Tämä asiakirja on ainoastaan dokumentointitarkoituksiin. Toimielimet eivät vastaa sen sisällöstä.

►B ►C1 **KOMISSION PÄÄTÖS,**

tehty 16 päivänä lokakuuta 2009,

toimenpiteistä sähköisten menettelyjen käytön edistämiseksi keskitettyjä asiointipisteitä käyttäen palveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston direktiivin 2006/123/EY mukaisesti

(tiedoksiannettu numerolla K (2009) 7806)

(ETA:n kannalta merkityksellinen teksti)

(2009/767/EY) ◄

(EUVL L 274, 20.10.2009, s. 36)

sellaisena kuin se on muutettuna seuraavilla:

		virallinen lehti		
		N:o	sivu	päivämäärä
►M1	Komission päätös 2010/425/EU, annettu 28 päivänä heinäkuuta 2010	L 199	30	31.7.2010
►M2	Komission asetus (EU) N:o 519/2013, annettu 21 päivänä helmikuuta 2013	L 158	74	10.6.2013

Oikaistu:

►C1 Oikaisu, EUVL L 299, 14.11.2009, s. 18 (2009/767/EY)

►C2 Oikaisu, EUVL L 4, 7.1.2011, s. 6 (2009/767/EY)

▼B
▼C1

KOMISSION PÄÄTÖS,

tehty 16 päivänä lokakuuta 2009,

toimenpiteistä sähköisten menettelyjen käytön edistämiseksi keskitettyjä asiointipisteitä käyttäen palveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston direktiivin 2006/123/EY mukaisesti

(tiedoksiannettu numerolla K (2009) 7806)

(ETA:n kannalta merkityksellinen teksti)

(2009/767/EY)

EUROOPAN YHTEISÖJEN KOMISSIO, joka

ottaa huomioon Euroopan yhteisön perustamissopimuksen,

ottaa huomioon palveluista sisämarkkinoilla 12 päivänä joulukuuta 2006 annetun Euroopan parlamentin ja neuvoston direktiivin 2006/123/EY ([1]) ja erityisesti sen 8 artiklan 3 kohdan,

sekä katsoo seuraavaa:

(1) Direktiivin 2006/123/EY II luvussa ja erityisesti sen 5 ja 8 artiklassa jäsenvaltioille säädettyihin hallinnollisen yksinkertaistamisen velvoitteisiin kuuluvat velvoite yksinkertaistaa palvelutoiminnan aloittamiseen ja harjoittamiseen sovellettavia menettelyjä ja muodollisuuksia ja velvoite varmistaa, että ne voidaan hoitaa vaivatta etäältä ja sähköisesti ”keskitettyjen asiointipisteiden” kautta.

(2) Direktiivin 2006/123/EY 8 artiklan mukaisesti menettelyt ja muodollisuudet on voitava hoitaa keskitettyjen asiointipisteiden kautta myös jäsenvaltioiden rajojen yli.

(3) Täyttääkseen vaatimuksen menettelyjen ja muodollisuuksien yksinkertaistamisesta ja keskitettyjen asiointipisteiden rajan yli tapahtuvan käytön edistämisestä sähköisten menettelyjen on perustuttava yksinkertaisiin ratkaisuihin, esimerkiksi sähköisten allekirjoitusten käyttöön. Mikäli korkea turvallisuustaso tai omakätisen allekirjoituksen vastaavuustaso katsotaan tarpeelliseksi konkreettisten menettelyjen ja muodollisuuksien asianmukaisen riskinarvioinnin perusteella, palveluntarjoajilta voitaisiin edellyttää tietyissä menettelyissä ja muodollisuuksissa kehittyneitä sähköisiä allekirjoituksia, jotka perustuvat hyväksyttyyn varmenteeseen, mahdollisesti yhdistettynä turvallisiin allekirjoituksen luomismenetelmiin.

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

▼C1

(4) Sähköisiä allekirjoituksia koskevat yhteisön puitteet määriteltiin sähköisiä allekirjoituksia koskevista yhteisön puitteista 13 päivänä joulukuuta 1999 annetussa Euroopan parlamentin ja neuvoston direktiivissä 1999/93/EY ([1]). Jotta hyväksyttyihin varmenteisiin perustuvien kehittyneiden sähköisten allekirjoitusten tosiasiallista rajat ylittävää käyttöä voitaisiin edistää, luottamusta kyseisiin sähköisiin allekirjoituksiin olisi lisättävä riippumatta siitä, mihin jäsenvaltioon allekirjoittaja tai hyväksytyn varmenteen myöntänyt varmennepalvelujen tarjoaja on sijoittautunut. Tähän voitaisiin päästä saattamalla sähköisten allekirjoitusten validointiin tarvittavat tiedot helpommin saataville luotettavassa muodossa. Erityisesti tämä koskee yksittäisessä jäsenvaltiossa valvottuja/akkreditoituja varmennepalvelujen tarjoajia ja niiden tarjoamia palveluja koskevia tietoja.

(5) On tarpeen varmistaa, että jäsenvaltiot saattavat nämä tiedot julkisesti saataville yhteisen mallin avulla. Näin helpotetaan tietojen käyttöä ja varmistetaan riittävän yksityiskohtaiset tiedot, joiden avulla vastaanottava osapuoli pystyy validoimaan sähköisen allekirjoituksen,

ON TEHNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Sähköisten allekirjoitusten käyttö ja hyväksyntä

1. Asiaan liittyvien riskien asianmukaisen arvioinnin perusteella ja direktiivin 2006/123/EY 5 artiklan 1 ja 3 kohdan mukaisesti jäsenvaltiot voivat edellyttää, että palveluntarjoaja käyttää tiettyjen menettelyjen ja muodollisuuksien hoitamisessa direktiivin 2006/123/EY 8 artiklassa tarkoitettujen keskitettyjen asiointipisteiden kautta hyväksyttyihin varmenteisiin perustuvia kehittyneitä sähköisiä allekirjoituksia, mahdollisesti yhdistettynä turvallisiin allekirjoitusten luomismenetelmiin, sellaisina kuin nämä käsitteet on määritelty ja niistä säädetään direktiivissä 1999/93/EY.

2. Jäsenvaltioiden tulee hyväksyä jokainen hyväksyttyyn varmenteeseen perustuva, mahdollisesti turvalliseen allekirjoituksen luomismenetelmään yhdistetty kehittynyt sähköinen allekirjoitus 1 kohdassa tarkoitettujen menettelyjen ja muodollisuuksien hoitamisessa, tämän kuitenkaan estämättä jäsenvaltioita rajoittamasta kyseistä hyväksyntää hyväksyttyyn varmenteeseen perustuviin ja turvallisella allekirjoituksen luomismenetelmällä luotuihin edistyneisiin sähköisiin allekirjoituksiin siinä tapauksessa, että tämä on 1 kohdassa tarkoitetun riskinarvioinnin mukaista.

3. Jäsenvaltiot eivät saa asettaa hyväksyttyyn varmenteeseen perustuvien, mahdollisesti turvalliseen allekirjoituksen luomismenetelmään yhdistettyjen kehittyvien sähköisten allekirjoitusten hyväksymisen ehdoksi vaatimuksia, jotka muodostavat esteitä palveluntarjoajien mahdollisuudelle hoitaa menettelyjä sähköisesti keskitettyjen asiointipisteiden kautta.

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

▼C1

4. Edellä oleva 2 kohta ei estä jäsenvaltioita hyväksymästä muitakin kuin hyväksyttyyn varmenteeseen perustuvia kehittyneitä sähköisiä allekirjoituksia, mahdollisesti turvalliseen allekirjoituksen luomismenetelmään yhdistettyinä.

2 artikla

Luotettavien luetteloiden laatiminen, ylläpitäminen ja julkaisu

1. Jokaisen jäsenvaltion on laadittava ja julkaistava liitteessä määriteltyjen teknisten eritelmien mukaisesti ”luotettava luettelo” ja ylläpidettävä sitä. Se sisältää vähimmäistiedot varmennepalvelujen tarjoajista, jotka myöntävät hyväksyttyjä varmenteita yleisölle ja joita jäsenvaltiot valvovat tai jotka ne ovat akkreditoineet.

▼M1

2. Jäsenvaltioiden on laadittava ja julkaistava luotettava luettelo sekä ihmisen luettavissa että koneellisesti luettavissa olevassa muodossa liitteessä määriteltyjen eritelmien mukaisesti.

2 a. Jäsenvaltioiden on allekirjoitettava koneellisesti luettavissa olevassa muodossa oleva luotettava luettelonsa sähköisesti ja julkaistava luotettava luettelo ainakin ihmisen luettavissa olevassa muodossa turvallisen kanavan kautta sen aitouden ja eheyden varmistamiseksi.

3. Jäsenvaltioiden on annettava komissiolle tiedoksi seuraavat:

a) ihmisen luettavissa ja koneellisesti luettavissa muodoissa olevan luotettavan luettelon laadinnasta, ylläpidosta ja julkaisusta vastaava laitos tai vastaavat laitokset;

b) ihmisen luettavissa olevassa muodossa ja koneellisesti luettavissa olevassa muodossa olevan luotettavan luettelon julkaisupaikat;

c) julkisen avaimen varmenne, jota käytetään ihmisen luettavassa muodossa olevan luotettavan luettelon julkaisuun käytettävän turvallisen kanavan toteutukseen, tai jos ihmisen luettavissa oleva luettelo allekirjoitetaan sähköisesti, julkisen avaimen varmenne, jota käytetään sen allekirjoittamiseen;

d) julkisen avaimen varmenne, jota käytetään koneellisesti luettavassa muodossa olevan luotettavan luettelon allekirjoittamiseen sähköisesti;

e) edellä a–d alakohdassa oleviin tietoihin mahdollisesti tehtävät muutokset.

4. Komission on asetettava 3 kohdassa tarkoitetut jäsenvaltioiden ilmoittamat tiedot turvallisen kanavan kautta kaikkien jäsenvaltioiden saataville varmennetulle WWW-palvelimelle sekä ihmisen luettavissa olevassa muodossa että koneellisesti luettavissa olevassa muodossa, joka on allekirjoitettu.

▼C1

3 artikla

Soveltaminen

Tätä päätöstä sovelletaan 28 päivästä joulukuuta 2009.

4 artikla

Osoitus

Tämä päätös on osoitettu kaikille jäsenvaltioille.

▼C1

LIITE

”VALVOTTUJEN/AKKREDITOITUJEN VARMENNEPALVELUJEN TARJOAJIEN LUOTETTAVIA LUETTELOITA” KOSKEVAN YHTEISEN MALLIN TEKNISET ERITELMÄT

JOHDANTO

1. **Yleistä**

Jäsenvaltioiden ”valvottujen/akkreditoitujen varmennepalvelujen tarjoajien luotettavan luettelon” yhteisen mallin tarkoituksena on vahvistaa yhteinen tapa, jolla kukin jäsenvaltio toimittaa tietoja jäsenvaltioiden direktiivin 1999/93/EY asiaa koskevien säännösten täyttämisen osalta valvomien varmennepalvelujen tarjoajien (CSP) ([1]) suorittamien varmennepalvelujen valvonta-/akkreditointistatuksesta. Tähän kuuluu myös valvottujen/akkreditoitujen varmennepalvelujen valvonta-/akkreditointistatusta koskevien historiatietojen toimittaminen.

Luotettavan luettelon (TL) pakollisiin tietoihin kuuluvat vähimmäistiedot valvotusta/akkreditoidusta varmennepalvelujen tarjoajasta, joka myöntää hyväksyttyjä varmenteita (QC) ([2]) direktiivin 1999/93/EY säännösten (3 artiklan 2 ja 3 kohdan ja 7 artiklan 1 kohdan a alakohdan) mukaisesti, mukaan luettuina tiedot sähköiseen allekirjoitukseen liittyvästä hyväksytystä varmenteesta ja siitä, onko allekirjoitus luotu turvallisen allekirjoituksen luomismenetelmän (SSCD) ([3]) avulla vai ei.

Luotettavaan luetteloon voi sisältyä kansallisen tason vapaaehtoisuuteen perustuvia lisätietoja muista valvotuista/akkreditoiduista varmennepalvelujen tarjoajista, jotka eivät myönnä hyväksyttyjä varmenteita vaan tarjoavat sähköisiin allekirjoituksiin liittyviä palveluja (esim. aikaleimauspalveluja tarjoavat ja aikaleimasanakkeita antavat varmennepalvelujen tarjoajat, muita kuin hyväksyttyjä varmenteita antavat varmennepalvelujen tarjoajat jne.).

Näiden tietojen pääasiallisena tarkoituksena on tukea hyväksyttyjen sähköisten allekirjoitusten (QES) ja hyväksyttyyn varmenteeseen ([4]) ([5]) perustuvien kehittyneiden sähköisten allekirjoitusten (AdES) ([6]) validointia.

Ehdotettu yhteinen malli on yhteensopiva ETSIn teknisen spesifikaation 102 231 ([7]) mukaisiin eritelmiin perustuvan toteutuksen kanssa. Eritelmiä käytetään tällaisten luetteloiden laadinnassa, julkaisussa, sijoittamisessa, käytössä, aidonnuksessa ja luotettaviksi toteamisessa.

([1]) Määritelmä direktiivin 1999/93/EY 2 artiklan 11 kohdassa.
([2]) Määritelmä direktiivin 1999/93/EY 2 artiklan 10 kohdassa.
([3]) Määritelmä direktiivin 1999/93/EY 2 artiklan 6 kohdassa.
([4]) Määritelmä direktiivin 1999/93/EY 2 artiklan 2 kohdassa.
([5]) Tässä asiakirjassa käytetään hyväksyttyyn varmenteeseen (”QC”) perustuvasta kehittyneestä sähköisestä allekirjoituksesta (”AdES”) lyhennettä ”AdESQC”.
([6]) On huomattava, että myös monien tavalliseen kehittyneeseen sähköiseen allekirjoitukseen (AdES) perustuvien sähköisten palvelujen rajat ylittävä käyttö helpottuu, edellyttäen että tukevat varmennepalvelut (esim. muiden kuin hyväksyttyjen varmenteiden myöntäminen) ovat osa jäsenvaltion luotettavien luetteloiden vapaaehtoisissa tiedoissa mainittuja valvottuja/akkreditoituja palveluja.
([7]) ETSI TS 102 231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

2. **Suuntaviivat luotettavan luettelon kohtien muokkausta varten**

2.1 *Valvottuihin/akkreditoituihin varmennepalveluihin keskittyvä luotettava luettelo*

Asiaankuuluvat varmennepalvelut ja varmennepalvelujen tarjoajat yhdessä luettelossa

Jäsenvaltion luotettava luettelo määritellään ”luetteloksi kyseisen jäsenvaltion sitä varten valvomien/akkreditoimien varmennepalvelujen tarjoajien tuottamien varmennepalvelujen valvonta-/akkreditointistatuksesta, jotta direktiivin 1999/93/EY niitä koskevat säännökset täytetään”.

Luotettavassa luettelossa on mainittava

— kaikki varmennepalvelujen tarjoajat direktiivin 1999/93/EY 2 artiklan 11 kohdan määritelmän mukaisesti eli yhteisöt tai oikeushenkilöt tai luonnolliset henkilöt, jotka myöntävät varmenteita tai tarjoavat muita sähköisiin allekirjoituksiin liittyviä palveluja ja

— joita valvotaan / jotka on akkreditoitu sitä varten, jotta direktiivin 1999/93/EY niitä koskevia säännöksiä noudatetaan.

Kun tarkastellaan direktiiviin 1999/93/EY sisältyviä määritelmiä ja säännöksiä, varsinkin niitä, jotka koskevat asiaankuuluvia varmennepalvelujen tarjoajia ja näiden valvontaa / vapaaehtoisuuteen perustuvia akkreditointijärjestelmiä, voidaan erottaa kaksi varmennepalvelujen tarjoajien ryhmää: hyväksyttyjä varmenteita yleisölle myöntävät varmennepalvelujen tarjoajat (CSP_{QC}) ja palveluntarjoajat, jotka eivät myönnä hyväksyttyjä varmenteita vaan tarjoavat muita sähköisiin allekirjoituksiin liittyviä (lisä)palveluja.

— Hyväksyttyjä varmenteita myöntävät varmennepalvelujen tarjoajat

  — Näiden varmennepalvelujen tarjoajien sijoittautumisjäsenvaltion (jos tarjoajat ovat sijoittautuneet jäsenvaltioon) on valvottava tarjoajia, ja niille voidaan myöntää myös akkreditointi direktiivin 1999/93/EY säännösten noudattamisesta, liitteen I (hyväksyttyjä varmenteita koskevat vaatimukset) ja liitteen II (hyväksyttyjä varmenteita myöntävien varmennepalvelujen tarjoajia koskevat vaatimukset) vaatimukset mukaan luettuina. Jossain jäsenvaltiossa akkreditoitujen hyväksyttyjä varmenteita myöntävien varmennepalvelujen tarjoajien on edelleen kuuluttava kyseisen jäsenvaltion asianmukaiseen valvontajärjestelmään, jos ne ovat sijoittautuneet kyseiseen jäsenvaltioon.

  — Sovellettava ”valvontajärjestelmä” on määritelty direktiivin 1999/93/EY asiaa koskevissa säännöksissä, joiden vaatimukset järjestelmän on myös täytettävä, erityisesti 3 artiklan 3 kohdan, 8 artiklan 1 kohdan, 11 artiklan ja johdanto-osan 13 kappaleen säännökset (”vapaaehtoisuuteen perustuvan akkreditointijärjestelmän” osalta 2 artiklan 13 kohdan, 3 artiklan 2 kohdan, 7 artiklan 1 kohdan a alakohdan, 8 artiklan 1 kohdan, 11 artiklan sekä johdanto-osan 4 ja 11–13 kappaleen säännökset).

— Varmennepalvelujen tarjoajat, jotka eivät myönnä hyväksyttyjä varmenteita

  — Nämä varmennepalvelujen tarjoajat voivat kuulua (direktiivin 1999/93/EY määritelmien ja vaatimusten mukaisen) ”vapaaehtoisuuteen perustuvan akkreditointijärjestelmän” piiriin ja/tai kansallisesti toteutetun kansallisesti määritellyn ”tunnustetun hyväksymisjärjestelmän” piiriin direktiivin säännösten ja mahdollisesti varmennepalvelujen tarjontaa koskevien kansallisten säännösten noudattamisen valvonnan osalta (direktiivin 2 artiklan 11 kohdan määritelmän mukaan).

  — Joillekin varmennepalvelun tarjonnan tuloksena luoduille tai myönnetyille fyysisille tai binaarisille (loogisille) kohteille voidaan antaa oikeus erityiseen ”kelpuutukseen” sillä perusteella, että ne täyttävät kansallisella tasolla annetut säännökset ja vaatimukset, mutta tällaisen ”kelpuutuksen” merkitys jää todennäköisesti pelkästään kansalliseksi.

