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

KOMMISJONENS GJENNOMFØRINGSBESLUTNING (EU) 2015/1505

av 8. september 2015

om fastsettelse av tekniske spesifikasjoner og formater for tillitslister i henhold til artikkel 22 nr. 5 i europaparlaments- og rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked

EUROPAKOMMISJONEN HAR —

under henvisning til traktaten om Den europeiske unions virkemåte,

under henvisning til europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF([1]), og særlig artikkel 22 nr. 5, og

ut fra følgende betraktninger:

1) Tillitslister er avgjørende for å skape tillit blant markedsdeltakere, ettersom de viser tjenestetilbyderens status på tidspunktet for tilsynet.

2) Det er blitt lettere å bruke elektroniske signaturer over landegrensene ved kommisjonsvedtak 2009/767/EF([2]), der det er fastsatt at medlemsstatene har plikt til å opprette, ajourføre og offentliggjøre tillitslister, med opplysninger om tilbydere av sertifiseringstjenester som utsteder kvalifiserte sertifikater til allmennheten i samsvar med europaparlaments- og rådsdirektiv 1999/93/EF([3]), og som er underlagt tilsyn og er akkreditert av medlemsstatene.

3) I artikkel 22 i forordning (EF) nr. 910/2014/EU er det fastsatt en forpliktelse for medlemsstatene til å opprette, ajourføre og offentliggjøre elektronisk signerte eller forseglede tillitslister på en sikker måte, i et format som er egnet for automatisert behandling, og gi Kommisjonen melding om hvilke organer som har ansvar for å opprette nasjonale tillitslister.

4) En tilbyder av tillitstjenester, og tillitstjenestene denne tilbyderen leverer, bør anses som kvalifisert når tilbyderen har status som kvalifisert i tillitslisten. For å sikre at andre forpliktelser som følger av forordning (EU) nr. 910/2014, særlig forpliktelsene i artikkel 27 og 37, lett kan oppfylles av tilbydere av fjernformidlede og elektroniske tjenester, og for å oppfylle de berettigede forventningene fra andre tilbydere av sertifiseringstjenester som ikke utsteder kvalifiserte sertifikater, men som leverer tjenester knyttet til elektroniske signaturer i henhold til direktiv 1999/93/EF og oppføres på listen innen 30. juni 2016, bør det være mulig for medlemsstatene å tilføye andre tillitstjenester enn de kvalifiserte tjenestene i tillitslistene, på frivillig basis og på nasjonalt plan, forutsatt at det klart framgår at de ikke er kvalifisert i samsvar med forordning (EU) nr. 910/2014.

5) I tråd med betraktning 25 i forordning (EU) nr. 910/2014 kan medlemsstatene tilføye andre typer nasjonalt definerte tillitstjenester enn dem som er definert i artikkel 3 nr. 16 i forordning (EU) nr. 910/2014, forutsatt at det klart framgår at de ikke er kvalifisert i samsvar med forordning (EU) nr. 910/2014.

6) Tiltakene fastsatt i denne beslutning er i samsvar med uttalelse fra komiteen nedsatt ved artikkel 48 i forordning (EU) nr. 910/2014 —

TRUFFET DENNE BESLUTNING:

Artikkel 1

Medlemsstatene skal opprette, offentliggjøre og ajourføre tillitslister med opplysninger om de kvalifiserte tilbyderne av tillitstjenester som står under deres tilsyn, samt opplysninger om de kvalifiserte tillitstjenestene disse tilbyderne leverer. Listene skal være i samsvar med de tekniske spesifikasjonene i vedlegg I.

Artikkel 2

I tillitslistene kan medlemsstatene tilføye opplysninger om ikke-kvalifiserte tilbydere av tillitstjenester, sammen med opplysninger om

([1]) EUT L 257 av 28.8.2014, s. 73.

