Dette dokument er et dokumentationsredskab, og institutionerne påtager sig intet ansvar herfor

►**B** ►**C1** **KOMMISSIONENS BESLUTNING**

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

(meddelt under nummer K(2009) 7806)

(EØS-relevant tekst)

(2009/767/EF) ◄

(EUT L 274 af 20.10.2009, s. 36)

Ændret ved:

		Tidende		
		nr.	side	dato
►**M1**	Kommissionens afgørelse 2010/425/EU af 28. juli 2010	L 199	30	31.7.2010

Berigtiget ved:

►**C1** Berigtigelse, EUT L 299 af 14.11.2009, s. 18 (2009/767/EF)
►**C2** Berigtigelse, EUT L 4 af 7.1.2011, s. 6 (2009/767/EF)

▼B
▼C1

KOMMISSIONENS BESLUTNING

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

(meddelt under nummer K(2009) 7806)

(EØS-relevant tekst)

(2009/767/EF)

KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER HAR —

under henvisning til traktaten om oprettelse af Det Europæiske Fællesskab,

under henvisning til Europa-Parlamentets og Rådets direktiv 2006/123/EF af 12. december 2006 om tjenesteydelser i det indre marked ([1]), særlig artikel 8, stk. 3, og

ud fra følgende betragtninger:

(1) De forpligtelser vedrørende administrativ forenkling, som medlemsstaterne pålægges i henhold til kapitel II i direktiv 2006/123/EF, særlig artikel 5 og 8, omfatter en forpligtelse til at forenkle procedurer og formaliteter i forbindelse med adgang til og udøvelse af en servicevirksomhed og en forpligtelse til at sikre, at tjenesteudbyderne let kan afvikle sådanne procedurer og formaliteter på afstand og ad elektronisk vej ved hjælp af »kvikskranker«.

(2) Det skal være muligt at afvikle procedurer og formaliteter ved hjælp af »kvikskranker« på tværs af medlemsstaternes grænser, jf. artikel 8 i direktiv 2006/123/EF.

(3) For at opfylde forpligtelsen til at forenkle procedurer og formaliteter og til at lette den grænseoverskridende anvendelse af »kvikskrankerne« bør elektroniske procedurer benytte sig af enkle løsninger, også for så vidt angår anvendelse af elektroniske signaturer. I tilfælde, hvor et højt sikkerhedsniveau eller ligeværdighed med en håndskrevet underskrift efter en passende risikovurdering af de konkrete procedurer og formaliteter skønnes at være nødvendig, kan tjenesteudbyderne i forbindelse med visse procedurer og formaliteter afkræves en avanceret elektronisk signatur, som er baseret på et kvalificeret certifikat med eller uden et sikkert signaturgenereringssystem.

([1]) EUT L 376 af 27.12.2006, s. 36.

▼C1

(4) Fællesskabsrammen for e-signaturer blev fastlagt i Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer ([1]). For at lette den grænseoverskridende anvendelse af avancerede elektroniske signaturer, som er baseret på et kvalificeret certifikat, bør tilliden til disse elektroniske signaturer forbedres, uanset i hvilken medlemsstat underskriveren eller den certificeringstjenesteudbyder, der udsteder det kvalificerede certifikat, er etableret. Dette vil kunne opnås ved at sikre en lettere adgang i en pålidelig form til de oplysninger, som er nødvendige for at validere de elektroniske signaturer, herunder især oplysninger om certificeringstjenesteudbydere, som overvåges/akkrediteres i en medlemsstat, og de udbudte tjenesteydelser.

(5) Det skal sikres, at medlemsstaterne offentliggør disse oplysninger ved hjælp af en fælles skabelon, således at det bliver lettere at anvende dem og sikre en passende detaljegrad, der gør det muligt for modtagerne at validere den elektroniske signatur —

VEDTAGET FØLGENDE BESLUTNING:

Artikel 1

Anvendelse og accept af elektroniske signaturer

1. Hvis det er begrundet ud fra en passende vurdering af de relevante risici og i overensstemmelse med artikel 5, stk. 1 og 3, i direktiv 2006/123/EF, kan medlemsstaterne med henblik på afvikling af visse procedurer og formaliteter gennem de i artikel 8 i direktiv 2006/123/EF omhandlede kvikskranker kræve, at tjenesteydelsesudbyderen anvender avancerede elektroniske signaturer, som er baseret på et kvalificeret certifikat med eller uden et sikkert signaturgenereringssystem, jf. definitionen og bestemmelserne i direktiv 1999/93/EF.

2. Medlemsstaterne accepterer eventuelle avancerede elektroniske signaturer, som er baseret på et kvalificeret certifikat med eller uden et sikkert signaturgenereringssystem med henblik på afvikling af de i stk. 1 nævnte procedurer og formaliteter, uden at det berører medlemsstaternes mulighed for at begrænse denne accept til avancerede elektroniske signaturer, som er baseret på et kvalificeret certifikat og er genereret af et sikkert signaturgenereringssystem, såfremt dette er i overensstemmelse med den i stk. 1 omhandlede risikoanalyse.

3. Medlemsstaterne må ikke gøre accepten af avancerede elektroniske signaturer, som er baseret på et kvalificeret certifikat med eller uden et sikkert signaturgenereringssystem, betinget af krav, som skaber hindringer for tjenesteydelsesudbydernes anvendelse af elektroniske procedurer gennem kvikskranker.

([1]) EFT L 13 af 19.1.2000, s. 12.

▼C1

4. Uanset stk. 2 kan medlemsstaterne acceptere andre elektroniske signaturer end avancerede elektroniske signaturer, som er baseret på et kvalificeret certifikat med eller uden et sikkert signaturgenereringssystem.

Artikel 2

Oprettelse, vedligeholdelse og offentliggørelse af positivlister

1. Hver medlemsstat opretter, vedligeholder og offentliggør i overensstemmelse med de tekniske forskrifter i bilaget en »positivliste«, som indeholder minimumsoplysninger om overvågede/akkrediterede certificeringstjenesteudbydere, der udsteder kvalificerede certifikater til offentligheden.

▼M1

2. Medlemsstaterne udarbejder og offentliggør både en menneskeligt læsbar og en maskinelt læsbar udgave af positivlisten i overensstemmelse med forskrifterne i bilaget.

2a. Medlemsstaterne underskriver den maskinelt læsbare udgave af positivlisten elektronisk og offentliggør som minimum den menneskeligt læsbare udgave af positivlisten gennem en sikker kommunikationsforbindelse for at sikre dens autenticitet og integritet.

3. Medlemsstaterne giver Kommissionen følgende oplysninger:

a) det eller de organer, der er ansvarlige for oprettelsen, vedligeholdelsen og offentliggørelsen af de menneskeligt og maskinelt læsbare udgaver af positivlisten

b) de steder, hvor de menneskeligt og maskinelt læsbare udgaver af positivlisten offentliggøres

c) den offentlige nøgle-kryptering, der anvendes til at etablere den sikre kommunikationsforbindelse, hvormed den menneskeligt læsbare udgave af positivlisten offentliggøres, eller, hvis den menneskeligt læsbare udgave af positivlisten underskrives elektronisk, den offentlige nøgle-kryptering, der anvendes til underskrivelse

d) den offentlige nøgle-kryptering, der anvendes til at underskrive den maskinelt læsbare udgave af positivlisten elektronisk

e) enhver ændring af oplysningerne i litra a) til d).

4. Kommissionen stiller de i stk. 3 nævnte oplysninger, der indgives af medlemsstaterne, til rådighed for de øvrige medlemsstater gennem en sikker kommunikationsforbindelse til en godkendt webserver, både i en menneskeligt læsbar udgave og en underskrevet maskinelt læsbar udgave.

▼C1

Artikel 3

Anvendelse

Denne beslutning finder anvendelse fra den 28. december 2009.

Artikel 4

Adressater

Denne beslutning er rettet til medlemsstaterne.

▼C1

BILAG

TEKNISKE FORSKRIFTER FOR DEN FÆLLES SKABELON FOR »POSITIVLISTEN OVER OVERVÅGEDE/AKKREDITEREDE CERTIFICERINGSTJENESTEUDBYDERE«

FORORD

1. **Generelt**

Formålet med den fælles skabelon til medlemsstaternes »positivliste over overvågede/akkrediterede certificeringstjenesteudbydere« er at indføre en fælles metode for de enkelte medlemsstaters afgivelse af oplysninger om overvågnings/akkrediteringsstatus for certificeringstjenesterne fra de certificeringstjenesteudbydere ([1]) (CSP), som overvåges/akkrediteres for overholdelse af de relevante bestemmelser i direktiv 1999/93/EF. Dette omfatter afgivelse af historiske oplysninger om overvågnings/akkrediteringsstatus for de overvågede/akkrediterede certificeringstjenester.

De obligatoriske oplysninger i positivlisten (TL) skal omfatte et minimum af oplysninger om overvågede/akkrediterede certificeringstjenesteudbydere (CSP), som udsteder kvalificerede certifikater (QC) ([2]) i overensstemmelse med bestemmelserne i direktiv 1999/93/EF (artikel 3, stk. 3, artikel 3, stk. 2 og artikel 7, stk. 1, litra a), herunder oplysninger om QC, som understøtter en elektronisk signatur, samt hvorvidt denne signatur genereres af et sikkert signaturgenereringssystem (SSCD) ([3]).

Yderligere oplysninger om andre overvågede/akkrediterede CSP'er, som ikke udsteder QC'er, men udbyder tjenesteydelser, som vedrører elektroniske signaturer (f.eks. en CSP, der udbyder tidsstemplingstjenester og udsteder tidsstemplingstokens, en CSP, der udsteder ikke-kvalificerede certifikater, osv.) kan medtages i positivlisten på nationalt plan på frivillig basis. Disse oplysninger har hovedsageligt til formål at støtte valideringen af kvalificerede elektroniske signaturer (QES) og avancerede elektroniske signaturer (AdES) ([4]), som understøttes af et kvalificeret certifikat ([5]) ([6]).

Den foreslåede skabelon er kompatibel med en implementering baseret på forskrifterne i ETSI TS 102 231 ([7]), som anvendes i forbindelse med sådanne listers oprettelse, offentliggørelse, placering, adgang, autentifikation og pålidelighed.

([1]) Som defineret i artikel 2, stk. 11, i direktiv 1999/93/EF.
([2]) Som defineret i artikel 2, stk. 10, i direktiv 1999/93/EF.
([3]) Som defineret i artikel 2, stk. 6, i direktiv 1999/93/EF.
([4]) Som defineret i artikel 2, stk. 2, i direktiv 1999/93/EF.
([5]) For en AdES, der understøttes af et QC, anvendes i dette dokument akronymet »$AdES_{QC}$«.
([6]) Bemærk, at der findes en række elektroniske tjenesteydelser, som er baseret på simple AdES, hvis anvendelse på tværs af grænserne også ville blive lettere, forudsat at de understøttende certificeringstjenester (f.eks. udstedelse af ikke-kvalificerede certifikater) indgår i de overvågede/akkrediterede tjenesteydelser, som er omfattet af den frivillige oplysningsdel af medlemsstatens positivliste.
([7]) ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

2. **Retningslinjer for redigering af angivelser i TL**

2.1. *En TL, der fokuserer på overvågede/akkrediterede certificeringstjenester*

Relevante certificeringstjenester og certificeringstjenesteudbydere på en enkelt liste

En medlemsstats positivliste defineres som »overvågnings/-akkrediteringsstatuslisten for certificeringstjenester fra certificeringstjenesteudbydere, som overvåges/akkrediteres af den pågældende medlemsstat for overholdelse af de relevante bestemmelser i direktiv 1999/93/EF«.

En sådan positivliste skal omfatte:

— alle certificeringstjenesteudbydere, jf. definitionen i artikel 2, stk. 11, i direktiv 1999/93/EF, dvs. »et organ eller en fysisk eller juridisk person, der udsteder certifikater eller udbyder andre tjenesteydelser i forbindelse med elektroniske signaturer«

— som overvåges/akkrediteres for overholdelse af de relevante bestemmelser i direktiv 1999/93/EF.

Ifølge definitionerne og bestemmelserne i direktiv 1999/93/EF, navnlig vedrørende de relevante CSP'ere og deres overvågningssystemer/frivillige akkrediteringssystemer, findes der to slags CSP'ere, nemlig CSP'ere, som udsteder QC'er til offentligheden (CSP_{QC}) og CSP'ere, der ikke udsteder QC'er til offentligheden, men udbyder »andre (understøttende) tjenesteydelser i forbindelse med elektroniske signaturer«:

— **CSP'ere, der udsteder QC'er:**

  — De skal overvåges af den medlemsstat, hvori de er etableret (hvis de er etableret i en medlemsstat), og kan også akkrediteres for overholdelse af bestemmelserne i direktiv 1999/93/EF, herunder kravene i bilag I (krav til QC) og i bilag II (krav til CSP'ere, der udsteder QC'er). CSP'ere, der udsteder QC'er, som er akkrediteret i en medlemsstat, skal stadig være omfattet af den pågældende medlemsstats relevante overvågningssystem, medmindre de ikke er etableret i denne medlemsstat.

  — Det relevante »overvågningssystem« (henholdsvis »den frivillige akkrediteringsordning«) er defineret og skal opfylde de relevante krav i direktiv 1999/93/EF, især artikel 3, stk. 3, artikel 8, stk. 1, artikel 11, betragtning 13 (henholdsvis artikel 2, stk. 13, artikel 3, stk. 2, artikel 7, stk. 1, litra a), artikel 8, stk. 1, artikel 11, betragtning 4 og betragtning 11-13).

— **CSP'ere, der ikke udsteder QC'er**

  — Disse kan være omfattet af en »frivillig akkrediteringsordning« (jf. definitionen og bestemmelserne i direktiv 1999/93/EF) og/eller en nationalt defineret anerkendt godkendelsesordning, som gennemføres på nationalt plan med henblik på overvågning af overholdelse af direktivets bestemmelser og eventuelt af nationale bestemmelser om levering af certificeringstjenester (som omhandlet i direktivets artikel 2, stk. 11).

  — Nogle af de fysiske eller binære (logiske) genstande, der genereres eller udstedes som følge af leveringen af en certificeringstjeneste, kan være berettiget til en særlig »kvalifikation«, fordi de overholder nationalt fastsatte bestemmelser og krav, men betydningen af en sådan »kvalifikation« vil sandsynligvis være begrænset udelukkende til det nationale plan.

▼C1

En medlemsstats oplysninger i positivlisten skal omfatte et minimum af oplysninger om overvågede/akkrediterede CSP'ere, som udsteder kvalificerede certifikater til offentligheden i overensstemmelse med bestemmelserne i direktiv 1999/93/EF (artikel 3, stk. 3, artikel 3, stk. 2 og artikel 7, stk. 1, litra a), oplysninger om QC, som understøtter den elektroniske signatur, og om hvorvidt signaturen genereres af et sikkert signaturgenereringssystem.

Yderligere oplysninger om andre overvågede/akkrediterede tjenester fra CSP'ere, som ikke udsteder QC'er til offentligheden (f.eks. CSP'er, der udbyder tidsstemplingstjenester og udsteder tidsstemplingstokens, CSP'er, der udsteder ikke-kvalificerede certifikater, osv.) kan medtages på positivlisten på nationalt plan på frivillig basis.

Formålet med positivlisten er at:

— angive og levere pålidelige oplysninger om overvågnings/akkrediteringsstatus for certificeringstjenester fra certificeringstjenesteudbydere, som overvåges/-akkrediteres af den medlemsstat, som er ansvarlig for oprettelsen og vedligeholdelsen af listen med henblik på overholdelse af de relevante bestemmelser i direktiv 1999/93/EF

— lette valideringen af elektroniske signaturer, der understøttes af de i listen angivne overvågede/akkrediterede certificeringstjenester fra de CSP'ere, der er angivet i listen.

