KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2015/1505

af 8. september 2015

om fastlæggelse af tekniske specifikationer og formater for positivlister i henhold til artikel 22, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF ([1]), særlig artikel 22, stk. 5, og

ud fra følgende betragtninger:

(1) Positivlister er afgørende for at opbygge tillid blandt markedsaktørerne, da de fastslår tjenesteudbyderens status på overvågningstidspunktet.

(2) Anvendelsen af elektroniske signaturer på tværs af landegrænser er blevet lettet via Kommissionens beslutning 2009/767/EF ([2]), som forpligter medlemsstaterne til at oprette, vedligeholde og offentliggøre positivlister med oplysninger om certificeringstjenesteudbydere, der udsteder kvalificerede certifikater til offentligheden i overensstemmelse med Europa-Parlamentets og Rådets direktiv 1999/93/EF ([3]), og som overvåges og akkrediteres af medlemsstaterne.

(3) I henhold til artikel 22 i forordning (EU) Nr. 910/2014 er medlemsstaterne forpligtede til under sikre forhold at oprette, ajourføre og offentliggøre positivlister, som er elektronisk underskrevne eller forseglede i en form, der er egnet til automatiseret behandling. Medlemsstaterne er også forpligtede til at meddele Kommissionen de organer, de er ansvarlige for at oprette de nationale positivlister.

(4) En tillidstjenesteudbyder og de tillidstjenester, som den udbyder, bør anses for at være kvalificerede, når udbyderen ifølge positivlisten er tildelt status som kvalificeret tillidstjenesteudbyder. For at sikre, at andre forpligtelser hidrørende fra forordning (EU) nr. 910/2014, især dem i artikel 27 og 37, uden besvær kan opfyldes af tjenesteudbyderne på afstand og ad elektronisk vej, og for at leve op til de berettigede forventninger fra andre certificeringstjenesteudbydere, som ikke udsteder kvalificerede certifikater, men yder tjenester vedrørende elektroniske signaturer i henhold til direktiv 1999/93/EF og opføres på listen inden den 30. juni 2016, bør det være muligt for medlemsstaterne på frivillig basis og på nationalt niveau at tilføje andre tillidstjenester end de kvalificerede tjenester på positivlisterne, forudsat at det klart fremgår, at de ikke er kvalificerede i henhold til forordning (EU) nr. 910/2014.

(5) I overensstemmelse med betragtning 25 i forordning (EU) nr. 910/2014 kan medlemsstaterne tilføje andre typer nationalt definerede tillidstjenester end dem, som er defineret i artikel 3, nr. 16, i forordning (EU) nr. 910/2014, forudsat at det klart fremgår, at de ikke er kvalificerede i henhold til forordning (EU) nr. 910/2014.

(6) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 48 i forordning (EU) nr. 910/2014 —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Medlemsstaterne opstiller, offentliggør og ajourfører positivlister med oplysninger om de kvalificerede tillidstjenesteudbydere, som de overvåger, samt oplysninger om de kvalificerede tillidstjenester, som disse udbydere udbyder. Disse lister skal overholde de tekniske specifikationer i bilag I.

([1]) EUT L 257 af 28.8.2014, s. 73.
([2]) Kommissionens beslutning 2009/767/EF af 16. oktober 2009 om fastlæggelse af foranstaltninger, der skal lette anvendelsen elektroniske procedurer ved hjælp af »kvikskranker« i henhold til Europa-Parlamentets og Rådets direktiv 2006/123/EF om tjenesteydelser i det indre marked (EUT L 274 af 20.10.2009, s. 36).
([3]) Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer (EFT L 13 af 19.1.2000, s. 12).

Artikel 2

I positivlisterne kan medlemsstaterne inkludere oplysninger om ikke kvalificerede tillidstjenesteudbydere sammen med oplysninger vedrørende de ikke kvalificerede tillidstjenester, som disse udbydere udbyder. Det skal fremgå klart af listen, hvilke tillidstjenesteudbydere og tillidstjenester ikke er kvalificerede.