([2]) Kommisjonsvedtak 2009/767/EF av 16. oktober 2009 om fastsettelse av tiltak for å forenkle bruken av elektroniske framgangsmåter ved hjelp av «felles kontaktpunkter» i samsvar med europaparlaments- og rådsdirektiv 2006/123/EF om tjenester i det indre marked (EUT L 274 av 20.10.2009, s. 36).

([3]) Europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer (EFT L 13 av 19.1.2000, s. 12).

de ikke-kvalifiserte tillitstjenestene disse tilbyderne leverer. Det skal framgå klart av listen hvilke tilbydere av tillitstjenester, og hvilke tillitstjenester disse tilbyderne leverer, som ikke er kvalifisert.

Artikkel 3

1) I henhold til artikkel 22 nr. 2 i forordning (EU) nr. 910/2014 skal medlemsstatene signere eller forsegle sin tillitsliste elektronisk i et format som er egnet for automatisert behandling, i samsvar med de tekniske spesifikasjonene i vedlegg I.

2) Dersom en medlemsstat offentliggjør tillitslisten elektronisk i et format som kan leses av mennesker, skal den sørge for at tillitslisten i dette formatet inneholder de samme opplysninger som i formatet som er egnet for automatisert behandling, og den skal signere eller forsegle den elektronisk i samsvar med de tekniske spesifikasjonene i vedlegg I.

Artikkel 4

1) Medlemsstatene skal melde opplysningene nevnt i artikkel 22 nr. 3 i forordning (EU) nr. 910/2014 til Kommisjonen ved å benytte malen i vedlegg II.

2) Opplysningene som er nevnt i nr. 1 skal inneholde to eller flere offentlige nøkkelsertifikater fra ordningens operatør, der gyldighetstiden er forskjøvet med minst tre måneder, som motsvarer de private nøklene som kan benyttes til elektronisk signering eller forsegling av tillitslisten i et format som er egnet for automatisert behandling, og i et format som kan leses av mennesker, når de offentliggjøres.

3) I henhold til artikkel 22 nr. 4 i forordning (EU) nr. 910/2014 skal Kommisjonen, via en sikker kanal til en autentisert nettjener, offentliggjøre opplysningene som er nevnt i nr. 1 og 2, og som er meldt inn av medlemsstatene, i et signert eller forseglet format som er egnet for automatisert behandling.

4) Kommisjonen kan, via en sikker kanal til en autentisert nettjener, offentliggjøre opplysningene som er nevnt i nr. 1 og 2, og som er meldt inn av medlemsstatene, i et signert eller forseglet format som kan leses av mennesker.

Artikkel 5

Denne beslutning trer i kraft den 20. dag etter at den er kunngjort i *Den europeiske unions tidende*.

Denne beslutning er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Brussel 8. september 2015.

For Kommisjonen

Jean-Claude JUNCKER

President

VEDLEGG I

TEKNISKE SPESIFIKASJONER FOR EN FELLES MAL FOR TILLITSLISTER

KAPITTEL I

GENERELLE KRAV

Tillitslister skal inneholde både aktuell og historisk informasjon om status for oppførte tillitstjenester, fra det tidspunkt en tilbyder av tillitstjenester føres opp i tillitslistene.

Uttrykkene «godkjent», «akkreditert» og/eller «under tilsyn» i disse spesifikasjonene omfatter også de nasjonale godkjenningsordningene, men ytterligere informasjon om slike nasjonale ordningers karakter vil bli gitt av medlemsstatene i deres tillitslister, blant annet med klargjøring av mulige forskjeller fra tilsynsordningene som gjelder for kvalifiserte tilbydere av tillitstjenester og de kvalifiserte tillitstjenestene disse tilbyderne leverer.

