Commission Decision of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States (notified under document C(2010) 5063) (Text with EEA relevance) (2010/425/EU)

COMMISSION DECISION

of 28 July 2010

amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States

(notified under document C(2010) 5063)

(Text with EEA relevance)

(2010/425/EU)

THE EUROPEAN COMMISSION,

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

Having regard to Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market[1], and in particular Article 8(3) thereof,

Whereas:

(1)   The cross-border use of advanced electronic signatures supported by a qualified certificate and created with or without a secure signature creation device has been facilitated through 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[2] which obliges Member States to make available information necessary for the validation of these electronic signatures. In particular, Member States must make available in their so-called 'trusted lists' information on 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[3] and supervised/accredited by them and on the services they offer.

(2)   A number of practical tests with the European Telecommunications Standards Institute (ETSI) have been organised to allow Member States to check the conformity of their trusted lists with the specifications set out in the Annex to Decision 2009/767/EC. These tests have demonstrated that some technical changes are needed in the technical specifications in the Annex to Decision 2009/767/EC, to ensure functioning and interoperable trusted lists.

(3)   These tests also confirmed the need for Member States to make publicly available not only the human readable versions of their trusted lists as required by Decision 2009/767/ EC but also the machine processable forms of these. The manual use of the human readable form of the trusted lists can be relatively complex and time consuming when Member States have a high number of certification service providers. The publication of the machine processable forms of trusted lists will facilitate their use by allowing for their automated processing and thereby enhance their use in public electronic services.

(4)   In order to facilitate access to the national trusted lists, Member States should notify to the Commission information related to the location and protection of their trusted lists. This information should be made available by the Commission to other Member States in a secure manner.

(5)   The results of these practical tests on Member States' trusted lists should be taken into account in order to allow for an automated use of the lists and to facilitate access to them.

(6)   Decision 2009/767/EC should therefore be amended accordingly.

(7)   For the purpose of allowing Member States to carry out the required technical changes to their current trusted lists it is appropriate that this Decision applies as of 1 December 2010.

(8)   The measures provided for in this Decision are in accordance with the opinion of the Services Directive Committee,

HAS ADOPTED THIS DECISION:

Article 1

Amendments to Decision 2009/767/EC

Decision 2009/767/EC is amended as follows:

1.   Article 2 is amended as follows:

   (a)   paragraph 2 is replaced by the following:

      2.   Member States shall establish and publish both a human readable and a machine processable form of the trusted list in accordance with the specifications set out in the Annex.;

   (b)   the following paragraph 2a is inserted:

      2a.   Member States shall sign electronically the machine processable form of their trusted list and they shall, as a minimum, publish the human readable form of the trusted list through a secure channel in order to ensure its authenticity and integrity.;

   (c)   paragraph 3 is replaced by the following:

      3.   Member States shall notify to the Commission the following information:

    a   the body or bodies responsible for the establishment, maintenance and publication of the human readable and machine processable forms of the trusted list;

    b   the locations where the human readable and machine processable forms of the trusted list are published;

    c   the public key certificate used to implement the secure channel through which the human readable form of the trusted list is published or, if the human readable list is electronically signed, the public key certificate used to sign it;

    d   the public key certificate used to electronically sign the machine processable form of the trusted list;

    e   any changes to the information in points (a) to (d).;

(d)   the following paragraph 4 is added:

4.   The Commission shall make available to all Member States, through a secure channel to an authenticated web server, the information, referred to in paragraph 3, as notified by Member States, both in a human readable form and in a signed machine processable form.;

2.   the Annex is amended as set out in the Annex to this Decision.

Article 2

Application

This Decision shall apply from 1 December 2010.

Article 3

Addressees

This Decision is addressed to the Member States.

Done at Brussels, 28 July 2010.

For the Commission

Michel BARNIER

Member of the Commission

ANNEX

The Annex to Decision 2009/767/EC is amended as follows:

1.   Chapter I is amended as follows:

    (a)   the first and second sentences of the second paragraph are replaced by the following:

        The present specifications are relying on the specifications and requirements stated in ETSI TS 102 231 v.3.1.2. When no specific requirement is stated in the present specifications, requirements from ETSI TS 102 231 v.3.1.2 SHALL apply entirely.;

    (b)   the second paragraph of section 'TSL tag (clause 5.2.1)' is deleted;

    (c)   the paragraph following the section title 'TSL sequence number (clause 5.3.2)' is replaced by the following:

        This field is REQUIRED. It SHALL specify the sequence number of the TSL. Starting from "1" at the first release of the TSL, this integer value SHALL be incremented at each subsequent release of the TSL. It SHALL NOT be recycled to "1" when the "TSL version identifier" above is incremented.;