Artikel 3

1. I henhold til artikel 22, stk. 2, i forordning (EU) nr. 910/2014 underskriver eller forsegler medlemsstaterne elektronisk deres positivliste i den form, der egner sig til automatiseret behandling, i overensstemmelse med de tekniske specifikationer i bilag I.

2. Hvis en medlemsstat elektronisk offentliggør en menneskeligt læsbar udgave af positivlisten, sikres det, at denne udgave af positivlisten indeholder de samme data som den udgave, der er egnet til automatiseret behandling, og den underskrives eller forsegles elektronisk i overensstemmelse med de tekniske specifikationer i bilag I.

Artikel 4

1. Medlemsstaterne meddeler Kommissionen de oplysninger, som der henvises til i artikel 22, stk. 3, i forordning (EU) nr. 910/2014, ved hjælp af skabelonen i bilag II.

2. Oplysningerne, som der henvises til i stk. 1, skal indeholde to eller flere operatører af offentlige nøglecertifikater med forskudte gyldighedsperioder på mindst tre måneder, der svarer til de private nøgler, der kan bruges til elektronisk at underskrive eller forsegle den udgave af positivlisten, der er egnet til automatiseret behandling, og den menneskeligt læsbare udgave, når de offentliggøres.

3. I henhold til artikel 22, stk. 4, i forordning (EU) nr. 910/2014 stiller Kommissionen de oplysninger, der er omhandlet i stk. 1 og 2, og som er indgivet af medlemsstaterne, til rådighed for offentligheden via en sikker kommunikationsforbindelse til en godkendt webserver og i en elektronisk underskrevet eller forseglet form, der egner sig til automatiseret behandling.

4. Kommissionen kan stille de oplysninger, der er omhandlet i stk. 1 og 2, og som er indgivet af medlemsstaterne, til rådighed for offentligheden via en sikker kommunikationsforbindelse til en godkendt webserver og i en underskrevet eller forseglet menneskeligt læsbar form.

Artikel 5

Denne afgørelse træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne afgørelse er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 8. september 2015.

På Kommissionens vegne

Jean-Claude JUNCKER

Formand

BILAG I

TEKNISKE SPECIFIKATIONER FOR DEN FÆLLES SKABELON FOR POSITIVLISTEN

KAPITEL I

ALMINDELIGE SPECIFIKATIONER

Positivlisterne skal indeholde både aktuelle og alle historiske oplysninger om de angivne tillidstjenesteudbydere fra det tidspunkt, hvor den pågældende tillidstjenesteudbyder optages på positivlisten.

Betegnelserne »godkendt«, »akkrediteret« og/eller »overvåget« i de nærværende specifikationer omfatter også de nationale godkendelsesordninger, men yderligere oplysninger om arten af sådanne eventuelle nationale ordninger vil blive afgivet af medlemsstaterne i deres positivliste, herunder afklaring af eventuelle forskelle fra de overvågningsordninger, der gælder for kvalificerede tillidstjenesteudbydere og de kvalificerede tillidstjenester, som de udbyder.

Hovedformålet med oplysningerne i positivlisten er at støtte valideringen af kvalificerede trust service tokens, dvs. fysiske eller binære (logiske) genstande, der genereres eller udstedes som følge af anvendelsen af en kvalificeret tillidstjeneste, f.eks. netop kvalificerede elektroniske signaturer/segl, avancerede elektroniske signaturer/segl understøttet af et kvalificeret certifikat, kvalificerede tidsstempler, kvalificerede elektroniske leveringsbeviser, osv.

KAPITEL II

DETALJEREDE SPECIFIKATIONER FOR DEN FÆLLES SKABELON FOR POSITIVLISTEN

Nærværende specifikationer bygger på de specifikationer og krav, som er angivet i ETSI TS 119 612 v2.1.1 (herefter kaldet ETSI TS 119 612).

Hvis der ikke er angivet noget specifikt krav i nærværende specifikationer, finder kravene i punkt 5 og 6 i ETSI TS 119 612 fuld anvendelse. Når der er angivet specifikke krav i nærværende specifikationer, har de forrang over de tilsvarende krav fra ETSI TS 119 612. I tilfælde af uoverensstemmelser mellem nærværende specifikationer og specifikationerne i ETSI TS 119 612, betragtes nærværende specifikationer som de normative.