Informasjonen i tillitslisten skal først og fremst underbygge valideringen av gjenkjenningstegn for kvalifiserte tillitstjenester, dvs. fysiske eller binære (logiske) objekter som genereres eller utstedes som en følge av bruken av en kvalifisert tillitstjeneste, for eksempel kvalifiserte elektroniske signaturer/segl, avanserte elektroniske signaturer/segl som understøttes av et kvalifisert sertifikat, kvalifiserte tidsstempler, kvalifiserte elektroniske leveringsbevis, osv.

KAPITTEL II

DETALJERTE SPESIFIKASJONER FOR DEN FELLES MALEN FOR TILLITSLISTENE

Disse spesifikasjonene bygger på spesifikasjonene og kravene som er oppført i ETSI TS 119 612 v2.1.1 (heretter kalt ETSI TS 119 612).

Når det ikke er oppført noe bestemt krav i disse spesifikasjonene, skal kravene i ETSI TS 119 612 nr. 5 og 6 få full anvendelse. Når det er oppført bestemte krav i disse spesifikasjonene, skal de gå foran de tilsvarende kravene i ETSI TS 119 612. Ved avvik mellom disse spesifikasjonene og spesifikasjonene i ETSI TS 119 612, skal disse spesifikasjonene gå foran.

Scheme name (nr. 5.3.6)

Dette feltet er obligatorisk, og skal være i samsvar med spesifikasjonene i TS 119 612 nr. 5.3.6, og følgende navn skal benyttes for ordningen:

«EN_name_value» = «tillitsliste, herunder opplysninger om kvalifiserte tilbydere av tillitstjenester som er under tilsyn av den utstedende medlemsstaten, sammen med opplysninger om de kvalifiserte tillitstjenestene disse tilbyderne leverer, i samsvar med de relevante bestemmelsene i europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF.»

Scheme information URI (nr. 5.3.7)

Dette feltet er obligatorisk, og skal være i samsvar med spesifikasjonene i TS 119 612 nr. 5.3.7, der «relevante opplysninger om ordningen» minst skal omfatte:

a) Innledende opplysninger som er felles for alle medlemsstatene, om tillitslistens virkeområde og bakgrunn, den underliggende tilsynsordningen, og eventuelt nasjonal(e) godkjenningsordning(er) (f.eks. akkreditering). Den felles teksten som skal brukes, er teksten nedenfor, der tekststrengen «(*medlemsstatens navn*)» skal erstattes med den aktuelle medlemsstatens navn:

> «Denne listen er tillitslisten, med opplysninger om de kvalifiserte tilbyderne av tillitstjenester som står under tilsyn av *(medlemsstatens navn)*, sammen med opplysninger om de kvalifiserte tillitstjenestene disse tilbyderne leverer, i samsvar med de relevante bestemmelsene i europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF.
>
> Det er blitt lettere å bruke elektroniske signaturer over landegrensene ved kommisjonsvedtak 2009/767/EF av 16. oktober 2009, der det er fastsatt at medlemsstatene har plikt til å opprette, ajourføre og offentliggjøre tillitslister med opplysninger om tilbydere av sertifiseringstjenester som utsteder kvalifiserte sertifikater til allmennheten i samsvar med europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer, og som er underlagt tilsyn og er akkreditert av medlemsstatene. Denne tillitslisten er en

videreføring av den tillitsliste som ble opprettet med vedtak 2009/767/EF.»

Tillitslister er avgjørende for å skape tillit mellom operatører i elektroniske markeder, ved at brukerne får mulighet til å fastslå kvalifisert status og statushistorikk for tilbydere av tillitstjenester og deres tjenester.

Medlemsstatenes tillitslister skal som et minimum inneholde de opplysninger som er oppført i artikkel 1 og 2 i Kommisjonens gjennomføringsbeslutning (EU) 2015/1505.

I tillitslistene kan medlemsstatene tilføye opplysninger om ikke-kvalifiserte tilbydere av tillitstjenester, sammen med opplysninger om de ikke-kvalifiserte tillitstjenestene disse tilbyderne leverer. Det skal klart framgå at de ikke er kvalifisert i samsvar med forordning (EU) nr. 910/2014.

