale Genehmigungssysteme (z. B. Akkreditierungssysteme). Zu verwenden ist der nachstehende gemeinsame Text, in dem die Zeichenkette „*[Name des betreffenden Mitgliedstaats]*" durch den Namen des betreffenden Mitgliedstaats ersetzt werden muss:

> „Bei der vorliegenden Liste handelt es sich um die Vertrauensliste mit Angaben zu den qualifizierten Vertrauensdiensteanbietern, die von *[Name des jeweiligen Mitgliedstaats]* beaufsichtigt werden, sowie mit Angaben zu den von ihnen angebotenen qualifizierten Vertrauensdiensten gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

Die grenzüberschreitende Verwendung elektronischer Signaturen wurde durch die Entscheidung 2009/767/EG der Kommission vom 16. Oktober 2009 erleichtert, mit der die Mitgliedstaaten erstmals zur Aufstellung, Führung und Veröffentlichung von Vertrauenslisten mit Angaben zu Zertifizierungsdiensteanbietern verpflichtet wurden, die gemäß der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen öffentlich qualifizierte Zertifikate ausstellen und von den Mitgliedstaaten beaufsichtigt/akkreditiert werden. Mit dieser Vertrauensliste wird die im Wege der Entscheidung 2009/767/EG aufgestellte Vertrauensliste fortgeschrieben."

Vertrauenslisten sind für die Vertrauensbildung unter den Betreibern der elektronischen Kommunikation von großer Bedeutung, da sie es den Nutzern ermöglichen, den qualifizierten Status sowie die Chronik des Status eines Vertrauensdiensteanbieters und seiner Dienste abzufragen.

Die Vertrauenslisten der Mitgliedstaaten enthalten mindestens die in den Artikeln 1 und 2 des Durchführungsbeschlusses (EU) 2015/1505 der Kommission genannten Angaben.

Die Mitgliedstaaten können in die Vertrauenslisten auch Angaben über nichtqualifizierte Vertrauensdiensteanbieter samt den von diesen bereitgestellten nichtqualifizierten Vertrauensdiensten aufnehmen. Dabei ist jedoch deutlich anzugeben, dass diese nicht gemäß der Verordnung (EU) Nr. 910/2014 qualifiziert sind.

Die Mitgliedstaaten können in die Vertrauenslisten auch Informationen über auf nationaler Ebene festgelegte Vertrauensdienste aufnehmen, die sich von den Vertrauensdiensten nach Artikel 3 Absatz 16 der Verordnung (EU) Nr. 910/2014 unterscheiden. Dabei ist jedoch deutlich anzugeben, dass diese nicht gemäß der Verordnung (EU) Nr. 910/2014 qualifiziert sind.

b) Besondere Informationen über das zugrunde liegende Aufsichtssystem und gegebenenfalls nationale Genehmigungssysteme (z. B. Akkreditierungssysteme), insbesondere ([1]):

(1) Angaben zum nationalen Aufsichtssystem, das für qualifizierte und nicht qualifizierte Vertrauensdiensteanbieter und die von ihnen angebotenen qualifizierten und nicht qualifizierten Vertrauensdienste gemäß der Verordnung (EU) Nr. 910/2014 gilt;

(2) gegebenenfalls Angaben zu den nationalen freiwilligen Akkreditierungssystemen für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate gemäß der Richtlinie 1999/93/EG ausstellen.

Diese besonderen Angaben müssen für jedes der obengenannten zugrunde liegenden Systeme zumindest Folgendes enthalten:

(1) allgemeine Beschreibung;

(2) Angaben zu dem im Rahmen des nationalen Aufsichtssystems angewandten Verfahren und gegebenenfalls dem Vorgehen im Rahmen eines nationalen Genehmigungsverfahrens;

(3) Angaben zu den Kriterien, nach denen Vertrauensdiensteanbieter beaufsichtigt werden oder gegebenenfalls eine Genehmigung erhalten;

(4) Angaben zu den Kriterien und Vorschriften für die Auswahl von Aufsichts- und Auditpersonal und zu den Methoden, die dieses zur Prüfung von Vertrauensdiensteanbietern und den von ihnen angebotenen Vertrauensdiensten anwendet;

(5) gegebenenfalls weitere Kontaktdaten und allgemeine Informationen über den Betrieb des Systems.