Et enkelt værdisæt vedrørende overvågnings/akkrediteringsstatus

Der skal oprettes og vedligeholdes en enkelt TL pr. medlemsstat for at angive overvågningsstatus og/eller akkrediteringsstatus for certificeringstjenester fra CSP'ere, som overvåges/akkrediteres af medlemsstaten.

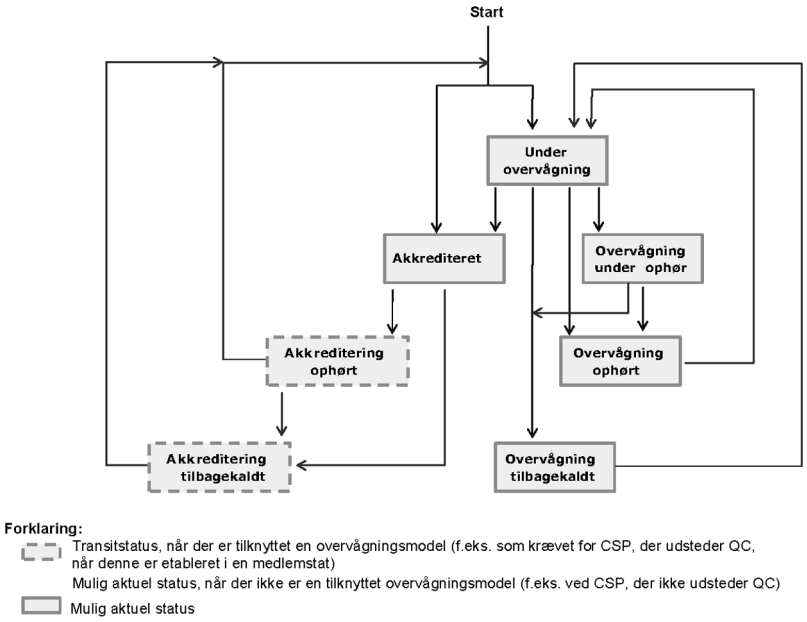
Det, at en tjeneste for tiden enten overvåges eller akkrediteres, indgår i dens aktuelle status. Desuden kan en overvågnings- eller akkrediteringsstatus være »igangværende«, »under ophør«, »ophørt« eller endda »tilbagekaldt«. Gennem sin levetid kan den samme certificeringstjeneste overgå fra overvågningsstatus til akkrediteringsstatus og omvendt ([1]).

Figur 1 neden for viser en enkelt certificeringstjenestes forventede bevægelse mellem de mulige overvågnings/akkrediteringsstatusser:

([1]) F.eks. kan en certificeringstjenesteudbyder, der er etableret i en medlemsstat, og som udbyder en certificeringstjeneste, som oprindeligt blev kontrolleret af medlemsstaten (tilsynsorgan), efter et bestemt tidsrum beslutte at indføre en frivillig akkreditering for den for tiden overvågede certificeringstjeneste. Modsat kan en certificeringsudbyder i en anden medlemsstat f.eks. af forretningsmæssige og/eller økonomiske årsager beslutte ikke at stoppe en akkrediteret certificeringstjeneste, men at flytte den fra akkrediteringsstatus til kontrolstatus.

▼C1

Forventet statusflow for overvågning/akkreditering af en enkelt CSP-tjeneste



Figur 1

En certificeringstjeneste, der udsteder QC'er skal overvåges (hvis den er etableret i en medlemsstat) og kan være frivilligt akkrediteret. Når den er opført i positivlisten, kan en sådan tjenestes statusværdi have en hvilken som helst af de oven for angivne statusværdier som »aktuel statusværdi«. Det skal dog bemærkes, at »akkreditering ophørt« og »akkreditering tilbagekaldt« begge kun må være »transitstatusværdier« i forbindelse med CSPQC-tjenester, som er etableret i en medlemsstat, idet sådanne tjenester som hovedregel skal overvåges (selv, når de ikke er/ikke længere er akkrediteret).

Medlemsstater, som etablerer eller har etableret en nationalt defineret anerkendt godkendelsesordning, der gennemføres på nationalt plan for at overvåge, at tjenester fra CSP'ere, der ikke udsteder QC'er, overholder bestemmelserne i direktiv 1999/93/EF og i eventuelle nationale bestemmelser om levering af certificeringstjenester (i betydningen i direktivets artikel 2, stk. 11), skal kategorisere sådanne godkendelsesordninger under følgende to kategorier:

— »frivillig akkreditering« som defineret og fastsat i direktiv 1999/93/EF (artikel 2, stk. 13, artikel 3, stk. 2, artikel 7, stk. l 1, artikel 8, stk. 1, artikel 11, betragtning 4 og 11-13)

— »overvågning« som påkrævet i direktiv 1999/93/EF og gennemført ved nationale bestemmelser og krav i overensstemmelse med nationale love.

▼C1

På samme måde kan en certificeringstjeneste, der ikke udsteder QC'er, overvåges eller frivilligt akkrediteres. Når den er opført i positivlisten, kan en sådan tjenestes statusværdi have en hvilken som helst af de oven for angivne statusværdier som »aktuel statusværdi« (se figur 1).

Positivlisten skal indeholde oplysninger om den/de pågældende overvågningssystem/akkrediteringsordning(er), herunder især:

— oplysninger om overvågningssystemet, som finder anvendelse på enhver CSP_{QC}

— eventuelle oplysninger om den nationale »frivillige akkrediteringsordning«, der finder anvendelse på enhver CSP_{QC}

— eventuelle oplysninger om det overvågningssystem, der finder anvendelse på enhver CSP, der ikke udsteder QC'er

— eventuelle oplysninger om den nationale »frivillige akkrediteringsordning«, der finder anvendelse på enhver CSP, der ikke udsteder QC'er.

De sidste to oplysninger er af afgørende betydning for, at afhængige parter kan vurdere kvaliteten og sikkerhedsniveauet ved sådanne overvågningssystemer/akkrediteringsordninger, der anvendes på nationalt plan for CSP'er, der ikke udsteder QC'er. Når der angives oplysninger om overvågnings/akkrediteringsstatus i positivlisten med hensyn til tjenester fra CSP'ere, der ikke udsteder QC'er, skal ovennævnte oplysninger angives på TL-niveau ved anvendelse af »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 valgfri specifikke oplysninger leveret af en medlemsstat) og »TSL policy/legal notice« (punkt 5.3.11 — en fælles tekst for alle medlemsstater, der henviser til direktiv 1999/93/EF, samtidig med at hver medlemsstat har mulighed for at tilføje medlemsstatsspecifik tekst/henvisninger). Yderligere »kvalifikationsoplysninger« defineret i forbindelse med nationale overvågnings/akkrediteringssystemer for CSP'ere, der ikke udsteder QC'er, kan i det omfang det er relevant angives ved tjenesteniveau (f.eks. for at skelne mellem flere kvalitets/sikkerhedsniveauer ved at anvende udvidelsen »additionalServiceInformation« (punkt 5.8.2) som led i »Service information extension« (punkt 5.5.9). Yderligere oplysninger om de tilhørende tekniske forskrifter findes i de detaljerede forskrifter i kapitel I.

Selv om flere organer i en medlemsstat kan være ansvarlige for overvågning og akkreditering af certificeringstjenester i den pågældende medlemsstat, forventes det, at der kun bruges én indgang for hver enkelt certificeringstjeneste (identificeret ved dens »Service digital identity« i henhold til ETSI TS 102 231 ([1])), og at dens overvågnings/akkrediteringsstatus opdateres i overensstemmelse hermed. Betydningen af de oven for beskrevne statusser er angivet i punkt 5.5.4 i de detaljerede tekniske forskrifter i kapitel I.

2.2. *TL-angivelser med henblik på at lette valideringen af QES og $AdES_{QC}$*

Det vigtigste i forbindelse med oprettelsen af positivlisten er etableringen af dens obligatoriske del, nemlig »List of services« pr. CSP, der udsteder QC'er, således at den korrekt afspejler den præcise udstedelsessituation for hver af disse QC-udstedende certificeringstjenester og sikrer, at oplysningerne i hver indgang er tilstrækkelige til at lette valideringen af QES og $AdES_{QC}$ (i kombination med indholdet i QC-slutenheden udstedt af CSP'en i forbindelse med den certificeringstjeneste, der er angivet i indgangen).

([1]) ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

For så vidt der ikke findes nogen fuldt interoperabel og grænseoverskridende profil for QC'et, kan de påkrævede oplysninger omfatte andre oplysninger end »Service digital identity« i en enkelt (Root) CA, især oplysninger, der angiver QC-status for det udstedte certifikat, og om, hvorvidt de understøttede signaturer er genereret med et SSCD. Det organ i en medlemsstat, som er udpeget til at oprette, redigere og vedligeholde TL (dvs. operatøren for ordningen i henhold til ETSI TS 102 231), skal derfor tage højde for indholdet i den aktuelle profil og det aktuelle certifikat i hver udstedt QC for CSP_{QC}, der er omfattet af TL.

Ideelt set bør hvert udstedt QC indeholde den i ETSI definerede erklæring om QcCompliance ([1]), når det hævdes, at der er tale om et QC, og bør indeholde den i ETSI definerede QcSSCD-erklæring, når det hævdes, at det understøttes af en SSCD til generering af elektroniske signaturer, og/eller at hver udstedt QC indeholder en af de QCP/QCP + certificate policy Object Identifiers (OIDs), som er defineret i ETSI TS 101 456 ([2]). QC-udstedende certificeringstjenesteudbyderes anvendelse af forskellige referencestandarder, den høje fortolkningsgrad af disse standarder samt manglende kendskab til en række normative tekniske forskrifter eller standarder og til den forrang disse har, har medført forskelle i det faktiske indhold i de QC'er, der for tiden udstedes (f.eks. hvorvidt de af ETSI definerede QcStatements anvendes eller ej), hvilket betyder, at modtagerparterne ikke uden videre kan have tillid til underskriverens certifikat (og dertil hørende kæde/sti) for i det mindste via en maskinaflæselig metode at kunne vurdere, hvorvidt certifikatet til understøttelse af en elektronisk signatur hævdes at være et QC, og hvorvidt det er knyttet til et SSCD, hvorigennem den elektroniske signatur er blevet genereret.

Ved at udfylde felterne »Service type identifier« (»Sti«), »Service name« (»Sn«), og »Service digital identity« (»Sdi«) ([3]) med de oplysninger, der er angivet i feltet »Service information extensions« (»Sie«), kan den foreslåede fælles TL-skabelon fuldt ud definere en specifik type kvalificeret certifikat udstedt af en på listen anført CSP-certificeringstjeneste, der udsteder QC'er, og give oplysninger om, hvorvidt det er understøttet af et SSCD (når sådanne oplysninger ikke findes i det udstedte QC). Der er naturligvis tilknyttet en specifik oplysning »Service current status« (»Scs«) til denne angivelse. Dette er illustreret i figur 2 nedenfor.

Når en tjeneste optages på listen ved blot at angive »Sdi« af (Root) CA betyder det, at det sikres (af den QC-udstedende CSP, men også af det organ, som er ansvarlig for overvågningen/akkrediteringen af den pågældende CSP), at et eventuelt slutenhedscertifikat under dette (Root) CA (hierarki) indeholder tilstrækkeligt mange ETSI-definerede og maskinprocesserbare oplysninger til at vurdere, hvorvidt det er et QC, og hvorvidt det er understøttet af et SSCD. Såfremt sidstnævnte påstand ikke er sand (f.eks. hvis der ikke er nogen ETSI-standardiseret maskinprocesserbar angivelse på QC'et af, hvorvidt det understøttes af et SSCD) kan det ved blot at angive »Sdi« for dette (Root) CA kun antages, at QC'er udstedt under dette (Root) CA-hierarki ikke er understøttet af et SSCD. For at betragte disse QC'er som værende understøttet af et SSCD, skal »Sie« anvendes til at angive denne kendsgerning (dette indikerer også, at det er garanteret af den QC-udstedende CSP og overvåget/akkrediteret af henholdsvis overvågningsorganet eller akkrediteringsorganet).

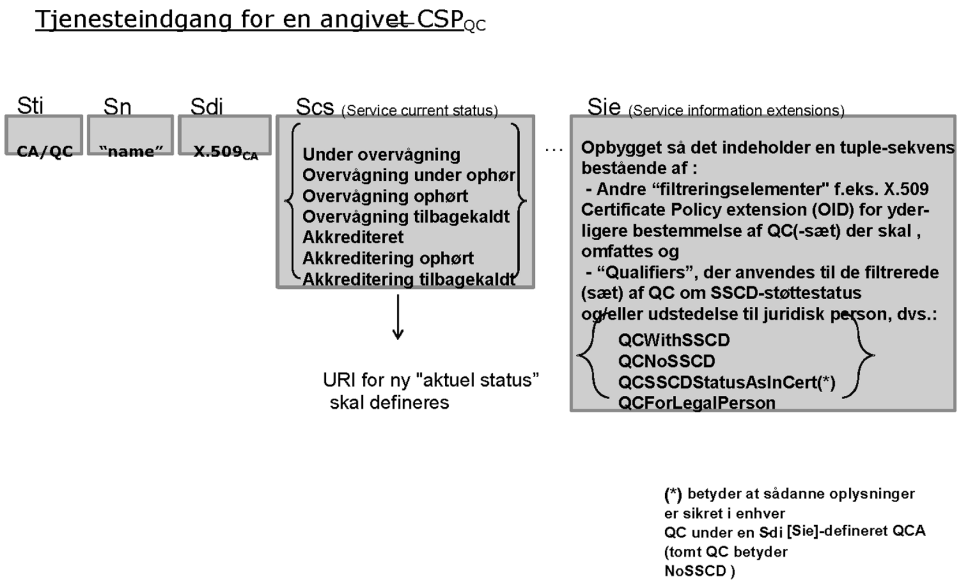
([1]) Jf. ETSI TS 101 862 — Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile

([2]) ETSI TS 101 456 — Electronic Signature and Infrastructures (ESI); Policy-krav til certificeringscentre, der udsteder kvalificerede certifikater.

([3]) Dvs. som minimum en et X.509 v3-certifikat fra det udstedende QCA eller fra et øvre CA i certificeringsstien.

▼C1

Generelle principper – Redigeringsregler – CSP_{QS}-indgange (angivne tjenester)



Figur 2

Tjenesteindgang i TL implementeret i TTS-format for en i listen angivet QC-udstedende CSP

Nærværende tekniske forskrifter for den fælles skabelon for TL muliggør en kombination af fem hovedområder for oplysninger i tjenesteangivelsen:

— »Service type identifier« (»Sti«), der f.eks. identificerer en CA, som udsteder QC'er (CA/QC)

— »Service name« (»Sn«)

— »Service digital identity« (»Sdi«) — oplysninger, der identificerer en angivet tjeneste, f.eks. X.509v3-certifikatet (som minimum) for en CA, der udsteder QC'ere

— For CA/QC-tjenester eventuelt »Service information extensions« (»Sie«) — oplysninger, som gør det muligt at inkludere en sekvens af en eller flere tuples, hvor hver tuple angiver:

  — kriterier, der skal anvendes til yderligere identificering (filtrering) til præcisering af den under »Sdi« angivne certificeringstjeneste (dvs. sæt af kvalificerede certifikater), for hvilke der kræves/angives yderligere oplysninger med hensyn til SSCD-støtte (og/eller udstedelse til en juridisk person), og

  — relaterede oplysninger (»qualifiers«) om, hvorvidt denne yderligere identificerede tjenestes sæt af kvalificerede certifikater er understøttet af et SSCD, eller om disse relaterede oplysninger indgår i QC i en standardiseret maskinprocesserbar form og/eller oplysninger om, at sådanne QC'ere er udstedt til juridiske personer (normalt betragtes de kun som udstedt til fysiske personer).