I tillitslistene kan medlemsstatene tilføye opplysninger om nasjonalt definerte tillitstjenester av en annen type enn dem som er definert i artikkel 3 nr. 16 i forordning (EU) nr. 910/2014. Det skal klart framgå at de ikke er kvalifisert i samsvar med forordning (EU) nr. 910/2014.

b) Spesifikke opplysninger om den underliggende tilsynsordningen og eventuelt nasjonal(e) godkjenningsordning(er) (f.eks. akkreditering), og særlig([4]):

1) opplysninger om den nasjonale tilsynsordningen som gjelder for kvalifiserte og ikke-kvalifiserte tilbydere av tillitstjenester og de kvalifiserte og ikke-kvalifiserte tillitstjenestene de leverer, i henhold til forordning (EU) nr. 910/2014,

2) eventuelt opplysninger om de nasjonale frivillige akkrediteringsordningene som gjelder for tilbydere av sertifiseringstjenester som har utstedt kvalifiserte sertifikater i henhold til direktiv 1999/93/EF.

Disse spesifikke opplysningene skal for hver underliggende ordning oppført ovenfor, minst inneholde:

1) en generell beskrivelse,

2) opplysninger om prosessen som følges for den nasjonale tilsynsordningen, og eventuelt for godkjenning i henhold til en nasjonal godkjenningsordning,

3) opplysninger om kriteriene for tilsyn med tilbydere av tillitstjenester, eller eventuelt for godkjenning,

4) opplysninger om kriteriene og reglene som skal benyttes til å velge ut tilsyns-/revisjonsorganer, og om hvordan hvordan de vurderer tilbydere av tillitstjenester og tillitstjenestene disse tilbyderne leverer,

5) eventuelt andre kontaktopplysninger og generelle opplysninger om hvordan ordningen virker.

Scheme type/community/rules (nr. 5.3.9)

Dette feltet er obligatorisk, og skal være i samsvar med spesifikasjonene i TS 119 612 nr. 5.3.9.

Det skal bare inneholde URI-ene på britisk-engelsk.

Det skal inneholde minst to URI-er:

1) En URI som er felles for alle medlemsstaters tillitslister, med lenke til en beskrivende tekst som skal gjelde for alle tillitslister:

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

([4]) Disse settene med opplysninger er av avgjørende betydning for at brukerne skal kunne vurdere kvaliteten og sikkerhetsnivået i slike ordninger. Disse settene med opplysninger skal gis på tillitsliste-nivå ved bruk av den foreliggende «Scheme information URI» (nr. 5.3.7 — opplysninger som gis av medlemsstaten), «Scheme type/community/rules» (nr. 5.3.9 — ved å benytte en tekst som er felles for alle medlemsstater) og «TSL policy/legal notice» (nr. 5.3.11 — en tekst som er felles for alle medlemsstater, samtidig som hver medlemsstat har mulighet til å tilføye tekst/referanser som er spesifikke for medlemsstaten). Ytterligere opplysninger om slike ordninger for ikke-kvalifiserte tillitstjenester og nasjonalt definerte (kvalifiserte) tillitstjenester kan gis på tjenestenivå når det er relevant og påkrevd (f.eks. for å skille mellom flere kvalitets-/sikkerhetsnivåer) ved å benytte «Scheme service definition URI» (nr. 5.5.6).

