Detta dokument är endast avsett som dokumentationshjälpmedel och institutionerna ansvarar inte för innehållet

►B ►C1 **KOMMISSIONENS BESLUT**

av den 16 oktober 2009

om åtgärder som underlättar användningen av förfaranden på elektronisk väg genom gemensamma kontaktpunkter i enlighet med Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden

[delgivet med nr K(2009) 7806]

(Text av betydelse för EES)

(2009/767/EG) ◄

(EUT L 274, 20.10.2009, s. 36)

Ändrad genom:

		Officiella tidningen		
		nr	sida	datum
►M1	Kommissionens beslut 2010/425/EU av den 28 juli 2010	L 199	30	31.7.2010

Rättad genom:

►C1 Rättelse, EUT L 299, 14.11.2009, s. 18 (2009/767/EG)
►C2 Rättelse, EUT L 4, 7.1.2011, s. 6 (2009/767/EG)

▼B
▼C1

KOMMISSIONENS BESLUT

av den 16 oktober 2009

om åtgärder som underlättar användningen av förfaranden på elektronisk väg genom gemensamma kontaktpunkter i enlighet med Europaparlamentets och rådets direktiv 2006/123/EG om tjänster på den inre marknaden

[delgivet med nr K(2009) 7806]

(Text av betydelse för EES)

(2009/767/EG)

EUROPEISKA GEMENSKAPERNAS KOMMISSION HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om upprättandet av Europeiska gemenskapen,

med beaktande av Europaparlamentets och rådets direktiv 2006/123/EG av den 12 december 2006 om tjänster på den inre marknaden ([1]), särskilt artikel 8.3, och

av följande skäl:

(1) I kapitel II i direktiv 2006/123/EG, särskilt artiklarna 5 och 8 i detta, åläggs medlemsstaterna att förenkla de administrativa förfaranden och formaliteter som är tillämpliga på tillträde till och utövande av tjänsteverksamhet, och att se till att dessa förfaranden och formaliteter enkelt kan fullgöras av tjänsteleverantörerna på distans och på elektronisk väg via gemensamma kontaktpunkter.

(2) Det ska vara möjligt att fullgöra förfaranden och formaliteter via de gemensamma kontaktpunkterna även över medlemsstatsgränserna, i enlighet med artikel 8 i direktiv 2006/123/EG.

(3) För att uppfylla skyldigheten att förenkla förfarandena och formaliteterna samt underlätta gränsöverskridande användning av gemensamma kontaktpunkter bör förfaranden på elektronisk väg bygga på enkla lösningar även när det gäller användningen av elektroniska signaturer. I de fall då det efter en ändamålsenlig riskbedömning av konkreta förfaranden och formaliteter anses vara nödvändigt med en hög säkerhetsnivå eller likvärdighet med handskrivna signaturer kan tjänsteleverantörerna för vissa förfaranden och formaliteter åläggas att införa avancerade elektroniska signaturer baserade på ett kvalificerat certifikat, med eller utan en säker anordning för skapande av signaturer.

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

▼C1

(4) Gemenskapens ramverk för elektroniska signaturer inrättades genom Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer ([1]). För att underlätta en effektiv gränsöverskridande användning av avancerade elektroniska signaturer baserade på ett kvalificerat certifikat bör förtroendet för dessa elektroniska signaturer förstärkas oberoende av i vilken medlemsstat undertecknaren eller den tillhandahållare av certifieringstjänster som utfärdar det kvalificerade certifikatet är etablerade. Detta går att åstadkomma genom att göra den information som behövs för att validera de elektroniska signaturerna, särskilt sådan information som rör tillhandahållare av certifieringstjänster som övervakas/-ackrediterats i en medlemsstat och de tjänster som de erbjuder, mer lättillgänglig och i en tillförlitlig form.

(5) Det är nödvändigt att se till att medlemsstaterna gör denna information allmänt tillgänglig med hjälp av en gemensam mall för att underlätta dess användning och att en lämplig detaljnivå upprätthålls, så att mottagarsidan kan validera den elektroniska signaturen.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Användning och godkännande av elektroniska signaturer

1. Om det är motiverat på grundval av en ändamålsenlig bedömning av berörda risker och i enlighet med artikel 5.1 och 5.3 i direktiv 2006/123/EG, får medlemsstaterna kräva att tjänsteleverantören för fullgörandet av vissa förfaranden och formaliteter genom de gemensamma kontaktpunkterna i enlighet med artikel 8 i direktiv 2006/123/EG ska använda avancerade elektroniska signaturer baserade på ett kvalificerat certifikat, med eller utan en säker anordning för skapande av signaturer, enligt vad som fastställs och regleras genom direktiv 1999/93/EG.

2. Medlemsstaterna ska godkänna alla avancerade elektroniska signaturer som är baserade på ett kvalificerat certifikat, med eller utan en säker anordning för skapande av signaturer, för att fullgöra de förfaranden och formaliteter som avses i punkt 1, utan att detta påverkar medlemsstaternas möjlighet att begränsa detta godkännande till avancerade elektroniska signaturer som är baserade på ett kvalificerat certifikat och som har skapats med hjälp av en säker anordning för skapande av signaturer, om detta sker i enlighet med den riskbedömning som avses i punkt 1.

3. För att godkänna avancerade elektroniska signaturer baserade på ett kvalificerat certifikat, med eller utan en säker anordning för skapande av signaturer, får medlemsstaterna inte ställa krav som skapar hinder för tjänsteleverantörernas användning av elektroniska förfaranden via de gemensamma kontaktpunkterna.

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

▼C1

4. Punkt 2 får inte hindra medlemsstaterna från att godkänna andra elektroniska signaturer än avancerade elektroniska signaturer baserade på ett kvalificerat certifikat, med eller utan en säker anordning för skapande av signaturer.

Artikel 2

Inrättande, underhåll och offentliggörande av tillförlitliga förteckningar

1. Varje medlemsstat ska i enlighet med de tekniska specifikationerna i bilagan inrätta, underhålla och offentliggöra en ”tillförlitlig förteckning” med minimiuppgifter om de tillhandahållare av certifieringstjänster som utfärdar kvalificerade certifikat till allmänheten och som medlemsstaten övervakar/ackrediterat.

▼M1

2. Medlemsstaterna ska inrätta och offentliggöra den tillförlitliga förteckningen i både människo- och maskinläsbart format i enlighet med specifikationerna i bilagan.

2a. Medlemsstaterna ska elektroniskt signera den tillförlitliga förteckningen i maskinläsbart format och ska åtminstone offentliggöra den tillförlitliga förteckningen i människoläsbart format genom en säker kanal för att säkerställa dess autenticitet och integritet.

3. Medlemsstaterna ska lämna följande information till kommissionen:

a) Vilket eller vilka organ som ansvarar för att inrätta, underhålla och offentliggöra de tillförlitliga förteckningarna i människo- och maskinläsbart format.

b) Var den tillförlitliga förteckningen i människo- och maskinläsbart format offentliggörs.

c) Det offentliga nyckelcertifikat som används för att tillämpa en säker kanal genom vilken den människoläsbara tillförlitliga förteckningen offentliggörs eller om den människoläsbara förteckningen är elektroniskt signerad, den offentliga certifieringsnyckel som används för att signera den.

d) Den offentliga certifieringsnyckel som används för att elektroniskt signera den tillförlitliga förteckningen i maskinläsbart format.

e) Eventuella ändringar av uppgifterna enligt punkterna a–d.

4. Kommissionen ska via en säker kanal till en godkänd webbserver tillhandahålla samtliga medlemsstater de uppgifter som avses i punkt 3, enligt anmälan från medlemsstaterna, både i människoläsbart och i ett signerat maskinläsbart format.

▼C1

Artikel 3

Tillämpning

Detta beslut ska tillämpas från och med den 28 december 2009.

Artikel 4

Adressater

Detta beslut riktar sig till medlemsstaterna.

▼C1

BILAGA

TEKNISKA SPECIFIKATIONER FÖR EN GEMENSAM MALL FÖR DEN TILLFÖRLITLIGA FÖRTECKNINGEN ÖVER ÖVERVAKADE/ACKREDITERADE TILLHANDAHÅLLARE AV CERTIFIERINGSTJÄNSTER

INLEDNING

1. **Allmänt**

Syftet med den gemensamma mallen för medlemsstaternas tillförlitliga förteckningar över övervakade/ackrediterade tillhandahållare av certifieringstjänster är att införa en gemensam metod för hur varje medlemsstat tillhandahåller information om certifieringstjänster från tillhandahållare av certifieringstjänster (nedan kallade *CSP*) ([1]) som de övervakar/ackrediterar med avseende på efterlevnaden av de relevanta bestämmelserna i direktiv 1999/93/EG. Detta omfattar tillhandahållande av historisk information om de övervakade/ackrediterade certifieringstjänsternas övervaknings-/ackrediteringsstatus.

De obligatoriska uppgifterna i den tillförlitliga förteckningen måste minst omfatta uppgifter om övervakade/ackrediterade CSP som utfärdar kvalificerade certifikat (nedan kallade *QC*) ([2]) i enlighet med bestämmelserna i direktiv 1999/93/EG (artikel 3.3, 3.2 och 7.1 a), inklusive uppgifter om det QC som stöder en elektronisk signatur och om huruvida signaturen har skapats av en säker anordning för skapande av signaturer (nedan kallad *SSCD*) ([3]).

Ytterligare information om andra CSP som inte utfärdar QC utan tillhandahåller tjänster som har anknytning till elektroniska signaturer (till exempel CSP som erbjuder tidsmärkningstjänster och som utfärdar igenkänningstecken för tidsmärkning, CSP som utfärdar icke-kvalificerade certifikat osv.) får ingå i den tillförlitliga förteckningen på nationell nivå och på frivillig basis.

Syftet med denna information är främst att underlätta valideringen av kvalificerade elektroniska signaturer (nedan kallade *QES*) och avancerade elektroniska signaturer (nedan kallade *AdES*) ([4]) som omfattas av ett kvalificerat certifikat ([5]) ([6]).

Den föreslagna gemensamma mallen är förenlig med en tillämpning som bygger på specifikationerna från Etsi TS 102231 ([7]), som används för att hantera inrättande, offentliggörande, lokalisering, åtkomst till, autentisering och förtroende för sådana förteckningar.

([1]) I enlighet med definitionen i artikel 2.11 i direktiv 1999/93/EG.
([2]) I enlighet med definitionen i artikel 2.10 i direktiv 1999/93/EG.
([3]) I enlighet med definitionen i artikel 2.6 i direktiv 1999/93/EG.
([4]) I enlighet med definitionen i artikel 2.2 i direktiv 1999/93/EG.
([5]) För en avancerad elektronisk signatur som stöds av ett QC kommer förkortningen ”$AdES_{QC}$” att användas i resten av dokumentet.
([6]) Observera att det finns ett antal elektroniska tjänster som är baserade på enkla AdES vars gränsöverskridande användning också skulle underlättas om de stödjande certifikattjänsterna (till exempel utfärdande av icke-kvalificerade certifikat) ingick i de övervakade/ackrediterade tjänster som omfattas av en medlemsstat i den frivilliga uppgiftsdelen av deras tillförlitliga förteckning.
([7]) Etsi TS 102231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

2. **Riktlinjer för att redigera uppgifter i den tillförlitliga förteckningen**

2.1 *En tillförlitlig förteckning som är inriktad på övervakade/ackrediterade certifieringstjänster*

Relevanta certifieringstjänster och tillhandahållare av certifieringstjänster i en enda förteckning

Med en medlemsstats tillförlitliga förteckning avses *förteckningen över övervakningS-/ackrediteringsstatus för tillhandahållare av certifieringstjänster som övervakas/ackrediteras av den angivna medlemsstaten med avseende på efterlevnaden av de relevanta bestämmelserna i direktiv 1999/93/EG*.

En sådan tillförlitlig förteckning måste omfatta

— samtliga tillhandahållare av certifieringstjänster i enlighet med definitionen i artikel 2.11 i direktiv 1999/93/EG, det vill säga ”organ eller en fysisk eller juridisk person som utfärdar certifikat eller tillhandahåller andra tjänster som har anknytning till elektroniska signaturer”,

— som övervakas/ackrediteras med avseende på efterlevnaden av de relevanta bestämmelserna i direktiv 1999/93/EG.

När man ser på definitionerna och bestämmelserna i direktiv 1999/93/EG, särskilt när det gäller de aktuella CSP och deras övervaknings-/ackrediteringssystem går det att urskilja två grupper av CSP, nämligen sådana som utfärdar QC till allmänheten (CSP_{QC}) och sådana som inte utfärdar QC till allmänheten utan erbjuder andra tjänster som stöder elektroniska signaturer.

— **CSP som utfärdar QC:**

  — Dessa måste övervakas av den medlemsstat som de är etablerade i (om de är etablerade i en medlemsstat) och de får också ackrediteras för överensstämmelse med bestämmelserna i direktiv 1999/93/EG, inklusive kraven i bilaga I (krav på QC) och i bilaga II (krav på CSP som utfärdar QC). CSP som utfärdar QC och som är ackrediterade i en medlemsstat måste ändå omfattas av det tillämpliga övervakningssystemet i den medlemsstaten, utom om de inte är etablerade i den medlemsstaten.

  — Det tillämpliga övervakningssystemet (respektive frivilliga ackrediteringssystemet) fastställs i och måste uppfylla de tillämpliga kraven i direktiv 1999/93/EG, särskilt dem som anges i artikel 3.3, 8.1 och 11 samt skäl 13 (respektive artikel 2.13, 3.2, 7.1 a, 8.1 och 11 samt skäl 4 och skälen 11–13).

— **CSP som inte utfärdar QC:**

  — Dessa kan omfattas av ett frivilligt ackrediteringssystem (enligt definitionen i och i enlighet med direktiv 1999/93/EG) och/eller ett nationellt system för godkännande som tillämpas på nationell basis för att se till att bestämmelserna i direktivet och eventuella nationella bestämmelser för tillhandahållande av certifieringstjänster (i den mening som avses i artikel 2.11 i direktivet) följs.

  — Vissa av de fysiska eller binära (logiska) objekt som genereras eller utfärdas till följd av tillhandahållandet av en certifieringstjänst kan ha rätt till en särskild kvalificering på grund av att de uppfyller de bestämmelser och krav som fastställs på nationell nivå, men innebörden av en sådan kvalificering är sannolikt begränsad enbart till den nationella nivån.

▼C1

En medlemsstats tillförlitliga förteckning måste innehålla minimiuppgifter om en övervakad/ackrediterad CSP som utfärdar kvalificerade certifikat till allmänheten i enlighet med bestämmelserna i direktiv 1999/93/EG (artikel 3.3, 3.2 och 7.1 a), uppgifter om det QC som stöder den elektroniska signaturen och om huruvida signaturen skapas genom en säker anordning för skapande av signaturer eller ej.

Ytterligare information om andra övervakade/ackrediterade tjänster från CSP som inte utfärdar QC till allmänheten (till exempel CSP som erbjuder tidsmärkningstjänster och som utfärdar igenkänningstecken för tidsmärken, CSP som utfärdar icke-kvalificerade certifikat osv.) får ingå i den tillförlitliga förteckningen på nationell nivå på frivillig basis.

Syftet med den tillförlitliga förteckningen är att

— förteckna och tillhandahålla tillförlitlig information om övervaknings-/ackrediteringsstatusen för CSP som övervakas/ackrediteras av den medlemsstat som ansvarar för att inrätta och underhålla förteckningen för att uppfylla de relevanta bestämmelserna i direktiv 1999/93/EC,

— underlätta valideringen av de elektroniska signaturer som stöds av de förtecknade övervakade/ackrediterade certifieringstjänsterna från de förtecknade CSP.

En enda uppsättning statusvärden för övervakning/ackreditering

En enda tillförlitlig förteckning ska inrättas och underhållas per medlemsstat för att ange övervaknings- och/eller ackrediteringsstatus för de certifieringstjänster från de CSP som övervakas/ackrediteras av medlemsstaten.

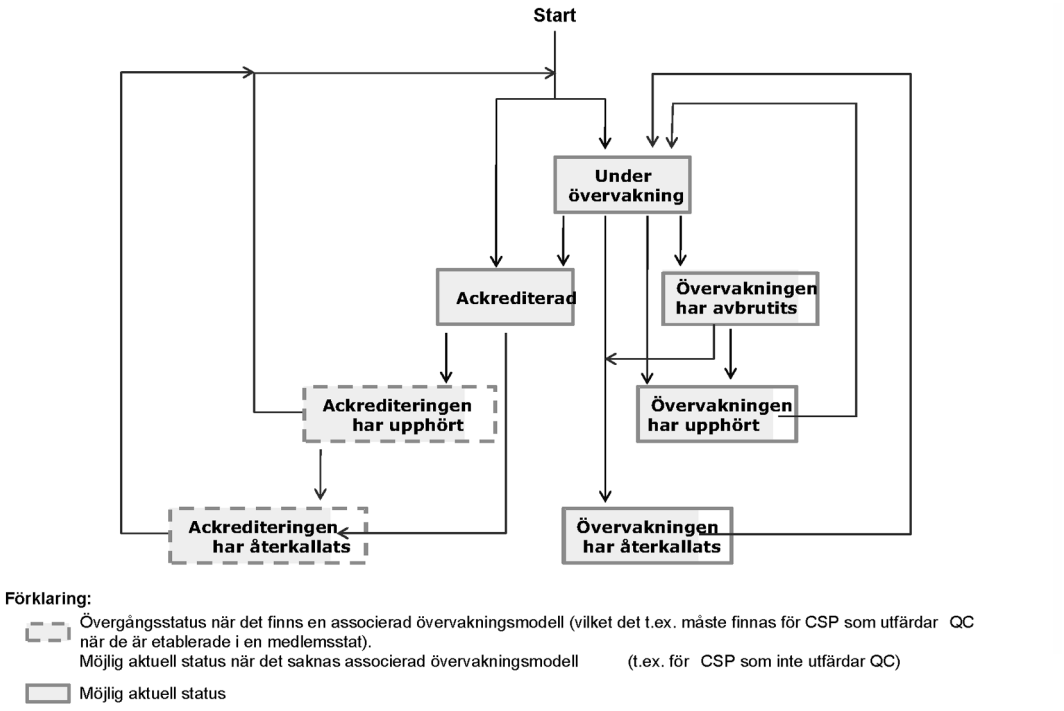
Det faktum att en tjänst för ögonblicket antingen övervakas och/eller är ackrediterad ska anges i dess aktuella status. Dessutom kan en övervakning eller ackreditering ha statusen ”pågår”, ”har avbrutits”, ”har upphört” eller ”har återkallats”. Samma certifieringstjänst kan med tiden gå från övervakningsstatus till ackrediteringsstatus och vice versa [1].

I figur 1 beskrivs det förväntade flödet för en enda certifieringstjänst mellan möjliga övervaknings-/ackrediteringsstatusar:

[1] En tillhandahållare av certifikattjänster som är etablerad i en medlemsstat och som tillhandahåller en certifikattjänst som till en början övervakas av den medlemsstaten (övervakningsorganet) kan t.ex. efter ett tag besluta sig för att inhämta en frivillig ackreditering för den övervakade certifikattjänsten. Å andra sidan kan en tillhandahållare i en annan medlemsstat besluta sig för att inte upphöra med en ackrediterad certifikattjänst utan att flytta den från en ackrediteringsstatus till en övervakningsstatus av affärsmässiga eller ekonomiska skäl.

▼C1

Förväntat övervaknings-/ackrediteringsflöde för en enda CSP-tjänst



Figur 1

En certifieringstjänst som utfärdar QC måste övervakas (om den är etablerad i en medlemsstat) och får ackrediteras frivilligt. En sådan tjänst som är upptagen i en tillförlitlig förteckning kan ha vilket som helst av de ovan angivna statusvärdena som ”aktuellt statusvärde”. Det bör emellertid noteras att ”Ackrediteringen har upphört” och ”Ackrediteringen återkallats” båda måste vara övergångsvärden endast när det gäller CSP_{QC}-tjänster som är etablerade i en medlemsstat, eftersom dessa tjänster alltid måste övervakas (också om de inte, eller inte längre, är ackrediterade).

Medlemsstater som inrättar eller har inrättat nationella erkända system för godkännande som tillämpas på nationell basis för att övervaka att tjänster från CSP som inte utfärdar QC uppfyller bestämmelserna i direktiv 1999/93/EG och eventuella nationella bestämmelser om tillhandahållande av certifieringstjänster (i den mening som avses i artikel 2.11 i direktivet) ska kategorisera dessa system för godkännande enligt följande två kategorier:

— ”Frivillig ackreditering” i enlighet med definitionen och bestämmelserna i direktiv 1999/93/EG (artikel 2.13, 3.2, 7.1 a, 8.1, 11 och skäl 4, 11–13).

— ”Övervakning” som uppfyller kraven i direktiv 1999/93/EG och som tillämpas genom nationella bestämmelser och krav som är förenlig med den nationella lagstiftningen.

▼C1

En certifieringstjänst som inte utfärdar QC kan alltså övervakas/ackrediteras frivilligt. Statusvärdet för en sådan tjänst i en tillförlitlig förteckning kan ha vilket som helst av de ovan angivna statusvärdena som ”aktuellt statusvärde” (se figur 1).

Den tillförlitliga förteckningen måste innehålla uppgifter om de underliggande övervaknings-/ackrediteringssystemen och särskilt uppgifter om följande:

— Det övervakningssystem som är tillämpligt på alla CSP_{QC}.

— I förekommande fall det nationella frivilliga ackrediteringssystem som är tillämpligt på alla CSP_{QC}.

— I förekommande fall det övervakningssystem som är tillämpligt på alla CSP som inte utfärdar QC.

— I förekommande fall det nationella frivilliga ackrediteringssystem som är tillämpligt på alla CSP som inte utfärdar QC.

De sista två uppsättningarna av uppgifter är av kritisk betydelse för att beroende parter ska kunna bedöma kvaliteten och säkerhetsnivån på övervaknings-/ackrediteringssystem som tillämpas på nationell nivå för CSP som inte utfärdar QC. När uppgifter om övervaknings-/ackrediteringsstatus tillhandahålls i den tillförlitliga förteckningen med avseende på tjänster från CSP som inte utfärdar QC ska de ovannämnda uppsättningarna av uppgifter tillhandahållas på tillförlitlig förteckningsnivå genom användning av en URI för systeminformation (klausul 5.3.7 – information som tillhandahålls av medlemsstaterna), information om typ/gemenskap/bestämmelser för systemet (klausul 5.3.9 – med en text som är gemensam för alla medlemsstater och valfri specifik information som tillhandahålls av en medlemsstat) samt policy/rättsligt meddelande om förteckningen över betrodda tjänster (klausul 5.3.11 – en text som är gemensam för alla medlemsstater med en hänvisning till direktiv 1999/93/EG, tillsammans med en möjlighet för varje medlemsstat att lägga till medlemsstatsspecifika texter/hänvisningar). Ytterligare kvalificeringsuppgifter som definieras i de nationella övervaknings-/ackrediteringssystemen för CSP som inte utfärdar QC får i förekommande fall och om så krävs tillhandahållas på tjänstenivå (till exempel för att skilja mellan flera kvalitets- eller säkerhetsnivåer) genom användning av tillägget ”additionalServiceInformation” (klausul 5.8.2) som en del av tillägget för tjänsteinformation (klausul 5.5.9). Ytterligare information om motsvarande tekniska specifikationer finns i de detaljerade specifikationerna i kapitel I.

Trots att separata organ i en medlemsstat kan ansvara för övervakning och ackreditering av certifieringstjänster i den medlemsstaten förväntas att endast en registerpost används för en enda certifieringstjänst (identifierad genom tjänstens digitala identitet i enlighet med Etsi TS 102231 ([1]) och att dess övervaknings-/ackrediteringsstatus uppdateras i enlighet med detta. Innebörden av de ovan återgivna statusarna beskrivs i klausul 5.5.4 i de detaljerade specifikationerna i kapitel I.

2.2. *Registerposter i den tillförlitliga förteckningen för att underlätta validering av QES och $AdES_{QC}$*

Den mest kritiska delen av inrättandet av den tillförlitliga förteckningen är att upprätta den obligatoriska delen av den tillförlitliga förteckningen, det vill säga förteckningen över tjänster per CSP som utfärdar QC för att korrekt avspegla den exakta utfärdandesituationen för varje sådan tjänst som utfärdar QC och se till att den information som tillhandahålls i varje registerpost är tillräcklig för att underlätta valideringen av QES och $AdES_{QC}$ (i kombination med innehållet i det slutliga QC som CSP utfärdar inom ramen för den certifieringstjänst som finns upptagen in denna registerpost).

([1]) Etsi TS 102231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

I den mån det saknas en verklig driftskompatibel och gränsöverskridande profil för QC kan den information som krävs omfatta annan information än tjänstens digitala identitet för en enda rotcertifikatutfärdare, särskilt uppgifter som bekräftar att det utfärdade certifikatet är kvalificerat och som anger huruvida de signaturer som stöds skapas med hjälp av en SSCD. Det organ i en medlemsstat som har utsetts att inrätta, redigera och underhålla den tillförlitliga förteckningen (det vill säga systemets operatör i enlighet med Etsi TS 102231) måste därför ta hänsyn till den aktuella profilen och certifikatsinnehållet i varje utfärdat QC per CSP_{QC} som omfattas av den tillförlitliga förteckningen.

Helst bör varje utfärdat QC omfatta Etsis QcCompliance ([1])-deklaration när det hävdas att det är fråga om ett QC och bör omfatta Etsis QcSSCD-deklaration när det hävdas att certifikatet stöds av en SSCD för att generera elektroniska signaturer och/eller att varje utfärdat QC omfattar en av de objektidentifierare (nedan kallad *OID*) för certifikatspolicyn för QCP/QCP + som fastställs i Etsi TS 101456 ([2]). CSP som utfärdar QC använder olika standarder som referenser, dessa standarder tolkas på många olika sätt och det saknas medvetenhet om att vissa normativa tekniska specifikationer eller standarder har företräde, vilket har lett till skillnader i det faktiska innehållet i aktuella utfärdade QC (till exempel huruvida Etsi-definierade ”QcStatements” används) vilket hindrar de mottagande parterna från att helt enkelt lita på undertecknarens certifikat (och tillhörande kedja/sökväg) för att åtminstone i maskinläsbar form kunna bedöma huruvida det certifikat som stöder en elektronisk signatur påstås vara ett QC och huruvida det är associerat till en SSCD som har använts för att skapa den elektroniska signaturen.

Genom fälten för identifiering av tjänstetyp (nedan kallad *Sti*), tjänstens namn (nedan kallad *Sn*) och tjänstens digitala identitet (nedan kallad *Sdi*) ([3]) fylls i med den information som lämnas i fältet för informationstillägg för tjänsten (nedan kallade *Sie*) innebär den föreslagna gemensamma mallen för tillförlitliga förteckningar att det blir möjligt att fullständigt ange en viss typ av kvalificerat certifikat som har utfärdats av en förtecknad certifieringstjänst från en CSP som utfärdar QC och upplysa om huruvida detta stöds av en SSCD eller ej (när denna information saknas i det utfärdade QC). En särskild upplysning om tjänstens nuvarande status (nedan kallad *Scs*) är förstås associerad till denna registerpost. Detta illustreras i figur 2 nedan.

Att registrera en tjänst i förteckningen genom att endast ange Sdi för en rotcertifikatutfärdare skulle innebära att man garanterar (av den CSP som utfärdar QC, men även av det övervaknings-/ackrediteringsorgan som ansvarar för övervakningen/ackrediteringen av den CSP som utfärdar QC) att eventuella slutanvändarcertifikat som utfärdats inom ramen för denna rotcertifikatutfärdare (hierarki) innehåller tillräckligt mycket Etsi-definierad och maskinläsbar information för att avgöra huruvida detta är ett QC eller ej och huruvida det stöds av en SSCD. Om det senare påståendet t.ex. inte är sant (det finns t.ex. ingen Etsi-standardiserad maskinläsbar angivelse i QC om huruvida det stöds av en SSCD), måste det förutsättas att enbart angivelsen Sdi för denna rotcertifikatutfärdare innebär att QC som utfärdas inom ramen för denna rotcertifikatutfärdarhierarki inte stöds av någon SSCD. För att dessa QC ska anses stödjas av en SSCD bör fältet Sie användas för att ange detta faktum (detta innebär också att detta garanteras av den CSP som utfärdar QC och övervakas/ackrediteras av övervaknings- eller ackrediteringsorganet).

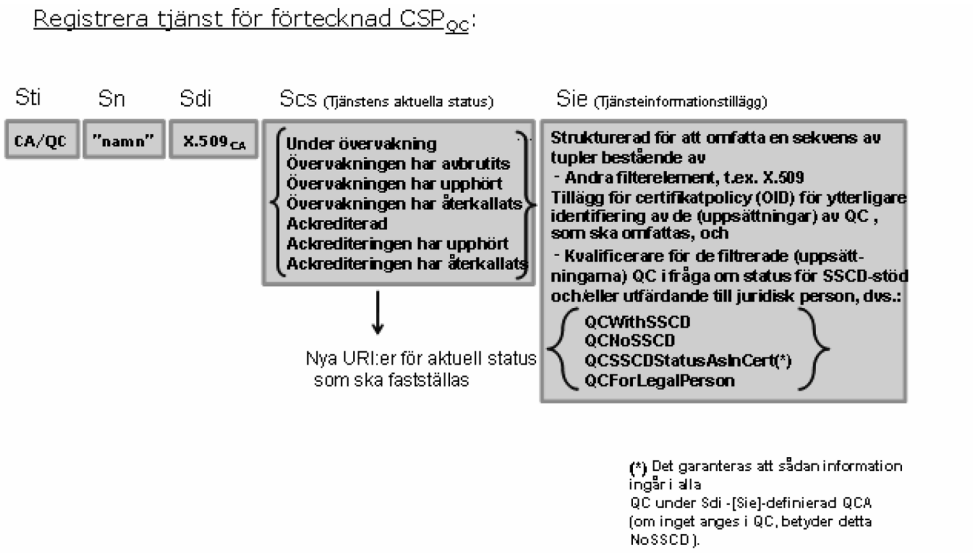
([1]) Se Etsi TS 101862 – Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.

([2]) Etsi TS 101456 - Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.

([3]) Dvs., som ett minimum, ett X.509 v3-certfikat för från utfärdande QCA eller en överordnad CA i certifieringssökvägen.

▼C1

Allmänna principer – Redigeringsregler –CSP_{QC}-poster (förtecknade tjänster)



Figur 2

Tjänst från en förtecknad CSP som utfärdar QC som är upptagna i TSL-tillämpningen av den tillförlitliga förteckningen.

Dessa tekniska specifikationer för den gemensamma mallen för den tillförlitliga förteckningen gör det möjligt att använda en kombination av fem huvuddelar av uppgifter i tjänsteregistreringen:

— Identifiering av typ av tjänst (nedan kallad *Sti*) – t.ex. en certifikatutfärdare som utfärdar QC (nedan kallad *CA/QC*).

— Tjänstens namn (nedan kallad *Sn*).

— Uppgifter om tjänstens digitala identitet (nedan kallad *Sdi*), som identifierar en förtecknad tjänst, t.ex. X.509v3-certifikatet för (minst) en CA/QC.

— För CA/QC-tjänster finns frivilliga informationstillägg (nedan kallade *Sie*) som gör det möjligt att lägga in en sekvens av en eller flera tupler, där varje tupel ska innehålla följande:

  — Kriterier som ska användas för att under den Sdi-identifierade certifieringstjänsten ytterligare identifiera (filtrera) exakt den tjänst (dvs. uppsättning av kvalificerade certifikat) för vilka ytterligare uppgifter krävs/tillhandahålls med avseende på SSCD-stöd (och/eller utfärdande till en juridisk person).

  — Därmed sammanhängande information (kvalificerare) om huruvida denna ytterligare identifierade tjänsteuppsättning av kvalificerade certifikat stöds av en SSCD eller huruvida den därmed sammanhängande informationen ingår i QC i en standardiserad maskinläsbar form och/eller information om att dessa QC utfärdas till juridiska personer (det förinställda värdet är att de ska betraktas som utfärdade till endast fysiska personer).

▼C1

— Information om den registrerade tjänstens aktuella status med uppgifter om

— huruvida tjänsten är övervakad/ackrediterad, och

— status för övervakningen/ackrediteringen.

2.3. *Riktlinjer för redigering och användning om registrerade CSP_{QC}-tjänster*

De **allmänna riktlinjerna för redigering** är följande:

1. Om det säkerställs (garanteras av CSP_{QC} och övervakas/ackrediteras av övervakningsorganet eller ackrediteringsorganet) att alla QC för en förtecknad tjänst som identifieras med en Sdi och som stöds av en SSCD verkligen innehåller den Etsi-definierade QcCompliance-deklarationen, och verkligen innehåller QcSSCD-deklarationen och/eller QCP + Object Identifier (OID), är det tillräckligt att använda en lämplig Sdi. Användningen av Sie-fältet är frivillig och detta fält behöver inte innehålla uppgifter om SSCD-stöd.

2. Om det säkerställs (garanteras av CSP_{QC} och övervakas/ackrediteras av övervakningsorganet eller ackrediteringsorganet) att alla QC för en förtecknad tjänst som identifieras med en Sdi och som inte stöds av en SSCD verkligen innehåller antingen en QcCompliance-deklaration eller en QCP + OID, och att det är av en sådan art att det är avsett att inte innehålla QcSSD-deklarationen eller QCP + OID, är det tillräckligt att använda en lämplig Sdi. Användningen av Sie-fältet är frivillig och detta fält behöver inte innehålla uppgifter om SSCD-stöd (dvs. att det saknas SSCD-stöd).

3. Om det säkerställs (garanteras av CSP_{QC} och övervakas/ackrediteras av ett övervaknings-/ackrediteringsorgan) att alla QC för en förtecknad tjänst som identifieras med en Sdi verkligen innehåller QcCompliance-deklarationen och vissa av dessa QC är avsedda att stödjas av en SSCD, medan andra inte är det (detta kan t.ex. särskiljas genom olika CSP-specifika OID:er för certifikatpolicy eller genom annan CSP-specifik information i QC, direkt eller indirekt, maskinläsbart eller ej), men den VARKEN innehåller QcSSCD-deklarationen ELLER Etsi QCP(+) OID, är det möjligt att det inte räcker med att ange en lämplig Sdi OCH att Sie-fältet måste användas för att ge uttrycklig information om SSCD-stöd tillsammans med ett eventuellt informationstillägg för att identifiera den certifikatuppsättning som omfattas. I så fall måste man sannolikt lägga in olika värden för SSCD-stöd för samma Sdi när man använder Sie-fältet.

4. Om det säkerställs (garanteras av CSP_{QC} och övervakas/ackrediteras av ett övervaknings-/ackrediteringsorgan) att inga QC för en förtecknad tjänst som identifieras med en Sdi innehåller någon QcCompliance-deklaration, QCP OID, QcSSCD-deklaration eller QCP + OID, men det säkerställs att vissa av de slutanvändarcertifikat som utfärdas inom ramen för denna Sdi är avsedda att vara QC och/eller stödjas av SSCD och vissa inte är det (detta kan t. ex. särskiljas genom olika CSP_{QC}-specifika OID:er för certifikatpolicy eller genom annan CSP_{QC}-specifik information i QC, direkt eller indirekt, maskinläsbart eller ej), är det inte tillräckligt med att ange en lämplig Sdi OCH Sie-fältet måste användas för att inkludera uttrycklig information om SSCD-stöd. I så fall måste man sannolikt lägga in olika värden för SSCD-stöd för samma Sdi när man använder Sie-fältet.

▼C1

Som en allmän standardprincip måste det för en CSP som är upptagen i den tillförlitliga förteckningen finnas en registrerad tjänst per enkelt X.509v3-certifikat för en certifieringstjänst av CA/QC-typ, dvs. en certifikatutfärdare som (direkt) utfärdar QC. Under vissa noggrant övervägda omständigheter och noggrant utformade villkor, får en medlemsstats övervaknings- eller ackrediteringsorgan besluta att använda X.509v3-certifikatet för en rotcertifikatutfärdare eller överordnad certifikatutfärdare (dvs. en certifikatutfärdare som inte direkt utfärdar slutliga QC utan som certifierar en hierarki av CA ner till en CA som utfärdar QC till slutanvändare) som Sdi för en enda registerpost i förteckningen över tjänster från en CSP som är upptagen i förteckningen. Konsekvenserna (fördelar och nackdelar) med att använda X.509v3 rotcertifikatutfärdare eller överordnad certifikatutfärdare som Sdi-värden för registrering av tjänster i den tillförlitliga förteckningen måste noggrant övervägas och godkännas av medlemsstaterna. När medlemsstaten utnyttjar detta tillåtna undantag från standardprincipen, måste den dessutom tillhandahålla den nödvändiga dokumentationen för att underlätta uppbyggnad av sökvägar och verifiering.

Detta exempel kan användas som illustration av de allmänna riktlinjerna för redigering: Om det är fråga om en CSP_{QC} som använder en rotcertifikatutfärdare under vilken flera CA utfärdar QC och icke-QC, men för vilken QC endast innehåller QcCompliance-deklarationen och saknar angivelse av huruvida den stöds av en SSCD, skulle en registrering av en rotcertifikatutfärdare Sdi enligt de bestämmelser som förklaras ovan endast innebära att QC som utfärdas under denna rotcertifikatutfärdarhierarki INTE stöds av en SSCD. Om dessa QC faktiskt stöds av en SSCD rekommenderas dock starkt att QcSSCD-deklarationen används i de QC som utfärdas i framtiden. Under tiden (tills det sista QC som inte innehåller denna information har löpt ut), bör man i statusförteckningen över betrodda tjänster (nedan kallad *TSL*) använda sig av Sie-fältet och tillhörande kvalificeringstillägg, t.ex. genom att filtrera certifikat genom särskilda CSP_{QC}-definierade OID:er som CSP_{QC} eventuellt använder för att skilja mellan olika typer av QC (där vissa stöds av en SSCD och andra inte) och som omfattar explicit information om SSCD-stöd – med avseende på de certifikat som filtreras genom användning av kvalificerare.

De allmänna riktlinjerna för användning av tillämpningar för elektroniska signaturer, tjänster eller produkter som bygger på en TSL-tillämpning av en tillförlitlig förteckning i enlighet med dessa tekniska specifikationer, är följande:

En registrering av CA/QC Sti (och även en CA/QC-registrering som kvalificeras som en RootCA/QC genom tillägget Sie additionalServiceInformation) innebär följande:

— Alla slutanvändarcertifikat som utfärdas från den CA som identifierats i Sdi (och även inom CA-hierarkin med början i den RootCA som identifieras i Sdi) är QC, under förutsättning att det hävdas att de är kvalificerade i certifikatet med hjälp av lämpliga QcStatements (dvs. QcC, QcSSCD) och/eller Etsi-definierade QCP (+) OID:er (och detta säkerställs av övervaknings-/ackrediteringsorganet, se de allmänna riktlinjerna för redigering ovan).

Anmärkning: Om det inte finns någon kvalificeringsinformation för Sie eller om ett slutanvändarcertifikat som påstås vara ett QC inte identifieras ytterligare genom en relaterad Sie-registering ska den maskinläsbara information som finns i QC övervakas/ackrediteras för att vara korrekt. Detta innebär att det ska säkerställas att användningen (eller ej) av lämpliga QcStatements (dvs. QcC, QcSSCD) och/eller Etsi-definierade QCP(+) OID:er är förenlig med vad CSP_{QC} påstår.

▼C1

— **Om** det finns kvalificeringsinformation för Sie gäller, i tillägg till ovannämnda tolkningsregel för standardanvändning, att de certifikat som identifieras genom användning av denna kvalificeringsregistrering för Sie, som bygger på principen med en sekvens av ”filter” som ytterligare identifierar en uppsättning certifikat och ger viss ytterligare information om SSCD-stöd och/eller att certifikatet utfärdats till en juridisk person (t.ex. certifikat som innehåller en viss OID i tillägget för certifikatpolicy eller har ett visst nyckelanvändningsmönster, och/eller filtreras genom användning av ett visst värde som ska visas i ett visst certifikatsfält eller tillägg osv.), ska betraktas i enlighet med följande uppsättning av kvalificerare, som ska kompensera bristen på information i motsvarande QC:

— För att ange SSCD-stöd:

— ”QCWithSSCD”, vilket betyder ”QC som stöds av en SSCD”, eller

— ”QCNoSSCD”, vilket innebär ”QC som inte stöds av en SSCD”, eller

— ”QCSSCDStatusAsInCert” vilket innebär att det garanteras att information om SSCD-stöd finns i alla QC som omfattas av den Sdi-/Sie-angivna informationen i denna CA/QC-post,

och/eller

— För att ange utfärdande till juridisk person:

— ”QCForLegalPerson”, vilket betyder ”certifikat utfärdat till en juridisk person”.

2.4. *Tjänster som stöder CA/QC-tjänster men som inte ingår i CA/QC Sdi*

De fall då CRL:er och OCSP-svar signeras med andra nycklar än dem som kommer från en CA/QC bör också omfattas. Det kan man göra genom att föra upp dessa tjänster som sådana i TSL-tillämpningen av den tillförlitliga förteckningen (dvs. med en identifiering av tjänstetyp som ytterligare kvalificeras med ett tillägg om ”additionalServiceInformation” som avspeglar antingen en OCSP eller en CRL-tjänst som del av utfärdandet av QC, t.ex. med en tjänstetyp OCSP/QC respektive CRL/QC) eftersom dessa tjänster kan anses vara en del av de övervakade/ackrediterade kvalificerade tjänsterna med anknytning till tillhandahållandet av QC-certifieringstjänster. OCSP-respondrar eller CRL-utfärdare vars certifikat signeras av CA inom hierarkin för en CA/QC-tjänst som är upptagen i förteckningen ska betraktas som giltiga och förenliga med statusvärdet för CA/QC-tjänsten i förteckningen.

En liknande bestämmelse kan tillämpas för certifieringstjänster som utfärdar icke-kvalificerade certifikat (av typen CA/PKC-tjänst) som använder Etsi TS 102231 OCSP- och CRL-standardtjänstetyper.

Observera att TSL-tillämpningen av den tillförlitliga förteckningen MÅSTE omfatta återkallningstjänster när den relaterade informationen inte finns i de slutliga certifikatens AIA-fält eller när de inte har signerats av en CA som är upptagen i förteckningen.

2.5. *Utveckling mot driftskompatibel QC-profil*

Rent generellt måste man så långt som möjligt förenkla (minska) antalet poster med registrerade tjänster (olika Sdi:er). Detta måste emellertid balanseras med en korrekt identifiering av de tjänster som har anknytning till utfärdande av QC och tillhandahållande av tillförlitlig information om huruvida dessa QC stöds av en SSCD eller ej, när denna information saknas i det utfärdade QC.

▼C1

Helst bör användningen av Sie-fältet och kvalificeringstillägget vara (strängt) begränsad till de specifika fall som behöver lösas på det sättet, eftersom QC bör innehålla tillräckligt med information i fråga om den påstådda kvalificerade statusen och det påstådda stödet eller ej från en SSCD.

Medlemsstaterna bör i så stor utsträckning som möjligt se till att driftskompatibla QC-profiler införs och används.

3. **Struktur för den gemensamma mallen för den tillförlitliga förteckningen**

Den föreslagna gemensamma mallen för medlemsstaternas tillförlitliga förteckningar kommer att struktureras enligt följande informationskategorier:

1. Information om den tillförlitliga förteckningen och dess system för utfärdande.

2. En sekvens av fält med otvetydig identifieringsinformation om varje CSP som övervakas/ackrediteras i enlighet med systemet (denna sekvens är valfri, vilket innebär att om den inte används kommer förteckningen att betraktas som tom, dvs. att ingen CSP övervakas/ackrediteras i den aktuella medlemsstaten inom ramen för den tillförlitliga förteckningens räckvidd).

3. För varje CSP som är upptagen i förteckningen, en sekvens av fält som innehåller otvetydig identifieringsinformation om en övervakad/ackrediterad certifieringstjänst som den tillhandahållaren erbjuder (denna sekvens måste innehålla minst en post).

4. För varje övervakad/ackrediterad certifieringstjänst som är upptagen i förteckningen, identifiering av tjänstens aktuella status och dess statushistorik.

När det gäller en CSP som utfärdar QC måste en otvetydig identifiering av en övervakad/ackrediterad certifieringstjänst som ska tas upp i förteckningen ta hänsyn till de situationer då det inte finns tillräckligt med information tillgänglig i QC om dess status som ”kvalificerat”, dess eventuella stöd från en SSCD och särskilt för att hantera det ytterligare faktum att de flesta (kommersiella) CSP använder en enda utfärdande kvalificerad CA för att utfärda flera typer av slutanvändarcertifikat, såväl kvalificerade som icke-kvalificerade.

Antalet poster i förteckningen per erkänd CSP kan minskas om det finns en eller flera överordnade CA-tjänster, t.ex. inom ramen för en kommersiell hierarki av CA från en rotcertifikatutfärdare ned till utfärdande CA. Men också i dessa fall måste principen om att säkerställa en otvetydig koppling mellan en certifieringstjänst från en CSP_{QC} och uppsättningen av certifikat som ska identifieras som QC upprätthållas och garanteras.

1. *Information om den tillförlitliga förteckningen och dess system för utfärdande*

Följande uppgifter kommer att ingå i denna kategori:

— En tillförlitlig förteckningstagg som gör det lättare att identifiera den tillförlitliga förteckningen under elektroniska sökningar och även bekräfta dess syfte när den är i läsbart format.

— Ett format och en formatversionidentifiering för den tillförlitliga förteckningen.

— Ett sekvens- (eller utgivnings-) nummer för den tillförlitliga förteckningen.

— Typinformation för den tillförlitliga förteckningen (t.ex. för att det ska gå att se att denna tillförlitliga förteckning innehåller information om övervaknings-/ackrediteringsstatus för certifieringstjänster från CSP som övervakas/ackrediteras av den aktuella medlemsstaten med avseende på efterlevnaden av bestämmelserna i direktiv 1999/93/EG).

▼C1

— Ägarinformation för den tillförlitliga förteckningen (t.ex. namn, adress, kontaktuppgifter osv. för det organ i medlemsstaten som ansvarar för att inrätta, offentliggöra på ett säkert sätt och underhålla den tillförlitliga förteckningen).

— Information om de underliggande övervaknings-/ackrediteringssystem som den tillförlitliga förteckningen är associerad till, vilket omfattar, men inte begränsas till

  — det land som den är tillämplig i,

  — information om eller hänvisning till var man kan hitta uppgifter om systemet/systemen (systemmodell, bestämmelser, kriterier, typ, m.m.),

  — information om hur länge (historisk) information sparas.

— Policy och eller rättsakt, förpliktelser och ansvarsområden för den tillförlitliga förteckningen.

— Utfärdandedag samt tidpunkt för nästa planerade uppdatering för den tillförlitliga förteckningen.

2. *Otvetydig identifieringsinformation om varje CSP som erkänns genom systemet*

Här ska minst följande uppgifter ingå:

— Det organisationsnamn för CSP som använts i formella juridiska registreringar (detta kan omfatta organisationens användar-ID, beroende på praxis i medlemsstaten).

— Adress- och kontaktuppgifter för CSP.

— Ytterligare information om CSP, antingen direkt eller i form av en hänvisning till en plats där denna information kan laddas ned.

3. *För varje CSP som är upptagen i förteckningen, en sekvens av fält som innehåller otvetydig identifieringsinformation om en certifieringstjänst som tillhandahållaren erbjuder och som övervakas/ackrediteras inom ramen för direktiv 1999/93/EG*

Dessa uppgifter ska minst omfatta följande för varje certifieringstjänst från en CSP som är upptagen i förteckningen:

— En identifikation för typen av certifieringstjänst (som t.ex. anger att den övervakade/ackrediterade certifieringstjänsten från CSP är en certifikatutfärdare som utfärdar QC).

— Denna certifieringstjänsts (handels-)namn.

— En unik otvetydig identifikation för certifieringstjänsten.

— Ytterligare information om certifieringstjänsten (kan t.ex. ges direkt eller genom en hänvisning till en plats som informationen kan laddas ned från, information om tillgång till tjänsten).

— För CA/QC-tjänster en valfri sekvens av tupler där varje tupel ger information om

  i) kriterier som ska användas för att inom den Sdi-identifierade certifieringstjänsten ytterligare identifiera (filtrera) exakt den tjänst (dvs. uppsättning av kvalificerade certifikat) för vilken ytterligare uppgifter krävs/tillhandahålls med avseende på indikationen av SSCD-stöd (och/eller utfärdande till en juridisk person),

  ii) de tillhörande kvalificerarna som ger information om huruvida uppsättningen av kvalificerade certifikat från denna ytterligare identifierade tjänst stöds av en SSCD eller ej, och/eller uppgifter om huruvida dessa QC utfärdas till en juridisk person (som standard ska de betraktas som utfärdade till endast fysiska personer).

▼C1

4. *För varje certifieringstjänst som är upptagen i förteckningen, identifiering av tjänstens aktuella status och dess statushistorik*

Här ska minst följande uppgifter ingå:

— En identifikation för aktuell status.

— Startdag och starttid för aktuell status.

— Historisk information om denna status.

4. **Definitioner och förkortningar**

I detta dokument används följande förkortningar och akronymer:

Term	Förkortning	Definition
Tillhandahållare av certifieringstjänster	CSP	I enlighet med definitionen i artikel 2.11 i direktiv 1999/93/EG.
Certifikatutfärdare	CA	En certifikatutfärdare är en CSP och kan använda flera tekniska certifikatutfärdares privata signeringsnycklar, där varje nyckel har ett associerat certifikat, för att utfärda slutanvändarcertifikat. En certifikatutfärdare är en utfärdare som betraktas som tillförlitlig av en eller flera användare för att skapa och utfärda certifikat. Certifikatutfärdaren får också skapa användarnycklar [Etsi TS 102 042]. CA anses vara identifierad genom den identifieringsinformation om finns i utfärdarfältet i CA-certifikatet för (som certifierar) den offentliga nyckel som är associerad till CA:s privata signeringsnyckel och som CA i praktiken använder för att utfärda enhetscertifikat. En CA kan ha flera signeringsnycklar. Varje signeringsnyckel identifieras med en unik identifikation i fältet för identifiering av utfärdarnyckel i CA:s certifikat.
Certifikatutfärdare som utfärdar kvalificerade certifikat	CA/QC	En CA som uppfyller kraven i bilaga II till direktiv 1999/93/EG och som utfärdar kvalificerade certifikat som uppfyller kraven i bilaga I till direktiv 1999/93/EG.
Certifikat	Certifikat	I enlighet med definitionen i artikel 2.9 i direktiv 1999/93/EG.
Kvalificerat certifikat	QC	I enlighet med definitionen i artikel 2.10 i direktiv 1999/93/EG.
Undertecknare	Undertecknare	I enlighet med definitionen i artikel 2.3 i direktiv 1999/93/EG.
Övervakning	Övervakning	”Övervakning” används i den mening som avses i direktiv 1999/93/EG (artikel 3.3). Enligt direktivet ska medlemsstaterna införa ett lämpligt system som gör det möjligt att övervaka de CSP som är etablerade på deras territorium och som utfärdar kvalificerade certifikat till allmänheten, för att se till att bestämmelserna i direktivet följs.
Frivillig ackreditering	Ackreditering	I enlighet med definitionen i artikel 2.13 i direktiv 1999/93/EG.
Tillförlitlig förteckning	TL	Förteckningen över övervaknings-/ackrediteringsstatus för certifieringstjänster från tillhandahållare av certifieringstjänster som övervakas/ackrediteras av den angivna medlemsstaten med avseende på efterlevnaden av de relevanta bestämmelserna i direktiv 1999/93/EG.

▼C1

Term	Förkortning	Definition
Statusförteckning över betrodda tjänster	TSL	En form av signerad förteckning som ligger till grund för presentation av uppgifter om status för betrodda tjänster enligt specifikationerna i Etsi TS 102231.
Betrodd tjänst		Tjänst som ökar tilliten till och förtroendet för elektroniska transaktioner (oftast, men inte nödvändigtvis, med hjälp av krypteringstekniker eller med hjälp av konfidentiellt material) (Etsi TS 102231).
Tillhandahållare av betrodda tjänster	TSP	Organisation som driver en eller flera (elektroniska) betrodda tjänster (denna term används i en bredare bemärkelse än CSP).
Igenkänningstecken för betrodd tjänst	TrST	Ett fysiskt eller binärt (logiskt) objekt som genereras eller utfärdas till följd av att en betrodd tjänst har använts. Exempel på binära TrST:er är certifikat, CRL:er, igenkänningstecken för tidsmärken och OCSP-responser.
Kvalificerad elektronisk signatur	QES	En avancerad elektronisk signatur (AdES) som stöds av ett QC och som skapas med en SSCD enligt artikel 2 i direktiv 1999/93/EG.
Avancerad elektronisk signatur	AdES	I enlighet med definitionen i artikel 2.2 i direktiv 1999/93/EG.
Avancerad elektronisk signatur som stöds av ett kvalificerat certifikat	$AdES_{QC}$	En elektronisk signatur som uppfyller kraven på en AdES och som stöds av ett QC enligt definitionen i artikel 2 i direktiv 1999/93/EG.
Säker anordning för skapande av signaturer	SSCD	I enlighet med definitionen i artikel 2.6 i direktiv 1999/93/EG.

KAPITEL I

DETALJERADE SPECIFIKATIONER FÖR DEN GEMENSAMMA MALLEN FÖR DEN ”TILLFÖRLITLIGA FÖRTECKNINGEN ÖVER ÖVERVAKADE/ACKREDITERADE TILLHANDAHÅLLARE AV CERTIFIERINGSTJÄNSTER”

I följande del av detta dokument ska nyckelorden ”MÅSTE”, ”FÅR INTE”, ”OBLIGATORISK”, ”SKA”, ”SKA INTE”, ”BÖR”, ”BÖR INTE”, ”REKOMMENDERAD”, ”FÅR” och ”FRIVILLIG” tolkas enligt beskrivningen i RFC 2119 ([1]).

►**M1** Dessa specifikationer bygger på specifikationerna och kraven enligt Etsi TS 102231 v.3.1.2. När inget särskilt krav anges i dessa specifikationer SKA kraven i Etsi TS 102231 v.3.1.2 tillämpas i sin helhet. ◄ När särskilda krav anges i dessa specifikationer SKA de ha företräde framför motsvarande krav i Etsi TS 102231 samtidigt som de kompletteras genom formatspecifikationerna i Etsi TS 102231. Vid avvikelser mellan dessa specifikationer och specifikationerna i Etsi TS 102231, SKA de här specifikationerna vara normativa.

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

▼C1

Språkstöd SKA genomföras och erbjudas minst på engelska (EN) och eventuellt även på ett eller flera nationella språk.

Datum- och tidsangivelser SKA göras i enlighet med klausul 5.1.4 i Etsi TS 102231.

URI:er SKA användas i enlighet med klausul 5.1.5 i Etsi TS 102231.

Information om systemet för att utfärda den tillförlitliga förteckningen

Tag

TSL tag (klausul 5.2.1)

Detta fält är OBLIGATORISKT och SKA följa klausul 5.2.1 i Etsi TS 102231.

▼M1

_____

▼C1

Scheme Information

TSL version identifier (klausul 5.3.1)

Detta fält är OBLIGATORISKT och SKA vara inställt på ”3” (heltal).

TSL sequence number (klausul 5.3.2)

▼M1

Detta fält är OBLIGATORISKT. Det SKA innehålla sekvensnumret för TSL:en. Med början från ”1” vid den första utgåvan av TSL SKA detta heltal höjas vid varje efterföljande utgåva av TSL. Det FÅR INTE återställas till ”1” när värdet i fält ”TSL version identifier” ovan höjs.

▼C1

TSL type (klausul 5.3.3)

▼M1

Detta fält är OBLIGATORISKT och anger typen av TSL. Det SKA vara inställt på http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (generiskt).

▼C1

Anm.: För att vara förenlig med klausul 5.3.3 i Etsi TS 102231 och ange den specifika typen av TSL och samtidigt hänvisa till förekomsten av dessa specifikationer, som styr inrättandet av TSL-tillämpningen av medlemsstaternas tillförlitliga förteckningar, ([1]) samt göra det möjligt för en parser att avgöra vilken av form av eventuellt efterföljande fält ([2]) som kan förväntas, där dessa fält har specifika (eller alternativa) betydelser beroende på vilken typ av TSL som representeras (i detta fall en tillförlitlig förteckning från en medlemsstat), SKA den ovannämnda specifika URI:n registreras och beskrivas enligt följande:

([1]) Dvs. förteckningen över övervaknings-/ackrediteringsstatus för certifikattjänster från tillhandahållare av certifikattjänster som övervakas/ackrediteras av den angivna medlemsstaten med avseende på efterlevnaden av de relevanta bestämmelserna i direktiv 1999/93/EG (den tillförlitliga förteckningen).

([2]) Dvs. de fält som anges i Etsi TS 102231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information och som ”profileras” genom de här specifikationerna för att närmare beskriva inrättandet av medlemstaternas tillförlitliga förteckningar.

▼M1

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

▼C1

Beskrivning: En TSL-tillämpning av en förteckning över övervaknings/ackrediteringsstatus för tillhandahållare av certifieringstjänster som övervakas/ackrediteras av den angivna medlemsstat som har ansvar för TSL-tillämpningen för att uppfylla de relevanta bestämmelserna i Europaparlamentets och rådets direktiv 1999/93/EG genom en process med direkt tillsyn (frivillig eller lagstadgad).

Scheme operator name (klausul 5.3.4)

Detta fält är OBLIGATORISKT. Det SKA innehålla namnet på det organ i medlemsstaten som ansvarar för att inrätta, offentliggöra och underhålla den nationella tillförlitliga förteckningen. Det SKA innehålla det formella namnet på den rättsliga enhet eller förordnade enhet (t.ex. på statliga administrativa organ) som är associerade med detta organ. Det MÅSTE vara det namn som används i den formella rättsliga registreringen eller auktorisationen och som ska användas vid all formell kommunikation. Det SKA vara en sekvens med flerspråkiga teckensträngar och SKA implementeras med engelska (EN) som obligatoriskt språk och eventuellt med ett eller flera nationella språk.

Anm.: Ett land FÅR ha separata övervaknings- och ackrediteringsorgan och får även ha ytterligare organ för eventuella driftsrelaterade verksamheter. ►M1 Det är upp till varje medlemsstat att utse systemoperatören för TSL-tillämpningen av medlemsstatens tillförlitliga förteckning. ◄ Det förväntas av övervakningsorganet, ackrediteringsorganet och systemets operatör (när de förefaller vara separata organ), vart och ett ska ha sina egna ansvarsområden och skyldigheter.

Alla situationer där flera organ har ansvar för övervakning, ackreditering eller drift SKA konsekvent avspeglas och identifieras som sådana i den systeminformation som ska ingå i den tillförlitliga förteckningen, inklusive den systemspecifika information som anges i fältet ”Scheme information URI” (klausul 5.3.7).

▼M1

Den namngivna systemoperatören (klausul 5.3.4) är den enhet som ska signera TSL.

▼C1

Scheme operator address (klausul 5.3.5)

Detta fält är OBLIGATORISKT. De SKA innehålla både post- och e-postadressen till den rättsliga enhet eller utsedda organisation som anges i fältet ”Scheme operator name” (klausul 5.3.4). Det SKA innehålla både ”PostalAddress” (dvs. gatuadress, ort, [stat eller provins], [postnummer] och ISO 3166–1 alfa 2-landkod) i enlighet med klausul 5.3.5.1 och ”ElectronicAddress” (dvs. e-postadress och/eller webbplatsens URI) i enlighet med klausul 5.3.5.2.

Scheme name (klausul 5.3.6)

Detta fält är OBLIGATORISKT och ska innehålla systemets namn. Det SKA vara en sekvens med flerspråkiga teckensträngar (med engelska (EN) som obligatoriskt språk och eventuellt med ett eller flera nationella språk) i enlighet med följande:

▼C1

— Den engelska versionen SKA vara en teckensträng som är uppbyggd på följande sätt:

CC:EN_name_value

där

— ”CC” = den ISO 3166–1 alfa 2-landkod som används i fältet ”Scheme territory” (klausul 5.3.10);

— ”:” = används 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

— Eventuella versioner på medlemsstatens nationella språk SKA vara en teckensträng som är uppbyggd på följande sätt:

CC:name_value

där:

— ”CC” = den ISO 3166–1 alfa 2-landkod som används i fältet ”Scheme territory” (klausul 5.3.10);

— ”:” = används som separator;

— ”name_value” = Officiell översättning till det nationella språket av ”EN_name_value”.

Systemets namn krävs för att ge en unik identitet för det system som avses med ”Scheme information URI” och även för att se till att alla system som hanteras av en operatör får ett särskilt namn.

Medlemsstater och systemoperatörer SKA se till att om en medlemsstat eller en systemoperatör driver mer än ett system, ska vart och ett av dessa system få ett särskilt namn.

Scheme information URI (klausul 5.3.7)

Detta fält är OBLIGATORISKT och SKA innehålla den eller de URI:er där användare (beroende parter) kan få systemspecifik information (med engelska som obligatoriskt språk och eventuellt med ett eller flera nationella språk). Det SKA vara en sekvens med flerspråkiga tecken (med engelska (EN) som obligatoriskt språk och eventuellt med ett eller flera nationella språk). Den eller de angivna URI:erna MÅSTE tillhandahålla en sökväg till information som beskriver ”ändamålsenlig information om systemet”.

▼C2

Den ”ändamålsenliga informationen om systemet” SKA minst innehålla följande:

— Allmän information som är gemensam för samtliga medlemsstater i fråga om den tillförlitliga förteckningens och underliggande övervaknings-/ackrediteringssystems omfattning och innehåll. Följande gemensamma text ska användas:

▼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

— Specifik information om de underliggande övervaknings-/ackrediteringssystemen och särskilt uppgifter om följande ([1]):

— Det övervakningssystem som är tillämpligt på alla CSP_{QC}.

([1]) De sista två uppsättningarna av uppgifter är av kritisk betydelse för att beroende parter ska kunna bedöma kvaliteten och säkerhetsnivån på dessa övervaknings-/ackrediteringssystem. Dessa uppsättningar av uppgifter ska tillhandahållas på tillförlitlig förteckningsnivå genom användning av fälten "Scheme information URI" (klausul 5.3.7 – information som tillhandahålls av medlemsstaten), "Scheme type/community/rules" (klausul 5.3.9 – med en text som är gemensam för alla medlemsstater) och "TSL policy/legal notice" (klausul 5.3.11 – en text som är gemensam för alla medlemsstater med en hänvisning till direktiv 1999/93/EG, tillsammans med en möjlighet för varje medlemsstat att lägga till medlemsstatsspecifika texter/hänvisningar). Ytterligare information i de nationella övervaknings-/ackrediteringssystemen för CSP som inte utfärdar QC får i förekommande fall och om så krävs tillhandahållas på tjänstenivå (till exempel för att skilja mellan flera kvalitets- eller säkerhetsnivåer) genom användning av fältet "Scheme service definition URI" (klausul 5.5.6).

▼C1

— I förekommande fall det nationella frivilliga ackrediteringssystem som är tillämpligt på alla CSP_{QC}.

— I förekommande fall det övervakningssystem som är tillämpligt på alla CSP som inte utfärdar QC.

— I förekommande fall det nationella frivilliga ackrediteringssystem som är tillämpligt på alla CSP som inte utfärdar QC:

— Denna specifika information SKA för varje underliggande system som anges ovan minst innehålla följande:

— En allmän beskrivning.

— Information om den process som övervaknings-/ackrediteringsorganet följer för att övervaka/ackreditera CSP och som CSP följer för att övervakas/ackrediteras.

— Information om de kriterier används för övervakningen/ackrediteringen av CSP.

— I förekommande fall, information om de särskilda kvalificeringar som vissa av de fysiska eller binära (logiska) objekt som genereras eller utfärdas till följd av tillhandahållandet av en certifieringstjänst kan ha rätt till på grund av att de uppfyller de bestämmelser och krav som fastställs på nationell nivå, inklusive innebörden av en sådan kvalificering och därmed sammanhängande nationella bestämmelser och krav.

Ytterligare medlemsstatsspecifik information om systemet FÅR lämnas på frivillig basis. Den informationen SKA omfatta följande:

— Uppgifter om de kriterier och bestämmelser som används för att välja ut övervakare/granskare och om hur CSP övervakas (kontrolleras)/ackrediteras (granskas) av dem.

— Andra kontaktuppgifter och allmän information om driften av systemet.

Status determination approach (klausul 5.3.8)

Detta fält är OBLIGATORISKT och ska innehålla identifikationen för metoden för att fastställa status. Följande specifika URI SKA användas:

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

Beskrivning: Tjänster i förteckningen får sin status fastställd av eller på uppdrag av systemets operatör enligt ett lämpligt system för en angiven medlemsstat som gör det möjligt att övervaka (och, i förekommande fall, frivilligt ackreditera) tillhandahållare av certifieringstjänster som är etablerade i den medlemsstatens territorium (eller är etablerad i ett tredjeland, om det är fråga om frivillig ackreditering) och som utfärdar kvalificerade certifikat till allmänheten i enlighet med artikel 3.3 (respektive artikel 3.2 eller 7.1 a) i Europaparlamentets och rådets direktiv 1999/93/EG, och som, i förekommande fall, tillåter övervakning/frivillig ackreditering av tillhandahållare av certifieringstjänster som inte utfärdar kvalificerade certifikat, i enlighet med ett eller flera nationellt utformade och inrättade erkända godkännandesystem som tillämpas på nationell basis för att kontrollera att tjänster från CSP som inte utfärdar QC är förenliga med bestämmelserna i direktiv 1999/93/EG och som eventuellt utvidgas med nationella bestämmelser om tillhandahållandet av sådana certifieringstjänster.

▼C1

Scheme type/community/rules (klausul 5.3.9)

Detta fält är OBLIGATORISKT och SKA minst innehålla följande registrerade URI:er:

— En URI som är gemensam för alla medlemsstaters tillförlitliga förteckningar och som länkar till en beskrivande text SKA tillämpas på samtliga tillförlitliga förteckningar:

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

— som innebär att medlemsstaternas system (identifierat genom ”TSL type” (klausul 5.3.3) och ”Scheme name” (klausul 5.3.6)) ingår i ett övergripande system (dvs. en TSL med länkar till alla medlemsstater som offentliggör och underhåller en tillförlitlig förteckning i form av en TSL),

— där användare kan få fram bestämmelser/regler som de tjänster som är upptagna i förteckningen SKA bedömas mot och som gör det möjligt att avgöra vilken typ av TSL (se klausul 5.3.3) det är fråga om,

— där användare kan få en beskrivning av hur innehållet i TSL-tillämpningen av den tillförlitliga förteckningen ska användas och tolkas. Dessa regler för användningen SKA vara gemensamma för alla medlemsstaters tillförlitliga förteckningar, oberoende av vilken typ av tjänster som förtecknas och vilka övervaknings-/ackrediteringssystem som används.

▼C2

Beskrivande text:

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 2009/767/EC 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 2009/767/EC for further details on the fields, description and meaning for the TSL implementation of the Member States' Trusted Lists.

▼C1

— En URI som är specifik för varje medlemsstats tillförlitliga förteckning och som länkar till en beskrivande text SKA tillämpas på denna medlemsstats tillförlitliga förteckning:

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

där CC = den ISO 3166–1 alfa 2-landkod som används i fältet ”Scheme territory” field (klausul 5.3.10)

— där användare kan få reda på den aktuella medlemsstatens specifika bestämmelser som de tjänster som tas upp i förteckningen SKA bedömas mot i enlighet med medlemsstatens övervakningssystem och frivilliga ackrediteringssystem,

— där användare kan hitta den aktuella medlemsstatens specifika beskrivning av hur innehållet i TSL-tillämpningen av den tillförlitliga förteckningen ska användas och tolkas när det gäller certifieringstjänster som inte har någon anknytning till utfärdandet av QC. Detta kan användas för att påpeka en potentiell granularitet i de nationella övervaknings-/-ackrediteringenssystemen för CSP som inte utfärdar QC och hur fälten ”Scheme service definition URI” (klausul 5.5.6) och ”Service information extension” används för detta ändamål.

Medlemsstaterna FÅR skapa ytterligare URI:er utifrån den ovannämnda medlemsstatsspecifika URI:n (dvs. URI:er som definierats ur denna hierarkiska specifika URI).

Scheme territory (innehåll 5.3.10)

I dessa specifikationer är detta fält OBLIGATORISKT och SKA ange det land där systemet är inrättat (ISO 3166–1 alfa 2-landkod).

TSL policy/legal notice (klausul 5.3.11)

I dessa specifikationer är detta fält OBLIGATORISKT och SKA ange stödets policy/rättsakt för systemets rättsliga status eller rättsliga krav som systemet uppfyller för den jurisdiktion inom vilken systemet är inrättat och/eller eventuella begränsningar och villkor för underhållet och offentliggörandet av den tillförlitliga förteckningen.

Detta SKA vara en flerspråkig teckensträng (klartext) som består av två delar:

— En första, obligatorisk del som är gemensam för alla medlemsstaters tillförlitliga förteckningar (med engelska som obligatoriskt språk och eventuellt ett eller fler nationella språk) där det anges att den tillämpliga rättsliga ramen är direktiv 1999/93/EG och dess motsvarande tillämpning i medlemsstaternas lagstiftning i enlighet med uppgiften i fältet ”Scheme Territory”.

Engelsk version av den gemensamma texten:

”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.”

Text på en medlemsstats nationella språk: [Officiell(a) översättning(ar) av den engelska texten].

▼C1

— En andra, valfri del, som är specifik för varje tillförlitlig förteckning (med engelska som det obligatoriska språket och eventuellt med ett eller flera nationella språk), med hänvisningar till särskilda tillämpliga nationella rättsliga ramar (t.ex. framför allt i fråga om nationella övervaknings-/ackrediteringssystem för CSP som inte utfärdar QC).

Historical information period (klausul 5.3.12)

Detta fält är OBLIGATORISKT och SKA ange den period (heltal) för vilken historisk information om TSL tillhandahålls. Detta värde i heltal ska anges i antal dagar och inom ramen för dessa specifikationer SKA värdet vara minst 3 653 (dvs. TSL-tillämpningen av medlemsstaternas tillämpliga förteckning MÅSTE innehålla historisk information som minst omfattar tio år). Högre värden bör ta vederbörlig hänsyn till de rättsliga kraven på uppgiftslagring i den medlemsstat som anges i ”Scheme Territory” (klausul 5.3.10).

Pointers to other TSLs (klausul 5.3.13)

I dessa specifikationer är detta fält OBLIGATORISKT och SKA, om den finns tillgänglig, innehålla en länk till en Etsi TS 102 231-förenlig version av Europeiska kommissionens sammanställning av länkar till samtliga TSL-tillämpningar av tillförlitliga förteckningar från medlemsstaterna. Specifikationer från Etsi TS 102231, klausul 5.3.13 ska tillämpas vid bemyndigandet av användningen av den frivilliga digitala identitet som representerar utfärdaren av den TSL som länken går till, formaterad enligt specifikationen i klausul 5.5.3.

Anmärkning: I väntan på den Etsi TS 102 231-förenliga tillämpningen av Europeiska kommissionens sammanställning av länkar till medlemsstaternas TSL-tillämpning av de tillförlitliga förteckningarna FÅR detta fält INTE användas.

List issue date and time (klausul 5.3.14)

Detta fält är OBLIGATORISKT och SKA ange datum och tidpunkt (UTC uttryckt som Greenwichtid) då TSL utfärdades med hjälp av datum- och tidsvärden enligt specifikationerna i Etsi TS 102231, klausul 5.1.4.

Next update (klausul 5.3.15)

Detta fält är OBLIGATORISKT och SKA ange datum och tidpunkt (UTC uttryckt som Greenwichtid) då nästa TSL senast kommer att utfärdas eller senast bli ogiltigt för att ange en stängd TSL (med hjälp av datum- och tidsvärden enligt specifikationerna i Etsi TS 102231, klausul 5.1.4).

Om det inte under tiden görs några statusförändringar hos någon TSP eller tjänst som omfattas av systemet MÅSTE TSL utfärdas på nytt när den senast utfärdade TSL upphör att gälla.

Enligt dessa specifikationer FÅR skillnaden mellan datum och tidpunkt för ”Next update” och ”List issue date and time” INTE överskrida **sex (6)** månader.

▼C1

Distribution points (klausul 5.3.16)

Detta fält är FRIVILLIGT. Om det används SKA det ange var den aktuella TSL-tillämpningen av den tillförlitliga förteckningen offentliggörs och var uppdateringar av den aktuella TSL finns. Om det anges flera distributionsställen MÅSTE samtliga ställen tillhandahålla identiska exemplar av den aktuella TSL eller dess uppdaterade version. När det används ska detta fält formateras som en icke-tom sekvens av strängar som var och en ska vara förenlig med RFC 3986 ([1]).

Scheme extensions (klausul 5.3.17)

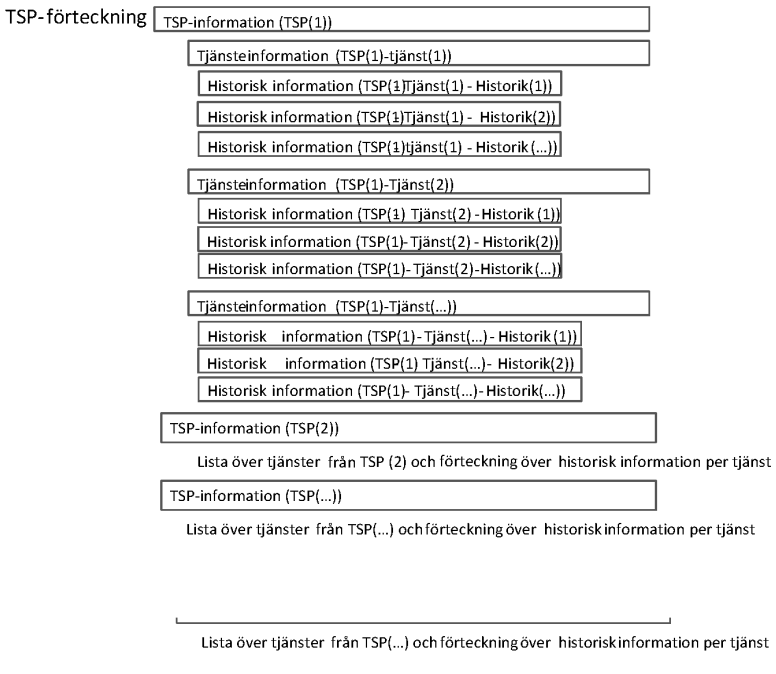
Detta fält är FRIVILLIGT och används inte inom ramen för dessa specifikationer.

List of Trust Service Providers

Detta fält är FRIVILLIGT.

Om det inte finns några CSP som är eller har varit övervakade/ackrediterade inom ramen för systemet i en medlemsstat SKA detta fält inte tas med. Även om en medlemsstat inte har någon tillhandahållare av certifikattjänster som är övervakad eller ackrediterad genom systemet SKA medlemsstaten ändå inrätta en TSL där detta fält inte tas med. Om det inte finns någon CSP i förteckningen SKA detta innebära att det inte finns någon CSP som är övervakad/ackrediterad i det land som anges i fältet ”Scheme Territory”.

Om en eller flera CSP-tjänster är eller har varit övervakade/ackrediterade genom systemet, SKA fältet innehålla en sekvens som identifierar varje CSP som tillhandahåller en eller flera av dessa övervakade/ackrediterade tjänster, med uppgifter om den övervakade/ackrediterade statusen och statushistoriken för var och en av tjänsterna från denna CSP (TSP = CSP i figuren nedan).



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

▼C1

Förteckningen över TSP ska organiseras enligt illustrationen i figuren ovan. För varje tillhandahållare av betrodda tjänster finns det en sekvens av fält med information om den tillhandahållaren (”TSP Information”), åtföljd av en förteckning över tjänster. För var och en av dessa förtecknade tjänster finns det en sekvens av fält med information om tjänsten (”Service Information”), och en sekvens av fält med historik över tjänstens godkännandestatus (”Service approval history”).

TSP Information

TSP(1)

TSP name (klausul 5.4.1)

Detta fält är OBLIGATORISKT och SKA innehålla namnet på den **rättsliga enhet** som har ansvar för de tjänster från CSP som är eller har varit övervakade/-ackrediterade inom ramen för systemet. Detta är en sekvens med flerspråkiga tecken (med engelska som obligatoriskt språk och eventuellt med ett eller flera nationella språk). Detta namn MÅSTE vara det namn som används i den formella rättsliga registreringen eller auktorisationen och som ska användas vid all formell kommunikation.

TSP trade name (klausul 5.4.2)

Detta fält är FRIVILLIGT och om det har tagits med SKA det innehålla ett alternativt namn som CSP använder för att identifiera sig vid tillhandahållandet av de tjänster som ingår i denna TSL under posten ”TSP name” (klausul 5.4.1).

Anmärkning: Om en enda rättslig enhet hos en CSP tillhandahåller tjänster under olika handelsnamn eller inom ramen för olika specifika sammanhang, kan det finnas lika många CSP-poster som det finns sådana specifika sammanhang (t.ex. poster för namn/handelsnamn). Ett alternativ är att registrera varje CSP (rättslig enhet) endast en gång och tillhandahålla information om det specifika sammanhanget. Det är upp till medlemsstatens systemoperatör att diskutera och komma överens om det lämpligaste tillvägagångssättet med CSP.

TSP address (klausul 5.4.3)

Detta fält är OBLIGATORISKT och SKA innehålla adressen till den rättsliga enhet eller förordnade organisation som angetts i fältet ”TSP name” (klausul 5.4.1) för både vanlig postgång och elektronisk kommunikation. Det SKA innehålla både ”PostalAddress” (dvs. gatuadress, ort, [stat eller provins], [postnummer] och ISO 3166–1 alfa 2-landkod) i enlighet med klausul 5.3.5.1 och ”ElectronicAddress” (dvs. e-postadress och/eller webbplatsens URI) i enlighet med klausul 5.3.5.2.

TSP information URI (klausul 5.4.4)

Detta fält är OBLIGATORISKT och SKA innehålla den eller de URI:er där användare (t.ex. beroende parter) kan få information om CSP. Det SKA vara en sekvens med flerspråkiga tecken (med engelska (EN) som obligatoriskt språk och eventuellt med ett eller flera nationella språk). Den eller de angivna URI:erna MÅSTE ge en sökväg till information som beskriver de allmänna villkoren för CSP, dennes praxis, rättsliga frågor, kundvårdspolicy och annan allmän information som gäller för alla tjänster som är upptagna under posten för denna CSP i TSL.

Anmärkning: Om en enda rättslig enhet i form av en CSP erbjuder tjänster under olika handelsnamn eller i olika specifik sammanhang, och detta har avspeglats i lika många TSP-poster som antalet specifika sammanhang, SKA detta fält innehålla information om den specifika uppsättning tjänster som registrerats under en viss post för TSP/handelsnamn.

▼C1

TSP information extensions (klausul 5.4.5)

Detta fält är FRIVILLIGT. Om det tas med FÅR det användas av systemoperatören, i enlighet med specifikationerna i Etsi TS 102231 (klausul 5.4.5), för att tillhandahålla specifik information som ska tolkas enligt bestämmelserna för det aktuella systemet.

List of Services

Detta fält är OBLIGATORISKT och SKA innehålla en sekvens som identifierar var och en av de erkända tjänsterna från CSP tillsammans med godkännandestatus (samt historik för denna status) för denna tjänst. Minst en tjänst måste vara upptagen i förteckningen (även om informationen enbart är historisk).

Eftersom det är OBLIGATORISKT att spara historisk information om förtecknade tjänster enligt dessa specifikationer, MÅSTE denna historiska information sparas även om tjänstens nuvarande status normalt sett inte skulle kräva att den togs upp i förteckningen (t.ex. tjänsten har upphört). En CSP MÅSTE alltså tas med, även om dess enda förtecknade tjänst har en sådan status, för att bevara historiken.

Service Information

TSP(1) tjänst(1)

Service type identifier (klausul 5.5.1)

▼M1

Detta fält är OBLIGATORISKT och SKA innehålla identifikationen för tjänstetypen beroende på typen i dessa TSL-specifikationer (dvs. ”/eSigDir-1999-93-EC-TrustedList/TSLType/generic”).

▼C1

När den förtecknade tjänsten avser utfärdande av kvalificerade certifikat SKA den angivna URI:n vara http://uri.etsi.org/TrstSvc/Svctype/CA/QC (en certifikatutfärdare som utfärdar kvalificerade certifikat).

Om den förtecknade tjänsten är relaterad till utfärdande av igenkänningstecken för betrodda tjänster som inte är QC och som inte stöder utfärdande av QC SKA den angivna URI:n vara en av de URI:er som definieras i Etsi 102231, och som anges i klausul D.2 i detta dokument, som gäller detta fält. Detta SKA tillämpas även för sådana igenkänningstecken för betrodda tjänster som är övervakade/ackrediterade för att uppfylla vissa specifika kvalifikationer i enlighet med medlemsstaternas nationella lagstiftning (t.ex. igenkänningstecken för kvalificerade tidsmärken i Tyskland eller Ungern). Den angivna URI:n SKA vara en av de URI:er som definieras i Etsi 102231, och som anges i klausul D.2 i detta dokument, som gäller detta fält (t.ex. TSA för nationellt fastställda igenkänningstecken för kvalificerade tidsmärken). När så är tillämpligt FÅR sådana specifika nationella kvalificeringar av igenkänningstecken för betrodda tjänster anges i posten där tjänsten registreras. Tillägget additionalServiceInformation (klausul 5.8.2) i klausul 5.5.9 (”Service information extension”) SKA i så fall användas för detta ändamål.

▼C1

Som allmän standardprincip SKA det endast finnas en post per enkelt X.509v3-certifikat (t.ex. en certifieringstjänst av CA/QC-typ) under de förtecknade certifieringstjänsterna från en CSP som är upptagen i den tillförlitliga förteckningen (t.ex. en certifikatutfärdare som (direkt) utfärdar QC). Under vissa noggrant övervägda omständigheter och noggrant utformade och godkända villkor, FÅR en medlemsstats övervaknings- eller ackrediteringsorgan besluta att använda X.509v3-certifikatet för en rotcertifikatutfärdare eller överordnad certifikatutfärdare (t.ex. en certifikatutfärdare som inte direkt utfärdar kvalificerade slutanvändarcertifikat utan som certifierar en hierarki av CA ner till en CA som utfärdar QC till slutanvändare) som Sdi för en enda registerpost i förteckningen över tjänster från en CSP som är upptagen i förteckningen. Konsekvenserna (fördelar och nackdelar) med att använda ett sådant X.509v3-certifikat från en rotcertifikatutfärdare eller överordnad certifikatutfärdare som Sdi-värde för registrering av tjänster i den tillförlitliga förteckningen måste noggrant övervägas och godkännas av medlemsstaterna ([1]). När medlemsstaten utnyttjar ett sådant tillåtet undantag från standardprincipen, MÅSTE den dessutom tillhandahålla den nödvändiga dokumentationen för att underlätta uppbyggnaden av certifieringsvägen och verifieringen.

Anm.: TSP:er som OCSP-respondrar och CRL-utfärdare som ingår i certifieringstjänster från CSP_{QC} och som omfattas av användning av separata nyckelpar för att signera OCSP-respondrar respektive CRL:er FÅR också förtecknas i denna TSL-mall med hjälp av följande kombination av URI:er:

— Sti-värde (klausul 5.5.1):

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

kombinerat med följande Sie-värde (klausul 5.5.9), tillägg additionalServiceInformation (klausul 5.8.2):

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

Beskrivning: en tillhandahållare av certifikatsstatus som driver en OCSP-server som ett led i en tjänst från en CSP som utfärdar kvalificerade certifikat.

— Sti-värde (klausul 5.5.1):

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

kombinerat med följande Sie-värde (klausul 5.5.9), tillägg additionalServiceInformation (klausul 5.8.2):

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

Beskrivning: en tillhandahållare av certifikatsstatus som driver en CRL som ett led i en tjänst från en CSP som utfärdar kvalificerade certifikat.

— Sti-värde (klausul 5.5.1):

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

([1]) Om systemoperatören använder ett RootCA X.509v3-certifikat som Sdi-värde för en förtecknad tjänst måste operatören betrakta hela uppsättningen av certifikattjänster från en sådan rotcertifikatutfärdare som en helhet med avseende på övervaknings-/ackrediteringsstatus. Eventuella statusförändringar som krävs av en enda certifikatutfärdare under den förtecknade rothierarkin innebär t.ex. att hela hierarkin måste omfattas av denna statusförändring.

▼C1

kombinerat med följande Sie-värde (klausul 5.5.9), tillägg additionalService-Information (klausul 5.8.2):

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

Beskrivning: en rotcertifikatutfärdare från vilken en certifieringsväg kan fastställas ned till en certifikatutfärdare som utfärdar kvalificerade certifikat.

— Sti-värde (klausul 5.5.1):

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

kombinerat med följande Sie-värde (klausul 5.5.9), tillägg additionalService-Information (klausul 5.8.2):

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

Beskrivning: en tidsmärkningstjänst som en del av en tjänst från en CSP som utfärdar kvalificerade certifikat som utfärdar TST som kan användas i verifieringsprocessen för kvalificerade signaturer för att kontrollera och utvidga signaturens giltighet när QC återkallas eller löper ut.

Service name (klausul 5.5.2)

Detta fält är OBLIGATORISKT och SKA innehålla det namn under vilket den CSP som anges i ”TSP name” (klausul 5.4.1) tillhandahåller den tjänst som anges i ”Service type identifier” (klausul 5.5.1). Det SKA vara en sekvens med flerspråkiga teckensträngar (med engelska som obligatoriskt språk och eventuellt med ett eller flera nationella språk).

Service digital identity (klausul 5.5.3)

Detta fält är OBLIGATORISKT och SKA minst innehålla en förekomst av en digital identifikation som är unik för den tjänst vars typ anges i ”Service type identifier” (klausul 5.5.1) och med vilken tjänsten kan identifieras otvetydigt.

I dessa specifikationer SKA den digitala identifiering som används i detta fält vara det relevanta X.509v3-certifikat som representerar den eller de allmänna nycklar som CSP använder för att tillhandahålla den tjänst vars typ anges i ”Service type identifier” (klausul 5.5.1) (dvs. den nyckel som används av en RootCA/QC, den nyckel som används för att signera certifikat [1]), eller för att utfärda igenkänningstecken för tidsmärken, eller signera CRL:er, eller signera OCSP-responser). Detta relaterade X.509v3-certifikat SKA användas som det minimum av digital identifiering som krävs (eftersom detta representerar den eller de allmänna nycklar som CSP använder för att tillhandahålla den förtecknade tjänsten). Ytterligare identifikationer FÅR användas enligt följande, men samtliga MÅSTE avse samma identitet (dvs. det relaterade X.509v3-certifikatet):

[1] Detta kan vara certifikatet för en CA som utfärdar slutanvändarcertifikat (t.ex. CA/PKC, CA/QC) **eller** certifikatet för en betrodd rotcertifikatutfärdare från vilken det går att fastställa en sökväg ner till slutliga kvalificerade certifikat. Beroende på om denna information och den information som finns i varje slutanvändarcertifikat som utfärdats under denna betrodda rot kan användas för att otvetydigt fastställa ändamålsenliga egenskaper hos alla kvalificerade certifikat eller ej, kan denna information (”Service digital identity”) behöva kompletteras med uppgifter i ”Service information extensions” (se klausul 5.5.9).

▼C1

a) Certifikatets särskiljande namn som kan användas för att verifiera elektroniska signaturer från den tjänst från tillhandahållaren av certifieringstjänster som anges i ”Service type identifier” (klausul 5.5.1).

b) Identifikation av den relaterade allmänna nyckeln (dvs. X.509v3 SubjectKeyIdentifier eller SKI-värde).

c) Den relaterade allmänna nyckeln.

Som allmän standardprincip FÅR den digitala identifikationen (dvs. det relaterade X.509v3-certifikatet) INTE förekomma mer än en gång i den tillförlitliga förteckningen, dvs. det SKA finnas en post per enkelt X.509v3-certifikat för en certifieringstjänst under de förtecknade certifieringstjänsterna från en CSP som är upptagen i den tillförlitliga förteckningen. Omvänt SKA ett enkelt X.509v3-certifikat användas som Sdi-värde vid en registrering av en enkel tjänst.

Anm. 1: Det enda fall då denna allmänna standardprincip inte får tillämpas är då ett enkelt X.509v3-certifikat används vid utfärdande av olika typer av igenkänningstecken för betrodda tjänster för vilka olika övervaknings-/ackrediteringssystem tillämpas, t.ex. då ett enkelt X.509v3-certifikat används av en CSP, dels vid utfärdande av QC inom ramen för ett lämpligt övervakningssystem, dels vid utfärdande av icke-kvalificerade certifikat inom ramen för en annan övervaknings-/ackrediteringsstatus. I detta fall och exempel bör två poster med olika Sti-värden (t.ex. CA/QC respektive CA/PKC i det aktuella exemplet) och med samma Sdi-värde (det relaterade X.509v3-certifikatet) användas.

Tillämpningar är ASN.1- eller XML-beroende och SKA följa Etsi TS 102 231-specifikationerna (för ASN.1, se bilaga A till Etsi TS 102231 och för XML, se bilaga B till Etsi TS 102231).

Anm. 2: När ytterligare kvalificeringsinformation behöver lämnas i fråga om posten för den identifierade tjänsten, SKA systemoperatören överväga att i förekommande fall använda tillägget ”additionalServiceInformation” (klausul 5.8.2) i fältet ”Service information extension” (klausul 5.5.9) i enlighet med syftet med att tillhandahålla sådan ytterligare kvalificeringsinformation. Systemoperatören får dessutom välja att använda klausul 5.5.6 (”Scheme service definition URI”).

S e r v i c e c u r r e n t s t a t u s (klausul 5.5.4)

▼C2

Detta fält är OBLIGATORISKT och SKA innehålla identifikationen för tjänstens status genom en av de följande URI:erna:

— **Under Supervision (Under övervakning)**

(http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision);

— **Supervision of Service in Cessation (Övervakningen av tjänsten har avbrutits)**

(http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation);

— **Supervision Ceased (Övervakningen har upphört)**

(http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased);

— **Supervision Revoked (Övervakningen har återkallats)**

(http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked);

— **Accredited (Ackrediterad)**

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

— **Accreditation Ceased (Ackrediteringen har upphört)**

(http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased);

— **Accreditation Revoked (Ackrediteringen har återkallats)**

(http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

De ovannämnda statusarna SKA inom ramen för dessa specifikationer för den tillförlitliga förteckningen tolkas enligt följande:

— ***Under övervakning:*** Den tjänst som identifieras i ”Service digital identity” (klausul 5.5.3) och som tillhandahålls av den tillhandahållare av certifieringstjänster (CSP) som identifieras i ”TSP name” (klausul 5.4.1) övervakas för närvarande med avseende på efterlevnaden av bestämmelserna i direktiv 1999/93/EG av den medlemsstat som identifieras i ”Scheme territory” (klausul 5.3.10), där CSP är etablerad.

▼M1

— ***Övervakningen av tjänsten har avbrutits:*** Den tjänst som identifieras i ”Service digital identity” (klausul 5.5.3) och som tillhandahålls av den CSP som identifieras i ”TSP name” (klausul 5.4.1) är för närvarande avbruten men är fortfarande under övervakning tills övervakningen upphör eller återkallas. Om en annan juridisk person än den som identifieras i ”TSP name” har tagit över ansvaret för att säkerställa denna avbrutna fas, SKA identifieringen av denna nya eller ersättande juridiska person fallback CSP) anges i ”Scheme service definition URI” (klausul 5.5.6) och i ”TakenOverBy” extension (klausul L.3.2) of the service entry.

▼C1

— ***Övervakningen har upphört:*** Övervakningsbedömningens giltighetstid har löpt ut och ingen ny bedömning har gjorts av den tjänst som anges i ”Service digital identity” (klausul 5.5.3). Tjänsten befinner sig inte längre under övervakning från och med dagen för denna status, eftersom tjänsten har upphört.

— ***Övervakningen har återkallats:*** Efter att tidigare ha övervakats har tjänsten från CSP och eventuellt CSP själv underlåtit att fortsätta att följa bestämmelserna i direktiv 1999/93/EG, enligt vad som konstaterats av den medlemsstat som anges i ”Scheme territory” (klausul 5.3.10) och där CSP är etablerad. Därför har tjänsten uppmanats att upphöra med sin verksamhet och måste därför betraktas som upphörd.

Anm. 1: Statusvärdet ”Övervakningen har återkallats” kan vara en slutgiltig status, även om CSP därefter helt och hållet upphör med sin verksamhet. I detta fall behöver man inte byta till status ”Övervakningen av tjänsten har avbrutits” eller ”Övervakningen har upphört”. Det enda sättet att ändra statusen ”Övervakningen har återkallats” är att på nytt börja följa bestämmelserna i direktiv 1999/93/EG i enlighet med det gällande övervakningssystemet i den medlemsstat som äger den tillförlitliga förteckningen och på så sätt få tillbaka statusen ”Under övervakning”. Statusen ”Övervakningen av tjänsten har avbrutits” eller ”Övervakningen har upphört” kan endast beviljas när en CSP direkt upphör med sina tillhörande tjänster under övervakning, inte när övervakningen har återkallats.

— ***Ackrediterad:*** Ackrediteringsorganet har utfört en ackrediteringsbedömning på uppdrag av den medlemsstat som anges i fältet ”Scheme territory” (klausul 5.3.10) och det konstateras att den tjänst som anges i ”Service digital identity” (klausul 5.5.3) och som tillhandahålls av den CSP ([1]) som anges i fält ”TSP name” (klausul 5.4.1) följer bestämmelserna i direktiv 1999/93/EG.

([1]) Observera att denna ackrediterade CSP kan vara etablerad i en annan medlemsstat än den som anges i fältet ”Scheme territory” i TSL-tillämpningen av den tillförlitliga förteckningen eller i ett tredjeland (se artikel 7.1 a i direktiv 1999/93/EG).

▼C1

Anm. 2: När de används i fråga om en CSP som utfärdar QC och som är etablerad i det område som anges i ”Scheme territory” (klausul 5.3.10), MÅSTE de båda statusarna ”Ackrediteringen har återkallats” och ”Ackrediteringen har upphört” betraktas som övergångsstatusar och FÅR INTE användas som värde för tjänstens aktuella status i ”Service current status”, eftersom de, om de används, omedelbart MÅSTE följas av statusvärdet ”Under övervakning”, eventuellt följt av något av de andra statusvärdena för övervakning som anges ovan och som illustreras i figur 1, i historiken över godkännande av tjänsten i fältet ”Service approval history information”. När de används i fråga om en CSP som inte utfärdar QC, där det endast finns ett associerat frivilligt ackrediteringssystem utan därmed sammanhängande övervakningssystem, eller i fråga om en CSP som utfärdar QC och som inte är etablerad i det område som anges i ”Scheme territory” (klausul 5.3.10) (t.ex. i ett tredjeland), FÅR statusvärdena ”Ackreditering återkallad” och ”Ackrediteringen har upphört” användas som värde för tjänstens aktuella status i fältet ”Service current status”.

— ***Ackrediteringen har upphört:*** Ackrediteringsbedömningens giltighetstid har löpt ut och ingen ny bedömning har gjorts av den tjänst som anges i ”Service digital identity” (klausul 5.5.3).

— ***Ackrediteringen har återkallats:*** Efter att tidigare ha konstaterats uppfylla systemets kriterier har den tjänst som anges ”Service digital identity” (klausul 5.5.3), och som tillhandahålls av den tillhandahållare av certifieringstjänster (CSP) som anges i ”TSP name” (klausul 5.4.1) och eventuellt den aktuella tillhandahållaren själv, underlåtit att följa bestämmelserna i direktiv 1999/93/EG.

Anm. 3: Exakt samma statusvärden måste användas för CSP som utfärdar QC och för CSP som inte utfärdar QC (tillhandahållare av tidsmärkningstjänster som utfärdar igenkänningstecken för tidsmärken, CSP som utfärdar icke-kvalificerade certifikat osv.). Fältet ”Service Type identifier” (klausul 5.5.1) ska användas för att särskilja mellan de tillämpliga övervaknings-/ackrediteringssystemen.

Anm. 4: Ytterligare statusrelaterade kvalificeringsuppgifter som definieras i de nationella övervaknings-/ackrediteringssystemen för CSP som inte utfärdar QC FÅR i förekommande fall och om så krävs anges på tjänstenivå (t.ex. för att skilja mellan flera kvalitets- eller säkerhetsnivåer). Systemoperatörerna SKA använda tillägget ”additionalServiceInformation” (klausul 5.8.2) i fält ”Service information extension” (klausul 5.5.9) beroende på syftet med att lämna denna ytterligare kvalificeringsinformation. Systemoperatören får dessutom välja att använda klausul 5.5.6 (”Scheme service definition URI”).

Current status starting date and time (klausul 5.5.5)

Detta fält är OBLIGATORISKT och SKA ange datum och tidpunkt då aktuell godkännandestatus trädde i kraft (datum- och tidsvärden enligt specifikationerna i Etsi TS 102231, klausul 5.1.4).

Scheme service definition URI (klausul 5.5.6)

Detta fält är FRIVILLIGT och om det används SKA det innehålla den eller de URI:er där beroende parter kan få tjänstespecifik information som tillhandahålls av systemoperatören som en sekvens av flerspråkiga tecken (med engelska (EN) som obligatoriskt språk och eventuellt med ett eller flera nationella språk).

När detta fält anges MÅSTE den eller de angivna URI:erna tillhandahålla en sökväg till information som beskriver tjänsten enligt specifikationen i systemet. I förekommande fall FÅR detta fält framför allt innehålla följande:

a) URI som anger identiteten för reserv-CSP om det sker en övervakning av en avbruten tjänst för vilken en reserv-CSP är involverad (se ”Service current status” – klausul 5.5.4).

▼C1

b) URI som leder till dokument med ytterligare information i fråga om användning en nationellt definierad specifik kvalifikation för en övervakad/ackrediterad tjänst som tillhandahåller igenkänningstecken för betrodda tjänster i enlighet med användningen av fältet ”Service information extension” (klausul 5.5.9) med ett ”additionalServiceInformation”-tillägg i enlighet med klausul 5.8.2.

Service supply points (klausul 5.5.7)

Detta fält är FRIVILLIGT och om det används SKA det innehålla den eller de URI:er där beroende parter kan få tillgång till tjänsten via en sekvens av teckensträngar vars syntax MÅSTE vara förenlig med RFC 3986.

TSP service definition URI (klausul 5.5.8)

Detta fält är FRIVILLIGT och om det används SKA det innehålla den eller de URI:er där beroende parter kan få tjänstespecifik information som tillhandahålls av TSP som en sekvens av flerspråkiga tecken (med engelska som obligatoriskt språk och eventuellt med ett eller flera nationella språk). Den eller de angivna URI:erna MÅSTE tillhandahålla en sökväg till information som beskriver tjänsten enligt specifikationen från TSP.

Service information extensions (klausul 5.5.9)

Inom ramen för dessa specifikationer är detta fält FRIVILLIGT, men det SKA användas när den information som ges i ”Service digital identity” (klausul 5.5.3) inte räcker för att otvetydigt identifiera de kvalificerade certifikat som utfärdas av denna tjänst och/eller informationen i de relaterade kvalificerade certifikaten inte tillåter maskinläsbar identifiering av huruvida QC stöds av en SSCD ([1]).

När det inom ramen för dessa specifikationer är OBLIGATORISKT att använda detta fält, t.ex. för CA/QC-tjänster, SKA det frivilliga informationsfältet Service information extensions (Sie) användas och struktureras i enlighet med det kvalificeringstillägg som fastställs i Etsi TS 102231 bilaga L.3.1, som en sekvens av en eller flera tupler, där varje tupel innehåller

— (filter) information som ska användas för att under den Sdi-identifierade certifieringstjänsten ytterligare identifiera exakt den tjänst (dvs. uppsättning av kvalificerade certifikat) för vilka ytterligare uppgifter krävs/tillhandahålls med avseende på indikationen av SSCD-stöd (och/eller utfärdande till en juridisk person), och

— därmed sammanhängande information (kvalificerare) om huruvida denna ytterligare identifierade tjänsteuppsättning av kvalificerade certifikat stöds av en SSCD (när denna information är ”QCSSCDStatusAsInCert” innebär detta att den därmed sammanhängande informationen ingår i QC i en Etsi-standardiserad maskinläsbar form ([2]) och/eller information om att dessa QC utfärdas till juridiska personer (det förinställda värdet är att de ska betraktas som utfärdade till endast fysiska personer).

— QCWithSSCD (http://uri.etsi.org/TrstSvc/eSigDir-1999–93-EC-TrustedList/SvcInfoExt/QCWithSSCD): Detta innebär att det säkerställs av CSP och kontrolleras (övervakningsmodell) eller granskas (ackrediteringsmodell) av medlemsstaten (övervakningsorgan respektive ackrediteringsorgan) att alla QC som utfärdas under den tjänst (QCA) som anges i ”Service digital identity” (klausul 5.5.3) och ytterligare identifieras genom ovannämnda (filter) information som används för att under den Sdi-identifierade certifieringstjänsten ytterligare identifiera just den uppsättning av kvalificerade certifikat för vilka denna ytterligare information krävs med avseende på förekomsten eller frånvaron av SSCD-stöd, HAR stöd av en SSCD (dvs. att den privata nyckel som är associerad med den allmänna nyckeln i certifikatet lagras i en säker anordning för skapande av signaturer i enlighet med bilaga III till direktiv 1999/93/EG).

([1]) Se avsnitt 2.2 i detta dokument.

([2]) Detta avser en lämplig kombination av Etsi-definierade QcCompliance-deklarationer, QcSSCD-deklarationer [Etsi TS 101 862] eller ett QCP/QCP + Etsi-definierat OID [Etsi TS 101 456].

▼C1

— QCNoSSCD (http://uri.etsi.org/TrstSvc/eSigDir-1999–93-EC-TrustedList/SvcInfoExt/QCNoSSCD): Detta innebär att det säkerställs av CSP och kontrolleras (övervakningsmodell) eller granskas (ackrediteringsmodell) av medlemsstaten (övervakningsorgan respektive ackrediteringsorgan) att alla QC som utfärdas under den tjänst (RootCA/QC eller CA/QC) som anges i ”Service digital identity” (klausul 5.5.3) och ytterligare identifieras genom ovannämnda (filter) information som används för att under den Sdi-identifierade certifieringstjänsten ytterligare identifiera just den uppsättning av kvalificerade certifikat för vilka denna ytterligare information krävs med avseende på förekomsten eller frånvaron av SSCD-stöd, INTE HAR stöd av en SSCD (dvs. att den privata nyckel som är associerad med den allmänna nyckeln i certifikatet inte lagras i en säker anordning för skapande av signaturer i enlighet med bilaga III till direktiv 1999/93/EG).

— QCSSCDStatusAsInCert (http://uri.etsi.org/TrstSvc/eSigDir-1999–93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert): Detta innebär att det säkerställs av CSP och kontrolleras (övervakningsmodell) eller granskas (ackrediteringsmodell) av medlemsstaten (övervakningsorgan respektive ackrediteringsorgan) att alla QC som utfärdas under den tjänst (CA/QC) som anges i ”Service digital identity” (klausul 5.5.3) och ytterligare identifieras genom ovannämnda (filter) information som används för att under den Sdi-identifierade certifieringstjänsten ytterligare identifiera just den uppsättning av kvalificerade certifikat för vilka denna ytterligare information krävs med avseende på förekomsten eller frånvaron av SSCD-stöd, SKA innehålla maskinläsbar information som anger huruvida denna QC stöds av en SSCD.

— QCForLegalPerson (http://uri.etsi.org/TrstSvc/eSigDir-1999–93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): Detta innebär att det säkerställs av CSP och kontrolleras (övervakningsmodell) eller granskas (ackrediteringsmodell) av medlemsstaten (övervakningsorgan respektive ackrediteringsorgan) att alla QC som utfärdas under den tjänst (QCA) som anges i ”Service digital identity” (klausul 5.5.3) och ytterligare identifieras genom ovannämnda (filter) information som används för att under den Sdi-identifierade certifieringstjänsten ytterligare identifiera just den uppsättning av kvalificerade certifikat för vilka denna ytterligare information krävs med avseende på utfärdande till juridiska personer, FAKTISKT utfärdas till juridiska personer.

Dessa kvalificerare ska användas som tillägg om tjänstetypen är http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Detta fält är tillämpningsspecifikt (ASN.1 eller XML) och MÅSTE följa specifikationerna i Etsi TS 102231, bilaga L.3.1.

▼M1

Inom ramen för en XML-tillämpning måste det specifika innehållet i denna ytterligare information kodas med hjälp av xsd-filen i bilaga C i Etsi TS 102231.

▼C1

Service Approval History

Detta fält är FRIVILLIGT, men MÅSTE finnas med om fältet ”Historical information period” (klausul 5.3.12) har något annat värde än noll. Inom ramen för dessa specifikationer MÅSTE systemet alltså innehålla historisk information. Om den historiska informationen är tänkt att sparas, men tjänsten inte har någon historik som föregår den aktuella statusen (dvs. en första registrerad status eller historisk information som inte sparas av systemoperatören) SKA detta fält vara tomt. Annars SKA information om den föregående godkännandestatusen anges i fallande ordning efter datum och tidpunkt för statusförändringen (dvs. datum och tidpunkt då den efterföljande godkännandestatusen trädde i kraft) för varje förändring av aktuell status för TSP-tjänsten som gjorts under den historiska informationsperioden enligt specifikationerna i Etsi TS 102231 klausul 5.3.12.

▼C1

Detta SKA vara en sekvens av historisk information enligt följande definitioner.

TSP(1) Tjänst (1) Historik(1)

Service type identifier (klausul 5.6.1)

Detta fält är OBLIGATORISKT och SKA innehålla identifikationen för tjänstetypen, med det format och den betydelse som används i ”TSP Service Information – Service type identifier” (klausul 5.5.1).

Service name (klausul 5.6.2)

Detta fält är OBLIGATORISKT och SKA innehålla det namn under vilket CSP:n tillhandahöll den tjänst som anges i ”TSP Service Information – Service type identifier” (klausul 5.5.1), med det format och den betydelse som används i ”TSP Service Information – Service name” (klausul 5.5.2). Denna klausul kräver inte att namnet är samma namn som anges i klausul 5.5.2. En namnändring KAN vara en av de omständigheter som kräver en ny status.

▼M1

Service digital identity (klausul 5.6.3)

Detta fält är OBLIGATORISKT och SKA minst innehålla en förekomst av en digital identifikation (t.ex. X.509v3 certifikat) som anges i ”TSP Service Information – Service digital identity” (klausul 5.5.3), med samma format och betydelse som i Etsi TS 102231, klausul 5.5.3.

Anm.: När det gäller X.509v3 certifikatvärdet som används i ”Service digital identity” (Sdi) klausul 5.5.3 för en tjänst, ska det finnas bara en registrering av en enkel tjänst i en tillförlitlig förteckning per ”Sti-värde Sti:Sie/-additionalServiceInformation”. Den ”Sdi”-information (klausul 5.6.3) som används i historiken ”Service approval history information” för tjänstens registerpost och den ”Sdi”-information (klausul 5.5.3) som används för denna registrerade tjänst måste avse samma X.509v3 certifikatvärde. När en förtecknad tjänst ändrar ”Sdi” (dvs. förnyat eller ny nyckel till ett X.509v3-certifikat för t.ex. CA/PKC eller CA/QC) eller om en ny ”Sdi” skapas för en sådan tjänst, även med identiska värden för associerade ”Sti”,”Sn”, och [”Sie”], innebär det att operatören MÅSTE skapa en annan registrerad tjänst än den tidigare tjänsten.

▼C1

Service previous status (klausul 5.6.4)

Detta fält är OBLIGATORISKT och SKA innehålla identifikationen för tjänstens föregående status, med det format och den betydelse som används i ”TSP Service Information – Service current status” (klausul 5.5.4).

Previous status starting date and time (klausul 5.6.5)

Detta fält är OBLIGATORISKT och SKA ange det datum och den tidpunkt då den föregående statusen trädde i kraft, med det format och den betydelse som används i ”TSP Service Information – Service current status starting date and time” (klausul 5.5.5).

Service information extensions (klausul 5.6.6)

▼C2

Detta fält är FRIVILLIGT och FÅR användas av systemoperatörer för att lämna specifik tjänsterelaterad information med det format och den betydelse som används i ”TSP Service Information – Service information extensions” (klausul 5.5.9).

▼C2

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

Samma som för TSP(1) Service(1) History(2) (före History1)

…

TSP(1) Service(2)

Samma som för TSP(1) Service 2 (i förekommande fall)

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

…

TSP(2) Information

Samma som för TSP 2 (i förekommande fall)

Samma som för TSP 2 Service 1

Samma som för TSP 2 Service 1 History 1

▼M1

Signed TSL

Den människoläsbara TSL-tillämpning av en tillförlitlig förteckning som inrättats enligt dessa specifikationer och i synnerhet kapitel IV, BÖR signeras av ”Scheme operator name” (klausul 5.3.4) för att säkerställa dess autenticitet och integritet ([1]) Signaturens format BÖR vara PAdES del 3 (Etsi TS 102 778–3 ([2])) men KAN även vara PAdESdel 2 (Etsi TS 102 778–2 ([3]) inom ramen för den särskilda tillförlitliga modell för tillförlitliga förteckningar som inrättats för offentliggörandet av de certifikat som används för signatur av den tillförlitliga förteckningen.

Den maskinläsbara TSL-tillämpningen av en tillförlitlig förteckning som inrättats enligt dessa specifikationer SKA signeras av ”Scheme operator name” (klausul 5.3.4) för att säkerställa dess autenticitet och integritet. Formatet för den maskinläsbara TSL-tillämpningen av den tillförlitliga förteckning som upprättats enligt gällande specifikationer SKA vara XML och SKA vara i överensstämmelse med specifikationerna i bilagorna B och C i Etsi TS 102231.

Signaturens format SKA vara XAdES BES eller EPES enligt definitionen i Etsi TS 101903 specifikationerna för XML-tillämpningar. Sådana tillämpningar av elektroniska signaturer SKA motsvara kraven i bilaga B till Etsi TS 102231 ([4]). Ytterligare allmänna krav för signaturen anges i följande avsnitt.

▼C1

Scheme identification (klausul 5.7.2)

Detta fält är OBLIGATORISKT och SKA innehålla en hänvisning som tilldelats av systemoperatören och som utgör en unik identifikation av det system som beskrivs i dessa specifikationer och i den upprättade TSL och MÅSTE inbegripas i beräkningen av signaturen. Detta förväntas vara en teckensträng eller en bitsträng.

([1]) Om den människoläsbara TSL-tillämpningen av den tillförlitliga förteckningen inte signeras SKA dess autenticitet och integritet säkerställas genom en lämplig kommunikationskanal med motsvarande säkerhetsnivå. Användning av TLS (IETF RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2) rekommenderas för detta ändamål och medlemsstaterna SKA göra fingeravtryck av certifikatet för TLS-kanalen tillgängligt utanför bandet för TSL-användarna.

([2]) Etsi TS 102 778–3 – Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Del 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; Del 2: PAdES Basic – Profil baserad på ISO 32000–1.

([4]) Det är obligatoriskt att skydda den systemoperatör som signerar certifikatet med signaturen på något av de sätt som anges i Etsi TS 101 903 och ds:keyInfo bör innehålla den relevanta certifikatkedjan.

▼M1

Inom ramen för dessa specifikationer SKA den angivna hänvisningen inbegripa ”TSL type” (klausul 5.3.3), ”Scheme name” (klausul 5.3.6) och värdet på tilllägget SubjectKeyIdentifier för det certifikat som systemoperatören använder för att elektroniskt signera TSL.

▼C1

Signature algorithm identifier (klausul 5.7.3)

Detta fält är OBLIGATORISKT och SKA innehålla den kryptografiska algoritm som har använts för att skapa signaturen. Beroende på vilken algoritm som används KAN detta fält kräva ytterligare parametrar. Detta fält MÅSTE ingå i beräkningen av signaturen.

Signature value (klausul 5.7.4)

Detta fält är OBLIGATORISKT och SKA innehålla den digitala signaturens faktiska värde. Alla fält i TSL (utom själva signaturvärdet) MÅSTE inbegripas i beräkningen av signaturen.

TSL extensions (klausul 5.8)

expiredCertsRevocationInfo – tillägg (klausul 5.8.1)

Detta tillägg är FRIVILLIGT. När det används MÅSTE det följa specifikationerna i Etsi TS 102231, klausul 5.8.1.

additionalServiceInformation – tillägg (klausul 5.8.2)

När detta FRIVILLIGA tillägg används, MÅSTE det uteslutande användas på tjänstenivå och endast i det fält som anges i klausul 5.5.9 (”Service information extension”). Det används för att ge ytterligare information om en tjänst. Denna SKA vara en sekvens av en eller flera tupler, där varje tupel innehåller

a) en URI som identifierar den ytterligare informationen, t.ex.

   — en URI som anger en nationellt definierad specifik kvalifikation för en övervakad/ackrediterad tjänst som t.ex. tillhandahåller igenkänningstecken för betrodda tjänster,

   — en specifik säkerhets-/kvalitetsgranularitetsnivå för nationella övervaknings-/ackrediteringssystem för CSP som inte utfärdar QC (t.ex. RGS */**/*** i Frankrike, specifik övervakningsstatus enligt nationell lagstiftning för specifika CSP som utfärdar QC i Tyskland), se anmärkning 4 till ”Service current status” – klausul 5.5.4,

   — eller en specifik rättslig status för övervakat/ackrediterat tillhandahållande av igenkänningstecken för betrodda tjänster (t.ex. nationellt definierade kvalificerade igenkänningstecken för betrodda tjänster, som i Tyskland eller Ungern),

   — eller innebörd i en viss policyidentifiering som finns i ett X.509v3-certifikat som angetts i Sdi-fältet,

   — eller en registrerad URI i enlighet med fältet ”Service type identifier”, klausul 5.5.1, för att ytterligare specificera att den tjänst som anges i Sti deltar som en tjänstekomponent hos en tillhandahållare av certifieringstjänster som utfärdar QC (t.ex. OCSP-QC, CRL-QC, och RootCA-QC),

b) en valfri sträng som innehåller serviceInformation-värdet, med den betydelse som anges i systemet (t.ex. *, ** eller ***),

c) eventuell frivillig ytterligare information som ges i ett systemspecifikt format.

▼**M1**

Namnåtergång för URI:n BÖR leda till människoläsbar information (på engelska och eventuellt ett eller flera språk) som anses vara lämplig och tillräcklig för att en beroende part ska förstå tillägget och bör i synnerhet förklara ifrågavarande URI:ns betydelse med de möjliga värdena för serviceInformation och betydelsen för varje enskilt värde.

Qualifications Extension (klausul L.3.1)

Beskrivning: Detta fält fylls i FRIVILLIGT men SKA finnas när det är OBLIGATORISKT att använda det, t.ex. för RootCA/QC- eller CA/QC-tjänster och när

— den information som lämnats i fältet ”Service digital identity” inte är tillräcklig för att otvetydigt identifiera de kvalificerade certifikat som utfärdas av denna tjänst,

— den information som finns i de relaterade kvalificerade certifikaten inte tillåter en maskinläsbar identifiering av huruvida QC stöds av en SSCD.

Om den används FÅR detta tillägg på tjänstenivå endast användas i ett fält som definieras i ”Service information extension” (klausul 5.5.9) och SKA vara i överensstämmelse med specifikationerna i bilaga L.3.1 till Etsi TS 102 231.

TakenOverBy Extension (klausul L.3.2)

Beskrivning: Detta tillägg är VALFRITT men ska finnas när en tjänst som tidigare omfattades av CSP:s juridiska ansvar tas över av en annan TSP och när den har till syfte att formellt ange tjänstens juridiska ansvar och för att göra det möjligt att i verifieringsmjukvaran visa juridiska uppgifter för användaren. Uppgifterna i detta tillägg SKA vara i överensstämmelse med användningen av klausul 5.5.6 och med specifikationerna i bilaga L.3.2 till Etsi TS 102 231.

▼**M1**

KAPITEL II

När medlemsstaterna upprättar tillförlitliga förteckningar ska de använda

gemener för språkkoder, och versaler för landskoder,

språk- och landskoder enligt nedanstående tabell.

När andra än latinska bokstäver används (med motsvarande språkkod) bifogas en translitterering med latinska bokstäver med den språkkod som anges i tabellen nedan.

Kortnamn (källspråk)	Kortnamn (engelska)	Landskod	Språkkod	Anmärkningar	Tranlitterering till latiska bokstäver
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	Landskod rekommenderad av EU	el-Latn
España	Spain	ES	es	även katalanska (ca),baskiska (eu), galiciska (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**

Kortnamn (källspråk)	Kortnamn (engelska)	Landskod	Språkkod	Anmärkningar	Tranlitterering till latiska bokstäver
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Landskod rekommenderad av EU	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtens-tein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Translitterering med latinska bokstäver: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

———————

▼C1

KAPITEL IV

SPECIFIKATIONER FÖR DEN LÄSBARA VERSIONEN AV TSL-TILLÄMPNINGEN AV DEN TILLFÖRLITLIGA FÖRTECKNINGEN

En läsbar version av TSL-tillämpningen av den tillförlitliga förteckningen MÅSTE göras allmänt tillgänglig och gå att komma åt elektroniskt. Den BÖR tillhandahållas i pdf-format (*Portable Document Format*) i ett dokument som följer ISO 32000 och som MÅSTE vara formaterat enligt profil PDF/A (ISO 19005).

Innehållet i den PDF/A-baserade läsbara versionen av TSL-tillämpningen av den tillförlitliga förteckningen BÖR uppfylla följande krav:

▼M1

— Titeln på det människoläsbara formatet av den tillförlitliga förteckningen ska bestå av en sammankoppling av följande element:

  — Valfri bild av medlemsstaternas nationella flaggor.

  — Tomt fält.

  — Landsnamn i kortform på källspråket/språken (enligt kolumn 1 i tabellen i kapitel II).

  — Tomt fält.

  — ”(”.

  — Landsnamn i kortform på engelska (enligt kolumn 2 i tabellen i kapitel II) inom parentes.

  — ”):” som avslutande parentes och skiljetecken.

  — Tomt fält.

  — ”Tillförlitlig förteckning”.

  — Valfri logo för medlemsstaternas operatör.

▼C1

— Den läsbara versionens struktur BÖR avspegla den logiska mall som beskrivs i avsnitt 5.1.2 i Etsi TS 102231.

— Varje fält som ingår BÖR visas och innehålla följande information:

  — Fältets rubrik (t.ex. ”Service type identifier”)

  — Fältets värde (t.ex. ”CA/QC”)

  — Innebörden (beskrivning) av fältets värde när så är tillämpligt och framför allt enligt vad som anges i bilaga D till Etsi TS 102231 eller i dessa specifikationer för registrerade URI:er (t.ex. ”En certifikatutfärdare som utfärdar allmänna nyckelcertifikat”).

  — Flera versioner på naturliga språk enligt vad som används i TSL-tillämpningen av den tillförlitliga förteckningen, när så är tillämpligt.

— Följande fält och motsvarande värden för de digitala certifikat som finns i fältet ”Service digital identity” BÖR minst återges i den läsbara versionen:

  — Version

  — Löpnummer

  — Signaturalgoritm

  — Utfärdare

  — Giltigt från

  — Giltigt till

  — Föremål

▼C1

— Allmän nyckel

— Certifikatpolicy

— Föremålets nyckelidentifiering

— CRL-distributionspunkter

— Utfärdares nyckelidentifiering

— Nyckelanvändningar

— Grundläggande begränsningar

— Tumavtrycksalgoritm

— Tumavtryck

— Den läsbara versionen BÖR vara lätt att skriva ut.

— Den läsbara versionen FÅR vara elektroniskt signerad. Om den signeras MÅSTE detta göras av systemoperatören enligt samma signeringsspecifikationer som för TSL-tillämpningen av den tillförlitliga förteckningen.