▼C1

— Aktuelle status-oplysninger for denne tjenesteindgang med oplysninger om:

— Hvorvidt det er en overvåget eller akkrediteret tjeneste, og

— Selve overvågnings/akkrediteringsstatussen.

2.3. *Retningslinjer vedrørende redigering og brug af CSP_{QC}-tjenesteindgange*

De generelle redigeringsretningslinjer er:

1) Hvis det i forbindelse med en angivet tjeneste, som er identificeret at en »Sdi«, sikres (garanteret af CSP_{QC} og overvåget/akkrediteret af et overvågningsorgan (SB)/akkrediteringsorgan (AB), at et QC, som er understøttet af et SSCD, faktisk indeholder den i ETSI definerede erklæring om QcCompliance og faktisk indeholder QcSSCD-erklæringen og/eller QCP + Object Identifier (OID), er anvendelsen af en passende »Sdi« tilstrækkelig og »Sie«-feltet kan anvendes valgfrit og behøver ikke indeholde oplysninger om SSCD-støtte.

2) Hvis det i forbindelse med en angivet tjeneste, som er identificeret at en »Sdi«, sikres (garanteret af CSPQC og overvåget/akkrediteret af SB/AB), at en QC, som ikke er understøttet af et SSCD, faktisk indeholder enten erklæringen om QcCompliance og/eller QCP OID og ikke skal indeholde QcSSCD-erklæringen og/eller QCP + OID, er anvendelsen af en passende »Sdi« tilstrækkelig og »Sie«-feltet kan anvendes valgfrit og behøver ikke indeholde oplysninger om SSCD-støtte (hvilket vil sige, at det ikke er understøttet af et SSCD).

3) Hvis det i forbindelse med en angivet tjeneste, som er identificeret at en »Sdi«, sikres (garanteret af CSP_{QC} og overvåget/akkrediteret af SB/AB), at et QC faktisk indeholder QcCompliance-erklæringen og kun nogle af disse QC'er skal understøttes af SSCD'er (dette kan f.eks. differentieres af forskellige CSP-specifikke Certificate Policy OIDs eller gennem andre CSP-specifikke oplysninger i QC'et, uanset om de er direkte eller indirekte, maskinprocesserbare eller ikke), men HVERKEN indeholder QcSSCD-erklæringen ELLER ETSI QCP(+) OID, er anvendelsen af en passende »Sdi« muligvis ikke tilstrækkelig OG »Sie«-feltet skal anvendes til at angive udtrykkelige oplysninger om SSCD-støtte sammen med eventuelt udvidede oplysninger for at identificere det omfattede certifikatsæt. Dette vil sandsynligvis kræve medtagelse af forskellige »SSCD support information values« for samme »Sdi«, når »Sie«-feltet anvendes.

4) Hvis det i forbindelse med en angivet tjeneste, som er identificeret at en »Sdi«, sikres (garanteret af CSP_{QC} og overvåget/akkrediteret af SB/AB), at et QC ikke indeholder QcCompliance-erklæring, QCP OID, QcSSCD-erklæring, eller QCP + OID, men det sikres, at kun nogle af disse slutenhedscertifikater udstedt under denne »Sdi« skal være QC'er og/eller understøttet af SSCD'er (dette kan f.eks. differentieres af forskellige CSP_{QC}-specifikke Certificate Policy OIDs eller gennem andre CSP-specifikke oplysninger i QC'et, uanset om de er direkte eller indirekte, maskinprocesserbare eller ikke), vil anvendelsen af en passende »Sdi« ikke være tilstrækkelig OG »Sie«-feltet skal anvendes til at angive udtrykkelige oplysninger om SSCD-støtte. Dette vil sandsynligvis kræve medtagelse af forskellige »SSCD support information values« for samme »Sdi«, når »Sie«-feltet anvendes.

▼C1

Som et generelt princip skal der for en CSP, som er angivet i positivlisten, være én tjeneste for hvert enkelt X.509v3-certifikat for en certificerende tjeneste af CA/QC-typen, dvs. en certificeringscenter, som (direkte) udsteder QC'ere. Under visse omhyggeligt forudsete og nøje styrede forhold kan et overvågningsorgan/-akkrediteringsorgan i en medlemsstat beslutte at anvende X.509v3-certifikatet fra et Root eller Upper level QC (dvs. en certificeringscenter, som ikke direkte udsteder slutenhedskvalificerede certifikater, men som certificerer et hierarki af certificeringscentre ned til certificeringscentre, som udsteder QC'er til slutenheder) som »Sdi« for en enkelt indgang i listen over tjenester fra en angivet CSP. Følgerne (fordele og ulemper) ved at bruge et sådant X.509v3 Root CA eller Upper CA som »Sdi«-værdier for TL-tjenesteindgange skal nøje overvejes og godkendes af medlemsstaterne. Desuden skal medlemsstaterne, når de anvender denne tilladte undtagelse for det generelle princip, levere den nødvendige dokumentation for at lette etableringen af certificeringsstien og verifikationen.

De generelle redigeringsretningslinjer kan illustreres med følgende eksempel: I forbindelse med en CSP_{QC}, der anvender ét Root CA, hvorunder flere CA'er udsteder kvalificerede certifikater og ikke-kvalificerede certifikater, men for hvilke QC'erne faktisk kun indeholder QcCompliance-erklæringen og ingen angivelse af, om den understøttes af et SSCD, ville angivelsen af Root CA »Sdi« alene i henhold de oven for forklarede regler betyde, at ethvert QC, der udstedes under dette Root CA-hierarki, IKKE er understøttet af et SSCD. Hvis disse QC'er faktisk understøttes af et SSCD, anbefales det kraftigt at anvende QcSSCD-erklæringen i de QC'er, der udstedes fremover. I mellemtiden (indtil det sidste QC, som ikke indeholder disse oplysninger, er udløbet) bør TSL gøre brug af »Sdi«-feltet og den dermed forbundne »Qualifications«-udvidelse, f.eks. filtrering af certifikater gennem specifikke CSP_{QC}-definerede OID, som potentielt anvendes af CSPQC til at skelne mellem forskellige typer QC'er (hvoraf nogle er og andre ikke er understøttet af et SSCD) og inklusive udtrykkelig »SSCD support information« for sådanne filtrerede certifikater gennem anvendelse af »Qualifiers«.

De generelle retningslinjer for brug af elektroniske signaturapplikationer, -tjenester eller -produkter, som afhænger af TSL-implementering af en positivliste i overensstemmelse med de nuværende tekniske forskrifter, er som følger:

En »CA/QC«»Sti«-indgang (eller tilsvarende en CA/QC-indgang yderligere kvalificeret som værende en »RootCA/QC« gennem anvendelse af udvidelsen »Sie« additionalServiceInformation)

— angiver, at alle udstedte slutenhedscertifikater fra det »Sdi«-identificerede CA (tilsvarende inden for CA-hierarkiet begyndende med det »Sdi«-identificerede RootCA) er QC'er **forudsat**, at det i certifikatet hævdes at være dette gennem anvendelse af passende QcStatements (dvs. QcC, QcSSCD) og/eller ETSI-definerede QCP(+) OIDs (og dette sikres af overvågnings/-akkrediteringsorganet, jf. ovenstående »generelle redigeringsretningslinjer«)

Bemærk: Hvis der ikke findes nogen »Sdi«-»Qualification«, eller hvis et slutenhedscertifikat, som hævdes at være et QC, ikke er yderligere identificeret gennem en tilknyttet »Sdi«-indgang, overvåges/akkrediteres de maskinprocesserbare oplysninger, som findes i QC'et, for nøjagtighed. Det betyder, at anvendelsen (eller ikke-anvendelsen) af de passende QC-erklæringer (dvs. QcC, QcSSCD) og/eller ETSI-definerede QCP(+) OIDs garanteres at være i overensstemmelse med, hvad der hævdes i CSP_{QC}.

▼C1

— og HVIS der findes en »Sdi«- »Qualification«-oplysning, så skal de certifikater, som identificeres i tilgift til den generelle ovenstående fortolkningsregel gennem anvendelsen af denne »Sdi-«Qualification-indgang, som konstrueres ud fra princippet om en sekvens af filtre, der yderligere identificerer et sæt certifikater og leverer visse yderligere oplysninger vedrørende SSCD-støtte og/eller »juridisk person som genstand« (f.eks. certifikater, der indeholder specifik OID i certifikatpolitikudvidelsen og/eller har et »Key usage«-mønster og/eller filtreres gennem anvendelse af en specifik værdi, der skal forekomme i et specifikt certifikatfelt eller udvidelse, osv.) overvejes i overensstemmelse med følgende sæt »qualifiers«, som kompenserer for de manglende oplysninger i det tilsvarende QC, dvs.:

— for at angive SSCD-støtte:

  — »QCWithSSCD« — en kvalifikatorværdi, der betyder »QC understøttet af et SSCD«, eller

  — »QCNoSSCD« — en kvalifikatorværdi, der betyder »QC ikke understøttet af et SSCD«, eller

  — »QCSSCDStatusAsInCert« — kvalifikatorværdi, der betyder, at det er sikret, at oplysninger om SSCD-understøttelse er indeholdt i ethvert QC under »Sdi»-«Sie« angivne oplysninger i denne CA/QC-indgang

og/eller

— for at angive udstedelse til juridisk person:

  — »QCForLegalPerson« — en kvalifikatorværdi, der betyder »certifikat udstedt til juridisk person«.

2.4. *Tjenester, der understøtter »CA/QC«-tjenester, men ikke indgår i »CA/QC«»Sdi«*

De tilfælde, hvor CRL'er og OCSP-svar underskrives med nøgler, som ikke stammer fra et CA, der udsteder QC'er (CA/QC), bør også omfattes. Dette kan gøres ved at angive disse tjenester som sådan i TSL-implementeringen af TL (dvs. med en »service type identifier«, som yderligere kvalificeres af en »additionalServiceInformation«-udvidelse, der afspejler en OCSP eller en CRL-tjeneste som en del af leveringen af QC'er, f.eks. med henholdsvis tjenestetypen »OCSP/-QC« eller »CRL/QC«), eftersom disse tjenester kan betragtes som del af de overvågede/akkrediterede kvalificerede tjenester, der vedrører levering af QC-certificeringstjenester. Selvfølgelig skal OCSP-respondenter eller CRL-udstedere, hvis certifikater er underskrevet af CA'er i hierarkiet for en angiven CA/QC-tjeneste, betragtes som »valide« i overensstemmelse med den angivne CA/QC-tjenestes statusværdi.

En lignende bestemmelse kan anvendes for certificeringstjenester, der udsteder ikke-kvalificerede certifikater (af tjenestetypen »CA/PKC«) ved at bruge standard OCSP- og CRL-tjenestetyperne i ETSI TS 102 231.

Bemærk at TSL-implementeringen af TL SKAL omfatte tilbagekaldelsestjenester, når der ikke findes relaterede oplysninger i slutcertifikaters AIA-felt, eller når de ikke er underskrevet af en CA, som er en af de angivne CA'ere.

2.5. *Mod en interoperabel QC-profil*

Som hovedregel skal det så vidt muligt forsøges at forenkle (reducere) antallet af angivne tjenester (forskellige »Sdi'er«). Dette skal dog holdes op imod behovet for en korrekt identifikation af de tjenester, som er knyttet til udstedelse af QC'er og levering af de pålidelige oplysninger om, hvorvidt disse QC'er understøttes af et SSCD, når sådanne oplysninger ikke findes i det udstedte QC.

▼C1

Ideelt set bør anvendelsen af »Sie«-feltet og »Qualification«-udvidelsen være (nøje) afgrænset til de særlige tilfælde, som skal løses på denne måde, idet QC'er bør indeholde tilstrækkelige oplysninger med hensyn til den påståede kvalificerede status og den påståede understøttelse eller ikke-understøttelse af et SSCD.

Medlemsstaterne bør i videst muligt omfang gennemtvinge indførelse og anvendelse af interoperable QC-profiler.

3. **Opbygningen af den fælles skabelon til positivlisten**

Den foreslåede fælles skabelon til medlemsstaternes positivlister vil være opdelt i følgende oplysningskategorier:

1. Oplysninger om positivlisten og ordningen for udstedelse heraf.

2. En sekvens af felter med entydige identifikationsoplysninger om hver overvåget/akkrediteret CSP i ordningen (denne sekvens er valgfri, dvs. når den ikke anvendes, vil listen blive betragtet som tom, hvilket vil sige, at der ikke er nogen overvåget eller akkrediteret CSP i den pågældende medlemsstat, som falder under positivlistens anvendelsesområde).

3. For hver angivet CSP en sekvens af felter med entydig identifikation af en overvåget/akkrediteret certificeringstjeneste, som udbydes af den pågældende CSP (der skal være mindst én indgang i denne sekvens).

4. For hver optegnet overvåget/akkrediteret certificeringstjeneste: identifikation af tjenestens aktuelle og historiske status.

I forbindelse med en CSP, der udsteder QC'er, skal den entydige identifikation af en overvåget/akkrediteret certificeringstjeneste, som skal angives, tage højde for situationer, hvor der ikke foreligger tilstrækkelige oplysninger i det kvalificerede certifikat om dets kvalificerede status, dets potentielle SSCD-understøttelse og især i lyset af, at de fleste (kommercielle) CSP'er benytter sig af ét enkelt udstedende kvalificeret CA til at udstede flere typer af slutenhedscertifikater, uanset om disse er kvalificerede eller ikke-kvalificerede.

Antallet af optegnelser i listen pr. anerkendt CSP kan mindskes i det omfang der findes én eller flere »Upper« CA-tjenester, f.eks. i forbindelse med et kommercielt hierarki af CA'ere fra Root CA ned til udstedende CA'er. Selv i sådanne tilfælde skal princippet om at sikre en entydig forbindelse mellem en CSP_{QC}-certificeringstjeneste og det sæt af certifikater, der fremstår som identificerede QC'er, dog opretholdes og sikres.

1. *Oplysninger om positivlisten og ordningen for dens udstedelse*

Følgende oplysninger vil indgå i denne kategori:

— Et positivlistemærke (tag), der letter identifikationen af positivlisten under elektroniske søgninger og desuden bekræfter dens formål, når den er i en menneskeligt læsbar form.

— En identifikation af positivlistens format og version

— Positivlistens sekvensnummer (eller udgivelsesnummer)

— Typeoplysninger for positivlisten (f.eks. identifikation af, at denne positivliste indeholder oplysninger om overvågnings/akkrediteringsstatus for certificeringstjenester fra CSP'er, som overvåges/akkrediteres af den pågældende medlemsstat for overholdelse af bestemmelserne i direktiv 1999/93/EF).

▼C1

— Ejeroplysninger om positivlisten (f.eks. navn, adresse, kontaktoplysninger osv. for det medlemsstatsorgan, som er ansvarligt for oprettelse, sikker offentliggørelse og vedligeholdelse af positivlisten).

— Oplysninger om den/de pågældende overvågnings/akkrediteringsordninger, som positivlisten er knyttet til, herunder bl.a.:

  — det land, som den gælder for

  — oplysninger om eller henvisning til den placering, hvor oplysningerne om ordningen/ordningerne kan findes (ordningens model, regler, kriterier, gældende område, type osv.)

  — opbevaringsperiode for (historiske) oplysninger.

— Politik og/eller juridisk meddelelse, forpligtelser og ansvar i forbindelse med positivlisten

— Positivlistens udstedelsesdato og -tidspunkt og næste forventede ajourføring.

2. *Entydige identifikationsoplysninger om hver CSP, som er anerkendt under ordningen*

Disse oplysninger vil som minimum omfatte følgende:

— CSP-organets navn som anvendt i formelle juridiske registreringer (kan omfatte CSP-organisationens UID afhængigt af praksis i af medlemsstaten).

