COMMISSION IMPLEMENTING DECISION (EU) 2015/1505

of 8 September 2015

laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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 [1], and in particular Article 22(5) thereof,

Whereas:

(1) Trusted lists are essential for the building of trust among market operators as they indicate the status of the service provider at the moment of supervision.

(2) The cross-border use of electronic signatures has been facilitated through Commission Decision 2009/767/EC [2] which has set the obligation for Member States to establish, maintain and publish trusted lists including information related to certification service providers issuing qualified certificates to the public in accordance with Directive 1999/93/EC of the European Parliament and of the Council [3] and which are supervised and accredited by the Member States.

(3) Article 22 of Regulation (EC) No 910/2014/EU provides the obligation for Member States to establish, maintain and publish trusted lists, in a secured manner, electronically signed or sealed in a form suitable for automated processing and to notify to the Commission the bodies responsible for establishing the national trusted lists.

(4) A trust service provider and the trust services it provides should be considered qualified when the qualified status is associated to the provider in the trusted list. In order to ensure that other obligations stemming from Regulation (EU) No 910/2014, in particular those set in Articles 27 and 37, may be easily fulfilled by the service providers at a distance and by electronic means and in order to meet the legitimate expectations of other certification-service-providers who are not issuing qualified certificates but provide services related to electronic signatures under Directive 1999/93/EC and are listed by 30 June 2016, it should be possible for Member States to add trust services other than the qualified ones in the trusted lists, on a voluntary basis, at national level, provided that it is clearly indicated that they are not qualified according to Regulation (EU) No 910/2014.

(5) In line with recital 25 of Regulation (EU) No 910/2014, Member States may add other types of nationally defined trust services than those defined under Article 3(16) of Regulation (EU) No 910/2014, provided that it is clearly indicated that they are not qualified according to Regulation (EU) No 910/2014.

(6) The measures provided for in this Decision are in accordance with the opinion of the Committee established by Article 48 of Regulation (EU) No 910/2014,

HAS ADOPTED THIS DECISION:

Article 1

Member States shall establish, publish and maintain trusted lists including information on the qualified trust service providers which they supervise, as well as information on the qualified trust services provided by them. Those lists shall comply with the technical specifications set out in Annex I.

[1] OJ L 257, 28.8.2014, p. 73.

[2] 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).

[3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L 13, 19.1.2000, p. 12).

Article 2

Member States may include in the trusted lists information on non-qualified trust service providers, together with information related to the non-qualified trust services provided by them. The list shall clearly indicate which trust service providers and the trust services provided by them are not qualified.

Article 3

(1) Pursuant to Article 22(2) of Regulation (EU) No 910/2014, Member States shall sign or seal electronically the form suitable for automated processing of their trusted list in accordance with the technical specifications set out in Annex I.

(2) If a Member State publishes electronically a human readable form of the trusted list, it shall ensure that this form of the trusted list contains the same data as the form suitable for automated processing and it shall sign or seal it electronically in accordance with the technical specifications set out in Annex I.

Article 4

(1) Member States shall notify to the Commission the information referred to in Article 22(3) of Regulation (EU) No 910/2014 using the template in Annex II.

(2) The information referred to in paragraph 1 shall include two or more scheme operator public key certificates, with shifted validity periods of at least 3 months, which correspond to the private keys that can be used to sign or seal electronically the form suitable for automated processing of the trusted list and the human readable form when published.

(3) Pursuant to Article 22(4) of Regulation (EU) No 910/2014, the Commission shall make available to the public, through a secure channel to an authenticated web server, the information referred to in paragraphs 1 and 2, as notified by Member States, in a signed or sealed form suitable for automated processing.

(4) The Commission may make available to the public, through a secure channel to an authenticated web server, the information referred to in paragraphs 1 and 2, as notified by Member States, in a signed or sealed human readable form.

Article 5

This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Decision shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 8 September 2015.

For the Commission
The President
Jean-Claude JUNCKER

ANNEX I

TECHNICAL SPECIFICATIONS FOR A COMMON TEMPLATE FOR TRUSTED LISTS

CHAPTER I

GENERAL REQUIREMENTS

The trusted lists shall include both current and all historical information, dating from the inclusion of a trust service provider in the Trusted Lists, about the status of listed trust services.

The terms 'approved', 'accredited' and/or 'supervised' in the present specifications also cover the national approval schemes but additional information on the nature of any such national schemes will be provided by Member States in their trusted list, including clarification on the possible differences with the supervision schemes applied to qualified trust service providers and the qualified trust services they provide.

The information provided in the trusted list is primarily aimed at supporting the validation of qualified trust service tokens, i.e. physical or binary (logical) objects generated or issued as a result of the use of a qualified trust service, e.g. namely qualified electronic signatures/seals, advanced electronic signatures/seals supported by a qualified certificate, qualified time-stamps, qualified electronic delivery evidences, etc.

CHAPTER II

DETAILED SPECIFICATIONS FOR THE COMMON TEMPLATE FOR THE TRUSTED LISTS

The present specifications rely on the specifications and requirements set in ETSI TS 119 612 v2.1.1 (here after referred to as ETSI TS 119 612).

When no specific requirement is set in the present specifications, requirements from ETSI TS 119 612 clauses 5 and 6 shall apply in their entirety. When specific requirements are set in the present specifications, they shall prevail over the corresponding requirements from ETSI TS 119 612. In case of discrepancies between the present specifications and specifications from ETSI TS 119 612, the present specifications shall prevail.

Scheme name (clause 5.3.6)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.6 where the following name shall be used for the scheme:

'EN_name_value' = 'Trusted list including information related to the qualified trust service providers which are supervised by the issuing Member State, 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.'

Scheme information URI (clause 5.3.7)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.7 where the 'appropriate information about the scheme' shall include as a minimum:

(a) Introductory information common to all Member States with regard to the scope and context of the trusted list, the underlying supervision scheme and when applicable national approval (e.g. accreditation) scheme(s). The common text to be used is the text below, in which the character string '(*name of the relevant Member State*)' shall be replaced by the name of the relevant Member State:

> 'The present list is the trusted list including information related to the qualified trust service providers which are supervised by (*name of the relevant Member State*), 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 cross-border use of electronic signatures has been facilitated through Commission Decision 2009/767/EC of 16 October 2009 which has set the obligation for Member States to establish, maintain and publish trusted lists with information related to certification service providers issuing qualified certificates to the public in accordance with Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and which are supervised/accredited by the Member States. The present trusted list is the continuation of the trusted list established with Decision 2009/767/EC.'

Trusted lists are essential elements in building trust among electronic market operators by allowing users to determine the qualified status and the status history of trust service providers and their services.

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

Member States may include in the trusted lists information on non-qualified trust service providers, together with information related to the non-qualified trust services provided by them. It shall be clearly indicated that they are not qualified according to Regulation (EU) No 910/2014.

Member States may include in the trusted lists information on nationally defined trust services of other types than those defined under Article 3(16) of Regulation (EU) No 910/2014. It shall be clearly indicated that they are not qualified according to Regulation (EU) No 910/2014.

(b) Specific information on the underlying supervision scheme and when applicable national approval (e.g. accreditation) scheme(s), in particular [1]:

(1) Information on the national supervision system applicable to qualified and non-qualified trust service providers and the qualified and non-qualified trust services they provide as regulated by Regulation (EU) No 910/2014;

(2) Information, where applicable, on the national voluntary accreditation schemes applicable to certification-service-providers having issued qualified certificates under Directive 1999/93/EC;

This specific information shall include, at least, for each underlying scheme listed above:

(1) General description;

(2) Information about the process followed for the national supervision system and, when applicable, for the approval under a national approval scheme.

(3) Information about the criteria against which trust service providers are supervised or, where applicable, approved.

(4) Information about the criteria and rules used to select supervisors/auditors and defining how they assess trust service providers and the trust services provided by them.

(5) When applicable, other contact and general information that applies to the scheme operation.

Scheme type/community/rules (clause 5.3.9)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.9.

It shall only include UK English URIs.

[1] Those sets of information are of critical importance for relying parties to assess the quality and security level of such systems. Those sets of information shall be provided at Trusted List level through the use of the present 'Scheme information URI' (clause 5.3.7 — information being provided by Member State), 'Scheme type/community/rules' (clause 5.3.9 — through the use of a text common to all Member States) and 'TSL policy/legal notice' (clause 5.3.11 — a text common to all Member States, together with the ability for each Member State to add Member State specific text/references). Additional information on such systems for non-qualified trust services and nationally defined (qualified) trust services may be provided at service level when applicable and required (e.g. to distinguish between several quality/security levels) through the use of 'Scheme service definition URI' (clause 5.5.6).

It shall include at least two URIs:

(1) A URI common to all Member States' Trusted Lists pointing towards a descriptive text that shall be applicable to all Trusted Lists, as follows:

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

Descriptive 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 (EU) 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, etc.). 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) A URI specific to each Member State's trusted list pointing towards a descriptive text that shall be applicable to this Member State trusted list:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC where CC = the ISO 3166-1 ([1]) alpha-2 Country Code used in the 'Scheme territory' field (clause 5.3.10)

— Where users can obtain the referenced Member State's specific policy/rules against which trust services included in the list are assessed, in compliance with the Member State's supervisory regime and where applicable, approval scheme.

— Where users can obtain a referenced Member State's specific description about how to use and interpret the content of the trusted list with regard to the listed non-qualified trust services and/or to nationally defined trust services. This may be used to indicate a potential granularity in the national approval system related to CSPs not issuing QCs and how the 'Scheme service definition URI' (clause 5.5.6) and the 'Service information extension' field (clause 5.5.9) are used for this purpose.

Member States MAY define and use additional URIs expanding the above Member State specific URI (i.e. URIs defined from this hierarchical specific URI).

TSL policy/legal notice (clause 5.3.11)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.3.11 where the policy/legal notice concerning the legal status of the scheme or legal requirements met by the scheme under the jurisdiction in which it is established and/or any constraints and conditions under which the trusted list is maintained and published

[1] ISO 3166-1:2006: 'Codes for the representation of names of countries and their subdivisions Part 1: Country codes'.

shall be a sequence of multilingual character strings (see clause 5.1.4) providing, in UK English as the mandatory language and optionally in one or more national languages, the actual text of any such policy or notice built as follows:

(1) A first mandatory part, common to all Member States' Trusted Lists indicating the applicable legal framework, and whose English version is the following:

> 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.

Text in a Member State's national language(s):

> 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.

(2) A second, optional part, specific to each trusted list, indicating references to specific applicable national legal frameworks

Service current status (clause 5.5.4)

This field shall be present and shall comply with the specifications from TS 119 612 clause 5.5.4.

The migration of the 'Service current status' value of services listed in EUMS trusted list as of the day before the date Regulation (EU) No 910/2014 applies (i.e. 30 June 2016) shall be executed on the day the Regulation applies (i.e. 1 July 2016) as specified in Annex J to ETSI TS 119 612.

CHAPTER III

CONTINUITY OF TRUSTED LISTS

Certificates to be notified to the Commission in accordance with Article 4(2) of this Decision shall meet the requirements of clause 5.7.1 from ETSI TS 119 612 and shall be issued in such a way that they:

— have at least a three months difference in their final date of validity ('Not After'),

— are created on new key pairs. Previously used key pairs must not be re-certified.

In case of expiry of one of the public key certificates that could be used to validate the trusted list's signature or seal that has been notified to the Commission and that is published in the Commission's central list of pointers, Member States shall:

— in case the currently published trusted list was signed or sealed with a private key whose public key certificate is expired, re-issue, without any delay, a new trusted list signed or sealed with a private key whose notified public key certificate is not expired;

— when required, generate new key pairs that could be used to sign or seal the trusted list and undertake the generation of their corresponding public key certificates;

— promptly notify to the Commission the new list of public key certificates corresponding to the private keys that could be used to sign or seal the trusted list.

In case of a compromise or decommissioning of one of the private keys corresponding to one of the public key certificates that could be used to validate the trusted list's signature or seal, that has been notified to the Commission and that is published in the Commission's central list of pointers, Member States shall:

— re-issue, without any delay, a new trusted list signed or sealed with a non-compromised private key in cases where the published trusted list was signed or sealed with a compromised or decommissioned private key;

— when required, generate new key pairs that could be used to sign or seal the trusted list and undertake the generation of their corresponding public key certificates;

— promptly notify to the Commission the new list of public key certificates corresponding to the private keys that could be used to sign or seal the trusted list.

In case of compromise or decommissioning of all the private keys corresponding to the public key certificates that could be used to validate the trusted list's signature, that have been notified to the Commission and that are published in the Commission's central list of pointers, Member States shall:

— generate new key pairs that could be used to sign or seal the trusted list and undertake the generation of their corresponding public key certificates;

— re-issue, without any delay, a new trusted list signed or sealed with one of those new private keys and whose corresponding public key certificate is to be notified;

— promptly notify to the Commission the new list of public key certificates corresponding to the private keys that could be used to sign or seal the trusted list.

CHAPTER IV

SPECIFICATIONS FOR THE HUMAN READABLE FORM OF THE TRUSTED LIST

When a human readable form of the trusted list is established and published, it shall be provided in the form of a Portable Document Format (PDF) document according to ISO 32000 [1] that shall be formatted according to the profile PDF/A (ISO 19005 [2]).

The content of the PDF/A based human readable form of the trusted list shall comply with the following requirements:

— The structure of the human readable form shall reflect the logical model described in TS 119 612;

— Every present field shall be displayed and provide:

  — The title of the field (e.g. '*Service type identifier*');

  — The value of the field (e.g. 'http://uri.etsi.org/TrstSvc/Svctype/CA/QC}');

  — The meaning (description) of the value of the field, when applicable (e.g. '*A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.*');

  — Multiple natural language versions as provided in the trusted list, when applicable.

— The following fields and corresponding values of the digital certificates [3], if present in the 'Service digital identity' field shall, as a minimum, be displayed in the human readable form:

  — Version

  — Certificate serial number

  — Signature algorithm

  — Issuer — all relevant distinguished name fields

  — Validity period

  — Subject — all relevant distinguished name fields

[1] ISO 32000-1:2008: Document management — Portable document format — Part 1: PDF 1.7

[2] ISO 19005-2:2011: Document management — Electronic document file format for long-term preservation — Part 2: Use of ISO 32000-1 (PDF/A-2)

[3] Recommendation ITU-T X.509 | ISO/IEC 9594-8: Information technology — Open systems interconnection — The Directory: Public-key and attribute certificate frameworks (see http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509)

  - Public key
  - Authority Key Identifier
  - Subject Key Identifier
  - Key Usage
  - Extended key usage
  - Certificate Policies — all policy identifiers and policy qualifiers
  - Policy mappings
  - Subject alternative name
  - Subject directory attributes
  - Basic constraints
  - Policy constraints
  - CRL Distribution Points [1]
  - Authority Information Access
  - Subject Information Access
  - Qualified Certificate Statements [2]
  - Hash algorithm
  - Hash value of certificate
- The human readable form shall be easily printable
- The human readable form shall be signed or sealed by the Scheme Operator according to PDF advanced signature specified in Articles 1 and 3 of the Commission Implementing Decision (EU) 2015/1505.

[1] RFC 5280: internet X.509 PKI Certificate and CRL Profile

[2] RFC 3739: internet X.509 PKI: Qualified Certificates Profile

ANNEX II

TEMPLATE FOR MEMBER STATES' NOTIFICATIONS

The information to be notified by Member States under Article 4(1) of the present Decision shall contain the following data and any changes thereto:

(1) Member State, using ISO 3166-1 [1] Alpha 2 codes with the following exceptions:

(a) The Country Code for United Kingdom shall be 'UK'.

(b) The Country Code for Greece shall be 'EL'.

(2) The body/bodies responsible for the establishment, maintenance and publication of the form suitable for automated processing and the human readable form of the trusted lists:

(a) Scheme operator name: the provided information must be identical — case sensitive — to the 'Scheme operator name' value present in the trusted list in as many languages as used in the trusted list.

(b) Optional information for internal Commission use only in cases where the relevant body needs to be contacted (the information will not be published in the EC compiled list of trusted lists):

— Address of the scheme operator;

— Contact details of the responsible person(s) (name, phone, e-mail address).

(3) The location where the form suitable for automated processing of the trusted list is published (*location where the current trusted list is published*).

(4) The location, when applicable, where the human readable trusted list is published (*location where the current trusted list is published*). In case a human readable trusted list is no longer published, an indication thereof.

(5) The public key certificates which correspond to the private keys that can be used to sign or seal electronically the form suitable for automated processing of the trusted list and human readable form of the trusted lists: those certificates shall be provided as Privacy Enhanced Mail Base64 encoded DER certificates. For a change notification, additional information in case a new certificate is to replace a specific certificate in the Commission's list and in case the notified certificate is to be added to the existing one(s) without any replacement.

(6) Date of submission of the data notified in points (1) to (5).

Data notified according to points (1), (2) (a), (3), (4) and (5) shall be included in the EC compiled list of trusted lists in replacement of the previously notified information included in that compiled list.

[1] ISO 3166-1: 'Codes for the representation of names of countries and their subdivisions — Part 1: Country codes'.