    (d)   the first paragraph following the section title 'TSL type (clause 5.3.3)' is replaced by the following:

        This field is REQUIRED specifying the type of TSL. It SHALL be set to http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/ generic (Generic).;

    (e)   the third paragraph following the section title 'TSL type (clause 5.3.3)' is replaced by the following:

        URI: (Generic)   http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic;

    (f)   the second sentence of the second paragraph following the section title 'Scheme operator name (clause 5.3.4)' is replaced by the following:

        It is up to each Member State to designate the Scheme operator of the TSL implementation of the Member State TL.;

    (g)   the fourth paragraph following the section title 'Scheme operator name (clause 5.3.4)' is replaced by the following:

        The named Scheme Operator (clause 5.3.4) is the entity who will sign the TSL.;

    (h)   the fourth indent following the section title 'Scheme name (clause 5.3.6)' is replaced by the following:

        "EN_name_value" = "Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State

for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State's laws.;

(i)   the first paragraph following the section title 'Service type identifier (clause 5.5.1)' is replaced by the following:

This field is REQUIRED and SHALL specify the identifier of the service type according to the type of the present TSL specifications (i.e. "/eSigDir-1999-93-EC-TrustedList/TSLType/generic").;

(j)   the fifth indent following the section title 'Service current status (clause 5.5.4)' is replaced by the following:

— **Accredited** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited);;

(k)   the ninth indent following the section title 'Service current status (clause 5.5.4)' is replaced by the following:

— Supervision of Service in Cessation	: The service identified in "Service digital identity" (clause 5.5.3) provided by the CSP identified in "TSP name" (clause 5.4.1) is currently in a cessation phase but still supervised until supervision is ceased or revoked. In the event a different legal person than the one identified in "TSP name" has taken over the responsibility of ensuring this cessation phase, the identification of this new or fallback legal person (fallback CSP) SHALL be provided in "Scheme service definition URI" (clause 5.5.6) and in the "TakenOverBy" extension (clause L.3.2) of the service entry.;

(l)   the fifth paragraph following the section title 'Service information extensions (clause 5.5.9)' is replaced by the following:

In the context of an XML implementation, the specific content of such additional information has to be coded using the xsd files provided in Annex C of ETSI TS 102 231.;

(m)   the section entitled 'Service digital identity (clause 5.6.3)' is replaced by the following:
Service digital identity (clause 5.6.3)

This field is REQUIRED and SHALL specify at least one representation of the digital identifier (i.e. X.509v3 certificate) used in "TSP Service Information — Service digital identity" (clause 5.5.3) with the format and meaning as defined in ETSI TS 102 231, clause 5.5.3.

Note: For an X.509v3 certificate value used in the "Sdi" clause 5.5.3 of a service, there must be only one single service entry in a Trusted List

per "Sti:Sie/additionalServiceInformation" value. The "Sdi" (clause 5.6.3) information used in the service approval history information associated to a service entry and the "Sdi" (clause 5.5.3) information used in this service entry MUST relate to the same X.509v3 certificate value. When a listed service is changing its "Sdi" (i.e. renewal or rekey of an X.509v3 certificate for e.g. a CA/PKC or CA/QC) or creating a new "Sdi" for such a service, even with identical values for the associated "Sti", "Sn", and ["Sie"], it means that the Scheme Operator MUST create a different service entry than the previous one.;

(n)   the section entitled 'Signed TSL' is replaced by the following:
Signed TSL

The human readable TSL implementation of the Trusted List, established under the present specifications and in particular Chapter IV, SHOULD be signed by the "Scheme operator name" (clause 5.3.4) to ensure its authenticity and integrity[4]. The format of the signature SHOULD be PAdES part 3 (ETSI TS 102 778-3[5]) but MAY be PAdES part 2 (ETSI TS 102 778-2[6]) in the context of the specific trust model established through the publication of the certificates used to sign the Trusted Lists.

The machine processable TSL implementation of the Trusted List, established under the present specifications, SHALL be signed by the "Scheme operator name" (clause 5.3.4) to ensure its authenticity and integrity. The format of the machine processable TSL implementation of the Trusted List, established under the present specifications, SHALL be XML and SHALL comply with the specifications stated in Annexes B and C of ETSI TS 102 231.