▼C1

Jäsenvaltion luotettavassa luettelossa (TL) on oltava vähimmäistiedot valvotuista/akkreditoiduista varmennepalvelujen tarjoajista, jotka myöntävät hyväksyttyjä varmenteita (QC) yleisölle direktiivin 1999/93/EY säännösten (3 artiklan 2 ja 3 kohdan ja 7 artiklan 1 kohdan a alakohdan) mukaisesti, tiedot sähköistä allekirjoitusta tukevasta hyväksytystä varmenteesta ja siitä, onko allekirjoitus luotu turvallisen allekirjoituksen luomismenetelmän avulla vai ei.

Luotettavaan luetteloon voi sisältyä kansallisen tason vapaaehtoisuuteen perustuvia lisätietoja sellaisista valvotuista/akkreditoiduista varmennepalvelujen tarjoajista, jotka eivät myönnä hyväksyttyjä varmenteita (esim. aikaleimauspalveluja tarjoavat ja aikaleimasanakkeita antavat varmennepalvelujen tarjoajat, muita kuin hyväksyttyjä varmenteita antavat varmennepalvelujen tarjoajat jne.).

Luotettavan luettelon tarkoituksena on

— luetella ja tarjota luotettavaa tietoa sellaisten varmennepalvelujen tarjoajien varmennepalvelujen valvonta-/akkreditointistatuksesta, joiden valvojana/akkreditoijana toimii jäsenvaltio, joka on vastuussa direktiivin 1999/93/EY asiaa koskevien säännösten noudattamista koskevan luettelon laadinnasta ja ylläpitämisestä,

— edistää luettelossa mainittujen varmennepalvelujen tarjoajien valvottujen/akkreditoitujen varmennepalvelujen tukemien sähköisten allekirjoitusten validointia.

Yhtenäiset valvonta-/akkreditointistatuksen arvot

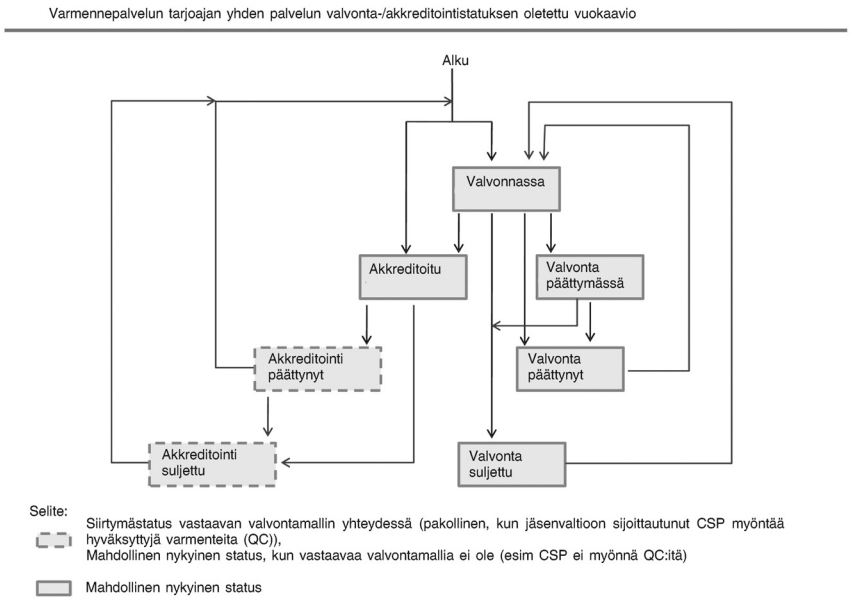
Kunkin jäsenvaltion on laadittava yksi ainoa luotettava luettelo ja ylläpidettävä sitä osoitukseksi kyseisen jäsenvaltion valvomien/akkreditoimien varmennepalvelujen tarjoajien varmennepalvelujen valvonta- ja/tai akkreditointistatuksesta.

Se, että palvelua valvotaan parhaillaan tai että palvelu on akkreditoitu, on osa palvelun kulloistakin statusta. Sen lisäksi valvonta- tai akkreditointistatus voi olla ”jatkuva”, ”päättyvä”, ”päättynyt” tai ”suljettu”. Sama varmennepalvelu voi elinkaarensa aikana siirtyä valvontastatuksesta akkreditointistatukseen ja päinvastoin ([1]).

Alla olevassa kaaviossa 1 kuvataan yksittäisen varmennepalvelun oletettu vuo mahdollisten valvonta-/akkreditointistatusten välillä:

([1]) Esimerkiksi jäsenvaltioon sijoittautunut varmennepalvelujen tarjoaja, joka tarjoaa varmennepalvelua ja jota jäsenvaltio (valvontaelin) on valvonut alun perin, voi jonkin ajan kuluttua päättää, että se hankkii vapaaehtoisuuteen perustuvan akkreditoinnin parhaillaan valvotulle varmennepalvelulle. Kääntäen johonkin toiseen jäsenvaltioon sijoittautunut varmennepalvelujen tarjoaja voi päättää, ettei se keskeytä akkreditoitua varmennepalveluaan vaan muuttaa sen akkreditointistatuksen valvontastatukseksi esimerkiksi liiketoiminnallisista ja/tai taloudellisista syistä.

▼C2



Kaavio 1

▼C1

Hyväksyttyjä varmenteita myöntävää varmennepalvelua on valvottava (jos se on sijoittautunut johonkin jäsenvaltioon), minkä lisäksi se voidaan akkreditoida vapaaehtoisuuteen perustuvana. Luotettavassa luettelossa lueteltu kyseisen palvelun ”nykyisen statuksen arvo” voi olla mikä tahansa edellä kuvatuista statuksen arvoista. On kuitenkin huomattava, että jäsenvaltioon sijoittautuneiden hyväksyttyjä varmenteita myöntävien varmennepalvelujen tarjoajien (CSP_{QC}) statukset ”Akkreditointi päättynyt” ja ”Akkreditointi suljettu” saavat olla ainoastaan ”siirtymästatuksen” arvoja, koska oletusarvoisesti tällaisia palveluja on valvottava – silloinkin, kun ne eivät ole (enää) akkreditoituja.

Jäsenvaltioiden, jotka laativat tai ovat laatineet kansallisesti määritellyn ja kansallisesti toteutetun ”tunnustetun hyväksymisjärjestelmän” tai useita sellaisia sen valvomiseksi, että niiden varmennepalvelujen tarjoajien, jotka eivät myönnä hyväksyttyjä varmenteita, tarjoamat palvelut ovat direktiivin 1999/93/EY säännösten ja (direktiivin 2 artiklan 11 kohdassa tarkoitettujen) varmennepalvelujen tarjontaa koskevien mahdollisten kansallisten säännösten mukaisia, on luokiteltava kyseiset hyväksymisjärjestelmät seuraaviin luokkiin:

— direktiivissä 1999/93/EY (2 artiklan 13 kohta, 3 artiklan 2 kohta, 7 artiklan 1 kohdan a alakohta, 8 artiklan 1 kohta, 11 artikla, johdanto-osan neljäs ja 11–13 kappale) määritelty ja säännelty ”vapaaehtoisuuteen perustuva akkreditointi”,

— direktiivissä 1999/93/EY säädetty pakollinen ”valvonta”, joka on pantu täytäntöön kansallisten lakien mukaisin kansallisin säännöksin ja vaatimuksin.

▼C1

Näin ollen varmennepalvelu, jossa ei myönnetä hyväksyttyjä varmenteita, voi olla valvottu tai vapaaehtoisuuteen perustuvana akkreditoitu. Luotettavassa luettelossa lueteltu kyseisen palvelun ”nykyisen statuksen arvo” voi olla mikä tahansa edellä kuvatuista statuksen arvoista (ks. kaavio 1).

Luotettavan luettelon pitää sisältää tiedot käytetystä valvonta-/akkreditointijärjestelmästä tai järjestelmistä, erityisesti

— tiedot hyväksyttyjä varmenteita myöntäviin varmennepalvelujen tarjoajiin (CSP_{QC}) sovellettavasta valvontajärjestelmästä,

— tiedot hyväksyttyjä varmenteita myöntäviin varmennepalvelujen tarjoajiin (CSP_{QC}) sovellettavasta kansallisesta ”vapaaehtoisuuteen perustuvasta akkreditointijärjestelmästä”, mikäli sellainen on,

— tiedot sellaisiin varmennepalvelujen tarjoajiin, jotka eivät myönnä hyväksyttyjä varmenteita, sovellettavasta valvontajärjestelmästä, mikäli sellainen on,

— tiedot niihin varmennepalvelujen tarjoajiin, jotka eivät myönnä hyväksyttyjä varmenteita (QC), sovellettavasta kansallisesta ”vapaaehtoisuuteen perustuvasta akkreditointijärjestelmästä”, mikäli sellainen on.

Kahdessa viimeisessä kohdassa mainitut tiedot ovat ratkaisevan tärkeitä, kun varmenteeseen luottavat osapuolet arvioivat varmennepalvelujen tarjoajiin, jotka eivät myönnä hyväksyttyjä varmenteita, sovellettavien kansallisten valvonta-/akkreditointijärjestelmien laatua ja turvallisuutta. Kun luotettavassa luettelossa esitetään varmennepalvelujen tarjoajista, jotka eivät myönnä hyväksyttyjä varmenteita, valvonta-/akkreditointistatusta koskevaa tietoa, edellä mainitut tiedot tarjotaan luettelokohtaisesti käyttämällä lausekkeita ”Scheme information URI” (lauseke 5.3.7 – jäsenvaltioiden tarjoamat tiedot), ”Scheme type/community/rules” (lauseke 5.3.9 – käyttämällä kaikille jäsenvaltioille yhteistä tekstiä ja vapaaehtoisia jäsenvaltion tarjoamia erityistietoja) ja ”TSL policy/legal notice” (lauseke 5.3.11 – kaikille jäsenvaltioille yhteinen direktiiviin 1999/93/EY viittaava teksti ja kunkin jäsenvaltion mahdollisuus lisätä jäsenvaltiokohtaisia tekstejä/viitteitä). Varmennepalvelujen tarjoajia, jotka eivät myönnä hyväksyttyjä varmenteita, koskevissa kansallisissa valvonta-/akkreditointijärjestelmissä määriteltyjä lisätietoja ”kelpuutuksesta” voidaan tarjota palvelutasokohtaisesti tarvittaessa ja silloin kun se on pakollista (esimerkiksi eri laatu-/palvelutasojen erottamiseksi toisistaan) käyttämällä osana ”Service information extension” -liitteeseen (lauseke 5.5.9) kuuluvaa ”additionalServiceInformation”-liitettä (lauseke 5.8.2). Muita tietoja vastaavista teknisistä eritelmistä on esitetty luvussa I olevissa yksityiskohtaisissa eritelmissä.

Vaikka jäsenvaltioon sijoittautuneiden varmennepalvelujen valvonnasta ja akkreditoinnista voivat vastata jäsenvaltion erilliset elimet, yhdessä varmennepalvelussa oletetaan käytettävän vain yhtä merkintää (ETSIn teknisessä spesifikaatiossa 102 231 ([1]) määritellyn ”Service digital identity” -tunnisteen mukaisesti) ja sen valvonta-/akkreditointistatusta oletetaan päivitettävän vastaavasti. Edellä kuvattujen statusten merkitys on kuvattu luvussa I olevien yksityiskohtaisten teknisten eritelmien asiaan liittyvässä lausekkeessa 5.5.4.

2.2 *Luotettavat luettelot hyväksyttyjen sähköisten allekirjoitusten (QES) ja hyväksyttyyn varmenteeseen perustuvien kehittyneiden sähköisten allekirjoitusten ($AdES_{QC}$) validoinnin edistämiseksi*

Luotettavan luettelon laadinnan kaikkein kriittisin vaihe on luotettavan luettelon pakollisen osan laadinta. Tällä tarkoitetaan kunkin hyväksyttyjä varmenteita myöntävän varmennepalvelujen tarjoajan ‘palveluluetteloa‘, jonka on vastattava totuudenmukaisesti kunkin hyväksyttyjä varmenteita myöntävän varmennepalvelun tarkkaa myöntämisstatusta ja jolla on varmistettava, että kussakin syötteessä annetut tiedot riittävät hyväksyttyjen sähköisten allekirjoitusten ja hyväksyttyihin varmenteisiin perustuvien kehittyneiden sähköisten allekirjoitusten validoinnin edistämiseen (yhdistettynä kyseisessä kohdassa mainitun varmennepalvelun tarjoavan varmennepalvelun tarjoajan myöntämän loppukäyttäjän hyväksytyn varmenteen sisältöön).

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

▼C1

Koska hyväksytylle varmenteelle ei ole tähän mennessä ollut olemassa aidosti yhteentoimivaa ja rajat ylittävää profiilia, pakollisiin tietoihin voi sisältyä muita tietoja kuin yksittäisen (juuritason) varmentajan ”Service digital identity” -tieto, erityisesti myönnetyn varmenteen QC-statuksen tunnistamisen mahdollistavat tiedot ja se, onko tuetut allekirjoitukset luotu turvallisen allekirjoituksen luomismenetelmän (SSCD) avulla. Tämän vuoksi sen jäsenvaltion elimen, joka on nimetty luotettavan luettelon laatijaksi, muokkaajaksi ja ylläpitäjäksi (eli ETSIn teknisessä spesifikaatiossa 102 231 tarkoitetuksi järjestelmäoperaattoriksi, ”Scheme operator”), pitää ottaa huomioon kunkin hyväksytyn varmenteen nykyinen profiili ja varmenteen sisältö kunkin luotettavaan luetteloon sisältyvän hyväksyttyjä varmenteita myöntävän varmennepalvelujen tarjoajan kohdalla.

Ihannetapauksessa jokaiseen myönnettyyn hyväksyttyyn varmenteeseen pitäisi sisältyä ETSIn määrittelemä QcCompliance ([1]) -kuvaus, kun varmenteen väitetään olevan hyväksytty varmenne, ja ETSIn teknisessä spesifikaatiossa määritelty QcSSCD-kuvaus, kun sen väitetään olevan sähköisten allekirjoitusten turvallisen luomismenetelmän tukema, ja/tai että myönnettyyn hyväksyttyyn varmenteeseen sisältyy yksi ETSIn teknisessä spesifikaatiossa 101 456 ([2]) määritelty varmennepolitiikan kohdetunniste (OID) QCP/QCP+. Koska varmennepalvelujen tarjoajat myöntävät hyväksyttyjä varmenteita käyttäen eri viitestandardeja, koska standardeja tulkitaan hyvin väljästi ja koska eräiden normatiivisten teknisten eritelmien tai standardien olemassaolo ja ensisijaisuus ei ole yleisesti tiedossa, nykyisin myönnettävien hyväksyttyjen varmenteiden tosiasiallisessa sisällössä on eroja (esimerkiksi ETSIn määrittelemien QcStatatements-lausumien käytön osalta). Tämän vuoksi vastaanottavat osapuolet eivät voi muitta mutkitta luottaa allekirjoittajan varmenteeseen (ja siihen liittyvään ketjuun/polkuun) arvioidessaan ainakaan koneellisesti luettavassa muodossa sitä, väitetäänkö sähköistä allekirjoitusta tukevan varmenteen olevan hyväksytty varmenne vai ei, ja sitä, liittyykö siihen turvallinen sähköisen allekirjoituksen luomismenetelmä, jolla sähköinen allekirjoitus on luotu.

Kun kenttiä ”Service type identifier” (”Sti”), ”Service name” (”Sn”) ja ”Service digital identity” (”Sdi”) ([3]) täydennetään kentässä ”Service information extensions” (”Sie”) annetuilla tiedoilla, ehdotetussa luotettavan luettelon yhteisessä mallissa voidaan määritellä tarkasti luettelossa mainitun, hyväksyttyjä varmenteita myöntävän varmennepalvelujen tarjoajan varmennepalvelun myöntämän hyväksytyn varmenteen erityistyyppi ja tarjota tietoa siitä, onko sen tukena turvallinen allekirjoituksen luomismenetelmä vai ei (mikäli tämä tieto puuttuu myönnetystä hyväksytystä varmenteesta). Tähän tietoon liittyy luonnollisesti erityinen ”Service current status” (”Scs”) -syöte. Tämä on kuvattu alla olevassa kaaviossa 2.

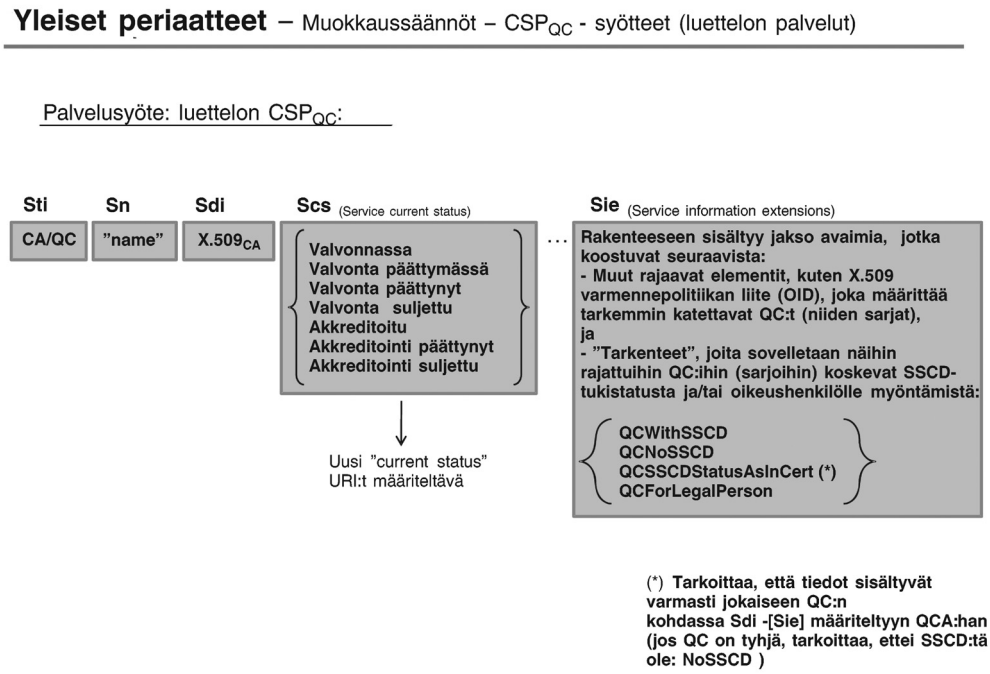
Jos luettelossa olevasta palvelusta ilmoitetaan ainoastaan (juuritason) varmentajan ”Sdi”-tieto, tämä merkitsee, että hyväksyttyjä varmenteita myöntävä varmennepalvelujen tarjoaja sekä tämän tarjoajan valvonnasta/akkreditoinnista vastaava valvonta-/akkreditointilaitos takaavat, että tämän (juuritason) varmentajan (hierarkian) puitteissa julkaistu loppukäyttäjän varmenne sisältää riittävästi ETSIn määrittelemää koneellisesti luettavaa tietoa sen arvioimiseksi, onko kyseessä hyväksytty varmenne ja onko se luotu varmalla luontimenetelmällä. Jollei esimerkiksi viimeinen väite pidä paikkaansa (eli hyväksytyssä varmenteessa ei ole ETSIn standardoimaa koneellisesti luettavaa tietoa siitä, onko varmenteen tukena käytetty turvallista allekirjoituksen luomismenetelmää), mainitsemalla luettelossa ainoastaan kyseisen (juuritason) varmentajan ”Sdi”-kenttä voidaan päätellä ainoastaan, ettei tämän (juuritason) varmentajan hierarkian puitteissa myönnettyjen hyväksyttyjen varmenteiden tukena ole mitään turvallista allekirjoituksen luomismenetelmää. Jotta hyväksyttyjen varmenteiden voidaan katsoa olevan turvallisen allekirjoituksen luomismenetelmän tukemia, asia on osoitettava ”Sie”-kentässä (samalla osoitetaan, että takaajana on hyväksyttyjä varmenteita myöntävä varmennepalvelujen tarjoaja ja valvojana/akkreditoijana valvonta- tai akkreditointilaitos).