Beskrivende tekst:

«*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) En URI som er spesifikk for hver medlemsstats tillitsliste, med lenke til en beskrivende tekst som skal gjelde for denne medlemsstatens tillitsliste:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC der CC = ISO 3166-1([5]) alfa-2 landkode som benyttes i feltet «Scheme territory' field» (nr. 5.3.10)

— der brukere kan finne den angitte medlemsstatens spesifikke policy/regler som tillitstjenester oppført på listen skal vurderes mot, i samsvar med medlemsstatens tilsynsordning og eventuelt godkjenningsordning,

— der brukere kan få en angitt medlemsstats spesifikke beskrivelse av hvordan de skal bruke og tolke innholdet i tillitslisten med hensyn til ikke-kvalifiserte tillitstjenester som er oppført på listen, og/eller nasjonalt definerte tillitstjenester. Dette kan brukes som indikasjon på en mulig granularitet i den nasjonale godkjenningsordningen knyttet til CSP-er som ikke utsteder QC-er, og hvordan feltene «Scheme service definition URI» (nr. 5.5.6) og «Service information extension» (nr. 5.5.9) benyttes til dette formålet.

Medlemsstatene KAN definere og benytte ytterligere URI-er som en utvidelse av ovennevnte medlemsstats spesifikke URI (dvs. URI-er som er definert ut fra denne hierarkiske spesifikke URI).

TSL policy/legal notice (nr. 5.3.11)

Dette feltet er obligatorisk, og skal være i samsvar med spesifikasjonene i TS 119 612 nr. 5.3.11 der policyen/den juridiske uttalelsen med hensyn til ordningens retttslige status eller de juridiske krav som ordningen oppfyller i jurisdiksjonen der den er etablert, og/eller eventuelle begrensninger og vilkår for ajourføring og offentliggjøring av tillitslisten, skal være en sekvens med flerspråklige tekststrenger (se nr. 5.1.4), som på britisk-engelsk – som er det obligatoriske språket – og ett eller flere valgfrie nasjonale språk gjengir den faktiske teksten i en slik policy eller uttalelse, på følgende måte:

1) En første, obligatorisk del som er felles for alle medlemsstatenes tillitslister, og som angir gjeldende rettslige ramme, der den engelske versjonen 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.»

Tekst på en medlemsstats nasjonale språk:

«Gjeldende rettslig ramme for den foreliggende tillitslisten er europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF.»

2) En andre, valgfri del som er spesifikk for hver tillitsliste, med henvisning til spesifikke, gjeldende nasjonale rettslige rammer.

Service current status (nr. 5.5.4)

Dette feltet er obligatorisk, og skal være i samsvar med spesifikasjonene i TS 119 612 nr. 5.5.4.

([5]) ISO 3166-1:2006: «Koder for presentasjon av navn på land og deres underinndeling — del 1: Landkoder»:

Migreringen av «Service current status»-verdien for tjenester oppført i medlemsstatenes tillitsliste dagen før den dato forordning (EU) nr. 910/2014 får anvendelse (dvs. 30. juni 2016) skal utføres den dag forordningen får anvendelse (dvs. 1. juli 2016), som angitt i vedlegg J til ETSI TS 119 612.

KAPITTEL III

TILLITSLISTENES KONTINUITET

Sertifikater som skal meldes til Kommisjonen i samsvar med artikkel 4 nr. 2 i denne beslutning, skal oppfylle kravene i nr. 5.7.1 i ETSI TS 119 612, og skal utstedes på en slik måte at:

— det er minst tre måneder mellom deres endelige gyldighetsdatoer («ikke etter»),

— de er generert på nye nøkkelpar. Nøkkelpar som er brukt tidligere, skal ikke sertifiseres på nytt.

Dersom ett av de offentlige nøkkelsertifikatene som kan benyttes til å validere tillitslistens signatur eller segl, og som er meldt til Kommisjonen og offentliggjort i Kommisjonens sentrale liste over lenker, er utløpt, skal medlemsstatene:

— dersom den aktuelle offentlige tillitslisten er signert eller forseglet med en privat nøkkel hvis offentlige nøkkel er utløpt, straks utstede en ny tillitsliste som er signert eller forseglet med en privat nøkkel hvis meldte offentlige nøkkel ikke er utløpt,

— om nødvendig generere nye nøkkelpar som kan benyttes til å signere eller forsegle tillitslistene, og generere de motsvarende offentlige nøkkelsertifikatene,

— umiddelbart gi Kommisjonen melding om den nye listen over offentlige nøkkelsertifikater som motsvarer de private nøklene som kan benyttes til å signere eller forsegle tillitslisten.