Systemart/Gemeinschaft/Regeln (Abschnitt 5.3.9)

Dieses Feld muss vorhanden sein und den Spezifikationen laut TS 119 612 Abschnitt 5.3.9 entsprechen.

Es enthält ausschließlich URIs in britischem Englisch.

([1]) Diese Informationen sind für die vertrauenden Beteiligten von entscheidender Bedeutung für die Beurteilung des Qualitäts- und Sicherheitsgrads solcher Systeme. Diese Informationen werden auf der Ebene der Vertrauensliste bereitgestellt, und zwar durch die Verwendung der vorhandenen Felder „URI zur Systeminformation" (Abschnitt 5.3.7 — von den Mitgliedstaaten bereitgestellte Informationen), „Systemart/Gemeinschaft/Regeln" (Abschnitt 5.3.9 — Verwendung eines allen Mitgliedstaaten gemeinsamen Texts) und „Vertrauenslistenrichtlinien/rechtlicher Hinweis" (Abschnitt 5.3.11 — ein allen Mitgliedstaaten einheitlicher Text, der die Möglichkeit bietet, einen länderspezifischen Text bzw. Verweise hinzuzufügen). Zusatzinformationen über solche Systeme für nicht qualifizierte Vertrauensdienste und auf nationaler Ebene festgelegte (qualifizierte) Vertrauensdienste können gegebenenfalls auf der Dienstebene und soweit erforderlich (z. B. zur Unterscheidung zwischen verschiedenen Qualitäts-/Sicherheitsstufen) durch die Verwendung der „URI zur Definition des Systemdienstes" (Abschnitt 5.5.6) zur Verfügung gestellt werden.

Es enthält mindestens zwei URIs:

(1) Einen allen Vertrauenslisten der Mitgliedstaaten gemeinsamen URI, der zu einem deskriptiven Text führt, der für alle Vertrauenslisten gilt:

URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

Deskriptiver Text:

„Participation in a scheme

Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in 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.

The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

Policy/rules for the assessment of the listed services

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision 2015/1505.

The trusted lists include both current and historical information about the status of listed trust services.

Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

Interpretation of the Trusted List

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows:

The ‚qualified' status of a trust service is indicated by the combination of the ‚Service type identifier' (‚Sti') value in a service entry and the status according to the ‚Service current status' field value as from the date indicated in the ‚Current status starting date and time'. Historical information about such a qualified status is similarly provided when applicable.

Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

A ‚CA/QC' ‚Service type identifier' (‚Sti') entry (possibly further qualified as being a ‚RootCA-QC' through the use of the appropriate ‚Service information extension' (‚Sie') additionalServiceInformation Extension)

— indicates that any end-entity certificate issued by or under the CA represented by the ‚Service digital identifier' (‚Sdi') CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:

  — the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),

  — the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. ‚undersupervision', ‚supervisionincessation', ‚accredited' or ‚granted') for that entry.

— **and IF** ‚Sie' ‚Qualifications Extension' information is present, then in addition to the above default rule, those certificates that are identified through the use of ‚Sie' ‚Qualifications Extension' information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the ‚SSCD support' and/or ‚Legal person as subject' (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific ‚Key usage' pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension usw.). These qualifiers are part of the following set of ‚Qualifiers' used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:

  — to indicate the qualified certificate nature:

    — ‚QCStatement' meaning the identified certificate(s) is(are) qualified under Directive 1999/93/EC;

    — ‚QCForESig' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation (EU) No 910/2014;

    — ‚QCForESeal' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation (EU) No 910/2014;

    — ‚QCForWSA' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation (EU) No 910/2014.