Scheme name (punkt 5.3.6)

Dette felt er påkrævet og skal være i overensstemmelse med specifikationerne fra TS 119 612 punkt 5.3.6, hvori det følgende navn skal anvendes for ordningen:

»EN_name_value« = »Positivliste med oplysninger om de kvalificerede tillidstjenesteudbydere, som overvåges af medlemsstaterne, samt oplysninger om de kvalificerede tillidstjenester, som udbyderne udbyder, i overensstemmelse med de relevante bestemmelser i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.«

Scheme information URI (punkt 5.3.7)

Dette felt er påkrævet og skal være i overensstemmelse med specifikationerne fra TS 119 612, punkt 5.3.7, hvori de »passende oplysninger om ordningen« mindst skal omfatte:

a) Indledende oplysninger, som er fælles for alle medlemsstaterne, vedrørende positivlistens anvendelsesområde og kontekst, den pågældende overvågningsordning og, hvor det er relevant, de national(e) godkendelsesordning(er) f.eks. til akkreditering. Den nedenstående tekst er den fælles tekst, der bruges, hvori tekststrengen »[*name of the relevant Member State*]« skal erstattes med navnet på den pågældende medlemsstat:

   »Nærværende liste er positivlisten med oplysninger om de kvalificerede tillidstjenesteudbydere, som overvåges af »[*name of the relevant Member State*]«, samt oplysninger om de kvalificerede tillidstjenester, som udbyderne udbyder, i overensstemmelse med de relevante bestemmelser i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.

Anvendelsen af elektroniske signaturer på tværs af landegrænser er blevet lettet via Kommissionens beslutning 2009/767/EF af 16. oktober 2009, som forpligter medlemsstaterne til at oprette, vedligeholde og offentliggøre positivlister med oplysninger om certificeringstjenesteudbydere, der udsteder kvalificerede certifikater til offentligheden i overensstemmelse med Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer, og som overvåges/akkrediteres af medlemsstaterne. Nærværende positivliste er en videreførelse af positivlisten, som blev opstillet i forbindelse med beslutning 2009/767/EF.«

Positivlister er afgørende elementer for at opbygge tillid blandt markedsaktørerne, da brugere kan anvende dem til at fastslå tillidstjenesteudbydernes og deres tjenesters kvalificerede status og statushistorik.

Medlemsstaternes positivlister omfatter som minimum de oplysninger, som der henvises til i artikel 1 og 2 i Kommissionens gennemførelsesafgørelse (EU) 2015/1505.

I positivlisterne kan medlemsstaterne inkludere oplysninger om ikke kvalificerede tillidstjenesteudbydere sammen med oplysninger vedrørende de ikke kvalificerede tillidstjenester, som disse udbydere udbyder. Det skal klart fremgå, at disse ikke er kvalificerede i henhold til forordning (EU) nr. 910/2014.

I positivlisterne kan medlemsstaterne inkludere oplysninger om nationalt definerede tillidstjenester af andre typer end dem, som er defineret i artikel 3, nr. 16, i forordning (EU) nr. 910/2014. Det skal klart fremgå, at disse ikke er kvalificerede i henhold til forordning (EU) nr. 910/2014.

b) Specifikke oplysninger om den pågældende overvågningsordning og, hvor det er relevant, de national(e) godkendelsesordning(er) f.eks. til akkreditering, især ([1]):

1) oplysninger om den nationale overvågningsordning, der finder anvendelse på kvalificerede og ikke kvalificerede tillidstjenesteudbydere samt de kvalificerede og ikke kvalificerede tillidstjenester, som udbyderne udbyder, i henhold til forordning (EU) nr. 910/2014

2) oplysninger, hvor det er relevant, om de nationale frivillige akkrediteringsordninger, der finder anvendelse på certificeringstjenesteudbydere, som har udstedt kvalificerede certifikater i henhold til direktiv 1999/93/EF.