— CSP'ens adresse og kontaktoplysninger.

— Yderligere oplysninger om CSP'en enten direkte medtaget eller ved henvisning til en placering, hvorfra sådanne oplysninger kan downloades.

3. *For hver angivet CSP: en sekvens af felter med entydig identifikation af en certificeringstjeneste, som udbydes af den pågældende CSP og overvåges/akkrediteres inden for rammerne af direktiv 1999/93/EF*

Disse oplysninger vil som minimum omfatte følgende for hver certificeringstjeneste fra en angivet CSP:

— en identifikator for certificeringstjenestens type (f.eks. en identifikator, som angiver, at den overvågede/akkrediterede certificeringstjeneste fra CSP'en er et certificeringscenter, der udsteder QC'er)

— (handels)navn for den pågældende certificeringstjeneste

— en entydig unik identifikator for certificeringstjenesten

— yderligere oplysninger om certificeringstjenesten (f.eks. direkte medtaget eller medtaget ved henvisning til en placering, hvorfra sådanne oplysninger kan downloades, oplysninger om adgang til tjenesten)

— for CA/QC-tjenester: en valgfri sekvens af informations-»tuples«, hvor hver tuple angiver:

  i) kriterier, der skal anvendes til yderligere identificering (filtrering) til præcisering af den i »Sdi« identificerede certificeringstjeneste (dvs. sæt af kvalificerede certifikater), for hvilke der kræves/leveres yderligere oplysninger med hensyn til SSCD-støtte (og/eller udstedelse til en juridisk person) og

  ii) De dermed forbundne »qualifiers«, der giver oplysninger om, hvorvidt sættet af kvalificerede certifikater fra denne yderligere identificerede tjeneste er understøttet af et SSCD, og/eller sådanne QC'er er udstedt til juridiske personer (normalt betragtes de kun som udstedt til fysiske personer).

▼C1

4. *For hver optegnet certificeringstjeneste: identifikation af tjenestens aktuelle og historiske status.*

Disse oplysninger vil som minimum omfatte følgende:

— en identifikator for aktuel status

— startdato og -tidspunkt for den aktuelle status

— historiske oplysninger om denne status.

4. **Definitioner og forkortelser**

I dette dokument anvendes følgende definitioner og forkortelser:

Udtryk	Forkortelse	Definition
Certificeringstjenesteudbyder (Certification Service Provider)	CSP	Som defineret i artikel 2, stk. 11, i direktiv 1999/93/EF
Certificeringscenter (Certification Authority)	CA	Et CA er en CSP og kan anvende flere tekniske CA'ers private signeringsnøgler, der har hvert sit tilknyttede certifikat, til at udstede slutenhedscertifikater. Et CA er en myndighed, som en eller flere brugere har tillid til i forbindelse med generering og tildeling af certifikater. Eventuelt kan certificeringscentret generere brugernes nøgler [[ETSI TS 102 042]. CA'et anses for identificeret gennem de identifikationsoplysninger, der findes i udstederfeltet i det CA-certifikat, der vedrører (certificering af) den offentlige nøgle, og som CA faktisk anvender til udstedelse af enhedscertifikater. Et CA kan have flere signeringsnøgler. Hver enkelt CA-signeringsnøgle er identificeret af en unik identifikatordel i feltet Authority Key Identifier i CA's certifikat.
Certificeringscenter, der udsteder kvalificerede certifikater (Certification Authority issuing Qualified Certificates)	CA/QC	Et CA, som opfylder kravene i bilag II til direktiv 1999/93/EF, og udsteder kvalificerede certifikater, som opfylder kravene i bilag I i direktiv 1999/93/EF.
Certifikat	Certifikat	Som defineret i artikel 2, stk. 9, i direktiv 1999/93/EF
Kvalificeret certifikat (Qualified Certificate).	QC	Som defineret i artikel 2, stk. 10, i direktiv 1999/93/EF
Underskriver	Underskriver	Som defineret i artikel 2, stk. 3, i direktiv 1999/93/EF
Overvågning	Overvågning	»Overvågning« anvendes i overensstemmelse med betydningen i direktiv 1999/93/EF (artikel 3, stk. 3). I henhold til direktivet skal medlemsstaterne oprette et passende system, der muliggør overvågning af CSP'er, som er etableret på deres område og udsteder kvalificerede certifikater til offentligheden, og sikrer overvågning og opfyldelse af direktivets bestemmelser.
Frivillig akkreditering	Akkreditering	Som defineret i artikel 2, stk. 13, i direktiv 1999/93/EF
Positivliste (Trusted List)	TL	Betegner den liste, der angiver overvågnings/akkrediteringsstatus for certificeringstjenester fra certificeringstjenesteudbydere, som overvåges/akkrediteres af den pågældende medlemsstat for overholdelse af bestemmelserne i direktiv 1999/93/EF.

▼C1

Udtryk	Forkortelse	Definition
Statusliste Trust-services (Trust-service Status List)	TSL	En form for underskrevet liste, der anvendes som grundlag for angivelse af statusoplysninger for Trust services, jf. forskrifterne i ETSI TS 102 231.
Trust Service		Tjeneste, som øger pålideligheden af og tilliden til elektroniske transaktioner (typisk, men ikke nødvendigvis, ved brug af krypteringsteknikker eller ved anvendelse af fortroligt materiale) (ETSI TS 102 231).
Trust Service-udbyder (Trust Service Provider)	TSP	Et organ, som driver en eller flere (elektroniske) Trust-services (dette udtryk har en bredere betydning end CSP).
Trust Service-token	TrST	En fysisk eller binær (logisk) genstand, der genereres eller udstedes i forbindelse med anvendelsen af en Trust Service. Som eksempel på binære TrST'er kan nævnes certifikater, CRL'er, tidsstemplingstokens og OCSP-svar.
Kvalificeret elektronisk signatur (Qualified Electronic Signature)	QES	En AdES, der understøttes af et QC, og som genereres af et SSCD, jf. definitionen i artikel 2 i direktiv 1999/93/EF.
Avanceret elektronisk signaturer (Advanced Electronic Signature)	AdES	Som defineret i artikel 2, stk. 2, i direktiv 1999/93/EF
Avanceret elektronisk signatur, understøttet af et kvalificeret certifikat (Advanced Electronic Signature supported by a Qualified Certificate)	$AdES_{QC}$	En elektronisk signatur, som opfylder kravene til en AdES, og som er understøttet af et QC, jf. definitionen i artikel 2 i direktiv 1999/93/EF.
Sikkert signaturgenererende system (Secure Signature Creation Device)	SSCD	Som defineret i artikel 2, stk. 6, i direktiv 1999/93/EF

KAPITEL I

TEKNISKE FORSKRIFTER FOR DEN FÆLLES SKABELON FOR »POSITIVLISTEN OVER OVERVÅGEDE/AKKREDITEREDE CERTIFICERINGSTJENESTEUDBYDERE«

I den følgende del af dokumentet skal nøgleordene »SKAL«, »KRÆVES«, »SKAL«, »MÅ IKKE«, »BØR«, »BØR IKKE«, »ANBEFALET«, »KAN« og VALGFRI tolkes som beskrevet i RFC 2119 ([1]).

►**M1** Nærværende forskrifter bygger på forskrifterne og kravene i ETSI TS 102 231 v.3.1.2. Hvis der ikke er angivet noget specifikt krav i nærværende forskrifter, SKAL kravene fra ETSI TS 102 231 v.3.1.2 finde fuld anvendelse. ◄ Når der er angivet specifikke krav i nærværende forskrifter, SKAL de have forrang over de tilsvarende krav i ETSI TS 102 231, samtidig med, at de suppleres af formatforskrifterne i ETSI TS 102 231. I tilfælde af uoverensstemmelser mellem nærværende forskrifter og forskrifterne i ETSI TS 102 231, SKAL nærværende forskrifter betragtes som de normative.

([1]) IETF RFC 2119: »Key words for use in RFCs to indicate Requirements Levels«.

▼C1

Der SKAL implementeres og ydes sprogunderstøttelse på engelsk (EN) som minimum og potentielt på yderligere et eller flere nationalsprog.

Dato- og tidsangivelse SKAL være i overensstemmelse med punkt 5.1.4 i ETSI TS 102 231.

Anvendelse af URI'er SKAL være i overensstemmelse med punkt 5.1.5 i ETSI TS 102 231.

Oplysninger om udstedelsesordningen for positivlisten

»*Tag*«

TSL tag (punkt 5.2.1)

Dette felt er PÅKRÆVET og SKAL være i overensstemmelse med punkt 5.2.1 i ETSI TS 102 231.

▼M1

———————

▼C2

Scheme Information

▼C1

TSL version identifier (punkt 5.3.1)

Dette felt er PÅKRÆVET og SKAL sættes til »3« (helt tal)

TSL sequence number (punkt 5.3.2)

▼M1

Dette felt er PÅKRÆVET. Det SKAL specificere TSL-sekvensnummeret. Dette hele tal begyndende med »1« ved den første udgivelse af TSL SKAL øges for hver efterfølgende udgivelse af TSL'en. Det MÅ IKKE sættes tilbage til »1«, når ovenstående »TSL version identifier« øges.

▼C1

TSL type (punkt 5.3.3)

▼M1

Dette felt er PÅKRÆVET ved specificering af TSL-type. Det SKAL sættes til http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Generic).

▼C1

Bemærkning: For at opfylde ETSI TS 102 231, punkt 5.3.3 og for at angive den specifikke TSL-type, samtidig med at der henvises til de nærværende forskrifter for etablering af TSL-implementeringen af medlemsstaternes positivlister ([1]) og gives mulighed for at en parser bestemmer, hvilken form efterfølgende felter ([2]) kan forventes at antage, og såfremt disse felter har specifikke (eller alternative) betydninger afhængigt af den angivne TSL (i dette tilfælde en medlemsstats positivliste), SKAL ovennævnte URI registreres og beskrives som følger:

([1]) Dvs. den liste, der angiver overvågnings/akkrediteringsstatus for certificeringstjenester fra certificeringstjenesteudbydere, som overvåges/akkrediteres af den pågældende medlemsstat for overholdelse af de relevante bestemmelser i direktiv 1999/93/EF (i kort form »positivlisten«).

([2]) Det vil sige de felter, som er specificeret i ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information, og som er nærmere beskrevet i nærværende forskrifter for at specificere medlemsstaternes oprettelse af positivlisten.

▼M1

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

▼C1

Beskrivelse: En TSL-implementering af en overvågnings/akkrediteringsstatusliste for certificeringstjenester fra certificeringstjenesteudbydere, som overvåges/akkrediteres af den pågældende medlemsstat, som ejer TSL-implementeringen, med henblik på opfyldelse af de relevante bestemmelser i direktiv 1999/93/EF gennem en direkte tilsynsproces (frivillig eller lovpligtig).

Scheme operator name (punkt 5.3.4)

Dette felt er PÅKRÆVET. Det SKAL indeholde navnet på det medlemsstatsorgan, der er ansvarligt for oprettelse, offentliggørelse og vedligeholdelse af den nationale positivliste. Det SKAL indeholde det formelle navn, som den dermed forbundne juridiske person eller bemyndigede enhed (f.eks. ved statslige administrative agenturer), som er forbundet med dette organ, opererer under. Det SKAL være det navn, der er anvendt i den formelle juridiske registrering, og som al formel kommunikation skal stiles til. Det SKAL være en sekvens af flersprogede tekststrenge og SKAL være implementeret med engelsk (EN) som det obligatoriske sprog og med potentielt ét eller flere nationalsprog.

Bemærkning: Et land KAN have separate overvågnings- og akkrediteringsorganer og endda yderligere organer til andre operationelle relaterede aktiviteter. ►M1 Det er op til den enkelte medlemsstat at udpege en Scheme operator for TSL-implementeringen af medlemsstatens TL. ◄ Det forventes, at overvågningsorganet, akkrediteringsorganet og operatøren (når disse er separate organer) får hvert sit ansvarsområde og hver sine forpligtelser.

En eventuel situation, hvor flere organer er ansvarlige for overvågning, akkreditering eller de operationelle aspekter, SKAL konsekvent afspejles og angives som sådan i oplysningerne om ordningen, der indgår i TL, herunder de oplysninger, der er specifikke for ordningen, og som er angivet i »Scheme information URI« (punkt 5.3.7).

▼M1

Den navngivne Scheme Operator (punkt 5.3.4) underskriver TSL'en.

▼C1

Scheme operator address (punkt 5.3.5)

Dette felt er PÅKRÆVET. Det SKAL indeholde adressen på den juridiske person eller bemyndigede organisation, som er angivet i feltet »Scheme operator name« (punkt 5.3.4), både til postformål og elektronisk kommunikation. Det skal indeholde både »PostalAddress« (dvs. vej, sted [stat eller region/kommune], [postnummer] og ISO 3166-1 alpha-2 landekode) i overensstemmelse med punkt 5.3.5.1 og »ElectronicAddress« (dvs. e-mail og/eller websted URI) i overensstemmelse med punkt 5.3.5.2.

Scheme name (punkt 5.3.6)

Dette felt er PÅKRÆVET ved specificering af det navn, som ordningen drives under. Det SKAL være en sekvens af flersprogede tekststrenge (med engelsk (EN) som det obligatoriske sprog og med potentielt et eller flere nationalsprog), der defineres som følger:

▼C1

— Den EN version SKAL være en tekststreng med følgende opbygning:

CC:EN_name_value

hvor

— »CC« = den ISO 3166-1 alpha-2 landekode, som anvendes i feltet »Scheme territory« (punkt 5.3.10)

— »:« = anvendes som separator

▼M1

— »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«

▼C1

— En medlemsstats nationale sprogversion SKAL være en tekststreng med følgende opbygning:

CC:name_value

hvor

— »CC« = den ISO 3166-1 alpha-2 landekode, som anvendes i feltet »Scheme territory« (punkt 5.3.10)

— »:« = anvendes som separator

— »name_value« = den officielle oversættelse til nationalsproget af ovenstående »EN_name_value«.

Ordningens navn er påkrævet for entydigt at angive den ordning, som »Scheme information URI« henviser til, samt for at sikre, at der gives et særligt navn til hver ordning, hvis operatøren driver mere end en ordning.

Medlemsstater og operatører SKAL, såfremt en medlemsstat eller en operatør driver mere end én ordning, sikre sig, at der gives et særligt navn til hver af disse.

Scheme information URI (punkt 5.3.7)

Dette felt er PÅKRÆVET og SKAL angive URI(»er«), hvor brugerne (afhængige parter) kan få oplysninger om den specifikke ordning (med EN som obligatorisk sprog og potentielt ét eller flere nationalsprog). Det SKAL være en sekvens af flersprogede pointers (med engelsk EN som det obligatoriske sprog og med potentielt et eller flere nationalsprog). Den/de URI(»er«), der henvises til, SKAL indeholde en sti til relevante oplysninger om ordningen.

De »relevante oplysninger om ordningen« SKAL mindst omfatte:

▼C2

— Generelle indledende oplysninger, som er fælles for alle medlemsstater, vedrørende positivlistens anvendelsesområde og kontekst og den/de pågældende overvågnings/akkrediteringsordning(er). Den fælles tekst, der skal anvendes, lyder som følger:

▼C2

'The present list is the TSL implementation of [name of the relevant Member State] "Trusted List of supervised/accredited Certification Service Providers" providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by [name of the relevant Member State] for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by [name of the relevant Member State] for compliance with the relevant provisions laid down in Directive 1999/93/EC;

— facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [name of the relevant Member State] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable "supervision" system (respectively "voluntary accreditation" system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art.2.13, Art. 3.2, Art 7.1(a), Art. 8.1, Art. 11)

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) are included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.'