  — to indicate that the certificate is not to be considered as qualified:

    — ‚NotQualified' meaning the identified certificate(s) is(are) not to be considered as qualified; and/or

  — to indicate the nature of the SSCD support:

    — ‚QCWithSSCD' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or

    — ‚QCNoSSCD' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or

    — ‚QCSSCDStatusAsInCert' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD;

  — to indicate the nature of the QSCD support:

    — ‚QCWithQSCD' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

    — ‚QCNoQSCD' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or

    — ‚QCQSCDStatusAsInCert' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;

    — ‚QCQSCDManagedOnBehalf' indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; and/or

— to indicate issuance to Legal Person:

— ‚QCForLegalPerson' meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under Directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

— if none of the id-etsi-qcs 1 statement, QCP OID or QCP+ OID information is included in an end-entity certificate, and

— if no ‚Sie' ‚Qualifications Extension' information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a ‚QCStatement' qualifier, or

— an ‚Sie' ‚Qualifications Extension' information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a ‚NotQualified' qualifier,

then the certificate is not to be considered as qualified.

‚Service digital identifiers' are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other ‚Sti' type entry is that, for that ‚Sti' identified service type, the listed service named according to the ‚Service name' field value and uniquely identified by the ‚Service digital identity' field value has the current qualified or approval status according to the ‚Service current status' field value as from the date indicated in the ‚Current status starting date and time'.

Specific interpretation rules for any additional information with regard to a listed service (e.g. ‚Service information extensions' field) may be found, when applicable, in the Member State specific URI as part of the present ‚Scheme type/community/rules' field.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists."

(2) Ein der Vertrauensliste eines Mitgliedstaats jeweils eigener URI, der auf einen deskriptiven Text verweist, der für diese Vertrauensliste des Mitgliedstaats gilt:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC; dabei ist CC der im Feld „Systemgebiet" (Abschnitt 5.3.10) verwendete ISO 3166-1 [1]-Alpha-2-Ländercode.

— Angaben dazu, wo Nutzer länderspezifische Richtlinien/Vorschriften des betreffenden Mitgliedstaats finden können, anhand derer die in die Liste aufgenommenen Vertrauensdienste gemäß dem Aufsichtssystem und gegebenenfalls dem Genehmigungssystem des Mitgliedstaats bewertet werden.

— Angaben dazu, wo Nutzer eine länderspezifische Anleitung des betreffenden Mitgliedstaats zur Verwendung und Auslegung des Inhalts der Vertrauensliste im Hinblick auf die aufgeführten nichtqualifizierten Vertrauensdienste und/oder auf nationaler Ebene definierten Vertrauensdienste finden können. Darin kann in Bezug auf Zertifizierungsdiensteanbieter, die keine qualifizierten Zertifikate ausstellen, auf eine potenzielle Granularität im einzelstaatlichen Genehmigungssystem hingewiesen und erläutert werden, wie die Felder „URI zur Definition des Systemdienstes" (Abschnitt 5.5.6) und „Dienstinformations-Endung" (Abschnitt 5.5.9) zu diesem Zweck verwendet werden.

Die Mitgliedstaaten KÖNNEN den obigen länderspezifischen URI erweitern, indem sie zusätzliche URIs definieren und verwenden (d. h. URIs, die auf diesem hierarchischen spezifischen URI basieren).

Vertrauenslistenrichtlinien/Rechtlicher Hinweis (Abschnitt 5.3.11)

Dieses Feld muss vorhanden sein und den Spezifikationen laut TS 119 612 Abschnitt 5.3.11 entsprechen. Es muss die Richtlinien bzw. einen rechtlichen Hinweis zum Rechtsstatus des Systems bzw. die vom System in der Rechtsordnung, der es angehört, erfüllten rechtlichen Anforderungen und/oder alle Beschränkungen und Bedingungen enthalten, unter denen die Vertrauensliste veröffentlicht und gepflegt wird. Dabei muss es sich um eine Abfolge von mehrsprachigen

[1] ISO 3166-1:2006: Codes für die Namen von Ländern und deren Untereinheiten — Teil 1: Codes für Ländernamen.

