

BESLUIT VAN DE COMMISSIE**van 28 juli 2010****tot wijziging van Beschikking 2009/767/EG wat betreft het opstellen, bijwerken en publiceren van vertrouwenslijsten van certificatie dienstverleners die onder toezicht staan of zijn geaccrediteerd in een lidstaat***(Kennisgeving geschied onder nummer C(2010) 5063)***(Voor de EER relevante tekst)****(2010/425/EU)**

DE EUROPESE COMMISSIE,

Gelet op het Verdrag betreffende de werking van de Europese Unie,

Gelet op Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt ⁽¹⁾, en met name op artikel 8, lid 3,

Overwegende hetgeen volgt:

- (1) Het grensoverschrijdende gebruik van geavanceerde elektronische handtekeningen die op een gekwalificeerd certificaat berusten en al dan niet met een veilig middel voor het aanmaken van handtekeningen zijn aangemaakt, is vergemakkelijkt door Beschikking 2009/767/EG van de Commissie van 16 oktober 2009 inzake maatregelen voor een gemakkelijker gebruik van elektronische procedures via het „één-loket” in het kader van Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt ⁽²⁾, waarbij lidstaten ertoe worden verplicht voor de validatie van deze elektronische handtekeningen benodigde informatie beschikbaar te stellen. De lidstaten moeten met name in hun zogeheten „vertrouwenslijsten” informatie verstrekken over hun onder toezicht staande of geaccrediteerde certificatie dienstverleners die overeenkomstig Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen ⁽³⁾ gekwalificeerde certificaten afgeven aan het publiek, alsook over de diensten die zij aanbieden.
- (2) Samen met het Europees Instituut voor telecommunicatienormen (ETSI) is een aantal praktische tests georganiseerd om de lidstaten in de gelegenheid te stellen na te gaan of hun vertrouwenslijsten in overeenstemming zijn met de specificaties die in de bijlage bij Beschikking 2009/767/EG zijn vermeld. Deze tests hebben uitgewezen dat in de technische specificaties die in de bijlage bij Beschikking 2009/767/EG zijn opgenomen, een aantal technische wijzigingen moeten worden aangebracht om tot goed functionerende en koppelbare vertrouwenslijsten te komen.

- (3) Deze tests hebben tevens bevestigd dat lidstaten niet alleen de menselijk leesbare versies van hun vertrouwenslijsten voor het publiek beschikbaar moeten stellen zoals bij Beschikking 2009/767/EG wordt voorgeschreven, maar ook de machinaal verwerkbare versies daarvan. Het manuele gebruik van de menselijk leesbare versie van de vertrouwenslijsten kan vrij ingewikkeld en tijdrovend zijn wanneer de lidstaten een groot aantal certificatie dienstverleners hebben. De publicatie van de machinaal verwerkbare versies van vertrouwenslijsten zal het gemakkelijker maken om deze lijsten te gebruiken doordat zij automatisch zullen kunnen worden verwerkt en aldus vlotter voor openbare elektronische diensten zullen kunnen worden aangewend.
- (4) Om de toegang tot de nationale vertrouwenslijsten te vergemakkelijken, dienen de lidstaten de Commissie in kennis te stellen van informatie over de plaats waar hun vertrouwenslijsten zich bevinden en over de wijze waarop zij zijn beschermd. Deze informatie dient door de Commissie op een veilige manier aan andere lidstaten beschikbaar te worden gesteld.
- (5) Er moet met de resultaten van de eerder genoemde praktische tests op de vertrouwenslijsten van de lidstaten rekening worden gehouden om een geautomatiseerd gebruik van de lijsten mogelijk te maken en de toegang tot de lijsten te vergemakkelijken.
- (6) Beschikking 2009/767/EG moet bijgevolg dienovereenkomstig worden gewijzigd.
- (7) Teneinde de lidstaten in de gelegenheid te stellen de vereiste technische wijzigingen in hun huidige vertrouwenslijsten aan te brengen, is het raadzaam dat dit besluit met ingang van 1 december 2010 van toepassing is.
- (8) De maatregelen waarin dit besluit voorziet, zijn in overeenstemming met het advies van het Comité dienstenrichtlijn,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

*Artikel 1***Wijzigingen in Beschikking 2009/767/EG**

Beschikking 2009/767/EG wordt als volgt gewijzigd:

⁽¹⁾ PB L 376 van 27.12.2006, blz. 36.⁽²⁾ PB L 274 van 20.10.2009, blz. 36.⁽³⁾ PB L 13 van 19.1.2000, blz. 12.