▼C1

— Specifikke oplysninger om den/de pågældende overvågnings/-akkrediteringsordning(er), herunder især ([1]):

— oplysninger om det overvågningssystem, som finder anvendelse på CSP_{QC}

([1]) De sidste to oplysningskategorier er af afgørende betydning for, at afhængige parter kan vurdere kvaliteten og sikkerhedsniveauet ved sådanne overvågningssystemer/-akkrediteringsordninger. Disse oplysningskategorier angives på TL-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, der henviser til direktiv 1999/93/EF, samtidig med at hver medlemsstat har mulighed for at tilføje medlemsstats-specifik tekst/henvisninger). Yderligere oplysninger om nationale overvågnings/-akkrediteringssystemer for CSP'er, der ikke udsteder QC'er, kan afgives på tjensteniveau i det omfang det er relevant (f.eks. for at skelne mellem flere kvalitets/sikkerhedsniveauer) gennem »Scheme service definition URI« (punkt 5.5.6).

▼C1

— eventuelle oplysninger om den nationale frivillige akkrediteringsordning, der finder anvendelse på CSP_{QC};

— eventuelle oplysninger om det overvågningssystem, der finder anvendelse på CSP'er, der ikke udsteder QC'er

— eventuelle oplysninger om den nationale frivillige akkrediteringsordning, der finder anvendelse på CSP'er, der ikke udsteder QC'er.

— Disse særlige oplysninger SKAL for hver af de pågældende oven for angivne ordninger mindst omfatte:

— en generel beskrivelse

— oplysninger om den proces, som overvågnings/akkrediteringsorganet følger med henblik på overvågning/akkreditering af CSP'er, og som CSP'er følger i forbindelse med overvågningen/akkrediteringen

— oplysninger om de kriterier, der anvendes ved overvågning/akkreditering af CSP'er.

— Eventuelle særlige oplysninger om specifikke »kvalifikationer«, som nogle af de fysiske eller binære (logiske) genstande, der er genereret som følge af den leverede certificeringstjeneste, kan være berettiget til, fordi de overholder nationalt fastsatte bestemmelser og krav, herunder betydningen af en sådan »kvalifikation« og de hermed forbundne nationale bestemmelser og krav.

Yderligere oplysninger om ordningen, som er specifikke for medlemsstaten, KAN afgives på frivillig basis. Disse SKAL omfatte:

— oplysninger om de kriterier og bestemmelser, som anvendes til at udvælge tilsynsførende/revisorer og definere, hvordan CSP'er overvåges (kontrolleres)/akkrediteres (revideres)

— andre generelle oplysninger, som vedrører ordningens drift, samt kontaktoplysninger.

Status determination approach (punkt 5.3.8)

Dette felt er PÅKRÆVET og SKAL indeholde identifikatoren for tilgangen til fastsættelse af status. Følgende særlige URI SKAL anvendes som registreret og beskrives således:

URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/-appropriate

Beskrivelse: Status for de angivne tjenester bestemmes af eller på vegne af operatøren gennem et passende system for den pågældende medlemsstat, som muliggør »overvågning« (og, hvis det er relevant, »frivillig akkreditering«) af certificeringstjenesteudbydere, som er etableret på statens område (eller for så vidt angår »frivillig akkreditering« er etableret i et tredjeland) og udsteder kvalificerede certifikater til offentligheden i overensstemmelse med artikel 3, stk. 3 (henholdsvis artikel 3, stk. 2, eller artikel 7, stk. 1, litra a)) i direktiv 1999/93/EF og, hvis relevant, muliggør »overvågning«/»frivillig akkreditering« af certificeringstjenesteudbydere, der ikke udsteder kvalificerede certifikater i overensstemmelse med en nationalt defineret og etableret »anerkendt godkendelsesordning«, som er gennemført på nationalt plan med henblik på overvågning af, at tjenester fra CSP'er, der ikke udsteder QC'er, opfylder bestemmelserne i direktiv 1999/93/EF og potentielt udvidet gennem nationale bestemmelser om levering af sådanne certificeringstjenester.

▼C1

Scheme type/community/rules (punkt 5.3.9)

Dette felt er PÅKRÆVET og SKAL mindst indeholde følgende registrerede URI'er:

— En URI, som er fælles for alle medlemsstaters positivlister, der peger mod en beskrivende tekst, som SKAL fælde for alle TL'er:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

— der indeholder oplysninger om medlemsstatens ordnings deltagere (denne identificeres via »TSL type« (punkt 5.3.3) og »Scheme name« (punkt 5.3.6)) i en ordning under andre ordninger (dvs. en TSL, der angiver pointers til alle medlemsstater, som offentliggør og vedligeholder en TL i form af en TSL)

— hvor brugere kan finde politikker/regler, i forhold til hvilke tjenesterne på listen SKAL vurderes, og på grundlag af hvilke TSL-typen (jf. punkt 5.3.3) kan bestemmes

— hvor brugere kan få en beskrivelse af, hvordan indholdet i TSL-implementeringen af positivlisten anvendes og fortolkes. Disse regler for brug SKAL være fælles for alle medlemsstaters positivlister, uanset typen af de angivne tjenester og uanset, hvilket/hvilke overvågnings/akkrediteringssystem(er) der er tale om.

Beskrivende tekst:

▼C2

Participation in a scheme

Each Member State must create a 'Trusted List of supervised/accredited Certification Service Providers' providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by the relevant Member State for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The present TSL implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's TSL implementation of their Trusted List, compiled by the European Commission.

Policy/rules for the assessment of the listed services

The Trusted List of a Member State must provide a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

▼C2

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable 'supervision' system (respectively 'voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art.2.13, Art. 3.2, Art 7.1(a), Art. 8.1, Art. 11)

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) may be included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.

CSPs not issuing QCs but providing ancillary services, may fall under a 'voluntary accreditation' system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined 'recognised approval scheme' implemented on a national basis for the supervision of compliance with the provisions laid down in Directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Art. 2.11 of the Directive). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific 'qualification' on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a 'qualification' is likely to be limited solely to the national level.

Interpretation of the TSL implementation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the Annex of Commission Decision [reference to the present Decision] are as follows:

A 'CA/QC''Service type identifier' ('Sti') entry (similarly a CA/QC entry further qualified as being a 'RootCA/QC' through the use of 'Service information extension' ('Sie') additionalServiceInformation extension)

— indicates that from the 'Service digital identifier' ('Sdi') identified CA (similarly within the CA hierarchy starting from the 'Sdi' identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) **provided** that it is claimed as such in the certificate through the use of appropriate ETSI TS 101 862 defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI TS 101 456 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

▼C2

Note: if no ‘Sie’‘Qualification’ information is present or if an end-entity certificate that is claimed to be a QC is not ‘further identified’ through a related ‘Sie’ entry, then the ‘machine-processable’ information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate ETSI defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP issuing QCs.

— **and IF**‘Sie’‘Qualification’ information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this ‘Sie’‘Qualification’ entry, which is constructed on the principle of a sequence of ‘filters’ further identifying a set of certificates, must be considered according to the associated ‘qualifiers’ providing some additional information regarding ‘SSCD support’ and/or ‘Legal person as subject’ (e.g. those 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.). Those qualifiers are part of the following set of ‘qualifiers’ used to compensate for the lack of information in the corresponding QC content, and that are used respectively:

— to indicate the nature of the SSCD support:

— ‘QCWithSSCD’ qualifier value meaning ‘QC supported by an SSCD’, or

— ‘QCNoSSCD’ qualifier value meaning ‘QC not supported by an SSCD’, or

— ‘QCSSCDStatusAsInCert’ qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the ‘Sdi’-‘Sie’ provided information in this CA/QC entry;

AND/OR

— to indicate issuance to Legal Person:

— ‘QCForLegalPerson’ qualifier value meaning ‘Certificate issued to a Legal Person’

The general interpretation rule for any other ‘Sti’ type entry is that the listed service named according to the ‘Sn’ field value and uniquely identified by the ‘Sdi’ field value has a current supervision/accreditation status according to the ‘Scs’ 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 Technical specifications for a Common Template for the ‘Trusted List of supervised/accredited Certification Service Providers’ in the Annex of Commission Decision [reference to the actual Decision] for further details on the fields, description and meaning for the TSL implementation of the Member States’ Trusted Lists.

▼C1

— En URI, som er specifik for den enkelte medlemsstats positivliste, der linker til en beskrivende tekst, som SKAL anvendes på denne medlemsstats TL:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CC

hvor CC = den ISO 3166-1 alpha-2 landekode, som anvendes i feltet »Scheme territory« (punkt 5.3.10)

— hvor brugere kan finde den pågældende medlemsstats særlige politikker/regler, i forhold til hvilke tjenesterne på listen SKAL vurderes i overensstemmelse med medlemsstatens relevante overvågningssystem og frivillige akkrediteringsordninger

— hvor brugere kan få den pågældende medlemsstats særlige beskrivelse af, hvordan indholdet i TSL-implementeringen af positivlisten anvendes og fortolkes for så vidt angår de certificeringstjenester, der ikke vedrører udstedelsen af QC'er. Dette kan bruges til at indikere en potentiel granularitet i de nationale overvågnings/akkrediteringssystemer med hensyn til CSP'er, som ikke udsteder QC'er, og hvordan felterne »Scheme service definition URI« (punkt 5.5.6) og »Service information extension« anvendes til dette formål.

Medlemsstater KAN definere yderligere URI'er fra ovennævnte medlemsstatsspecifikke URI (dvs. URI'er defineret af denne hierarkisk specifikke URI).

Scheme territory (punkt 5.3.10)

I forbindelse med nærværende forskrifter er dette felt PÅKRÆVET og SKAL angive det land, hvori ordningen er etableret (ISO 3166-1 alpha-2 landekode).

TSL policy/legal notice (punkt 5.3.11)

I forbindelse med nærværende forskrifter er dette felt PÅKRÆVET og SKAL angive ordningens politik eller indeholde en meddelelse vedrørende ordningens juridiske status eller de juridiske krav, som ordningen skal opfylde i det retsområde, hvor ordningen er etableret og/eller eventuelle begrænsninger og betingelser for vedligeholdelse og offentliggørelse af TL.

Angivelsen SKAL være en flersproget tekststreng (almindelig tekst) bestående af to dele:

— En første obligatorisk del, som er fælles for alle medlemsstaters TL (med EN som obligatorisk sprog og med potentielt et eller flere nationalsprog), hvori det angives, at de gældende retlige rammer er direktiv 1999/93/EF og den dertil svarende gennemførelse i medlemsstaternes love, som er angivet i feltet »ordningens område«.

Engelsk version af den fælles tekst:

»The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for [name of the relevant Member State] is the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.«

Teksten på medlemsstatens nationalsprog: [officiel oversættelse af den engelske tekst ovenfor].

▼C1

— En valgfri del, som er specifik for hver TL, (med EN som obligatorisk sprog og med potentielt et eller flere nationalsprog) med henvisninger til specifikke gældende retlige rammer (især for så vidt dette vedrører nationale overvågning/akkrediteringsordninger for CSP'er, som ikke udsteder QC'er).

Historical information period (punkt 5.3.12)

Dette felt er PÅKRÆVET og SKAL angive varigheden (helt tal) af den periode, hvori de historiske oplysninger i TSL er til rådighed. Dette hele tal angives som antal dage, og i henhold til nærværende forskrifter SKAL det være større end eller lig med 3653 (dvs., at TSL-implementeringen af medlemsstaternes TL SKAL indeholde historiske oplysninger i mindst ti år). Ved højere værdier tages højde for de juridiske krav til dataopbevaring i den medlemsstat, som er angivet i »Scheme Territory« (punkt 5.3.10).

Pointers to other TSLs (punkt 5.3.13)

I henhold til nærværende forskrifter er dette felt PÅKRÆVET og SKAL omfatte pointers til en formular, som opfylder kravene i ETSI TS 102 231, med den af Europa-Kommissionen sammensatte liste over links (pointers) til alle TSL-implementeringer af positivlister fra medlemsstaterne, såfremt en sådan formular er til rådighed. Forskrifterne i ETSI TS 102 231, punkt 5.3.13 finder anvendelse, ligesom der tillades brug af en valgfri digital identitet, som repræsenterer udstederen af det TSL, der linkes til, og som har det i punkt 5.5.3 specificerede format.

Bemærkning: Så længe der afventes en ETSI TS 102 231 overensstemmende implementering af Europa-Kommissionens samlede liste over links til medlemsstaternes TSL-implementering af deres TL'er, MÅ dette felt IKKE anvendes.

List issue date and time (punkt 5.3.14)

Dette felt er PÅKRÆVET og SKAL indeholde dato og tidspunkt (UTC udtrykt som Zulu) for udstedelse af TSL, idet der bruges den dato/tidsværdi, som er angivet i ETSI TS 102 231, punkt 5.1.4.

Next update (punkt 5.3.15)

Dette felt er PÅKRÆVET og SKAL indeholde dato og tidspunkt (UTC udtrykt som Zulu) for næste udstedelse af TSL eller sættes til nul for angivelse af et lukket TSL (der bruges dato/tidsværdi som angivet i ETSI TS 102 231, punkt 5.1.4).

Hvis der ikke er mellemliggende statusændringer for nogen TSP eller tjeneste, der er omfattet af ordningen, SKAL TSL'et genudstedes, når det senest udstedte TSL udløber.

For så vidt angår nærværende forskrifter MÅ forskellen mellem tidspunktet for »Next update« og »List issue date and time« IKKE være over seks (6) måneder.

▼C1

Distribution points (punkt 5.3.16)

Dette felt er VALGFRIT. Hvis det anvendes, SKAL det angive de placeringer, hvor den aktuelle TSL-implementering af TL offentliggøres, og hvor der kan findes ajourføringer af den aktuelle TSL. Hvis der angives flere distributionspunkter, SKAL alle disse levere identiske kopier af det aktuelle TSL eller de ajourførte udgaver heraf. Hvis feltet anvendes, formateres det som en sekvens af strenge (som ikke må være tom), der hver især opfylder RFC 3986 ([1]).

Scheme extensions (punkt 5.3.17)

Dette felt er VALGFRIT, og anvendes ikke i forbindelse med nærværende forskrifter.

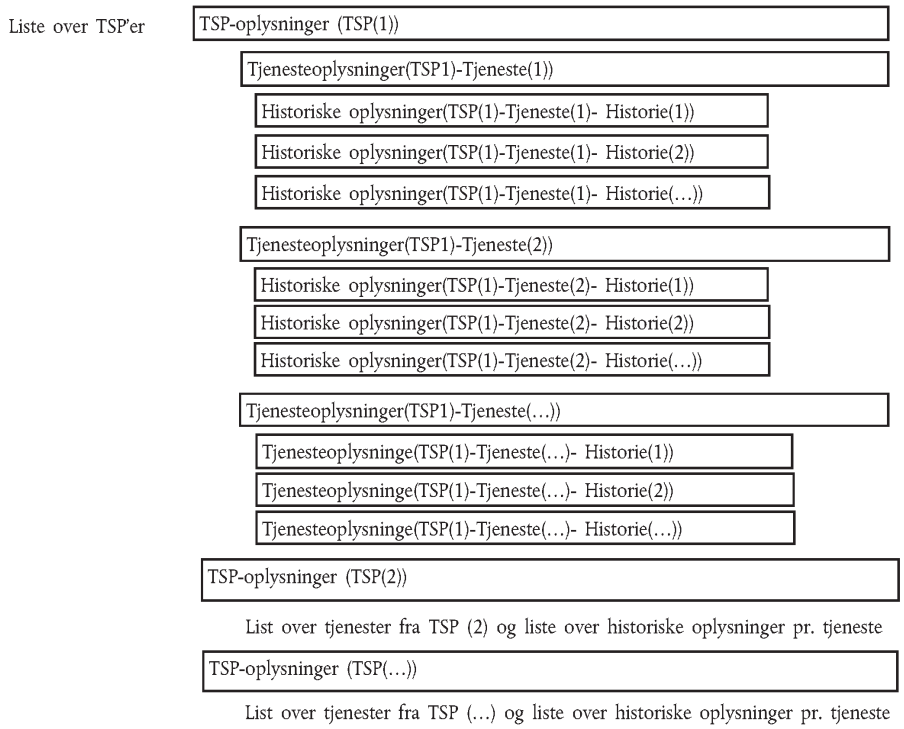
List of Trust Service Providers

Dette felt er VALGFRIT.