Zeichenketten (siehe Abschnitt 5.1.4) handeln, die den tatsächlichen Text der Richtlinie oder des Hinweises nach der folgenden Struktur — obligatorisch in britischem Englisch und optional in einer oder mehreren weiteren Sprache der Mitgliedstaaten — enthält und sich zusammensetzt aus:

(1) einem obligatorischen, allen Vertrauenslisten der Mitgliedstaaten gemeinsamen Teil, in dem auf den geltenden Rechtsrahmen hingewiesen wird und dessen englische Fassung wie folgt lautet:

> The applicable legal framework for the present trusted list is 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;

der Fassung des Texts in der/den Sprache(n) des Mitgliedstaats:

> Der für diese Vertrauenslisten geltende Rechtsrahmen ist die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG;

(2) einem zweiten optionalen Teil für jede einzelne Vertrauensliste, in dem auf besondere nationale Rechtsvorschriften hingewiesen wird.

Aktueller Dienststatus (Abschnitt 5.5.4)

Dieses Feld muss vorhanden sein und den Spezifikationen laut TS 119 612 Abschnitt 5.5.4 entsprechen.

Die Migration des vor dem Inkrafttreten der Verordnung (EU) Nr. 910/2014 (d. h. dem 30. Juni 2016) im Feld „Aktueller Dienststatus“ enthaltenen Wertes für die in den Vertrauenslisten der EU-Mitgliedstaaten aufgeführten Dienste erfolgt gemäß dem Anhang J der Spezifikationen TS 119 612 des ETSI an dem Tag, an dem die Verordnung anwendbar wird (d. h. am 1. Juli 2016).

KAPITEL III

KONTINUITÄT DER VERTRAUENSLISTEN

Zertifikate, die der Kommission gemäß Artikel 4 Absatz 2 dieses Beschlusses zu notifizieren sind, müssen die Anforderungen aus ETSI TS 119 612 Abschnitt 5.7.1 erfüllen und in einer Weise ausgestellt werden, dass

— ihr letzter Gültigkeitstag („Not After“) um mindestens drei Monate auseinander liegt,

— sie anhand neuer Schlüsselpaare generiert werden. Bereits verwendete Schlüsselpaare dürfen nicht neu zertifiziert werden.

Bei Ablauf eines Public-Key-Zertifikats, das zur Validierung der Signatur oder des Siegels der Vertrauensliste verwendet werden kann, die der Kommission notifiziert und in deren zentralen Zeigerlisten veröffentlicht wurde, müssen die Mitgliedstaaten

— im Falle, dass eine aktuell veröffentlichte Vertrauensliste mit einem privaten Schlüssel signiert oder besiegelt wurde, dessen Public-Key-Zertifikat abgelaufen ist, unverzüglich eine neue, mit einem privaten Schlüssel, dessen Public-Key-Zertifikat nicht abgelaufen ist, signierte oder besiegelte Vertrauensliste erstellen;

— erforderlichenfalls neue Schlüsselpaare erstellen, die für die Signatur oder Besiegelung der Vertrauensliste verwendet werden können, und die dazugehörigen Public-Key-Zertifikate erstellen;

— der Kommission unverzüglich die neue Liste der zu den privaten Schlüsseln gehörenden Public-Key-Zertifikate übermitteln, welche für die Signatur oder Besiegelung der Vertrauensliste verwendet werden können.

Bei Kompromittierung oder Außerkraftsetzung eines privaten Schlüssels, der zu einem Public-Key-Zertifikat gehört, das zur Validierung der Signatur oder des Siegels der Vertrauensliste verwendet werden kann und der Kommission notifiziert und in ihrer zentralen Zeigerliste veröffentlicht wurde, müssen die Mitgliedstaaten

— unverzüglich eine neue, mit einem nicht kompromittierten privaten Schlüssel signierte oder besiegelte Vertrauensliste ausstellen, sofern die veröffentlichte Liste mit einem kompromittierten oder außer Kraft gesetzten privaten Schlüssel signiert oder besiegelt wurde;

— erforderlichenfalls neue Schlüsselpaare erstellen, die für die Signatur oder Besiegelung der Vertrauensliste verwendet werden können, und die dazugehörigen Public-Key-Zertifikate erstellen;

— der Kommission unverzüglich die neue Liste der zu den privaten Schlüsseln gehörenden Public-Key-Zertifikate übermitteln, welche für die Signatur oder Besiegelung der Vertrauensliste verwendet werden können.