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

([2]) ETSI TS 101 456 – Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.

([3]) Tämä tarkoittaa vähintäänkin myöntävän varmentajan tai varmennepolussa ylemmän varmentajan X.509 v3 varmennetta.

▼C2



Kaavio 2

Luetteloon sisältyvän hyväksyttyjä varmenteita myöntävän varmennepalvelujen tarjoajan palvelusyöte, kun luotettava luettelo on toteutettu TSL-muodossa

▼C1

Tässä luotettavan luettelon yhteisen mallin teknisissä eritelmissä voidaan käyttää viiden tietoalkion yhdistelmää kussakin palvelusyötteessä:

— ”Service type identifier” (”Sti”), jolla tunnistetaan esimerkiksi hyväksyttyjä varmenteita myöntävä varmentaja (”CA/QC”),

— ”Service name” (”Sn”),

— ”Service digital identity” (”Sdi”) -tieto, jolla tunnistetaan lueteltu palvelu, esimerkiksi (ainakin) hyväksyttyjä varmenteita myöntävän varmentajan X.509v3 -varmenne,

— CA/QC-palvelun osalta vapaaehtoinen ”Service information extensions” (”Sie”) -tieto mahdollistaa yhden tai useamman monikon sisällyttämisen, jolloin kussakin monikossa ilmoitetaan

  — kriteerit, joilla tunnistetaan tarkemmin (rajataan) ”Sdi”-kohdassa yksilöity varmennepalvelu, jossa tarkennetaan palvelu (eli hyväksyttyjen varmenteiden sarja), jolle edellytetään/tarjotaan lisätietoja turvallisen allekirjoituksen luomismenetelmän tukitietojen osoittamiseksi (ja/tai oikeushenkilölle myöntämisestä), ja

  — asiaan liittyvät tiedot (”määreet”) siitä, onko tämä edelleen yksilöity hyväksyttyjen varmenteiden palvelusarja tuettu turvallisella allekirjoituksen luomismenetelmällä vai ei, tai siitä, ovatko nämä asiaan liittyvät tiedot vakiomuotoisena koneellisesti luettavana osana hyväksyttyä varmennetta, ja/tai tiedot siitä, onko kyseiset hyväksytyt varmenteet myönnetty oikeushenkilöille (muussa tapauksessa niitä oletetaan myönnetyn ainoastaan luonnollisille henkilöille),

▼C1

— tämän palvelusyötteen ”nykyisen statuksen” tiedot

— siitä, onko se valvottu tai akkreditoitu palvelu, ja

— varsinaisesta valvonta-/akkreditointistatuksesta.

2.3 *Hyväksyttyjä varmenteita myöntävien varmennepalvelujen tarjoajien palvelumerkintöjen muokkaus- ja käyttöohjeet*

Yleiset muokkausohjeet ovat seuraavat:

1. Mikäli taataan (hyväksyttyjä varmenteita myöntävän ja valvontaelimen (SB) / akkreditointielimen (AB) valvoman/akkreditoiman varmennepalvelujen tarjoajan antama takuu), että ”Sdi”-tiedon perusteella yksilöidyn luettelossa mainitun palvelun kohdalla mikä tahansa turvallisen allekirjoituksen luomismenetelmän tukema hyväksytty varmenne sisältää ETSIn määrittelemän QcCompliance-kuvauksen sekä QcSSCD-kuvauksen ja/tai QCP + OID:n, asianmukaisen ”Sdi”-tiedon käyttö riittää, minkä lisäksi ”Sie”-tietoa voidaan käyttää valinnaisena eikä sen tarvitse sisältää SSCD-tukitietoa.

2. Mikäli taataan (hyväksyttyjä varmenteita myöntävän ja SB:n/AB:n valvoman/akkreditoiman varmennepalvelujen tarjoajan antama takuu), että ”Sdi”-tiedon perusteella yksilöidyn luettelossa mainitun palvelun kohdalla mikä tahansa varmenne, jonka tukena ei ole turvallista allekirjoituksen luomismenetelmää, sisältää joko QcCompliance-kuvauksen ja/tai QCP OID:n eikä sen tarkoituksena ole sisältää QcSSCD-kuvausta tai QCP + OID:tä, asianmukaisen ”Sdi”-tiedon käyttö riittää, minkä lisäksi ”Sie”-tietoa voidaan käyttää valinnaisena eikä sen tarvitse sisältää SSCD-tukitietoa (mikä tarkoittaa, ettei sillä ole SSCD-tukea).

3. Mikäli taataan (hyväksyttyjä varmenteita myöntävän ja SB:n/AB:n valvoman/akkreditoiman varmennepalvelujen tarjoajan antama takuu), että ”Sdi”-tiedon perusteella yksilöidyn luettelossa mainitun palvelun kohdalla mikä tahansa hyväksytty varmenne sisältää QcCompliance-kuvauksen ja että osa hyväksytyistä varmenteista on tarkoitettu SSCD:n tukemiksi ja osa ei (ero voidaan osoittaa esimerkiksi tarjoajakohtaisen varmennepolitiikan OID:n avulla tai hyväksytyssä varmenteessa olevan muun tarjoajakohtaisen tiedon avulla joko suoraan tai välillisesti, riippumatta siitä, onko tieto koneellisesti luettavaa vai ei) mutta hyväksytty varmenne EI sisällä QcSSCD-kuvausta EIKÄ ETSI QCP(+) OID:tä, asianmukaisen ”Sdi”-tiedon käyttö ei välttämättä ole riittävä vaan ”Sie”-kenttää on käytettävä osoittamaan nimenomaista SSCD-tukitietoa yhdessä mahdollisen tietoliitteen avulla, jolla yksilöidään kulloinkin tarkoitetut varmennesarjat. Tämä vaatii todennäköisesti erilaiset ”SSCD-tukitietoarvot” samalle ”Sdi”:lle, kun käytetään ”Sie”-kenttää.

4. Mikäli taataan (hyväksyttyjä varmenteita myöntävän ja SB:n/AB:n valvoman/akkreditoiman varmennepalvelujen tarjoajan antama takuu), että ”Sdi”-tiedon perusteella yksilöidyn luettelossa mainitun palvelun kohdalla mikään hyväksytty varmenne ei sisällä QcCompliance-kuvausta, QCP OID:tä, QcSSCD-kuvausta eikä QCP + OID:tä mutta taataan, että osan näistä kyseisen ”Sdi”-tiedon sisältävistä myönnetyistä loppukäyttäjän varmenteista on tarkoitus olla hyväksyttyjä varmenteita ja/tai SSCD:n tukemia varmenteita ja osan ei (ero voidaan osoittaa esimerkiksi tarjoajakohtaisen erityisen varmennepolitiikan OID:n avulla tai hyväksytyssä varmenteessa olevan muun tarjoajakohtaisen tiedon avulla joko suoraan tai välillisesti, riippumatta siitä, onko tieto koneellisesti luettavaa vai ei), asianmukaisen ”Sdi”-tiedon käyttö ei riitä VAAN ”Sie”-kenttää on käytettävä nimenomaisen SSCD-tukitiedon sisällyttämiseen. Tämä vaatii todennäköisesti erilaiset ”SSCD-tukitietoarvot” samalle ”Sdi”:lle, kun käytetään ”Sie”-kenttää.

▼C1

Yleisenä oletusperiaatteena on, että luotettavassa luettelossa listatulla varmennepalvelun tarjoajalla on oltava yksi palvelusyöte yhtä X.509v3-varmennetta kohden CA/QC-tyypin varmennepalvelulle eli palvelulle, jossa varmentaja myöntää hyväksyttyjä varmenteita (suoraan). Eräissä tarkoin harkituissa olosuhteissa ja huolellisesti hallinnoiduin ehdoin jäsenvaltion valvontalaitos/akkreditointilaitos voi päättää, että se käyttää juuritason tai ylemmän tason varmentajan X.509v3-varmennetta (eli varmentaja ei suoraan myönnä loppukäyttäjän hyväksyttyjä varmenteita vaan varmentaa varmentajahierarkian alaspäin niihin varmentajiin saakka, jotka myöntävät hyväksyttyjä varmenteita loppukäyttäjille) luetteloon sisältyvän varmennepalvelujen tarjoajan palveluluettelon yksittäisen syötteen ”Sdi”-kentässä. Jäsenvaltioiden on huolellisesti harkittava, mitä seurauksia (hyötyjä ja haittoja) tällaisen juuritason varmentajan tai ylemmän tason varmentajan X.509v3-varmenteen käytöstä luotettavan luettelon palvelukohtien ”Sdi”-arvoina voi aiheutua, ja hyväksyttävä ne. Käyttäessään tällaista sallittua poikkeusta oletusperiaatteeseen jäsenvaltion pitää lisäksi tarjota tarpeellinen dokumentaatio varmennepolun muodostamisen ja todentamisen helpottamiseksi.

Yleisten muokkausohjeiden havainnollistamiseksi voidaan antaa seuraava esimerkki: Jos hyväksyttyjä varmenteita myöntävä varmennepalvelujen tarjoaja käyttää yhtä juuritason varmentajista, ja sen alaisuudessa useat varmentajat myöntävät hyväksyttyjä varmenteita ja muita kuin hyväksyttyjä varmenteita, ja jos hyväksytyt varmenteet sisältävät ainoastaan QcCompliance-kuvauksen eivätkä tietoa siitä, onko tukena SSCD vai ei, juuritason varmentajan ”Sdi”-tiedon luetteleminen tarkoittaisi ainoastaan sitä, että edellä selvitettyjen sääntöjen mukaisesti mikään tämän juuritason varmentajan hierarkian nojalla myönnetty hyväksytty varmenne EI ole SSCD:n tukema. Mikäli näillä hyväksytyillä varmenteilla tosiasiassa on SSCD-tuki, olisi erittäin suositeltavaa käyttää QcSSCD-kuvausta vastaisuudessa myönnettävissä hyväksytyissä varmenteissa. Sitä ennen (siihen saakka, kun viimeinen tätä tietoa sisältämätön hyväksytty varmenne on lakannut olemasta voimassa) TSL:ssä olisi käytettävä ”Sie”-kenttää ja siihen liittyvää ”Qualifications”-liitettä eli varmenteiden rajaamista sellaisten CSPQC-kohtaisesti määriteltyjen OID-arvojen avulla, joita CSPQC mahdollisesti käyttää erityyppisten (SSCD-tuettujen ja muiden) hyväksyttyjen varmenteiden erottamiseen, ja nimenomaisen ”SSCD-tukitiedon” sisällyttämistä rajattuihin varmenteisiin käyttämällä ”Qualifiers”-kenttiä.

Näiden teknisten eritelmien mukaisen luotettavan luettelon TSL-toteutukseen perustuvien sähköisten allekirjoitusten sovellusten, palvelujen ja tuotteiden yleiset käyttöohjeet ovat seuraavat:

”CA/QC””Sti” -syöte (tai CA/QC-syöte, joka on edelleen luokiteltu ”RootCA/QC”-syötteeksi käyttämällä ”Sie”-kentässä additionalServiceInformation-liitettä)

— osoittaa, että alkaen ”Sdi”-yksilöidystä varmentajasta (vastaavasti varmentajahierarkiassa alkaen ”Sdi”-yksilöidystä juuritason varmentajasta) kaikki myönnetyt loppukäyttäjän varmenteet ovat hyväksyttyjä varmenteita, mikäli varmenteessa näin väitetään käyttäen asianmukaisia QcStatements-lausumia (esim. QcC, QcSSCD) ja/tai ETSIn määrittelemiä QCP(+) OID-tunnisteita (ja valvonta-/akkreditointilaitos takaa tämän, katso edellä olevat yleiset muokkausohjeet);

Huomio: jollei mukana ole ”Sie””Qualification” -tietoa tai jollei loppukäyttäjän varmenteessa, jonka väitetään olevan hyväksytty varmenne, ole ”lisätunnisteena” siihen liittyvää ”Sie”-syötettä, hyväksytyssä varmenteessa oleva ”koneellisesti luettava” tieto on valvottu/akkreditoitu oikeelliseksi. Tämä tarkoittaa, että ETSIn määrittelemien asianmukaisten QcStatements-lausumien (esim. QcC, QcSSCD) ja/tai ETSIn määrittelemien QCP(+) OID-tunnisteiden käytön (tai käyttämättömyyden) taataan olevan hyväksyttyjä varmenteita myöntävän varmennepalvelujen tarjoajan väittämien mukaista.

▼C1

— ja mikäli mukana on ”Sie””Qualification” -syöte, edellä olevan oletuskäytön tulkintasäännön lisäksi ne varmenteet, jotka tunnistetaan käyttämällä tätä ”Sie””Qualification” -kohtaa perustuen peräkkäisten ”rajausten” sarjaan, joilla tunnistetaan varmennesarja ja annetaan lisätietoa ”SSCD support” ja/tai ”Legal person as subject” tiedoista (eli varmenteet, joissa on erityinen OID varmennepolitiikkaa koskevassa liitteessä ja/tai joissa on erityinen ”avaimen käytön” periaate ja/tai jotka on rajattu käyttämällä erityistä arvoa, joka näkyy yhdessä varmenteen kentässä tai liitteessä tms.), on luokiteltava perustuen seuraavaan ”määresarjaan”, joka korvaa vastaavan hyväksytyn varmenteen tiedon puutteen, eli

— SSCD-tuen osoituksena:

  — määreen arvo ”QCWithSSCD” tarkoittaa ”SSCD:n tukemaa hyväksyttyä varmennetta”,

  — määreen arvo ”QCNoSSCD” tarkoittaa ”hyväksyttyä varmennetta, jolla ei ole SSCD-tukea”, tai

  — määreen arvo ”QCSSCDStatusAsInCert” tarkoittaa, että SSCD-tukitieto sisältyy taatusti jokaiseen hyväksyttyyn varmenteeseen kyseisen CA/QC-syötteen ”Sdi”–”Sie”-syötteen tietoihin;

ja/tai

— oikeushenkilölle myöntämisen osoituksena:

  — määreen arvo ”QCForLegalPerson” tarkoittaa ”oikeushenkilölle myönnettyä varmennetta”.

2.4 *Palvelut, jotka tukevat ”CA/QC”-palveluja mutta eivät ole osa ”CA/QC””Sdi”:tä*

Myös ne tapaukset, joissa CRL:t ja OSCP-vastaukset on allekirjoitettu muilla kuin hyväksyttyjä varmenteita myöntävien varmentajien (”CA/QC”) antamilla avaimilla, olisi katettava. Ne voidaan kattaa luettelemalla kyseiset palvelut sellaisenaan luotettavan luettelon TSL-toteutuksessa (esim. käyttäen ”Palvelutyypin tunnistetta”, jota tarkennetaan ”additionalServiceInformation”-liitteellä, joka osoittaa, että OSCP tai CRL-palvelu on osa hyväksyttyjen varmenteiden tarjontaa, esim. palvelutyypillä ”OCSP/QC” tai ”CRL/QC”), koska nämä palvelut voidaan katsoa osaksi valvottuja/akkreditoituja ”tarkennettuja” palveluja, jotka liittyvät QC-varmennepalvelujen tarjontaan. OCSP-vastausten antajat tai CRL:n myöntäjät, joiden varmenteiden allekirjoittajina ovat luetellun CA/QC-palvelun hierarkiaan kuuluvat varmentajat, on katsottava ”voimassa oleviksi” luetellun CA/QC-palvelun statusarvon mukaisesti.

Vastaavaa säännöstä voidaan soveltaa varmennepalveluihin, joissa myönnetään muita kuin hyväksyttyjä varmenteita (palvelutyyppiä ”CA/PKC”) käyttäen ETSIn teknisen spesifikaation TS 102 231 oletusarvoisia OSCP- ja CRL-palvelutyyppejä.

Huomattakoon, että luotettavan luettelon TSL-toteutuksen PITÄÄ sisältää sulkemispalvelut, mikäli siihen liittyvät tiedot eivät ole mukana loppukäyttäjän varmenteiden AIA-kentässä tai kun allekirjoittajana ei ole lueteltuihin varmentajiin kuuluva varmentaja.

2.5 *Kohti yhteentoimivaa QC-profiilia*

Yleissääntönä pitää yrittää yksinkertaistaa (vähentää) mahdollisimman pitkälle palvelujen syötteiden määrää (eri ”Sdi”-kenttiä). Toisaalta tilannetta on tasapainotettava siten, että hyväksyttyjen varmenteiden myöntämiseen ja luotettavan tiedon tarjontaan liittyvät palvelut tunnistetaan oikein sen mukaan, onko hyväksyttyjen varmenteiden tukena turvallinen allekirjoituksen luomismenetelmä, riippumatta siitä, puuttuuko tämä tieto myönnetystä hyväksytystä varmenteesta.

▼C1

Ihannetapauksessa ”Sie”-kentän ja ”Qualification”-liitteen käyttö olisi (ehdottomasti) rajoitettava niiden avulla ratkaistaviin erikoistapauksiin, sillä hyväksyttyjen varmenteiden pitäisi sisältää riittävästi tietoa niiden väitetystä hyväksytystä statuksesta ja mahdollisesti tukena olevasta väitetystä turvallisesta allekirjoituksen luomismenetelmästä.

Jäsenvaltioiden pitäisi valvoa mahdollisuuksien rajoissa yhteentoimivien QC-profiilien hyväksymistä ja käyttöä.

3. **Luotettavan luettelon yhteisen mallin rakenne**

Ehdotettu jäsenvaltion luotettavan luettelon yhteinen malli rakentuu seuraavien tietokategorioiden varaan:

1. tiedot luotettavasta luettelosta ja sen julkaisujärjestelmästä;

2. niiden kenttien jakso, jotka sisältävät yksiselitteistä tunnistetietoa jokaisesta järjestelmässä valvotusta/akkreditoidusta varmennepalvelun tarjoajasta (tämä jakso on vapaaehtoinen, mikä tarkoittaa sitä, että kun sitä ei käytetä, luettelo katsotaan tyhjäksi, jolloin kyseisessä jäsenvaltiossa ei ole valvottua tai akkreditoitua varmennepalvelun tarjoajaa luotettavan luettelon soveltamisalan puitteissa);

3. jokaisesta luettelossa mainitusta varmennepalvelujen tarjoajasta sellaisten kenttien jakso, joka sisältää varmennepalvelun tarjoajan tarjoaman valvotun/akkreditoidun varmennepalvelun yksiselitteiset tunnistetiedot (tässä jaksossa on oltava ainakin yksi syöte);

4. jokaisen luettelossa mainitun valvotun/akkreditoidun varmennepalvelun nykyisen statuksen tunniste ja statuksen historiatiedot.

Hyväksyttyjä varmenteita myöntävän varmennepalvelujen tarjoajan yhteydessä luetteloon otettavan valvotun/akkreditoidun palvelun yksiselitteisessä tunnistamisessa pitää ottaa huomioon tilanteet, joissa ei ole saatavana tarpeeksi tietoa hyväksytyn varmenteen hyväksytystä statuksesta eikä siitä, onko varmenteen tukena mahdollisesti SSCD, erityisesti tarkoituksena selviytyä siitä tosiasiasta, että useimmat (kaupalliset) varmennepalvelujen tarjoajat käyttävät yhtä ainoaa hyväksyttyä myöntävää varmentajaa monenlaisten – sekä hyväksyttyjen että muunlaisten – loppukäyttäjän varmenteiden myöntämiseen.

Kunkin tunnustetun varmennepalvelujen tarjoajan syötteiden määrää luettelossa voidaan rajoittaa, jos olemassa on yksi tai useampi ylemmän tason varmentajien palvelu esimerkiksi juuritason varmentajasta varmenteita myöntäviin varmentajiin ulottuvassa kaupallisessa hierarkiassa. Näissäkin tapauksissa on säilytettävä ja varmistettava yksiselitteisen riippuvuuden periaate CSP_{QC}-varmennepalvelun ja hyväksytyiksi varmenteiksi tunnistettaviksi tarkoitettujen varmennesarjojen välillä.

1. *Tiedot luotettavasta luettelosta ja sen julkaisujärjestelmästä*

Tähän kategoriaan kuuluvat seuraavat tiedot:

— luotettavan luettelon tunniste, joka helpottaa luotettavan luettelon tunnistamista sähköisissä hauissa ja vahvistaa sen käyttötarkoituksen silloin, kun luettelo on ihmisen luettavissa olevassa muodossa,

— luotettavan luettelon muoto ja muotoversion tunniste,

— luotettavan luettelon järjestysnumero (tai julkaisunumero),

— luotettavan luettelon tyyppitieto (sen tunnistamiseksi, että kyseisessä luotettavassa luettelossa annetaan tietoa ilmoitetun jäsenvaltion valvomien/akkreditoimien varmennepalvelujen tarjoajien varmennepalvelujen valvonta-/akkreditointistatuksesta suhteessa siihen, että direktiivin 1999/93/EY säännökset täyttyvät),

▼C1

— luotettavan luettelon omistajatiedot (eli luotettavan luettelon laadinnasta, turvallisesta julkaisusta ja ylläpidosta vastuussa olevan jäsenvaltion elimen nimi, osoite, yhteystiedot jne.),

— tiedot käytetystä valvonta-/akkreditointijärjestelmästä tai -järjestelmistä, joihin luotettava luettelo liittyy, mukaan lukien seuraavat seikat, niihin kuitenkaan rajoittumatta:

  — maa, jossa järjestelmää sovelletaan,

  — tiedot paikasta tai viittaus paikkaan, jossa järjestelmää/järjestelmiä koskevat tiedot sijaitsevat (järjestelmän malli, säännöt, kriteerit, sovellettava yhteisö, tyyppi jne.),

  — (historia)tietojen säilytysaika,

— luotettavan luettelon politiikka ja/tai oikeudellinen huomautus, velvoitteet ja vastuukysymykset,

— luotettavan luettelon julkaisupäivä ja -aika ja seuraava suunniteltu päivitys.

2. *Yksiselitteiset tunnistustiedot jokaisesta järjestelmässä tunnustetusta varmennepalvelujen tarjoajasta*

Tähän tietosarjaan kuuluvat ainakin seuraavat tiedot:

— CSP-organisaation nimi sellaisena kuin se esiintyy virallisissa oikeudellisissa kirjauksissa (tähän voi sisältyä CSP-orgnisaation UID jäsenvaltion käytänteiden mukaisesti),

— CSP:n osoite- ja yhteystiedot,

— lisätiedot CSP:stä joko suoraan sisällytettyinä tai viitteenä kohteeseen, josta nämä tiedot voidaan ladata.

3. *Jokaisesta luettelossa mainitusta varmennepalvelujen tarjoajasta sellaisten kenttien jakso, joka sisältää varmennepalvelun tarjoajan tarjoaman, direktiivin 1999/93/EY puitteissa valvotun/akkreditoidun varmennepalvelun yksiselitteiset tunnistetiedot*

Tähän tietosarjaan sisältyvät ainakin seuraavat tiedot jokaisesta luettelossa mainitun CSP:n varmennepalvelusta:

— varmennepalvelun tyypin tunniste (esim. tunniste, joka osoittaa, että CSP:n tarjoama valvottu/akkreditoitu varmennepalvelu on hyväksyttyjä varmenteita myöntävä varmentaja),

— varmennepalvelun (kauppa)nimi,

— varmennepalvelun yksiselitteinen ainutkertainen tunniste,

— lisätiedot varmennepalvelusta (joko suoraan sisällytettynä tai sisällytettynä viitteenä kohteeseen, josta nämä tiedot voidaan ladata, kyseisen palvelun käyttötiedot),

— CA/QC-palvelujen osalta vapaaehtoinen tietomonikkojen jakso, jolloin kussakin monikossa ilmoitetaan

  i) kriteerit, joilla tunnistetaan tarkemmin (rajataan) ”Sdi”-kohdassa yksilöity varmennepalvelu, jossa tarkennetaan palvelu (eli hyväksyttyjen varmenteiden sarja), jolle edellytetään/tarjotaan lisätietoja turvallisen allekirjoituksen luomismenetelmän tukitietojen osoittamiseksi (ja/tai oikeushenkilölle myöntämisestä), ja

  ii) asiaan liittyvät ”määreet”, jotka antavat tietoa siitä, onko tämä edelleen yksilöity hyväksyttyjen varmenteiden sarja tuettu SSCD:llä vai ei, ja/tai siitä, onko nämä QC:t myönnetty oikeushenkilölle (muussa tapauksessa niitä oletetaan myönnetyn ainoastaan luonnollisille henkilöille).

▼C1

4. *Jokaisen luettelossa mainitun varmennepalvelun nykyisen statuksen tunniste ja statuksen historiatiedot*

Tähän tietosarjaan kuuluvat ainakin seuraavat tiedot:

— nykyisen statuksen tunniste,

— nykyisen statuksen alkamis- ja päättymispäivä ja -aika,

— statuksen historiatiedot.

4. **Määritelmät ja lyhenteet**

Tässä asiakirjassa tarkoitetaan alla mainituilla määritelmillä ja lyhenteillä seuraavaa:

Käsite	Lyhenne	Määritelmä
Varmennepalvelun tarjoaja	CSP	Määritelmä direktiivin 1999/93/EY 2 artiklan 11 kohdassa.
Varmentaja	CA	Varmentaja on varmennepalvelujen tarjoaja, ja se voi käyttää loppukäyttäjän varmenteita myöntäessään useita varmentajien teknisiä yksityisiä allekirjoitusavaimia, joista kussakin on oma, siihen liittyvä varmenne. Varmentaja on asiantuntija, jonka yksi tai useampi käyttäjä on valinnut luomaan ja nimeämään varmenteita. Valinnaisesti varmentaja voi luoda käyttäjien avaimet [ETSIn tekninen spesifikaatio 102 042]. Varmentaja katsotaan tunnistetuksi tunnistetiedosta, joka on myöntäjäkentässä varmentajan varmenteessa, joka liittyy varmentajan yksityiseen allekirjoitusavaimeen liittyvään julkiseen avaimeen (sen varmentamiseen) ja jota varmentaja tosiasiassa käyttää yksittäisten varmenteiden myöntämiseen. Varmentajalla voi olla useita allekirjoitusavaimia. Jokainen varmentajan allekirjoitusavain tunnistetaan ainutkertaisesti ainutkertaisella tunnisteella, joka on osa varmentajan varmenteen varmentaja-avaimen tunnistekenttää.
Hyväksyttyjä varmenteita myöntävä varmentaja	CA/QC	Varmentaja, joka täyttää direktiivin 1999/93/EY liitteessä II säädetyt vaatimukset ja myöntää direktiivin 1999/93/EY liitteessä I säädetyt vaatimukset täyttäviä hyväksyttyjä varmenteita.
Varmenne	Varmenne	Määritelmä direktiivin 1999/93/EY 2 artiklan 9 kohdassa
Hyväksytty varmenne	QC	Määritelmä direktiivin 1999/93/EY 2 artiklan 10 kohdassa.
Allekirjoittaja	Allekirjoittaja	Määritelmä direktiivin 1999/93/EY 2 artiklan 3 kohdassa.
Valvonta	Valvonta	”Valvontaa” käytetään direktiivissä 1999/93/EY tarkoitetussa merkityksessä (3 artiklan 3 kohta). Direktiivissä edellytetään, että jäsenvaltiot ottavat käyttöön asianmukaisen järjestelmän, jonka avulla voidaan valvoa sen alueelle asettautuneita, hyväksyttyjä varmenteita yleisölle myöntäviä varmennepalvelujen tarjoajia ja varmistaa direktiivin säännösten noudattamisen valvonta.
Vapaaehtoisuuteen perustuva akkreditointi	Akkreditointi	Määritelmä direktiivin 1999/93/EY 2 artiklan 13 kohdassa.
Luotettava luettelo	TL	Tarkoittaa luetteloa, jossa luetellaan niiden varmennepalvelujen tarjoajien varmennepalvelujen valvonta-/akkreditointistatus, joita mainittu jäsenvaltio valvoo / on akkreditoinut, jotta direktiivin 1999/93/EY säännöksiä noudatetaan.

▼C1

Käsite	Lyhenne	Määritelmä
Luottamuspalvelujen statusluettelo	TSL	Eräänlainen allekirjoitettu luettelo, jota käytetään pohjana luottamuspalvelujen statustietojen esittämiseksi ETSIn teknisessä spesifikaatiossa 102 231 määriteltyjen eritelmien mukaisesti.
Luottamuspalvelu		Palvelu, jolla lisätään luottamusta sähköisiin toimiin (tyypillisesti muttei välttämättä salaustekniikoita käyttämällä tai luottamukselliseen aineistoon liittyvänä) (ETSIn tekninen spesifikaatio 102 231)
Luottamuspalvelujen tarjoaja	TSP	Yhtä tai useampaa (sähköistä) luottamuspalvelua harjoittava laitos (käsitteen soveltamisala on laajempi kuin CSP:n).
Luottamuspalvelun sanake	TrST	Fyysinen tai binaarinen (looginen) kohde, joka on luotu tai myönnetty luottamuspalvelun käytön tuloksena. Esimerkkejä TrST:istä ovat varmenteet, CRL:t, aikaleimasanakkeet ja OSCP-vastaukset.
Hyväksytty sähköinen allekirjoitus	QES	Hyväksytyn varmenteen (QC) tukema kehittynyt sähköinen allekirjoitus (AdES), joka on luotu direktiivin 1999/93/EY 2 artiklassa määritellyllä turvallisella allekirjoituksen luomismenetelmällä.
Kehittynyt sähköinen allekirjoitus	AdES	Määritelmä direktiivin 1999/93/EY 2 artiklan 2 kohdassa.
Hyväksytyn varmenteen tukema kehittynyt sähköinen allekirjoitus	$AdES_{QC}$	Tarkoittaa kehittyneelle sähköiselle allekirjoitukselle (AdES) asetettavat vaatimukset täyttävää sähköistä allekirjoitusta, jonka tukena on direktiivin 1999/93/EY 2 artiklassa määritelty hyväksytty varmenne.
Turvallinen allekirjoituksen luomismenetelmä	SSCD	Määritelmä direktiivin 1999/93/EY 2 artiklan 6 kohdassa.

I LUKU

”VALVOTTUJEN/AKKREDITOITUJEN VARMENNEPALVELUJEN TARJOAJIEN LUOTETTAVAN LUETTELON” YHTEISEN MALLIN YKSITYISKOHTAISET ERITELMÄT

Asiakirjan seuraavassa osassa käytetään keskeisiä termejä PITÄÄ (MUST, SHALL), EI SAA (MUST NOT, SHALL NOT) ja PAKOLLINEN (REQUIRED), PITÄISI (SHOULD), EI PITÄISI (SHOULD NOT), SUOSITELTAVA (RECOMMENDED), SAA (MAY) ja VAPAAEHTOINEN (OPTIONAL) IETF:n (Internet Engineering Task Force) määrittämissä merkityksissä (RFC 2119) ([1]).

►**M1** Nämä eritelmät perustuvat ETSIn teknisessä spesifikaatiossa 102231 v.3.1.2 mainittuihin eritelmiin ja vaatimuksiin. Jollei näissä eritelmissä ole mainittu erityistä vaatimusta, PITÄÄ soveltaa sellaisenaan ETSIn teknisen spesifikaation 102231 v.3.1.2 vaatimuksia. ◄ Kun näissä teknisissä eritelmissä on mainittu erityisiä vaatimuksia, niitä PITÄÄ soveltaa ennen vastaavia ETSIn teknisen spesifikaation 102 231 vaatimuksia ja samalla täydentää niitä ETSIn teknisessä spesifikaatiossa 102 231 määritellyillä muotoeritelmillä. Mikäli näissä eritelmissä ja ETSIn teknisestä spesifikaatiosta 102 231 peräisin olevissa eritelmissä on eroja, tämän asiakirjan eritelmät PITÄÄ katsoa normatiivisiksi.

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

▼C1

Kielitukea PITÄÄ antaa ja tarjota ainakin englanniksi (EN) ja mahdollisesti vielä yhdellä tai useammalla kansallisella kielellä.

Päiväys ja aika PITÄÄ ilmoittaa ETSIn teknisen spesifikaation 102 231 lausekkeen 5.1.4 mukaisesti.

URI-tunnisteita PITÄÄ käyttää ETSIn teknisen spesifikaation 102 231 lausekkeen 5.1.5 mukaisesti.

Tiedot luotettavan luettelon julkaisujärjestelmästä

Tag

TSL tag (lauseke 5.2.1)

Tämä kenttä on PAKOLLINEN, ja sen PITÄÄ olla ETSIn teknisen spesifikaation 102 231 lausekkeen 5.2.1 mukainen.

▼M1

———————

▼C1

Scheme Information

TSL version identifier (lauseke 5.3.1)

Tämä kenttä on PAKOLLINEN, ja sen PITÄÄ olla kokonaisluku ”3”.

TSL sequence number (lauseke 5.3.2)

▼M1

Tämä kenttä on PAKOLLINEN. Siinä PITÄÄ määritellä TSL:n järjestysnumero. Kokonaislukuarvo on TSL:n ensimmäisen julkaisun yhteydessä 1, ja sitä PITÄÄ kasvattaa jokaisen seuraavan TSL:n julkaisun yhteydessä. Sitä EI SAA palauttaa ykköseksi, kun edellä mainittua ”TSL version identifier” -kenttää kasvatetaan.

▼C1

TSL type (lauseke 5.3.3)

▼M1

Tämä on PAKOLLINEN TSL:n tyypin määrittävä kenttä. Sen PITÄÄ olla http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Generic).

▼C1

Huomautus Täyttääkseen ETSIn teknisen spesifikaation 102 231 lausekkeen 5.3.3 ja osoittaakseen TSL:n erityistä tyyppiä viitatessaan näihin jäsenvaltioiden luotettavan luettelon ([1]) TSL-toteutuksen käyttöönottoa sääntéleviin eritelmiin ja antaessaan jäsentäjälle mahdollisuuden päätellä, minkä muotoisia seuraavat kentät ([2]) todennäköisesti ovat, sikäli kuin kentillä on erityisiä (tai vaihtoehtoisia) merkityksiä kuvatun TSL:n tyypin (tässä tapauksessa jäsenvaltion luotettava luettelo) mukaan, edellä mainittu erityinen URI PITÄÄ rekisteröidä ja kuvata seuraavasti:

([1]) Viittaa luetteloon, jossa luetellaan ”niiden varmennepalvelujen tarjoajien varmennepalvelujen valvonta-/akkreditointistatus, joita mainittu jäsenvaltio valvoo / jotka se on akkreditoinut direktiivin 1999/93/EY säännösten noudattamisen osalta” (lyhennettynä ”luotettava luettelo”).

([2]) Tarkoittaa ETSIn teknisessä spesifikaatiossa 102 231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information määriteltyjä kenttiä, jotka on profiloitu näissä eritelmissä siten, että niissä luodaan jäsenvaltioiden luotettava luettelo.

▼M1

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

▼C1

Kuvaus: Niiden varmennepalvelujen tarjoajien, joita TSL-toteutuksen omistava mainittu jäsenvaltio valvoo tai jotka se on akkreditoinut sähköisiä allekirjoituksia koskevista yhteisön puitteista direktiivin 1999/93/EY asiaa koskevien säännösten noudattamisen osalta suoran (vapaaehtoisen tai lakisääteisen) valvontaprosessin avulla, tarjoamien varmennepalvelujen valvonta-/akkreditointistatusluettelon TSL-toteutus.

Scheme operator name (lauseke 5.3.4)

Tämä kenttä on PAKOLLINEN. Siinä PITÄÄ määritellä sen jäsenvaltion laitoksen nimi, joka on vastuussa kansallisen luotettavan luettelon laadinnasta, julkaisusta ja ylläpitämisestä. Siinä PITÄÄ määritellä virallinen nimi, jolla kyseiseen laitoksiin liittyvä oikeushenkilö tai (esim. valtionhallinnon viraston osalta) valtuutettu henkilö toimii. Sen PITÄÄ olla virallisessa lakisääteisessä rekisteröinnissä tai luvassa käytetty nimi, jolle kaikki virallinen viestintä pitäisi osoittaa. Sen PITÄÄ olla monikielisten merkkijonojen jakso, ja se PITÄÄ toteuttaa käyttäen englannin kieltä (EN) pakollisena kielenä ja mahdollisesti yhtä tai useampaa kansallista kieltä.

Huomautus: Yksittäisellä maalla SAA olla erilliset valvonta- ja akkreditointilaitokset ja kansalliset laitokset mitä tahansa toimintaan liittyviä toimintoja varten. ►M1 Jokainen jäsenvaltio voi nimetä jäsenvaltion TL:n TSL-toteutuksen Scheme operatorin. ◄ Valvontaelimellä, akkreditointielimellä ja järjestelmäoperaattorilla (jotka toimivat erillisinä laitoksina) on jokaisella omat vastuut ja velvoitteet.

Tilanteen, jossa useampi laitos on vastuussa valvonnasta, akkreditoinnista tai toiminnallisista seikoista, PITÄÄ ilmetä johdonmukaisesti ja olla tunnistettavissa TL:n osana olevista järjestelmätiedoista (Scheme information), mukaan lukien järjestelmäkohtaiset tiedot, jotka ilmoitetaan kentässä ”Scheme information URI” (lauseke 5.3.7).

▼M1

Nimetty Scheme Operator (lauseke 5.3.4) on laitos, joka allekirjoittaa TSL:n.

▼C1

Scheme operator address (lauseke 5.3.5)

Tämä kenttä on PAKOLLINEN. Siinä PITÄÄ määritellä kentässä ”Scheme operator name” (lauseke 5.3.4) yksilöidyn oikeushenkilön tai valtuutetun organisaation osoite niin postilähetyksiä kuin sähköistä viestintääkin varten. Siinä PITÄÄ olla sekä ”PostalAddress” (eli lähiosoite, postitoimipaikka, [osavaltio tai maakunta], [postinumero] ja standardin ISO 3166-1 mukainen kaksimerkkinen maakoodi) lausekkeen 5.3.5.1 mukaisesti että ”ElectronicAddress” (eli sähköpostiosoite ja/tai verkkosivuston URI) lausekkeen 5.3.5.2 mukaisesti.

Scheme name (lauseke 5.3.6)

Tämä kenttä on PAKOLLINEN, ja siinä määritetään nimi, jolla järjestelmä toimii. Sen PITÄÄ olla monikielisten merkkijonojen jakso (pakollisena kielenä EN ja mahdollisesti yksi tai useampi kansallinen kieli) seuraavasti:

▼C1

— EN-toisinnon PITÄÄ olla seuraavasti jäsentyvä merkkijono:

CC:EN_name_value

jossa

— ”CC”	on kentässä ”Scheme territory” (lauseke 5.3.10) käytetty standardin ISO 3166-1 kaksimerkkinen maakoodi,
— ”:”	toimii erottimena,

▼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

— Mahdollisen jäsenvaltion kansallisen kielitoisinnon PITÄÄ olla seuraavasti jäsentyvä merkkijono:

CC:name_value

jossa

— ”CC”	on kentässä ”Scheme territory” (lauseke 5.3.10) käytetty standardin ISO 3166-1 kaksimerkkinen maakoodi,
— ”:”	toimii erottimena,
— ”name_value”	on edellä mainitun ”EN_name_value” kentän virallinen käännös kansalliselle kielelle.

Järjestelmän nimen tulee tunnistaa yksiselitteisesti nimeltä järjestelmä, johon kenttä ”Scheme information URI” viittaa, ja varmistaa, että yhden järjestelmäoperaattorin ylläpitäessä useampaa kuin yhtä järjestelmää jokaiselle järjestelmälle on annettu erottuva nimi.

Jäsenvaltioiden ja järjestelmäoperaattorien PITÄÄ varmistaa, että kun jäsenvaltiossa tai järjestelmäoperaattorilla on käytössä useampi kuin yksi järjestelmä, jokaiselle järjestelmälle on annettu erottuva nimi.

Scheme information URI (lauseke 5.3.7)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä URI(:t), jo(i)sta käyttäjät (varmenteeseen luottavat osapuolet) voivat saada järjestelmäkohtaista tietoa (pakollisena kielenä EN ja mahdollisesti yksi tai useampi kansallinen kieli). Sen PITÄÄ olla monikielisten osoittimien jakso (pakollisena kielenä EN ja mahdollisesti yksi tai useampi kansallinen kieli). Mainitun/mainittujen URI:(e)n PITÄÄ sisältää polku tietoon, jossa kuvataan ”asianmukaiset tiedot järjestelmästä”.

”Asianmukaisiin tietoihin järjestelmästä” PITÄÄ sisällyttää ainakin seuraavat:

— Yleiset johdantotiedot, jotka olisivat kaikille jäsenvaltioille yhteisiä ja koskisivat luotettavan luettelon soveltamisalaa ja käyttöyhteyttä sekä sen laadintaan vaikuttaneita valvonta-/akkreditointijärjestelmiä. Käytettävä yhteinen teksti on seuraavanlainen:

▼C1

”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.”

— Erityiset tiedot käytetyistä valvonta-/akkreditointijärjestelmistä, erityisesti seuraavat ([1]):

— tiedot hyväksyttyjä varmenteita myöntäviin varmennepalvelujen tarjoajiin (CSP_{QC}) sovellettavasta valvontajärjestelmästä,

([1]) Kahdessa viimeisessä kohdassa mainitut tiedot ovat ratkaisevan tärkeitä, kun listaa käyttävät osapuolet arvioivat valvonta-/akkreditointijärjestelmien laatua ja turvallisuustasoa. Nämä tietosarjat tarjotaan luettelokohtaisesti käyttämällä tämän asiakirjan kenttiä ”Scheme information URI” (lauseke 5.3.7 – jäsenvaltioiden tarjoamat tiedot), ”Scheme type/community/rules” (lauseke 5.3.9 – käyttämällä kaikille jäsenvaltioille yhteistä tekstiä) ja ”TSL policy/legal notice” (lause 5.3.11 – kaikille jäsenvaltioille yhteinen direktiiviin 1999/93/EY viittaava teksti ja kunkin jäsenvaltion mahdollisuus lisätä jäsenvaltiokohtaisia tekstejä/viitteitä). Varmennepalvelujen tarjoajia, jotka eivät myönnä hyväksyttyjä varmenteita, koskevista kansallisista valvonta-/akkreditointijärjestelmistä voidaan antaa palvelutasokohtaista tietoa tarvittaessa ja silloin, kun se on pakollista (esimerkiksi eri laatu-/palvelutasojen erottamiseksi toisistaan) (lauseke 5.5.6).

▼C1

— tiedot hyväksyttyjä varmenteita myöntäviin varmennepalvelujen tarjoajiin (CSP_{QC}) sovellettavasta kansallisesta ”vapaaehtoisuuteen perustuvasta akkreditointijärjestelmästä”, mikäli sellainen on,

— tiedot sellaisiin varmennepalvelujen tarjoajiin, jotka eivät myönnä hyväksyttyjä varmenteita, sovellettavasta valvontajärjestelmästä, mikäli sellainen on,

— tiedot niihin varmennepalvelujen tarjoajiin, jotka eivät myönnä hyväksyttyjä varmenteita (QC), sovellettavasta kansallisesta ”vapaaehtoisuuteen perustuvasta akkreditointijärjestelmästä”, mikäli sellainen on.

— Edellä mainittujen tietojen PITÄÄ sisältää jokaisesta edellä luetellusta järjestelmästä ainakin seuraavat tiedot:

— yleiskuvaus,

— tiedot prosessista, jota valvonta-/akkreditointilaitos noudattaa valvoessaan/akkreditoidessaan varmennepalvelujen tarjoajia ja joita valvotut/akkreditoidut varmennepalvelujen tarjoajat noudattavat,

— tiedot kriteereistä, joiden perusteella varmennepalvelujen tarjoajia valvotaan/akkreditoidaan.

— Mahdolliset erityiset tiedot joillekin varmennepalvelun tarjonnan tuloksena luoduille tai myönnetyille fyysisille tai binaarisille (loogisille) kohteille annetuista erityisistä ”kelpuutuksista”, jotka on myönnetty sillä perusteella, että tarjoajat täyttävät kansallisella tasolla annetut säännökset ja vaatimukset, samoin kuin tiedot tällaisen ”kelpuutuksen” ja siihen liittyvien kansallisten säädösten ja vaatimusten merkityksestä.

Muita jäsenvaltiokohtaisia erityisiä tietoja järjestelmästä SAA lisäksi tarjota vapaaehtoisuuteen perustuvana. Niiden PITÄÄ sisältää seuraavat:

— tiedot kriteereistä ja säännöistä, joilla valvojat/auditoijat valikoidaan ja määritellään, millä tavoin valvojat/auditoijat valvovat (tarkastavat) / akkreditoivat (auditoivat) varmennepalvelujen tarjoajia (CSP),

— muut yhteys- ja yleistiedot järjestelmän toiminnasta.

Status determination approach (lauseke 5.3.8)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä statuksen määrityksessä käytetyn lähestymistavan tunniste. Seuraavaa erityistä URI:tä PITÄÄ käyttää ja se PITÄÄ rekisteröidä ja kuvata seuraavasti:

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

Kuvaus: Luettelossa olevien palvelujen statuksen on määrittänyt järjestelmäoperaattori tai se on määritetty järjestelmäoperaattorin puolesta kyseisen jäsenvaltion asianmukaisessa järjestelmässä, joka mahdollistaa sen alueelle sijoittautuneiden (tai ”vapaaehtoisuuteen perustuvan akkreditoinnin” yhteydessä, mikäli sellainen on käytössä, kolmanteen maahan sijoittautuneiden), direktiivin 1999/93/EY 3 artiklan 3 kohdan (tai 3 artiklan 2 kohdan tai 7 artiklan 1 kohdan a alakohdan) mukaisesti hyväksyttyjä varmenteita yleisölle myöntävien varmennepalvelujen tarjoajien ”valvonnan” (ja ”vapaaehtoisuuteen perustuvan akkreditoinnin”), sekä tarvittaessa sellaisten varmennepalvelujen tarjoajien, jotka eivät myönnä hyväksyttyjä varmenteita, ”valvonnan” / ”vapaaehtoisuuteen perustuvan akkreditoinnin” kansallisesti määriteltyjen ja käyttöön otettujen ”tunnustettujen hyväksymisjärjestelmien” mukaisesti, jotka on toteutettu kansallisesti sen valvomiseksi, että varmennepalvelujen tarjoajien, jotka eivät myönnä hyväksyttyjä varmenteita, suorittamat palvelut ovat direktiivin 1999/93/EY säännösten ja niiden täydennykseksi mahdollisesti kansallisesti voimaan saatettujen, kyseisten varmennepalvelujen tarjontaa koskevien säännösten mukaisia.

▼C1

Scheme type/community/rules (lauseke 5.3.9)

Tämä kenttä on PAKOLLINEN, ja sen PITÄÄ sisältää ainakin seuraavat rekisteröidyt URI:t:

— Kaikkien jäsenvaltioiden luotettavien luetteloiden yhteinen URI viittaa kuvaustekstiin, jota PITÄÄ soveltaa kaikkiin luotettaviin luetteloihin:

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

— Sen avulla jäsenvaltion järjestelmän (joka yksilöidään kentissä ”TSL type” (lauseke 5.3.3) ja ”Scheme name” (lauseke 5.3.6)) ilmoitetaan kuuluvan järjestelmien järjestelmään (eli TSL-listausosoittimet kaikkiin niihin jäsenvaltioihin, jotka julkaisevat ja ylläpitävät luotettavaa luetteloa TSL-muodossa).

— Tästä URI:stä voidaan saada selville politiikka/säännöt, jonka/joiden suhteen luetteloon sisällytettyjä palveluja PITÄÄ arvioida ja määritellä TSL:n tyyppi (ks. lauseke 5.3.3).

— Tästä URI:stä käyttäjät voivat saada kuvauksen siitä, miten luotettavan luettelon TSL-toteutuksen sisältöä käytetään ja tulkitaan. Näiden käyttösääntöjen PITÄÄ olla yhteiset kaikkien jäsenvaltioiden luotettaville luetteloille riippumatta luettelon palvelun tyypistä ja käytössä olevista valvonta-/akkreditointijärjestelmistä.

Kuvausteksti:

”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.

▼C1

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)

▼C1

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

— Kunkin jäsenvaltion luotettavan luettelon erityinen URI viittaa kuvaustekstiin, jota PITÄÄ soveltaa kyseisen jäsenvaltion luotettavaan luetteloon:

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

jossa CC on ”Scheme territory” -kentässä (lauseke 5.3.10) käytetty standardin ISO 3166-1 kaksimerkkinen maakoodi.

— Tästä URI:stä käyttäjät voivat saada selville kyseisen jäsenvaltion erityisen politiikan/säännöt, jonka/joiden suhteen luetteloon sisällytettyjä palveluja PITÄÄ arvioida jäsenvaltion asianmukaisen valvontajärjestelmän ja vapaaehtoisuuteen perustuvien akkreditointijärjestelmien mukaisesti.

— Tästä URI:stä käyttäjät voivat saada selville kyseisen jäsenvaltion erityisen kuvauksen siitä, miten luotettavan luettelon TSL-toteutuksen sisältöä käytetään ja tulkitaan suhteessa varmennepalveluihin, jotka eivät liity hyväksyttyjen varmenteiden myöntämiseen. Sitä voidaan käyttää osoittamaan varmennepalvelujen tarjoajiin, jotka eivät myönnä hyväksyttyjä varmenteita, liittyvissä kansallisissa valvonta-/akkreditointijärjestelmissä mahdollisesti esiintyvää tarkkuusastetta ja sitä, miten kenttiä ”Scheme service definition URI” (lauseke 5.5.6) ja ”Service information extension” käytetään tähän tarkoitukseen.

Jäsenvaltio SAA määritellä muita URI-tunnisteita yllä mainitusta jäsenvaltiokohtaisesta URI:stä alkaen (eli hierarkiakohtaisesta URI:stä lähtien määriteltyjä URI-tunnisteita).

Scheme territory (lauseke 5.3.10)

Näissä eritelmissä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä maa, jossa järjestelmä on käytössä (standardin ISO 3166-1 kaksimerkkinen maakoodi).

TSL policy/legal notice (lauseke 5.3.11)

Näissä eritelmissä tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä järjestelmän politiikka tai antaa ilmoitus järjestelmän oikeudellisesta asemasta tai järjestelmän täyttämistä lakisääteisistä vaatimuksista sillä oikeudenkäyttöalueella, jossa järjestelmä on käytössä, ja/tai mahdolliset rajoitukset ja ehdot, joiden vallitessa luotettavaa luetteloa ylläpidetään ja julkaistaan.

Kentän PITÄÄ olla monikielinen merkkijono (selväkielitekstiä), joka koostuu kahdesta osasta:

— Ensimmäisessä pakollisessa ja kaikkien jäsenvaltioiden luotettaville luetteloille yhteisessä osassa (jonka pakollinen kieli on EN, mahdollisesti yksi tai useampi kansallinen kieli) osoitetaan, että sovellettava oikeusperusta on direktiivi 1999/93/EY ja sitä vastaavat ”Scheme Territory” -kentässä mainitun jäsenvaltion täytäntöönpanolait.

Yhteisen tekstin englanninkielinen toisinto:

”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.”

▼C1

Teksti jäsenvaltion kansallisella kielellä/kielillä: [yllä olevan englanninkielisen tekstin virallinen käännös/käännökset].

— Toinen vapaaehtoinen osa, joka on luettelokohtainen (pakollisena kielenä EN, mahdollisesti yksi tai useampi muu kansallinen kieli) ja jossa ilmoitetaan viitteet erityisesti sovellettaviin kansallisiin oikeusperustoihin (erityisesti muun muassa varmennepalvelujen tarjoajille, jotka eivät myönnä hyväksyttyjä varmenteita, tarkoitettujen kansallisten valvonta-/akkreditointijärjestelmien yhteydessä).

Historical information period (lauseke 5.3.12)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä kesto (kokonaisluku), jolta ajalta TSL:ssä ilmoitetaan historiatiedot. Kokonaisarvo on ilmoitettava päivinä, ja näiden eritelmien yhteydessä sen PITÄÄ olla suurempi tai yhtä suuri kuin 3 653 (mikä tarkoittaa, että jäsenvaltioiden luotettavan luettelon TSL-toteutuksen PITÄÄ sisältää historiatiedot vähintään kymmenen vuoden ajalta). Tätä suuremmissa arvoissa on otettava asianmukaisesti huomioon ”Scheme Territory” -kentässä (lauseke 5.3.10) mainitussa jäsenvaltiossa voimassa olevat tietojen säilytystä koskevat lakisääteiset vaatimukset.

Pointers to other TSLs (lauseke 5.3.13)

Näissä eritelmissä tämä kenttä on PAKOLLINEN, ja sen PITÄÄ sisältää osoitin ETSIn teknisen spesifikaation 102 231 mukaisessa muodossa olevaan EY:n yhdistettyyn linkkiluetteloon (osoitinluetteloon), joka viittaa kaikkiin jäsenvaltioiden luotettavien luetteloiden TSL-toteutuksiin, sikäli kuin edellä mainittu osoitin on käytettävissä. ETSIn teknisen spesifikaation 102 231 lausekkeen 5.3.13 eritelmiä on sovellettava sen vapaaehtoisen digitaalisen henkilöllisyyden (digital identity) käytön sallimiseen, joka ilmentää viittauksen kohteena olevaa TSL:n myöntäjää lausekkeessa 5.5.3 määritellyssä muodossa.

Huomautus: Tätä kenttää EI SAA käyttää, ennen kuin EY koostaa luettelon jäsenvaltioiden luotettavien luetteloiden TSL-toteutukseen viittaavista linkeistä ETSIn teknisen spesifikaation 102 231 mukaisessa toteutuksessa.

List issue date and time (lauseke 5.3.14)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä päiväys ja kellonaika (UTC koordinoituna maailmanaikana), jona TSL myönnettiin, käyttäen ETSIn teknisen spesifikaation lausekkeessa 5.1.4 määriteltyä Date-time value -arvoa.

Next update (lauseke 5.3.15)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä päiväys ja kellonaika (UTC koordinoituna maailmanaikana), jona seuraava TSL viimeistään myönnetään, tai kenttä PITÄÄ jättää tyhjäksi osoitukseksi siitä, että TSL on suljettu (käyttäen ETSIn teknisen spesifikaation lausekkeessa 5.1.4 määriteltyä Date-time value -arvoa).

Mikäli järjestelmän kattamaan TSP:hen tai palveluun ei ole tehty tilapäisiä statusmuutoksia, TSL PITÄÄ myöntää uudelleen siihen mennessä, kun viimeksi myönnetty TSL lakkaa olemasta voimassa.

Näissä eritelmissä kenttiin ”Next update” ja ”List issue date and time” merkittyjen päiväysten ja kellonaikojen ero EI SAA ylittää kuutta (6) kuukautta.

▼C1

Distribution points (lauseke 5.3.16)

Tämä kenttä on VAPAAEHTOINEN. Mikäli sitä käytetään, siinä PITÄÄ määritellä paikat, joissa luotettavan luettelon nykyinen TSL-toteutus on julkaistu ja mistä nykyisen TSL:n päivitykset ovat haettavissa. Mikäli ilmoitetaan useita jakelupisteitä, niissä kaikissa PITÄÄ olla yhtenäiset laitokset nykyisestä TSL:stä tai sen päivitetystä toisinnosta. Kun tätä kenttää käytetään, se on muotoiltava ei-tyhjäksi merkkijonojen jaksoksi. Jokaisen niistä on oltava RFC 3986:n ([1]) mukainen.

Scheme extensions (lauseke 5.3.17)

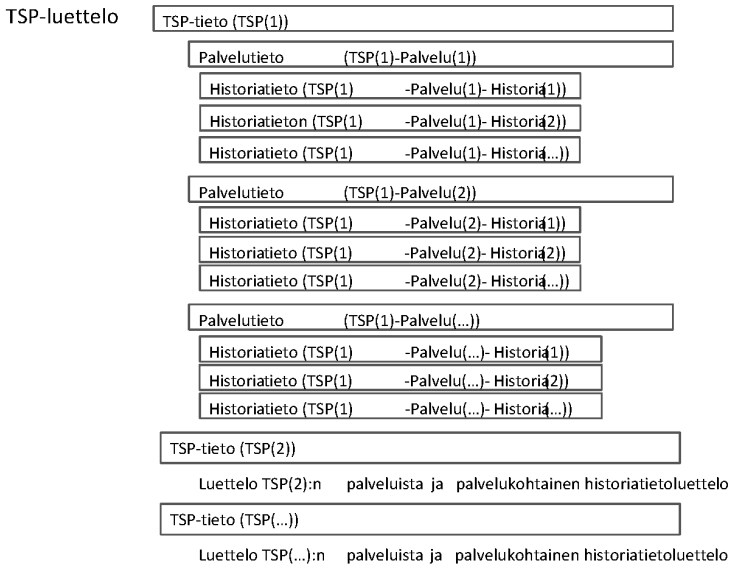
Tämä kenttä on VAPAAEHTOINEN, eikä sitä käytetä tämän eritelmän yhteydessä.

List of Trust Service Providers

Tämä kenttä on VAPAAEHTOINEN.

Jollei jäsenvaltion järjestelmässä ole (ollut) valvottuja/akkreditoituja varmennepalvelujen tarjoajia, tämän kentän PITÄÄ puuttua. On kuitenkin sovittu, että silloinkin, kun jäsenvaltiossa ei ole järjestelmässä valvottua eikä akkreditoitua varmennepalvelun tarjoajaa, jäsenvaltioiden PITÄÄ toteuttaa TSL ilman tätä kenttää. Varmennepalvelujen tarjoajien puuttumisen luettelosta PITÄÄ tarkoittaa, ettei ”Scheme Territory” kentässä määritellyssä maassa ole valvottuja/akkreditoituja varmennepalvelujen tarjoajia.

Mikäli järjestelmässä on valvottu/akkreditoitu yksi tai useampi varmennepalvelujen tarjoajien palvelu, kentän PITÄÄ sisältää jakso, jossa yksilöidään kukin varmennepalvelujen tarjoaja, joka tarjoaa yhtä tai useampaa näistä valvotuista/akkreditoiduista palveluista, sekä yksityiskohtaiset tiedot kunkin varmennepalvelun tarjoajan palvelun valvonta-/akkreditointistatuksesta ja statushistoriasta (alla olevassa kaaviossa TSP = CSP).



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

▼C1

TSP-luettelo on järjestetty yllä olevassa kaaviossa kuvatulla tavalla. Jokaisesta TSP:stä on mukana jakso kenttiä, jotka sisältävät tietoa TSP:stä (”TSP Information”), ja niiden jälkeen palvelujen luettelo. Jokaisesta näin luetellusta palvelusta on jakso kenttiä, jotka sisältävät tietoa palvelusta (”Service Information”), ja jakso kenttiä, jotka koskevat palvelun hyväksymisstatuksen historiaa (”Service approval history”).

TSP Information

TSP(1)

T S P n a m e (lauseke 5.4.1)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä järjestelmässä (aiemmin) valvotuista tai akkreditoiduista varmennepalvelun tarjoajan palveluista vastuullisen oikeushenkilön nimi. Sen on monikielisten merkkijonojen jakso (pakollisena kielenä EN ja mahdollisesti yksi tai useampi kansallinen kieli). Nimen PITÄÄ olla virallisissa lakisääteisissä rekisteröinneissä käytetty nimi, johon kaikki virallinen viestintä osoitetaan.

T S P t r a d e n a m e (lauseke 5.4.2)

Tämä kenttä on VAPAAEHTOINEN ja, mikäli se on mukana, siinä PITÄÄ määritellä vaihtoehtoinen nimi, jolla CSP tunnistautuu nimenomaisesti niiden palvelujen tarjonnan yhteydessä, jotka mainitaan tässä TSL:ssä kohdan ”TSP name” (lauseke 5.4.1) syötteessä.

Huomio: Mikäli yksi CSP-oikeushenkilö tarjoaa palveluja eri toiminimillä tai eri yhteyksissä, CSP-syötteitä voi olla yhtä monta kuin yhteyksiä (esim. Name / Trade Name -syötteet). Vaihtoehtona on luetella jokainen CSP (oikeushenkilö) vain kerran ja antaa palvelukohtaista taustatietoa. Jäsenvaltion järjestelmäoperaattorin tehtävänä on keskustella ja sopia CSP:n kanssa parhaiten soveltuva lähestymistapa.

T S P a d d r e s s (lauseke 5.4.3)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä kentässä ”TSP name” (lauseke 5.4.1) yksilöidyn oikeushenkilön tai valtuutetun organisaation osoite niin postilähetyksiä kuin sähköistä viestintääkin varten. Siinä PITÄÄ olla sekä ”PostalAddress” (eli lähiosoite, postitoimipaikka, [osavaltio tai maakunta], [postinumero] ja standardin ISO 3166-1 mukainen kaksimerkkinen maakoodi) lausekkeen 5.3.5.1 mukaisesti että ”ElectronicAddress” (eli sähköpostiosoite ja/tai verkkosivuston URI) lausekkeen 5.3.5.2 mukaisesti.

T S P i n f o r m a t i o n U R I (lauseke 5.4.4)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä URI(:t), jo(i)sta käyttäjät (eli varmenteeseen luottavat osapuolet) voivat saada CSP-kohtaista tietoa. Sen PITÄÄ olla monikielisten osoittimien jakso (pakollisena kielenä EN ja mahdollisesti yksi tai useampi kansallinen kieli). Ilmoitettujen URI-tunnisteiden PITÄÄ sisältää polku tietoihin, joissa kuvataan CSP:n yleiset ehdot, käytännöt, oikeudelliset seikat, asiakaspolitiikat ja muut yleiset tiedot, jotka koskevat kaikkia TSL:ssä sen CSP-syötteen kohdalla lueteltuja palveluja.

Huomio: Mikäli sama CSP-oikeushenkilö tarjoaa palveluja eri toiminimillä tai eri yhteyksissä ja tämä näkyy TSP-syötteiden lukumäärässä siten, että niitä on yhtä monta kuin eri yhteyksiä, kentässä PITÄÄ määritellä yksittäisen TSP/TradeName-syötteen alla lueteltujen erillisten palveluryhmien tiedot.

▼C1

TSP information extensions (lauseke 5.4.5)

Tämä kenttä on VAPAAEHTOINEN, ja mikäli se on mukana, järjestelmäoperaattori SAA käyttää sitä ETSIn teknisen spesifikaation 102 231 (lauseke 5.4.5) mukaisesti tarjotakseen erityisiä tietoja, jotka on tulkittava erityisjärjestelmän sääntöjen mukaan.

List of Services

Tämä kenttä on PAKOLLINEN, ja sen PITÄÄ sisältää jakso, jossa yksilöidään jokainen CSP:n tunnustama palvelu ja kyseisen palvelun hyväksymisstatus (ja statushistoria). Luettelossa on mainittava ainakin yksi palvelu (vaikka tieto olisikin kokonaisuudessaan historiatietoa).

Koska luettelossa olevien palvelujen historiatietojen säilytys on näiden eritelmien perusteella PAKOLLINEN, historiatiedot PITÄÄ säilyttää, vaikka palvelun nykyinen status ei yleisesti edellyttäisikään, että ne on mainittava luettelossa (esimerkiksi siksi, että palvelu on lakkautettu). Siksi CSP PITÄÄ sisällyttää luetteloon historiatietojen säilyttämiseksi, vaikka sen ainoan luettelossa olevan palvelun status olisikin edellä kuvattu.

Service Information

TSP(1) Service(1)

Service type identifier (lauseke 5.5.1)

▼M1

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä palvelutyypin tunniste näiden TSL-eritelmien tyypin mukaisesti (esim. ”/eSigDir-1999-93-EC-TrustedList/TSLType/generic”).

▼C1

Kun luettelon palvelu liittyy hyväksyttyjen varmenteiden myöntämiseen, ilmoitetun URI:n PITÄÄ olla http://uri.etsi.org/TrstSvc/Svctype/CA/QC (hyväksyttyjä varmenteita myöntävä varmentaja).

Kun luettelon palvelu liittyy muiden luottamuspalvelun sanakkeiden kuin hyväksyttyjen varmenteiden myöntämiseen eikä palvelu tue hyväksyttyjen varmenteiden myöntämistä, ilmoitetun URI:n PITÄÄ olla yksi URI-tunnisteista, jotka on määritelty ETSIn teknisessä spesifikaatiossa 102 231 ja lueteltu tätä kenttää koskevassa D.2-lausekkeessa. Tätä kohtaa PITÄÄ soveltaa silloinkin, kun luottamuspalvelun sanakkeita valvotaan / sanakkeet on akkreditoitu siten, että ne täyttävät jäsenvaltioiden kansallisten lakien mukaiset erityiset kelpuutukset (esim. niin sanottu Qualified Time Stamp Token, maa DE tai HU), ja ilmoitetun URI:n PITÄÄ olla yksi URI-tunnisteista, jotka on määritelty ETSIn teknisessä spesifikaatiossa 102 231 ja lueteltu tätä kenttää koskevassa D.2-lausekkeessa (esim. kansallisesti määriteltyjen Qualified Time Stamp Tokens -sanakkeiden TSA). Tarvittaessa luottamuspalvelujen sanakkeiden erityisen kansallisen kelpuutuksen SAA ilmoittaa palvelun syötteessä, ja tätä tarkoitusta varten PITÄÄ käyttää lausekkeessa 5.5.9 (”Service information extension”) olevaa additionalServiceInformation-liitettä (lauseke 5.8.2).

▼C1

Yleisenä oletusperiaatteena on, että luotettavassa luettelossa listatun varmennepalvelun tarjoajan (esim. (suoraan) hyväksyttyjä varmenteita myöntävän varmentajan) palveluissa on oltava yksi syöte yhtä X.509v3-varmennetta kohden (esim. CA/QC-tyypin varmennepalvelulle). Eräissä tarkoin harkituissa olosuhteissa ja huolellisesti hallinnoiduin ehdoin jäsenvaltion valvontalaitos/akkreditointilaitos SAA päättää, että se käyttää juuritason tai ylemmän tason varmentajan X.509v3-varmennetta (varmentaja ei esimerkiksi suoraan myönnä loppukäyttäjän hyväksyttyjä varmenteita vaan varmentaa varmentajahierarkian alaspäin niihin varmentajiin saakka, jotka myöntävät hyväksyttyjä varmenteita loppukäyttäjille) luetteloon sisältyvän varmennepalvelujen tarjoajan palveluluettelon yksittäisen syötteen ”Sdi”-kentässä. Jäsenvaltioiden on huolellisesti harkittava, mitä seurauksia (hyötyjä ja haittoja) tällaisen juuritason varmentajan tai ylemmän tason varmentajan X.509v3-varmenteen käytöstä luotettavan luettelon palvelusyötteiden ”Sdi”-arvoina voi aiheutua, ja hyväksyttävä ne ([1]). Käyttäessään tällaista sallittua poikkeusta oletusperiaatteeseen jäsenvaltioiden PITÄÄ lisäksi tarjota tarpeellinen dokumentaatio varmennepolun muodostamisen ja todentamisen helpottamiseksi.

Huomautus: Luottamuspalvelujen tarjoajat, kuten OSCP-vastaajat ja CRL-myöntäjät, jotka ovat osa CSP_{QC}-varmennepalveluja ja joiden on käytettävä erillisiä avainpareja OSCP-vastausten allekirjoittamiseen ja CRL:ien allekirjoittamiseen, SAA luetella myös tässä TSL-mallissa käyttäen seuraavaa URI-yhdistelmää:

— ”Service type identifier” (lauseke 5.5.1) -arvo:

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

yhdistettynä seuraavaan ”Service information extension” (lauseke 5.5.9) kentän additionalServiceInformation-liitteen (lauseke 5.8.2) arvoon:

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

Kuvaus: varmenteen statuksen tarjoaja, joka käyttää OSCP-palvelinta osana hyväksyttyjä varmenteita myöntävän varmennepalvelujen tarjoajan palvelua.

— ”Service type identifier” (lauseke 5.5.1) -arvo:

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

yhdistettynä seuraavaan ”Service information extension” (lauseke 5.5.9) -kentän additionalServiceInformation-liitteen (lauseke 5.8.2) arvoon:

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

Kuvaus: varmenteen statuksen tarjoaja, joka käyttää CRL:ää osana hyväksyttyjä varmenteita myöntävän varmennepalvelujen tarjoajan palvelua.

— ”Service type identifier” (lauseke 5.5.1) -arvo:

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

([1]) Kun juuritason varmentajan X.509v3-varmennetta käytetään luettelon palvelun ”Sdi”-arvona, järjestelmäoperaattorin on pakko tarkastella juuritason varmentajan koko varmennepalveluvalikoimaa kokonaisuutena suhteessa ”valvonta-/akkreditointistatukseen”. Näin luettelossa mainitun juurihierarkian alaisuuteen kuuluvalta yhdeltä varmentajalta edellytettävä statusmuutos pakottaa koko hierarkian omaksumaan kyseisen statuksen muutoksen.

▼C1

yhdistettynä seuraavaan ”Service information extension” (lauseke 5.5.9) -kentän additionalServiceInformation-liitteen (lauseke 5.8.2) arvoon:

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

Kuvaus: juuritason varmentaja, josta alkaen varmennepolku voidaan määritellä alaspäin hyväksyttyjä varmenteita myöntävään varmentajaan saakka.

— ”Service type identifier” (lauseke 5.5.1) -arvo:

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

yhdistettynä seuraavaan ”Service information extension” (lauseke 5.5.9) kentän additionalServiceInformation-liitteen (lauseke 5.8.2) arvoon:

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

Kuvaus: aikaleimauspalvelu osana hyväksyttyjä varmenteita myöntävän varmennepalvelujen tarjoajan palvelua; myönnettyä TST:tä voidaan käyttää hyväksytyn allekirjoituksen todennusprosessissa varmistamaan ja pidentämään allekirjoituksen voimassaoloa, kun hyväksytty varmenne on suljettu tai lakannut olemasta voimassa.

Service name (lauseke 5.5.2)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä nimi, jolla ”TSP name” -kentässä (lauseke 5.4.1) yksilöity varmennepalvelujen tarjoaja tarjoaa ”Service type identifier” -kentässä (lauseke 5.5.1) yksilöityä palvelua. Sen PITÄÄ olla monikielisten merkkijonojen jakso (pakollisena kielenä EN ja mahdollisesti yksi tai useampi kansallinen kieli).

Service digital identity (lauseke 5.5.3)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä ainakin yksi ainutkertaisen digitaalisen tunnisteen ilmentymä palvelulle, jonka tyyppi on määritelty ”Service type identifier” -kentässä (lauseke 5.5.1) ja jonka avulla palvelu voidaan yksilöidä yksiselitteisesti.

Näissä eritelmissä tässä kentässä käytettävän digitaalisen tunnisteen PITÄÄ olla asiaankuuluva X.509v3-varmenne, joka ilmentää julkista avainta/avaimia, jo(i)ta varmennepalvelujen tarjoaja käyttää tarjotessaan palvelua, jonka tyyppi on määritelty ”Service type identifier” -kentässä (lauseke 5.5.1) (eli juuritason CA/QC:n käyttämä avain, avain, jota käytetään varmenteiden allekirjoittamiseen [1]) tai aikaleimasanakkeiden myöntämiseen tai CRL:ien tai OSCP-vastausten allekirjoittamiseen). Tätä asiaan liittyvää X.509v3-varmennetta PITÄÄ käyttää vähintäänkin pakollisena digitaalisena tunnisteena (joka on varmennepalvelujen tarjoajan luettelossa olevan palvelun tarjontaan käyttämän julkisen avaimen tai avainten ilmentymä). Muita tunnisteita SAA käyttää seuraavasti, mutta niissä kaikissa PITÄÄ viitata samaan tunnukseen (eli asiaan liittyvään X.509v3-varmenteeseen):

[1] Kyseessä voi olla loppukäyttäjän varmenteita myöntävän varmentajan varmenne (esim. CA/PKC, CA/QC) tai luotetun juuritason varmentajan varmenne, jonka polku voidaan määritellä alaspäin loppukäyttäjän hyväksyttyihin varmenteisiin saakka. Sen mukaan, voidaanko tätä tietoa ja jokaisessa kyseisen luotetun juuren alaisuudessa myönnetyssä loppukäyttäjän varmenteessa olevaa tietoa käyttää yksiselitteisesti määrittämään minkä tahansa hyväksytyn varmenteen asianmukaiset ominaisuudet vai ei, kyseistä tietoa (”Service digital identity”) voidaan joutua täydentämään ”Service information extensions” -tiedoilla (katso lauseke 5.5.9).

▼C1

a) varmenteen luokiteltu nimi (DN), jota voidaan käyttää todentamaan ”Service type identifier” kentässä (lauseke 5.5.1) määritellyn varmennepalvelujen tarjoajan palvelun sähköisiä allekirjoituksia;

b) asiaan liittyvä julkisen avaimen tunniste (esim. X.509v3 SubjectKeyIdentifier eli SKI-arvo);

c) asiaan liittyvä julkinen avain.

Yleisenä oletusperiaatteena on, että digitaalinen tunniste (eli asiaan liittyvä X.509v3-varmenne) EI SAA esiintyä luotettavassa luettelossa useammin kuin kerran eli luotettavan luettelon varmennepalvelun tarjoajan luetelluissa varmennepalveluissa esiintyvän varmennepalvelun yhteydessä PITÄÄ olla yksi syöte kutakin yksittäistä X.509v3-varmennetta kohden. Kääntäen yhtä X.509v3-varmennetta PITÄÄ käyttää yhdessä ainoassa palvelussa ”Sdi”-arvona.

Huomautus (1): Ainoa tilanne, jossa edellä mainittua yleistä oletusperiaatetta ei välttämättä tarvitse soveltaa, on sellainen, jossa yksittäistä X.509v3-varmennetta käytetään myönnettäessä erityyppisiä luottamuspalvelujen sanakkeita, joihin sovelletaan erilaisia valvonta-/akkreditointijärjestelmiä, esimerkkinä yksi X.509v3-varmenne, jota CSP käyttää yhtäältä myöntäessään hyväksyttyjä varmenteita asianmukaisen valvontajärjestelmän puitteissa ja toisaalta myöntäessään muita kuin hyväksyttyjä varmenteita eri valvonta-/akkreditointistatuksella. Tässä tapauksessa ja esimerkissä käytettäisiin kahta syötettä, joissa on erilaiset ”Sti”-arvot (yllä olevassa esimerkiksi CA/QC ja CA/PKC) ja samat ”Sdi”-arvot (asiaan liittyvä X.509v3-varmenne).

Toteutukset ovat ASN.1- tai XML-riippuvaisia, ja niiden PITÄÄ täyttää ETSIn teknisen spesifikaation 102 231 eritelmät (katso ASN.1:n osalta ETSIn teknisen spesifikaation 102 231 Annex A ja XML:n osalta Annex B).

Huomautus (2): Kun yksilöidystä palvelusyötteestä on annettava ”kelpuutusta” koskevia lisätietoja, tarvittaessa järjestelmäoperaattorin PITÄÄ ottaa huomioon ”Service information extension” kentän (lauseke 5.5.9) ”additionalServiceInformation”-liitteen (lauseke 5.8.2) käyttö sen mukaan, mikä ”kelpuutusta” koskevien lisätietojen ilmoittamistarkoitus on. Lisäksi järjestelmäoperaattori voi valinnaisesti käyttää lauseketta 5.5.6 (”Scheme service definition URI”).

Service current status (lauseke 5.5.4)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä palvelun statuksen tunniste jollain seuraavista URI-tunnisteista:

▼C2

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

— **Palvelun valvonta päättymässä (Supervision of Service in Cessation** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation);

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

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

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

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

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

▼C1

Yllä mainitut statukset PITÄÄ tulkita näiden luotetun luettelon eritelmien yhteydessä seuraavasti:

— ***Under Supervision:*** ”Scheme territory” -kentässä (lauseke 5.3.10) yksilöity jäsenvaltio, johon CSP on sijoittautunut, valvoo parhaillaan ”Service digital identity” -kentässä (lauseke 5.5.3) yksilöityä palvelua, jota ”TSP name” -kentässä (lauseke 5.4.1) yksilöity varmennepalvelujen tarjoaja (CSP) tarjoaa, jotta direktiivin 1999/93/EY säännöksiä noudatetaan.

▼M1

— ***Supervision of Service in Cessation:*** ”TSP name” -kentässä (lauseke 5.4.1) yksilöidyn CSP:n tarjoama, ”Service digital identity” -kentässä (lauseke 5.5.3) yksilöidyn palvelun valvonta on päättymässä mutta jatkuu siihen saakka, kun valvonta päättyy tai suljetaan. Jos muu kuin ”TSP name” -kentässä yksilöity oikeushenkilö on ottanut vastuulleen päättyvän valvonnan varmistamisen, uuden tai varmistavan oikeushenkilön (varmistavan CSP:n) tunniste PITÄÄ ilmoittaa palvelusyötteen ”Scheme service definition URI” -liitteessä (lauseke 5.5.6) ja ”TakenOverBy” -liitteessä (lauseke L.3.2).

▼C1

— ***Supervision Ceased:*** Valvonta-arvioinnin voimassaoloaika on päättynyt ilman, että ”Service digital identity” -kentässä (lauseke 5.5.3) yksilöityä palvelua on ryhdytty arvioimaan uudelleen. Palvelua ei nykyisellään enää valvota, ja valvonta on lakannut palvelun nykyisen statuksen päiväyksestä lähtien, sillä palvelun on katsottu lakanneen.

— ***Supervision Revoked:*** Aiemmin valvottu CSP:n palvelu ja mahdollisesti myös CSP itse ei(vät) enää täytä direktiivin 1999/93/EY säännöksiä ”Scheme territory” -kentässä (lauseke 5.3.10) yksilöidyn jäsenvaltion, johon CSP on sijoittautunut, arvion perusteella. Näin ollen palvelun toiminta on vaadittu keskeytettäväksi, ja sen on katsottava lakanneen edellä mainitusta syystä.

Huomautus (1): Statusarvo ”Supervision Revoked” voi olla lopullinen status, vaikka CSP myöhemmin lopettaisikin kokonaan toimintansa; tässä tapauksessa ei ole tarpeen siirtyä ”Supervision of Service in Cessation”- tai ”Supervision Ceased” -statukseen. Ainoa tapa muuttaa ”Supervision Revoked” -status muuksi on palata ”Under Supervision” -statukseen siten, että ryhdytään uudelleen noudattamaan direktiivin 1999/93/EY säännöksiä ja tämä todetaan luotettavan luettelon omistavan jäsenvaltion voimassa olevan asianmukaisen valvontajärjestelmän avulla. ”Supervision of Service in Cessation” -status tai ”Supervision Ceased” status tulevat kyseeseen vain, kun CSP välittömästi lopettaa valvotut palvelunsa, eivät silloin, kun valvonta on peruutettu.

— ***Accredited:*** Akkreditointiarvion on tehnyt akkreditointilaitos ”Scheme territory” (lauseke 5.3.10) kentässä yksilöidyn jäsenvaltion puolesta ja ”TSP name” -kentässä (lauseke 5.4.1) yksilöidyn CSP:n [1] tarjoaman, ”Service digital identity” -kentässä (lauseke 5.5.3) yksilöidyn palvelun katsotaan täyttävän direktiivin 1999/93/EY säännökset.

[1] Huomattakoon, että kyseinen akkreditoitu CSP voi olla sijoittautuneena muuhun kuin luotettavan luettelon TSL-toteutuksen ”Scheme territory” -kentässä yksilöityyn jäsenvaltioon tai kolmanteen valtioon (katso direktiivin 1999/93/EY 7 artiklan 1 kohdan a alakohta).

▼C1

Huomautus (2): Kun ”Accreditation Revoked”- ja ”Accreditation Ceased” -statuksia käytetään ”Scheme territory” kentässä (lauseke 5.3.10) yksilöityyn jäsenvaltioon sijoittautuneen, hyväksyttyjä varmenteita tarjoavan CSP:n yhteydessä, kyseiset statukset PITÄÄ katsoa ”siirtymästatuksiksi”. Niitä EI SAA käyttää ”Service current status” -kentän arvoina, sillä tässä tapauksessa niiden jälkeen PITÄÄ välittömästi ilmoittaa palvelun hyväksymishistoria ”Service approval history information” -kentässä tai, ”Under supervision” -statuksen ollessa kyseessä ”Service current status” -kentässä, minkä jälkeen voi mahdollisesti seurata jokin muu edellä määritelty ja kaaviossa 1 kuvattu valvontastatus. Kun kyseisiä statuksia käytetään sellaisen CSP:n yhteydessä, joka ei myönnä hyväksyttyjä varmenteita, jolloin on mahdollisuus ainoastaan asiaan liittyvään ”vapaaehtoisuuteen perustuvaan akkreditointijärjestelmään” ilman valvontajärjestelmää, tai kun CSP myöntää hyväksyttyjä varmenteita eikä ole sijoittautunut ”Scheme territory” -kentässä (lauseke 5.3.10) yksilöityyn maahan (vaan kolmanteen maahan), ”Accreditation Revoked”- ja ”Accreditation Ceased” -tiloja SAA käyttää ”Service current status” -kentän nykyisinä arvoina:

— ***Accreditation Ceased:*** Akkreditointiarvioinnin voimassaoloaika on päättynyt ilman, että ”Service digital identity” -kentässä (lauseke 5.5.3) yksilöityä palvelua on ryhdytty arvioimaan uudelleen.

— ***Accreditation Revoked:*** ”TSP name” -kentässä (lauseke 5.4.1) yksilöidyn varmennepalvelujen tarjoajan (CSP) tarjoama, ”Service digital identity” -kentässä (lauseke 5.5.3) yksilöity palvelu, jonka on aiemmin todettu täyttävän järjestelmän kriteerit, ja mahdollisesti myös CSP itse eivät enää täytä direktiivin 1999/93/EY säännöksiä.

Huomautus (3): Hyväksyttyjä varmenteita myöntävien varmennepalvelujen tarjoajien ja varmennepalvelujen tarjoajien, jotka eivät myönnä hyväksyttyjä varmenteita (esim. aikaleimauspalvelun tarjoajat, jotka myöntävät TST-leimoja, muita kuin hyväksyttyjä varmenteita myöntävät CSP:t), on käytettävä tarkalleen samoja statusarvoja. ”Service Type identifier” -kentän (lauseke 5.5.1) avulla on eroteltava kulloinkin sovellettavat valvonta-/akkreditointijärjestelmät.

Huomautus (4): Varmennepalvelujen tarjoajia, jotka eivät myönnä hyväksyttyjä varmenteita, koskevissa kansallisissa valvonta-/akkreditointijärjestelmissä määriteltyjä muita statukseen liittyviä ”kelpuutustietoja” SAA tarjota palvelukohtaisesti tarvittaessa ja silloin, kun se on pakollista (esimerkiksi eri laatu-/palvelutasojen erottamiseksi toisistaan). Järjestelmäoperaattorin PITÄÄ käyttää ”Service information extension” kentän (lauseke 5.5.9) ”additionalServiceInformation”-liitettä (lauseke 5.8.2) sen mukaan, mikä ”kelpuutusta” koskevien lisätietojen ilmoittamistarkoitus on. Lisäksi järjestelmäoperaattori voi valinnaisesti käyttää lauseketta 5.5.6 (”Scheme service definition URI”).

Current status starting date and time (lauseke 5.5.5)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä päiväys ja kellonaika, jona nykyinen hyväksymisstatus tuli voimaan (päiväyksen ja kellonajan arvo ETSIn teknisen spesifikaation 102 231 lausekkeessa 5.1.4 määritellyssä muodossa).

Scheme service definition URI (lauseke 5.5.6)

Tämä kenttä on VAPAAEHTOINEN, ja mikäli se on mukana, siinä PITÄÄ määritellä URI(:t), jo(i)sta varmenteeseen luottavat osapuolet voivat saada järjestelmäoperaattorin tarjoamaa palvelukohtaista tietoa monikielisten osoittimien jaksona (EN pakollisena kielenä ja mahdollisesti yksi tai useampi kansallinen kieli).

Kun tätä kenttää käytetään, ilmoitettujen URI-tunnisteiden PITÄÄ sisältää polku palvelua kuvaavaan tietoon järjestelmässä määritellyllä tavalla. Tähän SAA tarvittaessa sisältyä erityisesti seuraavia:

a) URI, joka osoittaa varmistavan CSP:n henkilöllisyyden, mikäli kyseessä on varmistavan CSP:n hoitama palvelun päättyvä valvonta (katso ”Service current status” – lauseke 5.5.4);

▼C1

b) URI asiakirjoihin, joista saa lisätietoa eräiden kansallisesti määriteltyjen erityisten kelpuutusten käytöstä hyväksytyn/akkreditoidun luottamuspalvelusanakkeen tarjontapalvelun yhteydessä johdonmukaisesti suhteessa ”Service information extension” -kentän (lauseke 5.5.9) ja lausekkeessa 5.8.2 määritellyn ”additionalServiceInformation”-liitteen käyttöön.

Service supply points (lauseke 5.5.7)

tämä kenttä on VAPAAEHTOINEN, ja mikäli se on mukana, siinä PITÄÄ määritellä URI(:t), jo(i)sta varmenteeseen luottavat osapuolet voivat käyttää palvelua merkkijonojen jakson avulla. Jakson syntaksin PITÄÄ olla RFC 3986:n mukainen.

TSP service definition URI (lauseke 5.5.8)

Tämä kenttä on VAPAAEHTOINEN, ja mikäli se on mukana, siinä PITÄÄ määritellä URI(:t), jo(i)sta luottavat osapuolet voivat saada TSP:n tarjoamaa palvelukohtaista tietoa monikielisten osoittimien jaksona (EN pakollisena kielenä ja mahdollisesti yksi tai useampi kansallinen kieli). Ilmoitettujen URI-tunnisteiden PITÄÄ sisältää polku palvelua kuvaavaan tietoon TSP:n määrittelemällä tavalla.

Service information extensions (lauseke 5.5.9)

Näissä eritelmissä tämä kenttä on VAPAAEHTOINEN, mutta sen PITÄÄ olla mukana, kun ”Service digital identity” -kentässä (lauseke 5.5.3) annettu tieto ei riitä yksilöimään yksiselitteisesti tässä palvelussa myönnettyjä hyväksyttyjä varmenteita ja/tai kyseisissä hyväksytyissä varmenteissa olevat tiedot eivät mahdollista sellaisten tosiseikkojen koneellista tunnistamista, joilla selvitetään, onko hyväksytyn varmenteen tukena SSCD vai ei ([1]).

Kun vapaaehtoisen ”Service information extensions” (”Sie”) -tietokentän käyttö on PAKOLLINEN näiden eritelmien yhteydessä, esimerkiksi CA/QC-palvelujen yhteydessä, kenttää PITÄÄ käyttää ja se on jäsennettävä ETSIn teknisen spesifikaation 102 231 Annex L.3.1:ssä määritellyn ”Qualifications”-liitteen mukaisesti yhden tai useamman monikon jaksoksi, jonka jokaisessa monikossa on

— (rajaus)tiedot, joilla tunnistetaan tarkemmin ”Sdi”-kohdassa yksilöity varmennepalvelu, jossa tarkennetaan palvelu (eli hyväksyttyjen varmenteiden sarja), jolle edellytetään/tarjotaan lisätietoja turvallisen allekirjoituksen luomismenetelmän tukitietojen osoittamiseksi (ja/tai oikeushenkilölle myöntämisestä), ja

— asiaan liittyvät tiedot (”määreet”) siitä, onko tämä edelleen yksilöity hyväksyttyjen varmenteiden sarja tuettu turvallisella allekirjoituksen luomismenetelmällä vai ei (kun tietona on ”QCSSCDStatusAsInCert”, asiaan liittyvät tiedot ovat vakiomuotoisena koneellisesti luettavana osana ([2]) hyväksyttyä varmennetta), ja/tai tiedot siitä, onko kyseiset hyväksytyt varmenteet myönnetty oikeushenkilöille (muussa tapauksessa niitä oletetaan myönnetyn ainoastaan luonnollisille henkilöille).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD) tarkoittaa, että CSP varmistaa ja jäsenvaltio (sen valvontalaitos tai akkreditointilaitos) valvoo (valvontamalli) tai auditoi (akkreditointimalli), että jokainen hyväksytty varmenne, joka on myönnetty palvelussa, joka on yksilöity ”Service digital identity” -kentässä (lauseke 5.5.3) ja tarkennettu käyttäen yllä olevaa (rajaus)tietoa, jolla tarkennetaan ”Sdi”-kentässä yksilöidyn varmennepalvelun osalta ne tarkat hyväksyttyjen varmenteiden sarjat, joiden yhteydessä SSCD-tuen olemassaoloa tai puuttumista koskeva lisätieto on pakollinen, ON tuettu SSCD:n avulla (eli varmenteen julkiseen avaimeen liittyvä yksityinen avain on tallennettu direktiivin 1999/93/EY liitteen III mukaiseen turvallisen allekirjoituksen luomismenetelmään);

([1]) Katso tämän asiakirjan 2.2 kohta.

([2]) Tällä viitataan asianmukaiseen yhdistelmään ETSIn määrittämiä QcCompliance-lausumia, QcSSCD-lausumia [ETSIn tekninen spesifikaatio 101 862] tai QCP/QCP + ETSIn määrittelemä OID [ETSIn tekninen spesifikaatio 101 456].

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD) tarkoittaa, että CSP varmistaa ja jäsenvaltio (sen valvontalaitos tai akkreditointilaitos) valvoo (valvontamalli) tai auditoi (akkreditointimalli), että yhtään hyväksyttyä varmennetta, joka on myönnetty (juuritason CA/QC tai CA/QC) palvelussa, joka on yksilöity ”Service digital identity” -kentässä (lauseke 5.5.3) ja tarkennettu käyttäen yllä olevaa (rajaus)tietoa, jolla tarkennetaan ”Sdi”-kentässä yksilöidyn varmennepalvelun osalta ne tarkat hyväksyttyjen varmenteiden sarjat, joiden yhteydessä SSCD-tuen olemassaoloa tai puuttumista koskeva lisätieto on pakollinen, EI OLE tuettu SSCD:n avulla (eli varmenteen julkiseen avaimeen liittyvää yksityistä avainta ei ole tallennettu direktiivin 1999/93/EY liitteen III mukaiseen turvallisen allekirjoituksen luomismenetelmään).

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert) tarkoittaa, että CSP varmistaa ja jäsenvaltio (sen valvontalaitos tai akkreditointilaitos) valvoo (valvontamalli) tai auditoi (akkreditointimalli), että jokaisen hyväksytyn varmenteen, joka on myönnetty (CA/QC) palvelussa, joka on yksilöity ”Service digital identity” -kentässä (lauseke 5.5.3) ja tarkennettu käyttäen yllä olevaa (rajaus)tietoa, jolla tarkennetaan ”Sdi”-kentässä yksilöidyn varmennepalvelun osalta ne tarkat hyväksyttyjen varmenteiden sarjat, joiden yhteydessä SSCD-tuen olemassaoloa tai puuttumista koskeva lisätieto on pakollinen, PITÄÄ sisältää koneellisesti luettavat tiedot siitä, onko QC tuettu SSCD:n avulla vai ei;

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson) tarkoittaa, että CSP varmistaa ja jäsenvaltio (sen valvontalaitos tai akkreditointilaitos) valvoo (valvontamalli) tai auditoi (akkreditointimalli), että jokainen hyväksytty varmenne, joka on myönnetty (QCA) palvelussa, joka on yksilöity ”Service digital identity” -kentässä (lauseke 5.5.3) ja tarkennettu käyttäen yllä olevaa (rajaus)tietoa, jolla tarkennetaan ”Sdi”-kentässä yksilöidyn varmennepalvelun osalta ne tarkat hyväksyttyjen varmenteiden sarjat, joiden yhteydessä oikeushenkilölle myöntämistä koskeva lisätieto on pakollinen, ON myönnetty oikeushenkilölle.

Näitä määreitä on käytettävä ainoastaan liitteenä, jos palvelutyyppinä on http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Tämä kenttä on toteutuskohtainen (ASN.1 tai XML), ja sen PITÄÄ täyttää ETSIn teknisessä spesifikaatiossa 102 231, Annex L.3.1:ssä ilmoitetut eritelmät.

▼M1

XML-toteutuksen yhteydessä lisätietojen erityissisältö on koodattava ETSIn teknisen spesifikaation 102231 liitteessä C annettua xsd-tiedostoa käyttäen.