Hvis ingen CDP'er bliver eller er blevet overvåget/akkrediteret inden for rammerne af ordningen i en medlemsstat, SKAL dette felt udelades. Det er dog aftalt, at medlemsstaterne SKAL implementere en TSL med feltet udeladt, selv om en medlemsstat ikke har nogen CSP, som bliver eller er blevet overvåget eller akkrediteret under ordningen. Hvis der ikke er nogen CSP i listen SKAL det tolkes sådan, at ingen CSP'er bliver eller er blevet overvåget/akkrediteret i det land, som er angivet i »Scheme Territory«.

Hvis en eller flere CSP-tjenester bliver eller er blevet overvåget/akkrediteret under ordningen, SKAL feltet indeholde en sekvens, der identificerer hver CSP, der udbyder én eller flere af disse overvågede/akkrediterede tjenester, med detaljer om overvågnings/akkrediteringsstatus og statushistorie for hver af CSP'ens tjenester (TSP = CSP i figuren nedenfor).

▼C2



([1]) IETF RFC 3986: »Uniform Resource Identifiers (URI): Generic syntax«.

▼C2

Listen over TSP'er opstilles som angivet i figuren ovenfor. For hver TSP er der en sekvens af felter med oplysninger om TSP'en (»TSP-oplysninger«) efterfulgt af en liste over tjenester. For hver af sådanne angivne tjenester er der en sekvens af felter med oplysninger om tjenesten (»Tjenesteoplysninger«) og en sekvens af felter om tjenestens godkendelsesstatus (»Tjenestens godkendelsesstatus-historie«).

▼C1

TSP Information

TSP(1)

TSP name (punkt 5.4.1)

Dette felt er PÅKRÆVET og SKAL angive navnet på den juridiske person, som er ansvarlig for de af CSP'ens tjenester, som bliver eller er blevet overvåget/akkrediteret under ordningen. Det er en sekvens af flersprogede strenge (med engelsk EN som det obligatoriske sprog og med potentielt et eller flere nationalsprog). Dette navn SKAL være det navn, der er anvendt i den formelle juridiske registrering, og som al formel kommunikation stiles til.

TSP trade name (punkt 5.4.2)

Dette felt er VALGFRIT og, hvis det forekommer, SKAL det angive et alternativt navn, som CSP'en identificerer sig under i forbindelse med levering af de af dens tjenester, som findes i denne TSL under dens »TSP name« (punkt 5.4.1).

Bemærkning: Hvis en enkelt CSP som juridisk person udbyder tjenester under forskellige handelsnavne eller i forskellige specifikke sammenhænge, kan der være lige så mange CSP-angivelser som specifikke sammenhænge (f.eks. angivelser af navn/handelsnavn). Et alternativ hertil er kun at angive hver enkelt CSP (juridisk person) én gang og levere tjenestespecifikke oplysninger. Det er op til operatøren af ordningen i medlemsstaten at drøfte og aftale den mest hensigtsmæssige tilgang med CSP'en.

TSP address (punkt 5.4.3)

Dette felt er PÅKRÆVET og SKAL indeholde adressen på den juridiske person eller bemyndigede organisation, som er angivet i feltet »TSP name« (punkt 5.4.1), både til postformål og elektronisk kommunikation. Det skal indeholde både »PostalAddress« (dvs. vej, sted [stat eller region/kommune], [postnummer] og ISO 3166-1 alpha-2 landekode) i overensstemmelse med punkt 5.3.5.1 og »ElectronicAddress« (dvs. e-mail og/eller websted URI) i overensstemmelse med punkt 5.3.5.2.

TSP information URI (punkt 5.4.4)

Dette felt er PÅKRÆVET og SKAL angive den/de URI'er, hvor brugerne (f.eks. de afhængige parter) kan få CSP-specifikke oplysninger. Det SKAL være en sekvens af flersprogede angivelser (med engelsk EN som det obligatoriske sprog og med potentielt et eller flere nationalsprog). Den/de angivne URI'er SKAL linke til oplysninger, der beskriver CSP'ens generelle betingelser, dens praksis, juridiske spørgsmål, dens kundepolitikker og andre generiske oplysninger, som gælder alle de tjenester, der er angivet under dens CSP-indgang i TSL.

Bemærkning: Hvis en enkelt CSP som juridisk person udbyder tjenester under forskellige handelsnavne eller i forskellige specifikke sammenhænge, og dette er afspejlet i lige så mange TSP-indgange, som sådanne specifikke sammenhænge, SKAL dette felt indeholde oplysninger om de specifikke tjenester, der er angivet under en bestemt TSP/TradeName-indgang.

▼C1

TSP information extensions (punkt 5.4.5)

Dette felt er VALGFRIT og KAN, hvis det anvendes, bruges af operatøren i overensstemmelse med forskrifterne i ETSI TS 102 231 (punkt 5.4.5) til at levere specifikke oplysninger, som fortolkes i henhold til reglerne i den specifikke ordning.

List of Services

Dette felt er PÅKRÆVET og SKAL indeholde en sekvens, der angiver CSP'ens forskellige anerkendte tjenester samt godkendelsesstatus (og statushistorie) for den pågældende tjeneste. Der skal mindst være angivet én tjeneste (selv om de disponible oplysninger udelukkende er historiske)

Eftersom opbevaring af historiske oplysninger om de angivne tjenester er PÅKRÆVET i henhold til nærværende forskrifter, SKAL historiske oplysninger opbevares, selv om tjenestens aktuelle status normalt ikke ville kræve angivelse i listen (f.eks. hvis tjenesten er trukket tilbage). Derfor SKAL en CSP medtages af hensyn til de historiske oplysninger, selv om dens eneste angivne tjeneste har en sådan status.

Service Information

TSP(1) Service(1)

Service type identifier (punkt 5.5.1)

▼M1

Dette felt er PÅKRÆVET og SKAL indeholde identifikatoren for tjenesteydelsestypen i overensstemmelse med nærværende TSL-forskrifter (dvs. »/eSigDir-1999-93-EC-TrustedList/TSLType/generic«).

▼C1

Når den angivne tjenesteydelse vedrører udstedelse af kvalificerede certifikater, SKAL den angivne URI være http://uri.etsi.org/TrstSvc/Svctype/CA/QC (et certificeringscenter, der udsteder kvalificerede certifikater).

Når den angivne tjenesteydelse vedrører udstedelse af Trust Service-tokens, som ikke er QC'er og ikke understøtter udstedelse af QC'er, SKAL den angivne URI være en af de URI'er, der er defineret i ETSI 102 231 og anført i punkt D.2, som vedrører dette felt. Dette SKAL finde anvendelse selv for Trust Service-tokens, som overvåges/akkrediteres for overholdelse af visse særlige kvalifikationer i henhold til medlemsstaternes nationale love (f.eks. såkaldte Qualified Time Stamp Token på DE eller HU), den angivne URI SKAL være en af de URI'er, der er defineret i ETSI 102 231 og anført i punkt D.2, som vedrører dette felt (f.eks. TSA for nationalt definerede Qualified Time Stamp Tokens). Hvis det er relevant, KAN sådanne særlige nationale kvalifikationer af Trust Service-tokens angives i tjenesteangivelsen, og udvidelsen additionalServiceInformation (punkt 5.8.2) i punkt 5.5.9 (Service information extension) SKAL anvendes til dette formål.

▼C1

Som et generelt princip SKAL der være én indgang for hvert X.509v3- certifikat (f.eks. for en CA/QC-certificeringstjenestetype) under de anførte certificeringstjenester fra en angivet CSP i positivlisten (f.eks. et certificeringscenter, som (direkte) udsteder QC'ere). Under visse omhyggeligt forudsete og nøje styrede og godkendte forhold KAN et overvågningsorgan/akkrediteringsorgan i en medlemsstat beslutte at anvende X.509v3-certifikatet fra et Root eller Upper level QC (f.eks. en certificeringscenter, som ikke direkte udsteder slutenheds-QC'er, men som certificerer et hierarki af CA'er ned til CA'er, som udsteder QC'er til slutenheder) som »Sdi« for en enkelt angivelse i listen over tjenester fra en angivet CSP. Følgerne (fordele og ulemper) ved at bruge et sådant X.509v3 Root CA eller Upper CA-certifikat som »Sdi«-værdi for TL-tjenesteangivelser skal nøje overvejes og godkendes af medlemsstaterne ([1]). Desuden SKAL medlemsstaterne, når de anvender en sådan tilladt undtagelse for det generelle princip, levere den nødvendige dokumentation for at lette arbejdet i forbindelse med certificeringsstien og verifikationen.

Bemærkning: TSP'er KAN i lighed med OCSP-respondenter og CRL-udstedere, som indgår i CSP_{QC}-certificeringstjenester og er underlagt anvendelse af separate nøglepar til underskrivelse af henholdsvis OCSP-svar og CRL'er, også angives i nærværende TSL-skabelon ved at anvende følgende URI-kombination:

— Værdi for »Service type identifier« (punkt 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

kombineret med følgende »Service information extension« (punkt 5.5.9) additionalServiceInformation extension (punkt 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC

Beskrivelse: en udbyder af certifikatstatustjenester, som driver en OCSP-server som led i en tjeneste fra en CSP, der usteder kvalificerede certifikater.

— Værdien »Service type identifier« (punkt 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

kombineret med følgende værdi »Service information extension« (punkt 5.5.9) additionalServiceInformation extension (punkt 5.8.2)

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC

Beskrivelse: en udbyder af certifikatstatustjenester, som driver en CRL som led i en tjeneste fra en CSP, der usteder kvalificerede certifikater.

— Værdien »Service type identifier« (punkt 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

([1]) Anvendelse af et RootCA X.509v3-certifikat som »Sdi«-værdi for en angivet tjeneste, vil tvinge operatøren af ordningen til at overveje hele rækken af certificeringstjenester under et sådant Root CA som helhed for så vidt angår »overvågnings/akkrediteringsstatus«. Enhver ændring af status fra et enkelt CA under det angivne root-hierarki, vil f.eks. tvinge hele hierarkiet til at antage den pågældende statusændring.

▼C1

kombineret med følgende værdi »Service information extension« (punkt 5.5.9) additionalServiceInformation extension (punkt 5.8.2)

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

Beskrivelse: et Root-certificeringscenter, hvorfra der kan etableres en certificeringssti til et certificeringscenter, der udsteder kvalificerede certifikater.

— Værdien »Service type identifier« (punkt 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/TSA

kombineret med følgende værdi »Service information extension« (punkt 5.5.9) additionalServiceInformation extension (punkt 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

Beskrivelse: en tidsstemplingstjeneste i forbindelse med en tjenesteydelse fra en certificeringstjenesteyder, der udsteder kvalificerede certifikater, som udsteder TST, som i verifikationsprocessen for den kvalificerede underskrift kan anvendes til at fastslå og udvide signaturens validitet, når QC'et tilbagekaldes eller udløber.

Service name (punkt 5.5.2)

Dette felt er PÅKRÆVET og SKAL indeholde det navn, under hvilket CSP'en, som er identificeret i »TSP name« (punkt 5.4.1), udbyder den tjenesteydelse, som er angivet i »Service type identifier« (punkt 5.5.1). Det SKAL være en sekvens af flersprogede tekststrenge (med engelsk EN som det obligatoriske sprog og med potentielt et eller flere nationalsprog).

Service digital identity (punkt 5.5.3)

Dette felt er PÅKRÆVET og SKAL indeholde mindst én gengivelse af en digital identifikator, som er unik for den tjenesteydelse hvis type er angivet under »Service type identifier« (punkt 5.5.1), og som kan identificere tjenesten entydigt.

I nærværende forskrifter SKAL den anvendte digitale identifikator være det relevante X.509v3-certifikat, som gengiver den/de offentlige nøgle(r), som CSP'en anvender til at levere den tjeneste, hvis type er angivet af »Service type identifier« (punkt 5.5.1) (dvs. den nøgle, der anvendes af RootCA/QC, den nøgle, der anvendes til underskrivelse af certifikater [1]), eller alternativt til udstedelse af tidsstemplingstokens, underskrivelse af CRL'er eller underskrivelse af OCSP-svar). Dette relaterede X.509v3-certifikat SKAL anvendes som mindste påkrævede digitale identifikator (som er gengivelsen af de offentlige nøgler, som CSP'en bruger til levering af den angivne tjeneste). Der KAN anvendes yderligere følgende identifikatorer, men de SKAL alle henvise til samme identitet (dvs. det relaterede X.509v3-certifikat):

[1] Dette kan være certifikatet fra en CA, der udsteder slutenhedscertifikater (f.eks. CA/PKC, CA/QC), eller certifikatet fra et pålideligt root CA, hvorfra der kan findes en sti ned til kvalificerede slutenhedscertifikater. Afhængigt af, hvorvidt disse oplysninger og oplysningerne i de enkelte slutenhedscertifikater, som er udstedt under denne »trusted root«, kan anvendes til entydig bestemmelse af det kvalificerede certifikats relevante egenskaber, kan det være nødvendigt at supplere disse oplysninger (»Service digital identity« med data fra »Service information extensions« (jf. punkt 5.5.9).

▼C1

a) certifikatets »distinguished name« (DN), som kan anvendes til at verificere elektroniske signaturer fra den CSP-tjeneste, der er angivet i »Service type identifier« (punkt 5.5.1)

b) den relaterede identifikator for den offentlige nøgle (dvs. X.509v3 SubjectKeyIdentifier eller SKI-værdi)

c) den relaterede offentlige nøgle.

Som et generelt princip MÅ den digitale identifikator (dvs. det relaterede X.509v3-certifikat) IKKE forekomme mere end én gang i positivlisten, dvs. der SKAL være én indgang for hvert X.509v3-certifikat for en certificeringstjeneste under de angivne certificeringstjenester fra en angivet CSP i positivlisten. Modsat SKAL der anvendes ét enkelt X.509v3-certifikat i en enkelt tjenesteydelsesindgang som »Sdi«-værdi.

Bemærkning 1: Det eneste tilfælde, hvor det oven for nævnte generelle princip ikke finder anvendelse, er når et enkelt X.509v3-certifikat bruges ved udstedelse af forskellige typer af Trust Service-tokens, som er omfattet af forskellige overvågnings/akkrediteringsordninger, f.eks. bruges et enkelt X.509v3-certifikat på den ene side af en CSP ved udstedelse af QC'er under et relevant overvågningssystem og på den anden side ved udstedelse af ikke-kvalificerede certifikater under en anden overvågnings/akkrediteringsstatus. I dette tilfælde og eksempel ville der blive anvendt to indgange med forskellige »Sti«-værdier (f. eks. henholdsvis CA/QC og CA/PKC i det nævnte eksempel) og med samme »Sdi«-værdi (det relaterede X.509v3-certifikat).

Implementeringerne er ASN.1- eller XML-afhængige og SKAL opfylde forskrifterne i ETSI TS 102 231 (for ASN.1 henvises til bilag A til ETSI TS 102 231, og for XML henvises til bilag B til ETSI TS 102 231).

Bemærkning 2: Når det er nødvendigt at levere yderligere »kvalifikationsoplysninger« om den angivne tjenesteydelsesindgang, SKAL operatøren af ordningen, hvis det er relevant, overveje anvendelse af udvidelsen »additionalServiceInformation« (punkt 5.8.2) i feltet »Service information extension« (punkt 5.5.9) afhængigt af formålet med at angive sådanne yderligere »kvalifikationsoplysninger«. Desuden kan operatøren vælge at anvende punkt 5.5.6 (»Scheme service definition URI«).

Service current status (punkt 5.5.4)

▼C2

Dette felt er PÅKRÆVET og SKAL indeholde identifikatoren for tjenestens status ved hjælp af en af følgende URI'er:

— **Under Supervision (Under overvågning)**(http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision)

— **Supervision of Service in Cessation (Overvågning af tjenesten under ophør)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/-Svcstatus/supervisionincessation)

— **Supervision Ceased (Overvågning ophørt)** (http://uri.etsi.org/TrstSvc/-eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased)

— **Supervision Revoked (Overvågning tilbagekaldt)** (http://uri.etsi.org/-TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked)

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

— **Accreditation Ceased (Akkreditering ophørt)** (http://uri.etsi.org/TrstSvc/-eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased)

— **Accreditation Revoked (Akkreditering tilbagekaldt)** (http://uri.etsi.org/-TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

Ovenstående statusser SKAL inden for rammerne af nærværende specifikationer for positivlisten tolkes som følger:

— ***Under overvågning:*** Den tjeneste, der er angivet i »Service digital identity« (punkt 5.5.3), og som leveres af den certificeringstjenesteydbyder (CSP), som er angivet i »TSP name« (punkt 5.4.1), er for tiden under overvågning for overholdelse af bestemmelserne i direktiv 1999/93/EF af den medlemsstat, som er angivet i »Scheme territory« (punkt 5.3.10), hvori CSP'en er etableret.

▼M1

— ***Overvågning af tjenesten under ophør:*** Den tjeneste, der er angivet i »Service digital identity« (punkt 5.5.3), og som leveres af den CSP, der er angivet i »TSP name« (punkt 5.4.1), er for tiden under afvikling, men overvåges stadig, indtil overvågningen ophører eller tilbagekaldes. I tilfælde af, at en anden juridisk person end den i »TSP name« angivne har overtaget ansvaret med at gennemføre denne ophørsfase, SKAL denne nye »fallback«-persons (fallback CSP) identitet angives i »Scheme service definition URI« (punkt 5.5.6) og i »TakenOverBy«-udvidelsen (punkt L.3.2) i tjenesteydelsesindgangen.

▼C1

— ***Overvågning ophørt:*** Overvågningsvurderingens gyldighed er udløbet, uden at den i »Service digital identity« (punkt 5.5.3) angivne tjeneste revurderes. Tjenesten er fra datoen for den nuværende status ikke længere under overvågning, idet tjenesten anses for at have indstillet driften.

— ***Overvågning tilbagekaldt:*** Som tidligere overvåget kan CSP'ens tjenester og potentielt selve CSP'en ikke længere opfylde bestemmelserne i direktiv 1999/93/EF, i henhold til afgørelse truffet af den medlemsstat, der er angivet i »Scheme territory« (punkt 5.3.10), og hvori CSP'en er etableret. Derfor kræves det, at tjenestens drift indstilles og den betragtes som ophørt af ovennævnte årsag.

Bemærkning 1: Statusværdien »Supervision Revoked« kan være en definitiv status, selv om CSP'en som følge heraf fuldstændigt indstiller sin aktivitet; i dette tilfælde er det ikke nødvendigt at overgå til statussen »overvågning af tjenesten under ophør« eller »overvågning ophørt«. Faktisk er den eneste måde at ændre statussen »overvågning tilbagekaldt« på, at vende den manglende overholdelse til overholdelse af bestemmelserne i direktiv 1999/93/EF i overensstemmelse med det relevante gældende overvågningssystem i den medlemsstat, der ejer TL, og således genvinde status som »under overvågning«. Statussen »overvågning af tjenesten under ophør« eller »overvågning ophørt« forekommer kun, når en CSP direkte indstiller en tjeneste under overvågning, ikke når overvågningen er blevet tilbagekaldt.

— ***Akkrediteret:*** Akkrediteringsorganet har på vegne af den medlemsstat, der er angivet i »Scheme territory« (punkt 5.3.10) gennemført en akkrediteringsvurdering og fundet, at den tjeneste, der er angivet i »Service digital identity« (punkt 5.5.3), leveret af den CSP ([1]), der er angivet i »TSP name« (punkt 5.4.1), er i overensstemmelse med bestemmelserne i direktiv 1999/93/EF.

([1]) Bemærk, at denne akkrediterede CSP kan være etableret i en anden medlemsstat end i den, som er angivet i »Scheme territory« i TSL-implementeringen af TL, eller i et tredjeland (jf. artikel 7, stk. 1, litra a), i direktiv 1999/93/EF).

▼C1

Bemærkning 2: Når statusserne »akkreditering tilbagekaldt« og »akkreditering ophørt« anvendes i forbindelse med en CSP, som udsteder QC'er, og som er etableret i »Scheme territory« (klausul 5.3.10), SKAL de betragtes som »transitstatusser« og MÅ ikke anvendes som værdi for »aktuel status for tjenesten«, fordi de i »Service approval history information« eller i »Service current status«, såfremt de anvendes, SKAL følges umiddelbart af status »under overvågning«, eventuelt fulgt af en anden overvågningsstatus, som er defineret ovenfor og er illustreret i figur 1. Når statusserne »akkreditering tilbagekaldt« og »akkreditering ophørt« anvendes i forbindelse med en CSP, der ikke udsteder QC'er, når der kun er en tilknyttet »frivillig akkrediteringsordning« uden tilhørende overvågningsordning eller i forbindelse med en CSP, der udsteder QC'er, hvor CSP'en ikke er etableret i »Scheme territory« (punkt 5.3.10) (f.eks. i et tredjeland), KAN de anvendes som værdi for »Service current status«:

— ***Akkreditering ophørt:*** Akkrediteringsvurderingens gyldighed er udløbet, uden at den i »Service digital identity« (punkt 5.5.3) angivne tjeneste revurderes.

— ***Akkreditering tilbagekaldt:*** Efter tidligere at have været i overensstemmelse med ordningens kriterier opfylder den tjeneste, der er angivet i »Service digital identity« (punkt 5.5.3), og som leveres af den certificeringstjenesteydbyder (CSP), som er angivet i »TSP name« (punkt 5.4.1), og potentielt selve CSP'en ikke længere bestemmelserne i direktiv 1999/93/EF.

Bemærkning 3: Der skal anvendes nøjagtigt samme statusværdier for CSP'er, der udsteder QC'er og for CSP'er, der ikke udsteder QC'er (f.eks. udbydere af tidsstemplingstjenester, der udsteder TST'er, CSP'er, der udsteder ikke-kvalificerede certifikater, osv.). »Service Type identifier« (punkt 5.5.1) anvendes til at skelne mellem gældende overvågnings/akkrediteringssystemer.

Bemærkning 4: Yderligere statusrelaterede »kvalifikationsoplysninger« defineret i forbindelse med nationale overvågnings/akkrediteringssystemer for CSP'ere, der ikke udsteder QC'er, KAN, i det omfang det er relevant og påkrævet, angives på tjenesteniveau (f.eks. for at skelne mellem flere kvalitets/sikkerhedsniveauer). Operatører SKAL anvende udvidelsen »additionalServiceInformation« (punkt 5.8.2) i feltet »Service information extension« (punkt 5.5.9) afhængigt af formålet med at angive sådanne yderligere »kvalifikationsoplysninger«. Desuden kan operatøren vælge at anvende punkt 5.5.6 (»URI for definition af tjenesteordning«).

Current status starting date and time (punkt 5.5.5)

Dette felt er PÅKRÆVET og SKAL angive dato og tidspunkt for indtrædelse af den nuværende godkendelsesstatus (dato/tidsværdi, som er angivet i ETSI TS 102 231, punkt 5.1.4).

Scheme service definition URI (punkt 5.5.6)

Dette felt er VALGFRIT og SKAL i givet fald angive URI(»er«), hvor afhængige parter kan få tjenestespecifikke oplysninger, som leveres af operatøren som en sekvens af flersprogede pointers (med EN som obligatorisk sprog og potentielt ét eller flere nationalsprog).

Den/de URI(»er«), der henvises til, SKAL indeholde en sti til oplysninger, der beskriver tjenesten som angivet i ordningen. Dette KAN i givet fald omfatte:

a) URI, som angiver fallback-CSP'ens identitet i tilfælde af overvågning af en tjeneste under ophør, som en fallback-CSP er involveret i (jf. »Service current status« (punkt 5.5.4)

▼C1

b) URI til dokumenter med yderligere oplysninger om brug af visse nationalt definerede særlige kvalifikationer til en overvåget/akkrediteret tjeneste, der benytter sig af Trust Service-token i overensstemmelse med anvendelsen af feltet »Service information extension« (punkt 5.5.9) med en »additionalServiceInformation«-udvidelse som defineret i punkt 5.8.2.

Service supply points (punkt 5.5.7)

Dette felt er VALGFRIT og SKAL i givet fald angive URI(»er«), hvor de afhængige parter kan få adgang til tjenesten ved hjælp af en sekvens af tekststrenge med en syntaks, der SKAL være i overensstemmelse med RFC 3986.

TSP service definition URI (punkt 5.5.8)

Dette felt er VALGFRIT og SKAL i givet fald angive URI(»er«), hvor afhængige parter kan få tjenestespecifikke oplysninger, som leveres af TSP'en som en sekvens af flersprogede pointers (med EN som obligatorisk sprog og potentielt ét eller flere nationalsprog). Den/de URI(»er«), der henvises til, SKAL indeholde en sti til oplysninger, der beskriver tjenesten som specificeret af TSP'en.

Service information extensions (punkt 5.5.9)

Inden for rammerne af nærværende forskrifter er dette felt VALGFRIT, men SKAL være til stede, når oplysningerne i »Service digital identity« (punkt 5.5.3) ikke er tilstrækkelige til entydigt at identificere de kvalificerede certifikater, som er udstedt af denne tjeneste og/eller oplysningerne i de tilknyttede kvalificerede certifikater ikke muliggør maskinprocesserbar bestemmelse af, hvorvidt QC'et er understøttet af et SSCD ([1]).

Hvis anvendelse inden for rammerne af nærværende forskrifter er PÅKRÆVET f.eks. til CA/QC-tjenester, SKAL det valgfri oplysningsfelt »Service information extensions« (Sie) anvendes og opbygges i overensstemmelse med den »kvalifikationsudvidelse«, der er defineret i ETSI TS 102 231 bilag L.3.1, som en sekvens af en eller flere tuples, hvor hver tuple angiver:

— Oplysninger, der skal anvendes til yderligere identificering (filtrering) til præcisering af den i »Sdi« identificerede certificeringstjeneste (dvs. sæt af kvalificerede certifikater), for hvilke der kræves/leveres yderligere oplysninger med hensyn til anvendelse eller ikke-anvendelse af SSCD-støtte (og/eller udstedelse til en juridisk person) og

— Relaterede oplysninger (kvalifikatorer) om, hvorvidt denne yderligere identificerede tjenestes sæt af kvalificerede certifikater er understøttet af et SSCD (når disse oplysninger er »QCSSCDStatusAsInCert«, betyder det, at de tilknyttede oplysninger indgår i QC'et i en ETSI-standardiseret maskinprocesserbar form ([2]), og/eller oplysninger om, hvorvidt sådanne QC'er er udstedt til juridiske personer (normalt betragtes de kun som udstedt til fysiske personer).

— QCWithSSCD (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD): betyder, at det sikres af CSP og kontrolleres (overvågningsmodel) eller revideres (akkrediteringsmodel) af medlemsstaten (henholdsvis dennes overvågningsorgan eller akkrediteringsorgan), at alle QC'er, der udstedes i forbindelse med den tjeneste (QCA), der er angivet i »Service digital identity« (punkt 5.5.3) og yderligere identificeret af ovenstående (filtre) oplysninger, som under den »Sdi«-angivne certificeringstjeneste anvendes til yderligere at identificere det præcise sæt af kvalificerede certifikater, for hvilke disse yderligere oplysninger kræves med hensyn til anvendelse eller ikke-anvendelse af SSCD-støtte, UNDERSTØTTES at et SSCD (dvs. at den private nøgle, der er knyttet til den offentlige nøgle i certifikatet, opbevares i et sikkert signaturgenereringssystem i overensstemmelse med bilag III i direktiv 1999/93/EF).

([1]) Se punkt 2.2 i nærværende dokument.

([2]) Dette henviser til en passende kombination af ETSI-definerede QcCompliance-erklæringer, QcSSCD-erklæringer [ETSI TS 101 862] eller et QCP/QCP + ETSI-defineret OID [ETSI TS 101 456].

▼C1

— QCNoSSCD (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/-SvcInfoExt/QCNoSSCD): betyder, at det sikres af CSP og kontrolleres (overvågningsmodel) eller revideres (akkrediteringsmodel) af medlemsstaten (henholdsvis dennes overvågningsorgan eller akkrediteringsorgan), at alle QC'er, der udstedes i forbindelse med den tjeneste (RootCA/QC eller CA/QC), der er angivet i »Service digital identity« (punkt 5.5.3) og yderligere identificeret af ovenstående (filtre) oplysninger, som under den »Sdi«-angivne certificeringstjeneste anvendes til yderligere at identificere det præcise sæt af kvalificerede certifikater, for hvilke disse yderligere oplysninger kræves med hensyn til anvendelse eller ikke-anvendelse af SSCD-støtte, IKKE UNDERSTØTTES at et SSCD (dvs. at den private nøgle, der er knyttet til den offentlige nøgle i certifikatet, ikke opbevares i et sikkert signaturgenereringssystem i overensstemmelse med bilag III i direktiv 1999/93/EF).

— QCSSCDStatusAsInCert (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert): betyder, at det sikres af CSP og kontrolleres (overvågningsmodel) eller revideres (akkrediteringsmodel) af medlemsstaten (henholdsvis dennes overvågningsorgan eller akkrediteringsorgan), at alle QC'er, der udstedes i forbindelse med den tjeneste (CA/QC), der er angivet i »Service digital identity« (punkt 5.5.3) og yderligere identificeret af ovenstående (filtre) oplysninger, som under den »Sdi«-angivne certificeringstjeneste anvendes til yderligere at identificere det præcise sæt af kvalificerede certifikater, for hvilke disse yderligere oplysninger kræves med hensyn til anvendelse eller ikke-anvendelse af SSCD-støtte, SKAL indeholde maskinprocesserbare oplysninger, der angiver, hvorvidt QC'et undersøttes af at et SSCD.

— QCForLegalPerson (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): betyder, at det sikres af CSP og kontrolleres (overvågningsmodel) eller revideres (akkrediteringsmodel) af medlemsstaten (henholdsvis dennes overvågningsorgan eller akkrediteringsorgan), at alle QC'er, der udstedes i forbindelse med den tjeneste (QCA), der er angivet i »Service digital identity« (punkt 5.5.3) og yderligere identificeret af ovenstående (filtre) oplysninger, som under den »Sdi«-angivne certificeringstjeneste anvendes til yderligere at identificere det præcise sæt af kvalificerede certifikater, for hvilke disse yderligere oplysninger kræves med hensyn til udstedelse til en juridisk person, UDSTEDES til juridiske personer.

Disse kvalifikatorer skal kun bruges som udvidelse, hvis tjenestetypen er http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Dette felt er implementeringsspecifikt (ASN.1 eller XML) og SKAL opfylde forskrifterne i ETSI TS 102 231, bilag L.3.1.

▼M1

I forbindelse med en XML-implementering skal det specifikke indhold i sådanne yderligere oplysninger kodes ved hjælp af de xsd-filer, der er angivet i bilag C til ETSI TS 102 231.