Bei Kompromittierung oder Außerkraftsetzung aller privaten Schlüssel, die zu den Public-Key-Zertifikaten gehören, welche zur Validierung der Signatur der Vertrauensliste verwendet werden konnten und der Kommission notifiziert und in deren zentralen Zeigerlisten veröffentlicht wurden, müssen die Mitgliedstaaten

— neue Schlüsselpaare erstellen, die für die Signatur oder Besiegelung der Vertrauensliste verwendet werden können, und die dazugehörigen Public-Key-Zertifikate generieren;

— unverzüglich eine neue, mit einem dieser neuen privaten Schlüssel signierte oder besiegelte Vertrauensliste erstellen und das das dazugehörige Public-Key-Zertifikat übermitteln;

— der Kommission unverzüglich die neue Liste der zu den privaten Schlüsseln gehörenden Public-Key-Zertifikate übermitteln, welche für die Signatur oder Besiegelung der Vertrauensliste verwendet werden können.

KAPITEL IV

SPEZIFIKATIONEN FÜR DIE MENSCHENLESBARE FASSUNG DER VERTRAUENSLISTE

Wird eine menschenlesbare Fassung der Vertrauensliste erstellt und veröffentlicht, muss die Bereitstellung im PDF-Format gemäß ISO 32000 ([1]) erfolgen; die Formatierung muss dem Profil PDF/A (ISO 19005 ([2])) entsprechen.

Der Inhalt der auf PDF/A beruhenden menschenlesbaren Fassung der Vertrauensliste muss folgende Anforderungen erfüllen:

— Die Struktur der menschenlesbaren Fassung muss dem in TS 119 612 beschriebenen logischen Modell entsprechen.

— Jedes vorhandene Feld muss sichtbar sein und Folgendes enthalten:

  — die Bezeichnung des Felds (z. B. „*Dienstart-Identifikator*“);

  — den Wert des Felds (z. B. „http://uri.etsi.org/TrstSvc/Svctype/CA/QC“);

  — gegebenenfalls die Bedeutung (Beschreibung) des Feldwertes (z. B. „*Ein Zertifikatsgenerierungsdienst, mit dem qualifizierte Zertifikate anhand der Identität und anderer, von den zuständigen Registrierungsstellen geprüfter Merkmale erstellt und signiert werden.*“);

  — gegebenenfalls mehrere Fassungen in natürlichen Sprachen, wie in der Vertrauensliste vorgesehen.

— Die menschenlesbare Fassung muss mindestens die nachstehenden Felder und dazugehörigen Werte der digitalen Zertifikate ([3]) enthalten, sofern sie sich im Feld „Digitale Dienstidentität“ befinden:

  — Version,

  — Seriennummer des Zertifikats,

  — Signaturalgorithmus,

  — Aussteller — alle relevanten eindeutigen Namensfelder,

  — Gültigkeitszeitraum,

  — Inhaber — alle relevanten eindeutigen Namensfelder,

([1]) ISO 32000-1/2008: Dokumenten-Management — Portables Dokumenten Format — Teil 1: PDF 1.7
([2]) ISO 19005-2:2011: Dokumenten-Management. Elektronisches Dokumenten-Dateiformat für die Langzeitarchivierung — Teil 2: Anwendung der ISO 32000-1 (PDF/A-2)
([3]) Empfehlung ITU-T X.509 | ISO/IEC 9594-8: Informationstechnik — Kommunikation offener Systeme — Verzeichnisdienst: Rahmenrichtlinien für „Public Key“ und Attribut-Zertifikat (siehe http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509)

— öffentlicher Schlüssel,

— Ausstellerschlüssel-Identifikator,

— Inhaberschlüssel-Identifikator,

— Schlüsselverwendung,

— erweiterte Schlüsselverwendung,

— Zertifikatrichtlinien — alle Richtlinien-Identifikatoren und Richtlinien-Qualifikatoren,

— Richtlinienzuordnungen,

— alternativer Inhabername,

— Inhaberverzeichnisattribute,

— grundlegende Beschränkungen,

— Richtlinienbeschränkungen,

— CRL-Verteilungspunkte ([1]),

— Zugang zu Daten über zuständige Stellen,

— Zugang zu Daten über Inhaber,

— Erklärungen zu qualifizierten Zertifikaten ([2]),

— Hash-Algorithmus,

— Hashwert des Zertifikats.