Disse særlige oplysninger skal for hver af de pågældende ovenfor angivne ordninger mindst omfatte:

1) en generel beskrivelse

2) oplysninger om processen i den nationale overvågningsordning og, hvor det er relevant, for godkendelse efter en national godkendelsesordning

3) oplysninger om de kriterier, som tillidstjenesteudbydere overvåges eller, hvor det er relevant, godkendes efter

4) oplysninger om de kriterier og bestemmelser, som anvendes til at udvælge tilsynsførende/revisorer og fastlægge, hvordan disse vurderer tillidstjenesteudbydere og de tillidstjenester, som udbyderne udbyder

5) andre generelle oplysninger, som vedrører ordningens drift, samt kontaktoplysninger, hvor det er relevant.

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]) Disse sæt af oplysninger er af afgørende betydning for, at modtagerparter kan vurdere kvaliteten og sikkerhedsniveauet ved sådanne ordninger. Disse sæt af oplysninger skal angives på positivliste-niveau ved anvendelse af nærværende »Scheme information URI« (punkt 5.3.7 — oplysninger, der leveres af medlemsstaten), »Scheme type/community/rules« (punkt 5.3.9 — gennem anvendelse af en fælles tekst for alle medlemsstater) og »TSL policy/legal notice« (punkt 5.3.11 — en fælles tekst for alle medlemsstater, hvor hver medlemsstat har mulighed for at tilføje medlemsstatsspecifik tekst/medlemsstatsspecifikke henvisninger). Yderligere oplysninger om sådanne ordninger for ikke kvalificerede tillidstjenester og nationalt definerede (kvalificerede) tillidstjenester kan afgives på tjenesteniveau, i det omfang det er relevant og påkrævet (f.eks. for at skelne mellem flere kvalitets-/sikkerhedsniveauer) gennem anvendelse af »Scheme service definition URI« (punkt 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 (punkt 5.3.11)

Dette felt er påkrævet og skal være i overensstemmelse med specifikationerne fra TS 119 612, punkt 5.3.11, hvor den politiske/juridiske erklæring om ordningens retslige status eller retslige krav, som ordningen overholder i henhold til den jurisdiktion, hvor den er oprettet, og/eller enhver hindring og betingelse for vedligeholdelsen og offentliggørelsen af

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

positivlisten, skal være en række multisprogede tekststrenge (se punkt 5.1.4), som på følgende måde formidler en sådan erklærings faktiske tekst på britisk engelsk som obligatorisk sprog og eventuelt på et eller flere andre nationale sprog på valgfri basis:

(1) En første obligatorisk del, som er fælles for alle medlemsstaters positivlister, hvori de relevante retlige rammer angives, og hvis engelske version lyder:

> 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.

Teksten på medlemsstatens nationalsprog:

> De relevante retlige rammer for nærværende positivliste er Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF.

(2) En anden, valgfri del, som er specifik for hver positivliste, med henvisninger til specifikke gældende nationale retlige rammer

Service current status (punkt 5.5.4)

Dette felt er påkrævet og skal være i overensstemmelse med specifikationerne fra TS 119 612, punkt 5.5.4.

Overførslen af »Service current status«-værdien for de tjenester, der optræder på medlemsstaternes positivlister på dagen før datoen, hvorfra forordning (EU) nr. 910/2014 finder anvendelse, dvs. 30. juni 2016, skal udføres på datoen, hvorfra forordningen finder anvendelse, dvs. 1. juli 2016, som anført i bilag J til ETSI TS 119 612.

KAPITEL III

POSITIVLISTERS KONTINUITET

Certifikater, der skal meddeles til Kommissionen i overensstemmelse med artikel 4, stk. 2, i denne afgørelse, skal leve op til kravene i punkt 5.7.1 fra ETSI TS 119 612 og skal udstedes sådan, at:

— der er mindst tre måneder mellem deres sidste gyldighedsdatoer (»ikke efter«)

— de er genereret på nye nøglepar. Ingen tidligere anvendte nøglepar må gencertificeres.