▼C1

Service Approval History

Tämä kenttä on VAPAAEHTOINEN, mutta sen PITÄÄ olla mukana, jos ”Historical information period” -kenttä (lauseke 5.3.12) on muu kuin nolla. Siksi näissä eritelmissä järjestelmän PITÄÄ säilyttää historiatiedot. Mikäli historiatiedot on tarkoitettu säilytettäviksi mutta palvelulla ei ole sen nykyistä statusta edeltävää historiaa (eli kyseessä on ensimmäinen kirjattu status tai järjestelmäoperaattori ei ole säilyttänyt historiatietoja), tämä kenttä PITÄÄ jättää tyhjäksi. Muussa tapauksessa ETSIn teknisen spesifikaation 102 231 lausekkeessa 5.3.12 määritellyn historiatietojakson aikana tapahtuneen jokaisen TSP-palvelun nykyisen statuksen muutoksen yhteydessä tiedot edeltävästä hyväksymisstatuksesta PITÄÄ ilmoittaa alenevassa järjestyksessä statuksen muuttumispäiväyksen ja ajan mukaan (eli sen mukaan, minä päivänä ja mihin aikaan seuraava hyväksymisstatus tuli voimaan).

▼C1

Tiedon PITÄÄ olla alla määritelty historiatietojen jakso.

▼C2

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

▼C1

Service type identifier (lauseke 5.6.1)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä palvelutyypin tunniste ”TSP Service Information – Service type identifier” -kentässä (lauseke 5.5.1) käytetyssä muodossa ja merkityksessä.

Service name (lauseke 5.6.2)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä nimi, jolla CSP tarjosi palvelua, joka on yksilöity ”TSP Service Information – Service type identifier” -kentässä (lauseke 5.5.1), ”TSP Service Information – Service name” -kentässä (lauseke 5.5.2) käytetyssä muodossa ja merkityksessä. Tämä lauseke ei edellytä nimen olevan sama kuin lausekkeessa 5.5.2 määritelty nimi. Nimenmuutos SAA olla yksi uutta statusta edellyttävistä tapahtumista.

▼M1

Service digital identity (lauseke 5.6.3)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä ainakin yksi digitaalisen tunnisteen ilmentymä (ts. X.509v3.-varmenne), jota on käytetty ”TSP Service Information – Service digital identity” -kentässä (lauseke 5.5.3) samaa muotoa ja merkitystä käyttäen kuin ETSIn teknisen spesifikaation 102231 lausekkeessa 5.5.3.

Huomautus: Palvelun ”Sdi”-tiedossa (lauseke 5.5.3) käytettävän X.509v3-varmennearvon osalta luotettavassa luettelossa on oltava vain yksi ainoa palvelusyöte kutakin ”Sti:Sie/additionalServiceInformation”-arvoa kohden. Palvelusyötteeseen liittyvissä tiedoissa palvelun hyväksymisstatuksen historiasta käytetyn ”Sdi”-tiedon (lauseke 5.6.3) ja kyseisessä palvelusyötteessä käytetyn ”Sdi”-tiedon (lauseke 5.5.3) PITÄÄ liittyä samaan X.509v3-varmennearvoon. Kun luettelossa olevan palvelun ”Sdi”-tietoja muutetaan (ts. X.509v3-varmenteen uusiminen tai ”rekey” esim. CA/PKC:lla tai CA/QC:lla) tai palvelulle luodaan uusi ”Sdi”, Scheme Operatorin PITÄÄ luoda aiemman palvelusyötteen tilalle uusi syöte, vaikka palveluun liittyvien ”Sti”-, ”Sn”-, ja [”Sie”]-tietojen arvot olisivat identtiset.

▼C1

Service previous status (lauseke 5.6.4)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä palvelun aiemman statuksen tunniste ”TSP Service Information – Service current status” -kentässä (lauseke 5.5.4) käytetyssä muodossa ja merkityksessä.

Previous status starting date and time (lauseke 5.6.5)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä päiväys ja kellonaika, jolloin edeltävä status tuli voimaan, ”TSP Service Information – Service current status starting date and time” -kentässä (lauseke 5.5.5) käytetyssä muodossa ja merkityksessä.

Service information extensions (lauseke 5.6.6)

Tämä kenttä on VAPAAEHTOINEN, ja järjestelmäoperaattori SAA käyttää sitä antamaan palvelukohtaista erityistietoa ”TSP Service Information – Service information extensions” -kentässä (lauseke 5.5.9) käytetyssä muodossa ja merkityksessä.

▼C2

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

Kuten edellä mutta TSP(1) Service(1) History(2) (ennen History 1:tä)

…

TSP(1) Service(2)

Kuten edellä mutta TSP(1) Service 2 (mikäli sovellettava)

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

…

TSP (2) Information

Kuten edellä mutta TSP 2 (mikäli sovellettava)

Kuten edellä mutta TSP 2 Service 1

Kuten edellä mutta TSP 2 Service 1 History 1

…

▼M1

Signed TSL

”Scheme operator name” -kentässä yksilöidyn tahon (lauseke 5.3.4) PITÄISI allekirjoittaa näiden eritelmien ja erityisesti IV luvun mukaisesti laadittu ihmisen luettavissa olevassa muodossa oleva luotettavan luettelon TSL-toteutus sen aitouden ja eheyden varmistamiseksi. ([1]) Allekirjoituksen muodon PITÄISI olla PAdES part 3 (ETSIn tekninen spesifikaatio 102 778-3 ([2])), mutta se SAA olla PAdES part 2 (ETSIn tekninen spesifikaatio 102 778-2 ([3])) luotettavien luetteloiden allekirjoitukseen käytettyjen varmenteiden julkaisemisen kautta luodun erityisen luottamusmallin yhteydessä.

”Scheme operator name” -kentässä yksilöidyn tahon (lauseke 5.3.4) PITÄÄ allekirjoittaa näiden eritelmien mukaisesti laadittu koneellisesti luettavassa muodossa oleva luotettavan luettelon TSL-toteutus sen aitouden ja eheyden varmistamiseksi. Näiden eritelmien mukaisesti laaditun koneellisesti luettavassa muodossa olevan luotettavan luettelon TSL-toteutuksen muodon PITÄÄ olla XML ja sen PITÄÄ olla ETSIn teknisen spesifikaation 102231 liitteissä B ja C olevien eritelmien mukainen.

Allekirjoituksen muodon PITÄÄ olla ETSIn teknisessä spesifikaatiossa 101903 XML-toteutuksille määritelty XAdES BES tai EPES. Tämän sähköisen allekirjoituksen toteutuksen PITÄÄ täyttää ETSIn teknisen spesifikaation 102231 liitteen B mukaiset vaatimukset. ([4]) Seuraavissa kohdissa on täydentäviä yleisiä vaatimuksia, jotka koskevat allekirjoitusta.

▼C1

Scheme identification (lauseke 5.7.2)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä järjestelmäoperaattorin nimeämä viite, joka yksilöi yksiselitteisesti näissä eritelmissä kuvatun järjestelmän ja käyttöön otetun TSL:n, ja se PITÄÄ sisällyttää allekirjoituksen laskentaan. Kentän oletetaan olevan merkki- tai bittijono.

([1]) Jos luotettavan luettelon TSL-toteutuksen ihmisen luettavissa olevaa muotoa ei allekirjoiteta, sen aitous ja eheys PITÄÄ varmistaa turvallisuustasoltaan vastaavalla asianmukaisella tietoliikennekanavalla. Tähän tarkoitukseen suositellaan käytettäväksi TLS:ää (IETF RFC 5246: ”The Transport Layer Security (TLS) Protocol Version 1.2”) ja jäsenvaltion PITÄÄ asettaa TLS-kanavan varmenteen sormenjälki TSL:n käyttäjien saataville kaistan ulkopuolelle.

([2]) ETSI TS 102 778-3 – Electronic Signatures and Infrastructures (ESI): PDF kehittynyt sähköinen allekirjoitus; Osa 3. PAdES Enhanced – PAdES-BES ja PAdES-EPES Profiles.

([3]) ETSI TS 102 778-2 – Electronic Signatures and Infrastructures (ESI): PDF kehittynyt sähköinen allekirjoitus; Osa 2. ISO 32000-1:een perustuva PAdES Basic – Profile based on ISO 32000-1.

([4]) Järjestelmäoperaattorin allekirjoitusvarmenne on ehdottomasti suojattava allekirjoituksella jollain ETSIn teknisessä spesifikaatiossa 101 903 määritellyllä tavalla ja ds:keyInfon pitäisi tarvittaessa sisältää asianmukainen varmenne.

▼M1

Näissä eritelmissä nimetyn viitteen PITÄÄ koostua järjestelmäoperaattorin TSL:n sähköiseen allekirjoitukseen käyttämän varmenteen toisiinsa kytketyistä kentistä ”TSL type” (lauseke 5.3.3), ”Scheme name” (lauseke 5.3.6) ja SubjectKeyIdentifier-liitteen arvosta.

▼C1

Signature algorithm identifier (lauseke 5.7.3)

Tämä kenttä on PAKOLLINEN, ja siinä PITÄÄ määritellä allekirjoituksen luomiseen käytetty salausalgoritmi. Käytetyn algoritmin mukaan tämä kenttä SAA edellyttää täydentäviä parametreja. Tämä kenttä PITÄÄ sisällyttää allekirjoituksen laskentaan.

Signature value (lauseke 5.7.4)

Tämä kenttä on PAKOLLINEN, ja sen PITÄÄ sisältää digitaalisen allekirjoituksen todellinen arvo. Kaikki TSL:n kentät (varsinaista allekirjoituksen arvoa lukuun ottamatta) PITÄÄ sisällyttää allekirjoituksen laskentaan.

TSL extensions (lauseke 5.8)

expiredCertsRevocationInfo-liite (lauseke 5.8.1)

Tämä liite on VAPAAEHTOINEN. Kun sitä käytetään, sen PITÄÄ täyttää ETSIn teknisen spesifikaation 102 231 lausekkeen 5.8.1 eritelmät.

additionalServiceInformation-liite (lauseke 5.8.2)

Tämä liite on VAPAAEHTOINEN, mutta jos sitä käytetään, sitä PITÄÄ käyttää ainoastaan palvelun tasolla ja ainoastaan lausekkeessa 5.5.9 määritellyssä kentässä (”Service information extension”). Sitä käytetään antamaan lisätietoa palvelusta. Sen PITÄÄ olla yhden tai useamman monikon jakso, ja jokaiseen monikkoon sisältyy:

a) lisätiedot yksilöivä URI, esimerkiksi

   — URI, joka osoittaa jonkin kansallisesti määritellyn erityisen kelpuutuksen hyväksytyn/akkreditoidun luottamuspalvelun sanakkeen tarjoamispalvelulle, esimerkiksi

      — erityinen turvallisuuteen/laatuun liittyvä tarkkuusaste, joka koskee valvonta-/akkreditointijärjestelmää, jota sovelletaan varmennepalvelujen tarjoajiin, jotka eivät myönnä hyväksyttyjä varmenteita (esim. Ranskan RGS */**/***, Saksan erityinen ”valvontastatus”, joka kansallisessa lainsäädännössä määritellään tietyille hyväksyttyjä varmenteita myöntäville varmennepalvelujen tarjoajille), katso huomautus (4) kohdassa ”Service current status” – lauseke 5.5.4;

      — tai valvotun/akkreditoidun luottamuspalvelun sanakkeen myöntämisen erityinen oikeudellinen status (esim. kansallisesti määritelty ”kelpuutettu TST”, kuten Saksassa tai Unkarissa);

      — tai ”Sdi”-kentässä annetussa X.509v3-varmenteessa olevan erityisen politiikkatunnistimen merkitys.

   — tai rekisteröity URI, joka on määritelty ”Service type identifier” -kentässä, lauseke 5.5.1, ja jolla tarkennetaan ”Sti”-kentässä yksilöidyn palvelun kuulumista osana hyväksyttyjä varmenteita myöntävän palveluntarjoajan palveluun (esim. OCSP-QC, CRL-QC ja RootCA-QC);

b) vapaaehtoinen jono, joka sisältää serviceInformation-arvon, jonka merkitys on määritetty järjestelmässä (esim. *, ** tai ***);

c) muut mahdolliset vapaaehtoiset lisätiedot, jotka on annettu järjestelmäkohtaisessa muodossa.

▼**M1**

Kun URI:n viitettä seurataan, sen PITÄISI johtaa ihmisen luettavissa olevassa muodossa oleviin tietoihin (vähintään englannin kielellä ja mahdollisesti kahdella tai useammalla kansallisella kielellä), joiden varmennukseen luottavat osapuolet katsovat olevan asianmukaisia ja riittäviä liitteen ymmärtämiseksi ja erityisesti annettujen URI-tunnisteiden merkityksen selvittämiseksi ja joissa määritellään mahdolliset serviceInformation-arvot ja kunkin arvon merkitys.

Qualifications Extension (lauseke L.3.1)

Kuvaus: Tämä kenttä on VAPAAEHTOINEN, mutta sitä PITÄÄ käyttää, kun sen käyttö on PAKOLLINEN, esim. RootCA/QC- tai CA/QC-palveluissa ja kun

— ”Service digital identity” -kentässä annetut tiedot eivät riitä yksilöimään yksiselitteisesti tässä palvelussa myönnettyjä hyväksyttyjä varmenteita

— kyseisissä hyväksytyissä varmenteissa olevat tiedot eivät mahdollista sellaisten tosiseikkojen koneellista tunnistamista, joilla selvitetään, onko hyväksytyn varmenteen tukena SSCD vai ei.

Kun tätä palvelutason liitettä käytetään, sitä PITÄÄ käyttää yksinomaan ”Service information extension” -kentässä (lauseke 5.5.9) määritellyssä kentässä ja sen PITÄÄ olla ETSIn teknisen spesifikaation 102231 liitteessä L.3.1 määriteltyjen eritelmien mukaista.

TakenOverBy Extension (lauseke L.3.2)

Kuvaus: Tämä liite on VAPAAEHTOINEN, mutta sitä PITÄÄ käyttää, kun CSP:n oikeudellisella vastuulla aiemmin ollut palvelu siirtyy toisen TSP:n vastuulle, ja sen tarkoituksena on ilmoittaa virallisesti taho, jonka oikeudellisella vastuulla palvelu on, ja mahdollistaa se, että todentamisessa käytettäviin ohjelmistoihin voidaan asettaa käyttäjän nähtäville joitakin oikeudellisia yksityiskohtia. Tässä liitteessä annettavien tietojen PITÄÄ olla lausekkeen 5.5.6 tähän liittyvän käytön mukaisia ja niiden PITÄÄ olla ETSIn teknisen spesifikaation 102231 liitteessä L.3.2 olevien eritelmien mukaisia.

▼M1

II LUKU

Laatiessaan luotettavia luetteloitaan jäsenvaltiot merkitsevät

kielikoodit pienaakkosin ja maakoodit suuraakkosin

kieli- ja maakoodit jäljempänä olevan taulukon mukaan

lisäksi translitteroinnin latinalaisin aakkosin seuraavan taulukon mukaisine kielikoodeineen, kun luettelossa käytetään latinalaisia aakkosia (kielikoodeineen).

Lyhytnimi (alkukielellä)	Lyhytnimi (englanniksi)	Maakoodi	Kielikoodi	Huomautukset	Translitterointi latinalaisin aakkosin
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	EU:n suosittelema maakoodi	el-Latn
España	Spain	ES	es	Myös katalaani (ca), baski (eu), galego (gl)	
France	France	FR	fr		

▼M2

Hrvatska	Croatia	HR	hr		

▼M1

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**

Lyhytnimi (alkukielellä)	Lyhytnimi (englanniksi)	Maakoodi	Kielikoodi	Huomautukset	Translitterointi latinalaisin aakkosin
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	EU:n suosittelema maakoodi	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Translitterointi latinalaisin aakkosin: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

_____

▼C1

IV LUKU

LUOTETTAVAN LUETTELON TSL-TOTEUTUKSEN IHMISEN LUETTAVISSA OLEVAN MUODON ERITELMÄT

Luotettavan luettelon TSL-toteutuksen ihmisille lukukelpoisen (HR) muodon PITÄÄ olla julkisesti saatavissa ja sähköisesti luettavissa. Se PITÄISI tarjota Portable Document Format (PDF) asiakirjana standardin ISO 32000 mukaisesti, ja sen formatoinnin PITÄÄ olla profiilin PDF/A (ISO 19005) mukainen.

Luotettavan luettelon TSL-toteutuksen profiiliin PDF/A perustuvan HR-muodon PITÄISI täyttää seuraavat vaatimukset:

▼M1

— Ihmisen luettavissa olevassa muodossa olevien luotettavien luetteloiden otsikon on koostuttava seuraavista seikoista:

  — Vapaavalinnainen kuva jäsenvaltion kansallisesta lipusta

  — Tyhjä tila

  — Maan lyhytnimi alkukielellä (-kielillä) (luvussa II olevan taulukon ensimmäisen sarakkeen mukaisesti)

  — Tyhjä tila

  — «(»

  — Maan lyhytnimi englannin kielellä (luvussa II olevan taulukon toisen sarakkeen mukaisesti) suluissa

  — «):» sulkumerkkinä ja erottimena

  — Tyhjä tila

  — «Trusted List»

  — Mahdollisesti jäsenvaltion järjestelmäoperaattorin logo.

▼C1

— HR-muodon PITÄISI vastata ETSIn teknisen spesifikaation 102 231 kohdassa 5.1.2 kuvattua loogista mallia.

— Jokaisessa mukana olevassa kentässä PITÄISI näyttää ja ilmoittaa seuraavat tiedot:

  — kentän otsikko (esim. ”Palvelutyypin tunniste”),

  — kentän arvo (esim. ”CA/QC”),

  — tarvittaessa kentän arvon merkitys (kuvaus) ja erityisesti ETSIn teknisen spesifikaation 102 231 Annex D:ssä tai näissä eritelmissä kuvatussa muodossa rekisteröityjen URI-tunnisteiden osalta (esim. ”Julkisen avaimen varmenteita myöntävä varmentaja”),

  — tarvittaessa useita luonnollisten kielten kielimuunnoksia, jotka mainitaan luotettavan luettelon TSL-toteutuksessa.

— Seuraavien kenttien ja digitaalisten varmenteiden vastaavat arvot, jotka sijaitsevat kentässä ”Service digital identity”, PITÄISI ainakin näyttää HR-muodossa:

  — versio

  — sarjanumero

  — allekirjoituksen algoritmi

  — myöntäjä

  — voimassaolon alkupäivä

  — viimeinen voimassaolopäivä

  — aihe

▼C1

— julkinen avain

— varmennepolitiikat

— aiheen varmentajatunniste

— CRL:n jakelupisteet

— varmentaja-avaimen tunniste

— avaimen käyttö

— perusrajoitteet

— algoritmin tunniste

— Thumbprint

— HR-muodon PITÄISI olla helposti tulostettavissa.

— HR-muoto SAA olla sähköisesti allekirjoitettu. Jos se on allekirjoitettu, sen allekirjoittajan PITÄÄ olla järjestelmäoperaattori ja allekirjoittajan on noudatettava samoja allekirjoituseritelmiä kuin luotettavan luettelon TSL-toteutuksessa noudatetaan.