— Die menschenlesbare Fassung muss leicht auszudrucken sein.

— Die menschenlesbare Fassung muss vom Systembetreiber mit der in den Artikeln 1 und 3 des Durchführungsbeschlusses (EU) 2015/1505 beschriebenen fortgeschrittenen PDF-Signatur unterzeichnet oder besiegelt werden.

([1]) RFC 5280: Internet X.509 PKI Certificate and CRL Profile.
([2]) RFC 3739: Internet X.509 PKI: Qualified Certificates Profile.

ANHANG II

MUSTER FÜR DIE MELDUNGEN DER MITGLIEDSTAATEN

Die von den Mitgliedstaaten nach Artikel 4 Absatz 1 dieses Beschlusses zu übermittelnden Angaben umfassen folgende Daten sowie deren etwaige Änderungen:

(1) Mitgliedstaat, unter Verwendung der ISO 3166-1 ([1])-Alpha-2-Ländercodes mit den folgenden Ausnahmen:

a) der Ländercode für das Vereinigte Königreich lautet „UK“,

b) der Ländercode für Griechenland lautet „EL“;

(2) die Stelle(n), die für die Aufstellung, Führung und Veröffentlichung der Vertrauenslisten in für die automatisierte Verarbeitung geeigneter sowie in menschenlesbarer Fassung zuständig ist (sind):

a) Name des Systembetreibers: Die Angaben müssen in allen in der Vertrauensliste verwendeten Sprachen mit dem Wert „Name des Systembetreibers“ *(Scheme operator name)* in der Vertrauensliste identisch sein (auch in Groß- und Kleinschreibung);

b) fakultative Angaben für den internen Gebrauch der Kommissionsdienststellen nur falls die zuständige Stelle kontaktiert werden muss (diese Angaben werden in der von der Europäischen Kommission geführten Liste der Vertrauenslisten nicht veröffentlicht):

— Anschrift des Systembetreibers;

— Kontaktdaten der zuständigen Person(en) (Name, Telefon, E-Mail-Adresse);

(3) der Ort, an dem die für die automatisierte Verarbeitung geeignete Fassung der Vertrauensliste veröffentlicht wird *(Ort, an dem die derzeitige Vertrauensliste veröffentlicht wird)*;

(4) gegebenenfalls der Ort, an dem die menschenlesbare Fassung der Vertrauensliste veröffentlicht wird *(Ort, an dem die derzeitige Vertrauensliste veröffentlicht wird)*. Wird eine menschenlesbare Form der Vertrauensliste nicht mehr veröffentlicht, ist ein entsprechender Hinweis anzubringen;

(5) die Public-Key-Zertifikate, die den privaten Schlüsseln entsprechen, die zur elektronischen Unterzeichnung oder Besiegelung der zur automatisierten Verarbeitung geeigneten Fassung und der menschenlesbaren Fassung der Vertrauenslisten verwendet werden können: Diese Zertifikate werden als DER-Zertifikate im Base64-kodierten PEM-Format bereitgestellt. Bei Änderungsmeldungen zusätzliche Informationen, wenn ein neues Zertifikat ein bestimmtes Zertifikat auf der Liste der Kommission ersetzen soll und wenn ein gemeldetes Zertifikat zu dem/den vorhandenen ohne Ersetzung hinzugefügt werden soll;

(6) Meldezeitpunkt der unter Punkt 1 bis 5 gemeldeten Daten.

Daten, die nach Nummer 1, Nummer 2 Buchstabe a oder den Nummern 3, 4 und 5 gemeldet werden, werden in die von der Europäischen Kommission geführte Liste der Vertrauenslisten anstelle der zuvor für diese Liste gemeldeten Angaben aufgenommen.

([1]) ISO 3166-1: „Codes für die Namen von Ländern und deren Untereinheiten — Teil 1: Ländercodes“.