Hvis et af de offentlige nøglecertifikater, der kan anvendes til at validere positivlistens signatur eller segl, og som er blevet meddelt til Kommissionen og offentliggjort i Kommissionens centrale pointerliste, er udløbet, skal medlemsstaterne:

— hvis den aktuelt offentliggjorte positivliste var underskrevet eller forseglet med en privat nøgle, hvis offentlige nøglecertifikat er udløbet, straks udstede en ny positivliste, som er underskrevet eller forseglet med en privat nøgle, hvis meddelte offentlige nøglecertifikat ikke er udløbet

— når det er påkrævet, generere nye nøglepar, der kan bruges til at underskrive eller forsegle positivlisten, og generere deres tilsvarende offentlige nøglecertifikater

— straks underrette Kommissionen om den nye liste over offentlige nøglecertifikater, der svarer til de private nøgler, der kan bruges til at underskrive eller forsegle positivlisten.

Hvis en af de private nøgler, der svarer til et af de offentlige nøglecertifikater, der kan bruges til at validere positivlistens signatur eller segl, og som er blevet meddelt til Kommissionen og offentliggjort i Kommissionens centrale pointerliste, er blevet kompromitteret eller afviklet, skal medlemsstaterne:

— straks genudstede en ny positivliste, som er underskrevet eller forseglet med en ikke-kompromitteret privat nøgle, i tilfælde hvor den offentliggjorte positivliste var underskrevet eller forseglet med en kompromitteret eller afviklet privat nøgle

— når det er påkrævet, generere nye nøglepar, der kan bruges til at underskrive eller forsegle positivlisten, og generere deres tilsvarende offentlige nøglecertifikater

— straks underrette Kommissionen om den nye liste over offentlige nøglecertifikater, der svarer til de private nøgler, der kan bruges til at underskrive eller forsegle positivlisten.

Hvis alle de private nøgler, der svarer til de offentlige nøglecertifikater, der kan bruges til at validere positivlistens signatur, og som er blevet meddelt til Kommissionen og offentliggjort i Kommissionens centrale pointerliste, er blevet kompromitteret eller afviklet, skal medlemsstaterne:

— generere nye nøglepar, der kan bruges til at underskrive eller forsegle positivlisten, og generere deres tilsvarende offentlige nøglecertifikater

— straks genudstede en ny positivliste, der er underskrevet eller forseglet med en af disse nye private nøgler, og hvis tilsvarende offentlige nøglecertifikat skal meddeles

— straks underrette Kommissionen om den nye liste over offentlige nøglecertifikater, der svarer til de private nøgler, der kan bruges til at underskrive eller forsegle positivlisten.

KAPITEL IV

SPECIFIKATIONER FOR DEN MENNESKELIGT LÆSBARE UDGAVE AF POSITIVLISTEN

Når en menneskeligt læsbar form af positivlisten er genereret og offentliggjort, skal den foreligge som et PDF-dokument (Portable Document Format) i overensstemmelse med ISO 32000 ([1]), som skal have et format i overensstemmelse med profil PDF/A (ISO 19005 ([2])).

Indholdet i de PDF/A-baserede menneskeligt læsbare udgaver af positivlisten skal opfylde følgende krav:

— Opbygningen af den menneskeligt læsbare udgave skal afspejle den logiske model, der er beskrevet i TS 119 612

— Hvert forekommende felt skal vises og angive:

  — Feltets titel (f.eks. »*Service type identifier*«)

  — Feltets værdi (f.eks. http://uri.etsi.org/TrstSvc/Svctype/CA/QC)

  — Betydningen (beskrivelse) af feltets værdi, såfremt dette er relevant (f.eks. »En certifikatgenereringstjeneste, der genererer og underskriver kvalificerede certifikater på basis af identiteten og andre egenskaber, som er bekræftet af de relevante registreringstjenester.«)

  — Flere versioner i naturligt sprog som angivet i positivlisten, såfremt dette er relevant.