▼C1

Service Approval History

Dette felt er VALGFRIT, men SKAL forefindes, hvis »Historical information period« (punkt 5.3.12) ikke er nul. Således SKAL ordningen inden for rammerne af nærværende forskrifter opbevare historiske oplysninger. Såfremt de historiske oplysninger skal opbevares, men tjenesten ikke har nogen historie forud for den aktuelle status (dvs. at den første registrerede status eller historiske oplysninger ikke er opbevaret af operatøren), SKAL dette felt være tomt. Ellers SKAL der for enhver ændring af TSP-tjenestens aktuelle status, som forekom inden for den historiske oplysningsperiode som specificeret i ETSI TS 102 231, punkt 5.3.12, angives oplysninger om den tidligere godkendelsesstatus med dato og tidspunkt for statusændringer opstillet i rækkefølge (dvs. dato og tidspunkt for indtrædelse af den efterfølgende godkendelsesstatus).

▼C1

Dette SKAL være en sekvens af historiske oplysninger som defineret nedenfor.

TSP(1) Service(1) History(1)

Service type identifier (punkt 5.6.1)

Dette felt er PÅKRÆVET og SKAL angive identifikatoren for tjenesteydelsestype i det format og den betydning, der anvendes i »TSP Service Information — Service type identifier« (punkt 5.5.1).

Service name (punkt 5.6.2)

Dette felt er PÅKRÆVET og SKAL indeholde det navn, under hvilket CSP'en udbød den angivne tjeneste i »TSP Service Information — Service type identifier« (punkt 5.5.1) i det format og den betydning, som anvendes i »TSP Service Information — Service name« (punkt 5.5.2). Denne bestemmelse kræver ikke, at navnet er det samme som de i punkt 5.5.2 angivne. En navneændring KAN være en af de betingelser, som udløser krav om en ny status.

▼M1

Service digital identity (punkt 5.6.3)

Dette felt er PÅKRÆVET og SKAL indeholde mindst én gengivelse af en digital identifikator (dvs. X.509v3-certifikat), der anvendes i »TSP Service Information — Service digital identity« (punkt 5.5.3) i samme format og betydning som defineret i ETSI TS 102 231, punkt 5.5.3.

Bemærkning: Der må for en X.509v3 certifikatværdi, der anvendes i en tjenestes »Sdi« punkt 5.5.3, kun være en enkelt tjenesteydelsesindgang i en positivliste pr. »Sti:Sie/additionalServiceInformation«-værdi. De »Sdi«-oplysninger (punkt 5.6.3), der anvendes i oplysningerne om godkendelsesstatus, som er forbundet med en tjenesteindgang, og »Sdi«-oplysningerne (punkt 5.5.3), der anvendes i denne tjenesteindgang, SKAL henvise til samme X.509v3 certifikatværdi. Når en angivet tjeneste ændrer sin »Sdi« (dvs. fornyelse eller »rekey« af et X.509v3-certifikat for f.eks. en CA/PKC eller CA/QC) eller opretter en ny »Sdi« for en sådan tjeneste, selv med identiske værdier for de tilknyttede »Sti«, »Sn«, og [»Sie«], betyder det, at Scheme Operator SKAL oprette en anden tjenesteydelsesindgang end den forrige.

▼C1

Service previous status (punkt 5.6.4)

Dette felt er PÅKRÆVET og SKAL angive identifikatoren for tjenestens tidligere status i det format og den betydning, der anvendes i »TSP Service Information — Service current status« (punkt 5.5.4).

Previous status starting date and time (punkt 5.6.5)

Dette felt er PÅKRÆVET og SKAL angive dato og tidspunkt for indtrædelse af den tidligere pågældende status i det format og den betydning, der anvendes i »TSP Service Information — Service current status starting date and time« (punkt 5.5.5).

Service information extensions (punkt 5.6.6)

Dette felt er VALGFRIT og KAN anvendes af operatører til at angive tjenesterelaterede oplysninger i det format og den betydning, der anvendes i »TSP Service Information — Service information extensions« (punkt 5.5.9).

▼C1

TSP(1) Service(1) History(2)

Idem for TSP(1) Service(1) History(2) (prior to History 1)

…

TSP(1) Service(2)

Idem for TSP(1) Service 2 (i det omfang det er relevant)

TSP(1)Service(2)History(1)

…

TSP(2) Information

Idem for TSP 2 (i det omfang det er relevant)

Idem for TSP(2) (i det omfang det er relevant)

Idem for TSP 2 Service 1 History 1

…

▼M1

Signed TSL

Den menneskeligt læsbare TSL-implementering af positivlisten, der oprettes i henhold til nærværende forskrifter, særlig kapitel IV, BØR underskrives af »Scheme operator name« (punkt 5.3.4) for at sikre dens autenticitet og integritet ([1]). Signaturens format SKAL være PAdES part 3 (ETSI TS 102 778-3 ([2])), men KAN være PAdES part 2 (ETSI TS 102 778-2 ([3])) inden for rammerne af den specifikke model af positivlister, der er fastsat ved offentliggørelsen af de certifikater, der anvendes til at underskrive positivlisterne.

Den maskinelt læsbare TSL-implementering af positivlisten, der oprettes i henhold til nærværende forskrifter, SKAL underskrives af »Scheme operator name« (punkt 5.3.4) for at sikre dens autenticitet og integritet. Formatet af den maskinelt læsbare TSL-implementering af positivlisten, der oprettes i henhold til nærværende forskrifter, SKAL være XML og SKAL være i overensstemmelse med forskrifterne i bilag B og C til ETSI TS 102 231.

Underskriftens format SKAL være XAdES BES eller EPES som defineret i ETSI TS 101 903-forskrifterne for XML-implementeringer. Sådanne implementeringer af elektroniske signaturer SKAL opfylde kravene i bilag B til ETSI TS 102 231 ([4]). Yderligere generelle krav vedrørende signaturen er angivet i de følgende afsnit.

▼C1

Scheme identification (punkt 5.7.2)

Dette felt er PÅKRÆVET og SKAL angive en af operatøren tildelt reference, som entydigt identificerer den ordning, der er beskrevet i nærværende forskrifter og den oprettede TSL, og SKAL indgå i beregningen af signaturen. Dette forventes at være en tekststreng eller bitstreng.

([1]) Hvis den menneskeligt læsbare TSL-implementering af positivlisten ikke underskrives, SKAL dens autenticitet og integritet garanteres gennem en passende kommunikationsforbindelse med et tilsvarende sikkerhedsniveau. Anvendelse af TLS (IETF RFC 5246: »The Transport Layer Security (TLS) Protocol Version 1.2«) anbefales til dette formål, og medlemsstaterne SKAL gøre »fingeraftrykket« af certifikatet for TLS-kanalen tilgængeligt uden for båndet for TSL-brugerne.

([2]) 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.

([3]) 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.

([4]) Det er obligatorisk at beskytte den operatør, der underskriver certifikatet med signaturen, på en af de måder, der foreskrives i ETSI TS 101 903, og ds:keyInfo bør efter omstændighederne indeholde den relevante certifikatkæde.

▼M1

I forbindelse med nærværende forskrifter SKAL den tildelte reference omfatte »TSL type« (punkt 5.3.3), »Scheme name« (punkt 5.3.6) og værdien af SubjectKeyIdentifier-udvidelsen i det certifikat, som operatøren anvender til elektronisk underskrivelse af TSL'en.

▼C1

Signature algorithm identifier (punkt 5.7.3)

Dette felt er PÅKRÆVET og SKAL indeholde den kryptografiske algoritme, som er anvendt ved generering af signaturen. Afhængigt af den anvendte algoritme KAN dette felt kræve yderligere parametre. Dette felt SKAL indgå i beregningen af signaturen.

Signature value (punkt 5.7.4)

Dette felt er PÅKRÆVET og SKAL indeholde den digitale signaturs faktiske værdi. Alle felter i TSL (bortset fra selve signaturværdien) SKAL indgå i beregningen af signaturen.

TSL extensions (punkt 5.8)

expiredCertsRevocationInfo Extension (punkt 5.8.1)

Denne udvidelse er VALGFRI. Hvis anvendt, SKAL den opfylde forskrifterne i ETSI TS 102 231, punkt 5.8.1.

additionalServiceInformation Extension (punkt 5.8.2)

Denne VALGFRI udvidelse SKAL, hvis den benyttes, anvendes udelukkende på tjenesteniveau og kun i det felt, som er defineret i punkt 5.5.9 (»Service information extension«). Den anvendes til at angive yderligere oplysninger om en tjeneste. Den SKAL være en sekvens af én eller flere tuples, idet hver tuple giver:

a) en URI, der identificerer de yderligere oplysninger, f.eks.:

   — en URI, der angiver en nationalt defineret særlig kvalifikation vedrørende en overvåget/akkrediteret tjeneste, der benytter sig af Trust Service-token, f.eks.

      — et specielt sikkerheds/kvalitets- eller granularitetsniveau med hensyn til nationale overvågnings/akkrediteringsordninger for CSP'er, der ikke udsteder QC'er (f.eks. RGS */**/*** i FR, særlig »overvågningsstatus« i kraft af national lovgivning om specifikke CSP'er, der udsteder QC'er i DE), jf. bemærkning 4) i »Service current status« — punkt 5.5.4

      — eller en særlig juridisk status for levering af en overvåget/akkrediteret Trust Service-token (f.eks. nationalt defineret »kvalificeret TST« som i DE eller HU)

      — eller en særlig politikidentifikator i et X.509v3-certifikat angivet i »Sdi«-feltet

   — eller en registreret URI som angivet i »Service type identifier«, punkt 5.5.1, for yderligere at specificere deltagelsen af den under »Sti«-identificerede tjeneste som en komponenttjeneste fra en certificeringstjenesteudbyder, der udsteder QC (f.eks. OCSP-QC, CRL-QC og RootCA-QC)

b) en valgfri streng, der indeholder værdien serviceInformation med den i ordningen specificerede betydning (f.eks. *, ** eller ***)

c) en valgfri yderligere oplysning angivet i et ordningsspecifikt format.

▼**M1**

Når URI renses for referencer, BØR det resultere i menneskeligt læsbare oplysninger (som et minimum på engelsk og eventuelt på et eller flere nationale sprog), der anses for passende og tilstrækkelige til, at en afhængig part kan forstå udvidelsen, og navnlig forklarer de pågældende URI'ers betydning med angivelse af de mulige værdier for serviceInformation og betydningen af de enkelte værdier.

Qualifications Extension (punkt L.3.1)

Beskrivelse: Dette felt er VALGFRIT, men SKAL forefindes, hvis anvendelsen heraf er PÅKRÆVET, f.eks. til RootCA/QC eller CA/QC-tjenester, og når

— de oplysninger, der er angivet i »Service digital identity« er ikke tilstrækkelige til entydigt at identificere de kvalificerede certifikater, der udstedes af denne tjeneste

— oplysningerne i de tilknyttede kvalificerede certifikater ikke muliggør maskinprocesserbar bestemmelse af, hvorvidt QC'et er understøttet af et SSCD.

Hvis den benyttes, MÅ denne udvidelse af tjenesteniveau kun anvendes i det felt, som er defineret i »Service information extension« (punkt 5.5.9), og den SKAL overholde forskrifterne i bilag L.3.1 til ETSI TS 102 231.

TakenOverBy Extension (punkt L.3.2)

Beskrivelse: Denne udvidelse er VALGFRI, men SKAL forefindes, når en tjeneste, der tidligere var omfattet af en CSP's juridiske ansvar, overtages af en anden TSP, og når den har til formål formelt at angive en tjenestes juridiske ansvar samt at gøre det muligt for verifikationssoftwaren at vise visse juridiske oplysninger til brugeren. Oplysningerne i denne udvidelse SKAL være i overensstemmelse med den tilknyttede anvendelse af punkt 5.5.6 og SKAL overholde forskrifterne i bilag L.3.2 til ETSI TS 102 231.

▼**M1**

KAPITEL II

Ved oprettelsen af deres positivlister anvender medlemsstaterne:

Sprogkoder med små bogstaver og landekoder med store bogstaver

Sprog- og landekoder i henhold til nedenstående tabel

Når der forefindes latinske bogstaver (med den pågældende sprogkode), tilføjes en translitteration med latinske bogstaver med den pågældende sprogkode som specificeret i nedenstående tabel.

Kort form (kildesprog)	Kort form (engelsk)	Landekode	Sprogkode	Noter	Translitteration til latin
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	Landekode anbefalet af EU	el-Latn
España	Spain	ES	es	også catalansk (ca), baskisk (eu), galicisk (gl)	
France	France	FR	fr		
Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	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		

▼**M1**

Kort form (kildesprog)	Kort form (engelsk)	Landekode	Sprogkode	Noter	Translitteration til latin
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Landekode anbefalet af EU	
Ísland	Iceland	IS	is		
Liechtenstein	Liechten-stein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Latinsk translitteration: България = Bulgaria Ελλάδα = Elláda Κύπρος = Kýpros.

_____

▼C1

KAPITEL IV

FORSKRIFTER FOR DEN MENNESKELIGT LÆSBARE UDGAVE AF TSL-IMPLEMENTERINGEN AF POSITIVLISTEN

En menneskeligt læsbar (Human Readable — HR) udgave af TSL-implementering af positivlisten SKAL være offentligt tilgængelig og kunne konsulteres gennem elektroniske midler. Den BØR foreligge som pdf (Portable Document Format) i overensstemmelse med ISO 32000, som SKAL have et format i overensstemmelse med profil PDF/A (ISO) 19005).

Indholdet i de PDF/A-baserede HR-udgaver af TSL-implementeringen af positivlisten BØR opfylde følgende krav:

▼M1

— Titlen på den menneskeligt læsbare udgave af positivlisterne skal bestå af en sammenkædning af følgende elementer

  — valgfrit billede af medlemsstatens nationale flag

  — mellemrum

  — landenavn i kortform på kildesproget (-sprogene) (som angivet i første kolonne i tabellen i kapitel II)

  — mellemrum

  — »(«

  — landenavn i kort form på engelsk (som angivet i anden kolonne i tabellen i kapitel II) inden for parentesen

  — »):« som afsluttende parentes og separator

  — mellemrum

  — »Trusted List«

  — valgfrit logo for medlemsstatens operatør

▼C1

— Opbygningen af HR-udgaven BØR afspejle den logiske model, der er beskrevet i punkt 5.1.2 i ETSI TS 102 231

— Hvert forekommende felt BØR vises og angive:

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

  — Feltets værdi (f.eks. »CA/QC«)

  — Betydningen (beskrivelse) af feltets værdi, i det omfang det er relevant, og navnlig som angivet i bilag D til ETSI TS 102 231 eller i nærværende specifikationer for registrerede URI'er (f.eks. »Et certificeringscenter, der udsteder offentlige nøglecertifikater«)

  — Flere versioner i naturligt sprog som angivet i TSL-implementeringen af positivlisten, såfremt dette er relevant.

— Følgende felter med tilhørende værdier i de digitale certifikater, som findes i feltet »Service digital identity«, BØR som minimum vises i HR-udgaven:

  — Version

  — Serienummer

  — Signaturalgoritme

  — Udsteder

  — Gyldig fra

  — Gyldig til

  — Emne

▼C1

— Offentlig nøgle

— Certifikatpolitikker

— Identifikator for emnenøgle

— CRL-distributionspunkter

— Identifikator for Authority Key

— Nøglebrug

— Grundlæggende begrænsninger

— Thumbprint-algoritme

— Thumbprint

— HR-udgaven BØR let kunne udskrives

— HR-udgaven KAN være elektronisk underskrevet. I så tilfælde SKAL den være underskrevet af operatøren for ordningen i overensstemmelse med signaturforskrifter som for TSL-implementeringen af positivlisten.