The format of the signature SHALL be XAdES BES or EPES as defined by ETSI TS 101 903 specifications for XML implementations. Such electronic signature implementation SHALL meet requirements as stated in Annex B of ETSI TS 102 231[7]. Additional general requirements regarding this signature are stated in the following sections.;

(o)   the second paragraph after the section title 'Scheme identification (clause 5.7.2)' is replaced by the following:

In the context of the present specifications the assigned reference SHALL include the "TSL type" (clause 5.3.3), the "Scheme name" (clause 5.3.6) and the value of the SubjectKeyIdentifier extension of the certificate used by the Scheme operator to electronically sign the TSL.;

(p)   the second paragraph following the section title 'additionalServiceInformation Extension (clause 5.8.2)' is replaced by the following:

Dereferencing the URI SHOULD lead to human readable information (as a minimum in EN and potentially in one or more national languages) which is deemed appropriate and sufficient for a relying party to understand the extension, and in particular explaining the meaning of the given URIs, specifying the possible values for serviceInformation and the meaning for each value.;

(q)   the section entitled 'Qualifications Extension (clause L.3.1)' is replaced by the following:

Qualifications Extension (clause L.3.1)

Description	:	This field is OPTIONAL but SHALL be present when its use is REQUIRED, e.g. for RootCA/QC or CA/QC services, and when

— the information provided in the "Service digital identity" is not sufficient to unambiguously identify the qualified certificates issued by this service,

— the information present in the related qualified certificates does not allow machine-processable identification of the facts about whether or not the QC is supported by an SSCD.

When used, this service level extension MUST only be used in the field defined in "Service information extension" (clause 5.5.9) and SHALL comply with specifications laid down in Annex L.3.1 of ETSI TS 102 231.;

(r)   after section 'Qualifications Extension (clause L.3.1)', section TakenOverBy Extension (clause L.3.2) is inserted as follows:

TakenOverBy Extension (clause L.3.2)

Description	:	This extension is OPTIONAL but SHALL be present when a service that was formerly under the legal responsibility of a CSP is taken over by another TSP and is meant to state formally the legal responsibility of a service and to enable the verification software to display to the user some legal detail. The information provided in this extension SHALL be consistent with the related use of clause 5.5.6 and SHALL comply with specifications in Annex L.3.2 of ETSI TS 102 231.;

2.   Chapter II is replaced by the following:

CHAPTER II   When establishing their Trusted Lists, Member States will use:

Language codes in lower case and country codes in upper case;

Language and country codes according to the Table provided here below.

When a Latin script is present (with its proper language code) a transliteration in Latin script with the related language codes specified in the Table below is added.

Short name(source language)	Short name(English)	Country Code	Language Code	Notes	Transliteration in Latin script
Belgique/ België	Belgium	BE	nl, fr, de		
България[a]	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα[a]	Greece	EL	el	Country code recommended by EU	el-Latn
España	Spain	ES	es	also Catalan (ca), Basque (eu), Galician (gl)	
France	France	FR	fr		
Italia	Italy	IT	it		
Κύπρος/ Kıbrıs[a]	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		

[a]   Latin transliteration: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/ Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Country code recommended by EU	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/ Noreg	Norway	NO	no, nb, nn		

a   Latin transliteration: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

3.   Chapter III is deleted;

4.   in Chapter IV, the following indent is inserted after the introductory phrase 'The content of the PDF/A based HR form of the TSL implementation of the Trusted List SHOULD comply with the following requirements:':

—   The title of the Human readable form of Trusted Lists shall be constructed as the concatenation of the following elements:

—   Optional picture of the Member State national flag;

—   Blank space;

—   Country Short Name in source language(s) (as provided in the first column of Chapter II Table);

—   Blank space;

—   "(";

—   Country Short Name in English (as provided in the second column of Chapter II Table) inside the parenthesis;

—   "):" as closing parenthesis and separator;

—   Blank space;

—   "Trusted List";

—   Optional logo of the Member State Scheme Operator.

(**1**)   OJ L 376, 27.12.2006, p. 36.

(**2**)   OJ L 274, 20.10.2009, p. 36.

(**3**)   OJ L 13, 19.1.2000, p. 12.

(**4**)   In case the human readable TSL implementation of the Trusted List is not signed, its authenticity and integrity MUST be guaranteed by an appropriate communication channel with an equivalent security level. Use of TLS (IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2") is recommended for this purpose and the fingerprint of the certificate of the TLS channel MUST be made available out of band to the TSL users by the Member State.

(**5**)   ETSI TS 102 778-3 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced — PAdES-BES and PAdES-EPES Profiles.

(**6**)   ETSI TS 102 778-2 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic — Profile based on ISO 32000-1.

(**7**)   It is mandatory to protect the Scheme Operator signing certificate with the signature in one of the ways specified by ETSI TS 101 903 and the ds:keyInfo should contain the relevant certificate chain when applicable.';