— Følgende felter med tilhørende værdier i de digitale certifikater ([3]) skal, hvis de forefindes i feltet »Service digital identity«, som minimum vises i den menneskeligt læsbare udgave:

  — Version

  — Certifikatets serienummer

  — Signaturalgoritme

  — Udsteder — alle relevante særskilte navnefelter

  — Gyldighedsperiode

  — Bruger — alle relevante særskilte navnefelter

([1]) ISO 32000-1:2008: Dokumentstyring — Portable document format — Del 1: PDF 1.7
([2]) ISO 19005-2:2011: Dokumentstyring — Filformat for elektroniske dokumenter til langtidsopbevaring — Del 2: Brug af 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 (se http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— Offentlig nøgle

— Identifikator for myndighedsnøgle

— Identifikator for brugernøgle

— Nøglebrug

— Forlænget nøglebrug

— Certifikatpolitikker — alle politikidentifikatorer og politikkvalifikatorer

— Kortlægning af politikker

— Alternativt brugernavn

— Brugerens katalogegenskaber

— Grundlæggende begrænsninger

— Politikbegrænsninger

— CRL-distributionspunkter ([1])

— Myndighedens adgang til oplysninger

— Brugerens adgang til oplysninger

— Bemærkninger til det kvalificerede certifikat ([2])

— Hash-algoritme

— Certifikatets hash-værdi

— Den menneskeligt læsbare udgave skal let kunne udskrives

— Den menneskeligt læsbare udgave skal underskrives eller forsegles af ordningens operatør i henhold til avanceret PDF-signatur som beskrevet i artikel 1 og 3 i Kommissionens gennemførelsesafgørelse (EU) 2015/1505.

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

BILAG II

SKABELON FOR MEDLEMSSTATERNES MEDDELELSER

Oplysningerne, som medlemsstaterne skal meddele i henhold til artikel 4, stk. 1, i nærværende afgørelse, skal indeholde de følgende oplysninger og eventuelle ændringer heraf:

1) Medlemsstat, hvor ISO 3166-1 ([1]) Alpha 2-koderne anvendes med følgende undtagelser:

   a) Landekoden for Det Forenede Kongerige er »UK«.

   b) Landekoden for Grækenland er »EL«.

2) Organet/organerne med ansvar for oprettelsen, vedligeholdelsen og offentliggørelsen af positivlisterne i en form, der er egnet til automatiseret behandling, og i en menneskeligt læsbar udgave:

   a) Navnet på ordningens operatør: de angivne oplysninger skal være identiske — også med hensyn til forskel på store og små bogstaver — med værdien »Navnet på ordningens operatør« i positivlisten og på lige så mange sprog, som der anvendes i positivlisten

   b) Valgfrie oplysninger til intern brug i Kommissionen, kun i tilfælde hvor der er behov for kontakt til det relevante organ (oplysningerne offentliggøres ikke i den af Europa-Kommissionen sammensatte liste over positivlister):

      — Adressen på ordningens operatør

      — Kontaktoplysninger for den eller de ansvarlige person(er) (navn, telefonnummer, e-mailadresse).

3) Stedet, hvor positivlisten offentliggøres i en form, der er egnet til automatiseret behandling *(stedet, hvor den aktuelle positivliste er offentliggjort)*.

4) Stedet, om muligt, hvor positivlisten offentliggøres i en menneskeligt læsbar form *(stedet, hvor den aktuelle positivliste er offentliggjort)*. Hvis en menneskeligt læsbar udgave af positivlisten ikke længere offentliggøres, angives dette.

5) De offentlige nøglecertifikater, der svarer til de private nøgler, som kan anvendes til at underskrive eller forsegle positivlisten i den form, der egner sig til automatiseret behandling, og den menneskeligt læsbare udgave af positivlisten. Disse certifikater skal indsendes som DER-certifikater indkodet med Privacy Enhanced Mail Base64. Hvad angår meddelelser om ændring, tilføjes yderligere oplysninger, hvis et nyt certifikat skal erstatte et specifikt certifikat i Kommissionens liste, og hvis det meddelte certifikat skal føjes til det eksisterende certifikat i stedet for at erstatte det.

6) Dato for indgivelse af oplysninger, der meddeles i henhold til punkt 1) til 5).

Oplysninger, der meddeles i henhold til punkt 1), punkt 2), litra a), punkt 3), punkt 4) og punkt 5) indarbejdes i den af Europa-Kommissionen sammensatte liste over positivlister og erstatter de tidligere meddelte oplysninger i denne sammensatte liste.

([1]) ISO 3166-1: »Koder for navne på lande og deres underinddelinger — Del 1: Landekoder«.