Dersom en av de private nøklene som motsvarer ett av de offentlige nøkkelsertifikater som kan benyttes til å validere tillitslistens signatur eller segl, og som er meldt til Kommisjonen og offentliggjort i Kommisjonens sentrale liste over lenker, svekkes eller deaktiveres, skal medlemsstatene:

— straks utstede en ny tillitsliste som er signert eller forseglet med en sikker privat nøkkel dersom den offentliggjorte tillitslisten er signert eller forseglet med en svekket eller deaktivert nøkkel,

— om nødvendig generere nye nøkkelpar som kan benyttes til å signere eller forsegle tillitslistene, og generere de motsvarende offentlige nøkkelsertifikatene,

— umiddelbart gi Kommisjonen melding om den nye listen over offentlige nøkkelsertifikater som motsvarer de private nøklene som kan benyttes til å signere eller forsegle tillitslisten.

Dersom alle de private nøklene som motsvarer de offentlige nøkkelsertifikatene som kan benyttes til å validere tillitslistens signatur, og som er meldt til Kommisjonen og offentliggjort i Kommisjonens sentrale liste over lenker, svekkes eller deaktiveres, skal medlemsstatene:

— generere nye nøkkelpar som kan benyttes til å signere eller forsegle tillitslistene, og generere de motsvarende offentlige nøkkelsertifikatene,

— straks utstede en ny tillitsliste som er signert eller forseglet med en av disse private nøklene, og hvis motsvarende offentlige nøkkelsertifikat skal meldes,

— umiddelbart gi Kommisjonen melding om den nye listen over offentlige nøkkelsertifikater som motsvarer de private nøklene som kan benyttes til å signere eller forsegle tillitslisten.

KAPITTEL IV

SPESIFIKASJONER FOR TILLITSLISTEN I ET FORMAT SOM KAN LESES AV MENNESKER

Når det opprettes og offentliggjøres en tillitsliste i et format som kan leses av mennesker, skal den foreligge som et PDF-dokument i samsvar med ISO

32000([6]), som skal formateres i samsvar med profilen PDF/A (ISO 19005([7]).

Innholdet i den PDF/A-baserte tillitslisten i et format som kan leses av mennesker, skal oppfylle følgende krav:

— strukturen i dette formatet skal avspeile den logiske modellen som er beskrevet i TS 119 612,

— alle felt skal vises, med følgende opplysninger:

  — feltets tittel (f.eks. «*Service type identifier*»),

  — feltets verdi (f.eks. «http://uri.etsi.org/TrstSvc/Svctype/CA/QC}}»),

  — betydningen (beskrivelse) av feltets verdi, når det er relevant (f.eks. *«En sertifikatgenereringstjeneste som generer og signerer kvalifiserte sertifikater basert på identitet og andre egenskaper som er verifisert av de relevante registreringstjenestene.»*),

  — flere versjoner av naturlig språk som oppført i tillitslisten, når det er relevant,

— følgende felt og tilhørende verdier for digitale sertifikater([8]) skal som et minimum, dersom de forekommer i feltet «Service digital identity», vises i formatet som kan leses av mennesker:

  — versjon

  — sertifikatets serienummer

  — signaturalgoritme

  — utsteder – alle relevante, egne navnefelt

  — gyldighetstid

  — bruker – alle relevante, egne navnefelt

  — offentlig nøkkel

  — identifikator for myndighetsnøkkel

  — identifikator for brukernøkkel

  — nøkkelbruk

  — utvidet nøkkelbruk

  — sertifikatpolicy – alle identifikatorer og kvalifikatorer for policy

  — kartlegging av policy

  — alternativt brukernavn

  — brukerens katalogattributter

  — grunnleggende begrensninger

  — policybegrensninger

  — CRL-distribusjonspunkter([9])