1) Artikel 2 wordt als volgt gewijzigd:

a) lid 2 wordt vervangen door:

„2. De lidstaten stellen een vertrouwenslijst op en publiceren deze in zowel een menselijk leesbare als een machinaal verwerkbare versie overeenkomstig de specificaties in de bijlage.”;

b) het volgende lid 2 bis wordt ingevoegd:

„2 bis. De lidstaten ondertekenen elektronisch de machinaal verwerkbare versie van hun vertrouwenslijst en publiceren ten minste de menselijk leesbare versie van de vertrouwenslijst via een beveiligd kanaal teneinde de authenticiteit en de integriteit ervan te verzekeren.”;

c) lid 3 wordt vervangen door:

„3. De lidstaten delen de volgende informatie aan de Commissie mede:

- a) de instantie of instanties verantwoordelijk voor het opstellen, bijwerken en publiceren van de menselijk leesbare en de machinaal verwerkbare versies van de vertrouwenslijst;
- b) de plaatsen waar de menselijk leesbare en de machinaal verwerkbare versies van de vertrouwenslijst worden gepubliceerd;
- c) het publieke sleutelcertificaat waarvan is gebruikgemaakt om het beveiligde kanaal op te zetten waarlangs de menselijk leesbare versie van de vertrouwenslijst is gepubliceerd of, indien de menselijk leesbare

lijst elektronisch is ondertekend, het publieke sleutelcertificaat waarvan is gebruikgemaakt om de lijst te ondertekenen;

- d) het publieke sleutelcertificaat waarvan is gebruikgemaakt om de machinaal verwerkbare versie van de vertrouwenslijst elektronisch te ondertekenen;

- e) alle wijzigingen in de onder a) tot en met d) bedoelde informatie.”;

d) het volgende lid 4 wordt toegevoegd:

„4. Via een beveiligd kanaal naar een geauthenticeerde webserver stelt de Commissie aan alle lidstaten de in lid 3 bedoelde, door de lidstaten meegedeelde informatie beschikbaar, zowel in een menselijk leesbare versie als in een ondertekende machinaal verwerkbare versie.”.

2) De bijlage wordt gewijzigd overeenkomstig de bijlage bij dit besluit.

*Artikel 2***Toepassing**

Dit besluit is van toepassing met ingang van 1 december 2010.

*Artikel 3***Adressaten**

Dit besluit is gericht tot de lidstaten.

Gedaan te Brussel, 28 juli 2010.

Voor de Commissie

Michel BARNIER

Lid van de Commissie

BIJLAGE

De bijlage bij Beschikking 2009/767/EG wordt als volgt gewijzigd:

1) Hoofdstuk I wordt als volgt gewijzigd:

a) de eerste zin en de tweede zin van de tweede alinea worden vervangen door:

„De onderhavige specificaties zijn gebaseerd op de specificaties en vereisten in ETSI TS 102 231 v3.1.2. Indien de onderhavige specificaties geen specifieke vereisten stellen, DIENEN de vereisten van ETSI TS 102 231 v3.1.2 volledig van toepassing te zijn.”;

b) de tweede alinea van de afdeling „TSL tag (clause 5.2.1)” wordt geschrapt;

c) de alinea volgend op de afdelingstitel „TSL sequence number (clause 5.3.2)” wordt vervangen door:

„Dit veld is VERPLICHT. Het DIENT het volgnummer van de TSL te bevatten. Bij de eerste uitgave van de TSL wordt „1” gebruikt. Deze eenheid DIENT te worden verhoogd bij elke volgende uitgave van de TSL. Het MAG NIET terug op „1” worden gezet wanneer de bovenvermelde „TSL version identifier” wordt verhoogd.”;

d) de eerste alinea volgend op de afdelingstitel „TSL type (clause 5.3.3)” wordt vervangen door:

„Dit veld is VERPLICHT en geeft het type TSL weer. Het DIENT te worden ingesteld op <http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic> (Generic).”;

e) de derde alinea volgend op de afdelingstitel „TSL type (clause 5.3.3)” wordt vervangen door:

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

f) de tweede zin van de tweede alinea volgend op de afdelingstitel „Scheme operator name (clause 5.3.4)” wordt vervangen door:

„Elke lidstaat moet zelf een Scheme operator aanduiden voor de TSL-implementatie van de TL van de lidstaat.”;

g) de vierde alinea volgend op de afdelingstitel „Scheme operator name (clause 5.3.4)” wordt vervangen door:

„De genoemde Scheme Operator (clause 5.3.4) is de entiteit die de TSL zal ondertekenen.”;

h) het vierde streepje volgend op de afdelingstitel „Scheme name (clause 5.3.6)” wordt vervangen door:

„„EN_name_value”= Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/credited 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) de eerste alinea volgend op de afdelingstitel „Service type identifier (clause 5.5.1)” wordt vervangen door:

„Dit veld is VERPLICHT en DIENT de identificator te vermelden van het diensttype overeenkomstig het type van deze TSL-specificaties (d.w.z. „[eSigDir-1999-93-EC-TrustedList/TSLType/generic](http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic)”).”;

j) het vijfde streepje volgend op de afdelingstitel „Service current status (clause 5.5.4)” wordt vervangen door:

„— **geaccrediteerd** (<http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/credited>).”;

k) het negende streepje volgend op de afdelingstitel „Service current status (clause 5.5.4)” wordt vervangen door:

„— **toezicht op een aflopende dienst**: De dienst die in „Service digital identity” (clause 5.5.3) wordt geïdentificeerd en wordt verleend door de CSP die in „TSP name” (clause 5.4.1) wordt geïdentificeerd, zit momenteel in een aflopende fase, maar staat nog steeds onder toezicht totdat het toezicht wordt stopgezet of ingetrokken. Indien een andere rechtspersoon dan de rechtspersoon die in „TSP name” wordt geïdentificeerd, de verantwoordelijkheid voor deze aflopende fase heeft overgenomen, DIENT deze nieuwe of reserve-rechtspersoon (reserve-CSP) te worden vermeld in „Scheme service definition URI” (clause 5.5.6) en in de uitbreiding „TakenOverBy” (clause L.3.2) van het dienstenartikel.”;

- l) de vijfde alinea volgend op de afdelingstitel „Service information extensions (clause 5.5.9)” wordt vervangen door:

„Voor een XML-implementatie moet de specifieke inhoud van deze bijkomende informatie worden gecodeerd aan de hand van de xsd-bestanden in bijlage C bij ETSI TS 102 231.”;

- m) de afdeling met als titel „Service digital identity (clause 5.6.3)” wordt vervangen door:

„Service digital identity (clause 5.6.3)

Dit veld is VERPLICHT en DIENT ten minste één voorstelling van de digitale identicator (d.w.z. het X.509v3-certificaat) te vermelden die in „TSP Service Information — Service digital identity” (clause 5.5.3) wordt gebruikt en het formaat en de betekenis heeft als omschreven in ETSI TS 102 231, clause 5.5.3.

Opmerking: In een vertrouwenslijst mag er voor een in de „Sdi” (clause 5.5.3) van een dienst gebruikte waarde van het X.509v3-certificaat slechts één enkel dienstenartikel per „Sti:Sie/additionalServiceInformation”-waarde voorkomen. De informatie in de „Sdi” (clause 5.6.3) waarvan wordt gebruikgemaakt in de informatie over de geschiedenis van de goedkeuring van de dienst welke bij een dienstenartikel hoort, en de informatie in de „Sdi” (clause 5.5.3) waarvan in het dienstenartikel wordt gebruikgemaakt, MOETEN op dezelfde waarde van het X.509v3-certificaat betrekking hebben. Wanneer de „Sdi” van een dienst op de lijst wijzigt (d.w.z. vernieuwing of heruitgifte van een X.509v3-certificaat voor bijvoorbeeld een CA/PKC of CA/QC) of er een nieuwe „Sdi” voor een dergelijke dienst wordt aangemaakt, zelfs met identieke waarden voor de gelinkte „Sti”, „Sn” en [„Sie”], dan houdt dat in dat de Scheme Operator een dienstenartikel MOET aanmaken dat verschilt van het vorige.”;

- n) de afdeling met als titel „Signed TSL” wordt vervangen door:

„Signed TSL

De menselijk leesbare TSL-implementatie van de vertrouwenslijst, die onder deze specificaties, en met name hoofdstuk IV, wordt opgesteld, DIENT door de „Scheme operator name” (clause 5.3.4) te worden ondertekend om de authenticiteit en de integriteit ervan te verzekeren (*). Het formaat van de handtekening ZOU PAdES part 3 (ETSI TS 102 778-3 (**)) MOETEN ZIJN maar MAG ook PAdES part 2 (ETSI TS 102 778-2 (***)) zijn in de context van het specifieke model dat is opgesteld via de publicatie van de certificaten waarvan voor de ondertekening van de vertrouwenslijsten is gebruikgemaakt.

De machinaal verwerkbare TSL-implementatie van de vertrouwenslijst, die volgens deze specificaties wordt opgesteld, MOET door de „Scheme operator name” (clause 5.3.4) worden ondertekend om de authenticiteit en de integriteit ervan te verzekeren. Het formaat van de machinaal verwerkbare TSL-implementatie van de vertrouwenslijst die volgens deze specificaties wordt opgesteld, MOET XML zijn en tevens in overeenstemming zijn met de specificaties die in de bijlagen B en C bij ETSI TS 102 231 zijn vermeld.

Het formaat van de handtekening MOET XAdES BES of EPES zijn, als omschreven in de specificaties van ETSI TS 101 903 voor XML-implementaties. Deze implementatie voor elektronische handtekening MOET voldoen aan de vereisten van bijlage B bij ETSI TS 102 231 (****). Aanvullende algemene vereisten voor deze handtekening worden in de volgende afdelingen besproken.

(*) Ingeval de menselijk leesbare TSL-implementatie van de vertrouwenslijst niet is ondertekend, MOETEN de authenticiteit en de integriteit ervan worden verzekerd via een passend communicatiekanaal met een evenwaardig veiligheidsniveau. Aanbevolen wordt daartoe gebruik te maken van TLS (IETF RFC 5246: „The Transport Layer Security (TLS) Protocol Version 1.2”), en de vingerafdruk van het certificaat van het TLS-kanaal MOET buiten de band aan de TSL-gebruikers beschikbaar worden gesteld door de lidstaat.

(**) 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.

(***) 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.

(****) Het ondertekeningscertificaat van de Scheme Operator met de handtekening moet worden beschermd op een van de in ETSI TS 101 903 beschreven manieren en de ds:keyInfo DIENT, indien toepasselijk, de desbetreffende certificaatketen te bevatten.”;

- o) de tweede alinea volgend op de afdelingstitel „Scheme identification (clause 5.7.2)” wordt vervangen door:

„In het kader van de onderhavige specificaties DIENT de referentie het volgende te omvatten: het „TSL type” (clause 5.3.3), de „Scheme name” (clause 5.3.6) en de waarde van de uitbreiding SubjectKeyIdentifier van het certificaat dat door de Scheme operator wordt gebruikt om de TSL elektronisch te ondertekenen.”

- p) de tweede alinea volgend op de afdelingstitel „additionalServiceInformation Extension (clause 5.8.2)” wordt vervangen door:

„Het volgen van de URI DIENT te leiden naar menselijk leesbare informatie (ten minste in het EN en eventueel in een of meer nationale talen) die passend en voldoende wordt geacht voor derden om de uitbreiding te begrijpen, en in het bijzonder om de betekenis van alle URI's te verduidelijken en de mogelijke waarden voor service-Information en de betekenis van elke waarde te specificeren.”;

- q) de afdeling met als titel „Qualifications Extension (clause L.3.1)” wordt vervangen door:

„Qualifications Extension (clause L.3.1)

Omschrijving: Dit veld is FACULTATIEF, maar DIENT te worden gebruikt indien dit VERPLICHT is, bv. voor RootCA/QC- of CA/QC-diensten en indien

- de informatie in „Service digital identity” niet toereikend is om de gekwalificeerde certificaten die door deze dienst worden afgegeven, ondubbelzinnig te identificeren;
- op basis van de informatie die in deze gekwalificeerde certificaten staat, niet op een machinaal verwerkbaar manier kan worden nagegaan of het QC al dan niet door een SSCD wordt ondersteund.

Indien van deze uitbreiding op dienstniveau wordt gebruikgemaakt, MAG dat alleen in het veld dat is omschreven in „Service information extension” (clause 5.5.9) en MOET worden voldaan aan de specificaties die zijn vastgelegd in bijlage L.3.1 bij ETSI TS 102 231.”;

- r) na de afdeling „Qualifications Extension” (clause L.3.1) wordt de volgende afdeling „TakenOverBy Extension” (clause L 3.2) ingevoegd:

„TakenOverBy Extension (clause L.3.2)

Omschrijving: Deze uitbreiding is FACULTATIEF maar MOET aanwezig zijn wanneer een dienst die eerder onder de juridische verantwoordelijkheid van een CSP viel, door een andere TSP is overgenomen, en is bedoeld voor de formele mededeling van de juridische verantwoordelijkheid voor een dienst en om de verificatiesoftware in staat te stellen enige juridische bijzonderheden weer te geven ten behoeve van de gebruiker. De in deze uitbreiding verstrekte informatie MOET in overeenstemming zijn met het gerelateerde gebruik van clause 5.5.6 en MOET voldoen aan de specificaties in bijlage L.3.2 bij ETSI TS 102 231.”.

- 2) Hoofdstuk II wordt vervangen door:

„HOOFDSTUK II

Bij het opstellen van hun vertrouwenslijsten maken de lidstaten gebruik van:

taalcodes in kleine letters en landencodes in hoofdletters;

de taal- en landencodes die in onderstaande tabel zijn vermeld;

wanneer een Latijnse schrijfwijze (met een eigen taalcode) bestaat, wordt in onderstaande tabel de transcriptie in Latijns schrift met de bijbehorende taalcodes toegevoegd.

Courante benaming (in de oorspronkelijke taal/talen)	Courante benaming (in het Engels)	Landencode	Taalcode	Opmerkingen	Transcriptie (in Latijns schrift)
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	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 (*)	Greece	EL	el	Door de EU aanbevolen landencode	el-Latn
España	Spain	ES	es	ook Catalaans (ca), Baskisch (eu), Galicisch (gl)	
France	France	FR	fr		
Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		

Courante benaming (in de oorspronkelijke taal/talen)	Courante benaming (in het Engels)	Landencode	Taalcode	Opmerkingen	Transcriptie (in Latijns schrift)
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		
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Door de EU aanbevolen landencode	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) In Latijns schrift: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

3) Hoofdstuk III wordt geschrapt.

4) In hoofdstuk IV wordt het volgende streepje ingevoegd na de aanhef „De inhoud van de menselijk leesbare versie van de TSL-implementatie van de vertrouwenslijst in PDF/A, ZOU moeten voldoen aan de volgende vereisten”:

„— De titel van de menselijk leesbare versie van vertrouwenslijsten is opgebouwd als een aaneenschakeling van de volgende elementen:

- facultatieve afbeelding van de nationale vlag van de lidstaat;
- blanco spatie;
- courante benaming van het land in de oorspronkelijke taal/talen (als vermeld in de eerste kolom van de tabel in hoofdstuk II);
- blanco spatie;
- „(“;
- courante benaming van het land in het Engels (als vermeld in de tweede kolom van de tabel in hoofdstuk II) binnen de haakjes;
- „)” als sluitend haakje en scheidingsteken;
- blanco spatie;
- „Trusted List“;
- facultatief logo van de Scheme Operator van de lidstaat.”.