  — myndighetens tilgang til opplysninger

  — brukerens tilgang til opplysninger

([6]) ISO 32000-1:2008: Dokumentstyring – PDF-format – Del 1: PDF 1.7

([7]) ISO 19005-2:2011: Dokumentstyring – filformat for elektroniske dokumenter til langtidsoppbevaring – Del 2: Bruk av ISO 32000-1 (PDF/A-2)

([8]) 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)

([9]) RFC 5280: internet X.509 PKI Certificate and CRL Profile

— merknader til kvalifisert sertifikat([10])

— hash-algoritme

— sertifikatets hash-verdi

— formatet som kan leses av mennesker, skal være lett å skrive ut,

— formatet som kan leses av mennesker, skal signeres eller forsegles av ordningens operatør i samsvar med avansert PDF-signatur som angitt i artikkel 1 og 3 i kommisjonens gjennomføringsbeslutning (EU) 2015/1505.

([10]) RFC 3739: internet X.509 PKI: Qualified Certificates Profile

VEDLEGG II

MAL FOR MEDLEMSSTATENES MELDINGER

Opplysningene som medlemsstatene skal melde i henhold til artikkel 4 nr. 1 i denne beslutning, skal inneholde følgende opplysninger, og eventuelle endringer av dem:

1) Medlemsstat, ved å benytte ISO 3166-1([11]) Alfa2-koder, med følgende unntak:

   a) Landkoden for Det forente kongerike skal være «UK».

   b) Landkoden for Hellas skal være «EL».

2) Organet/organene som har ansvar for å utarbeide, ajourføre og offentliggjøre tillitslisten i et format som er egnet for automatisert behandling, og i et format som kan leses av mennesker,

   a) navnet på ordningens operatør: opplysningene som gis skal være identiske – også med hensyn til store og små bokstaver – med verdien «Scheme operator name» i tillitslisten, og på like mange språk som i tillitslisten,

   b) valgfrie opplysninger til intern bruk i Kommisjonen, brukes bare når det er behov for å kontakte det relevante organet (vil ikke bli offentliggjort i EFs sammenstilte liste over tillitslister):

      — adresse til ordningens operatør,

      — kontaktopplysninger for en eller flere ansvarlige personer (navn, telefon, e-postadresse).

3) Stedet der tillitslisten offentliggjøres i et format som er egnet for automatisert behandling (*stedet der den aktuelle tillitslisten er offentliggjort*).

4) Eventuelt stedet der tillitslisten offentliggjøres i et format som kan leses av mennesker (*stedet der den aktuelle tillitslisten er offentliggjort*). Dersom en tillitsliste i et format som kan leses av mennesker ikke lenger offentliggjøres, skal det opplyses om dette.

5) De offentlige nøkkelsertifikatene som motsvarer de private nøklene som kan benyttes til å signere eller forsegle tillitslisten i formatet som er egnet for automatisert behandling, og tillitslisten i formatet som kan leses av mennesker: disse sertifikatene skal sendes inn som DER-sertifikater kodet som *Privacy Enhanced Mail Base64*. Ved melding om endring skal det tilføyes ytterligere opplysninger dersom et nytt sertifikat skal erstatte et bestemt sertifikat i Kommisjonens liste, og dersom det meldte sertifikatet skal føyes til det eller de eksisterende, uten at noen av dem erstattes.

6) Dato for innsending av opplysninger meldt i henhold til i nr. 1)–5).

Opplysninger meldt i samsvar med nr. 1, nr. 2 bokstav a), nr. 3, nr. 4 og nr. 5, skal føres opp i EFs sammenstilte liste over tillitslister, og erstatter tidligere meldte opplysninger i denne sammenstilte listen.

([11]) ISO 3166-1: «Koder for presentasjon av navn på land og deres underinndeling — del 1: Landkoder»: