

## FRAMKVÆMDARÁKVÖRÐUN FRAMKVÆMDASTJÓRNARINNAR

2015/EES/63/10

frá 14. október 2013

um breytingu á ákvörðun 2009/767/EB að því er varðar að semja, viðhalda og birta áreiðanlega lista yfir vottunaraðila sem aðildarríkin hafa eftirlit með eða veita faggildingu

(tilkynnt með númeri C(2013) 6543)

(2013/662/ESB) (\*)

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS  
HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af tilskipun Evrópuþingsins og ráðsins 2006/123/EB frá 12. desember 2006 um þjónustu á innri markaðnum <sup>(1)</sup>, einkum 3. mgr. 8. gr.,

og að teknu tilliti til eftirfarandi:

- 1) Samkvæmt ákvörðun framkvæmdastjórnarinnar 2009/767/EB frá 16. október 2009 um ráðstafanir sem greiða fyrir notkun rafrænnar málsmeðferðar með upplýsinga- og þjónustumiðstöðvum samkvæmt tilskipun Evrópuþingsins og ráðsins 2006/123/EB um þjónustu á innri markaðnum <sup>(2)</sup> er aðildarríkjunum skylt að gera aðgengilegar þær upplýsingar sem nauðsynlegar eru til að staðfesta útfærðar rafrænar undirskriftir sem eru studdar fullgildu vottorði. Þessar upplýsingar skal setja fram á samræmdan hátt í svokölluðum „áreiðanlegum listum“ (e. trusted lists), sem hafa að geyma upplýsingar um vottunaraðila sem gefa út fullgild vottorð til handa almenningi í samræmi við tilskipun Evrópuþingsins og ráðsins 1999/93/EB frá 13. desember 1999 um ramma Bandalagsins varðandi rafrænar undirskriftir <sup>(3)</sup> og sem aðildarríkin hafa eftirlit með eða veita faggildingu.
- 2) Fengin reynsla af framkvæmd ákvörðunar 2009/767/EB af hálfu aðildarríkjanna hefur sýnt að tiltekna úrbætur eru nauðsynlegar til að hámarka ávinninginn af áreiðanlegum listum. Enn fremur hefur Fjarskiptastaðlastofnun Evrópu (ETSI) birt nýjar tækniforskriftir fyrir áreiðanlega lista (TS 119 612), sem byggjast á forskriftunum sem nú er að finna í viðaukanum við ákvörðunina en gera jafnframt ýmsar úrbætur á núverandi forskriftum.
- 3) Því ætti að breyta ákvörðun 2009/767/EB þannig að hún vísi til tækniforskrifta Fjarskiptastaðlastofnunar Evrópu 119 612 og taki upp breytingar sem taldar eru nauðsynlegar til að bæta og auðvelda framkvæmd og notkun áreiðanlegra lista.

(\*) Þessi EB-gerð birtist í Stjtið. ESB L 306, 16.11.2013, bls. 21. Hennar var getið í ákvörðun sameiginlegu EES-nefndarinnar nr. 189/2014 frá 25. september 2014 um breytingu á X. viðauka (Almenn þjónusta) við EES-samninginn, sjá EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 43, 30.7.2015, s. 41.

<sup>(1)</sup> Stjtið. ESB L 376, 27.12.2006, bls. 36.

<sup>(2)</sup> Stjtið. ESB L 274, 20.10.2009, bls. 36.

<sup>(3)</sup> Stjtið. EB L 13, 19.1.2000, bls. 12.

4) Til að gera aðildarríkjunum kleift að gera nauðsynlegar tæknilegar breytingar á núverandi áreiðanlegum listum sínum ætti þessari ákvörðun að vera beitt frá og með 1. febrúar 2014.

5) Ráðstafanirnar, sem kveðið er á um í þessari ákvörðun, eru í samræmi við álit nefndarinnar um þjónustutilskipunina.

SAMBÝKKT ÁKVÖRÐUN ÞESSA:

1. gr.

**Breytingar á ákvörðun 2009/767/EB**

Ákvörðun 2009/767/EB er breytt sem hér segir:

1) Ákvæðum 2. gr. er breytt sem hér segir:

a) Í stað 1. mgr., 2. mgr. og 2. mgr. a komi eftirfarandi:

„1. Sérhvert aðildarríki skal semja, viðhalda og birta, í samræmi við tækniforskriftir sem settar eru fram í viðaukanum, „áreiðanlegan lista“ (e. trusted list) sem inniheldur að lágmarki upplýsingar um þá vottunaraðila sem gefa út fullgild vottorð til handa almenningi og sem aðildarríkin hafa eftirlit með/veita faggildingu.

2. Aðildarríki skulu semja og birta tölvutæka útgáfu af áreiðanlega listanum í samræmi við forskriftirnar sem settar eru fram í viðaukanum. Kjósi aðildarríki að birta útgáfu af áreiðanlegum lista sínum sem er læsileg mönnum skal sú útgáfa áreiðanlega listans vera í samræmi við forskriftirnar sem settar eru fram í viðaukanum.

2a. Aðildarríki skulu undirrita rafrænt tölvutæka útgáfuna af áreiðanlegum lista sínum til að tryggja sannvottaðan uppruna hans og heilleika. Ef aðildarríki birtir útgáfu af áreiðanlega listanum sem er læsileg mönnum skal það tryggja að þessi útgáfa áreiðanlega listans innihaldi sömu upplýsingar og tölvutæka útgáfan og undirrita hana rafrænt með sömu skilríkjum og notað eru fyrir tölvulesanlegu útgáfuna.“

b) Eftirfarandi 2. mgr. b bætist við:

„2b. Aðildarríki skulu tryggja að tölvutæk útgáfa af áreiðanlegum lista þeirra sé ætíð aðgengileg á útgáfustað, án þess að rof verði á, nema vegna viðhalds.“

c) Í stað 3. mgr. komi eftirfarandi:

„3. Aðildarríkin skulu tilkynna framkvæmdastjórninni um eftirfarandi:

a) þann eða þá aðila sem bera ábyrgð á því að semja, viðhalda og birta tölvutæka útgáfu af áreiðanlega listanum,

b) þann stað þar sem tölvutæk útgáfa áreiðanlega listans er birt,

c) tvö eða fleiri dreifilyklaskilríki rekstraraðila kerfisins, með gildistíma sem eru hliðraðir um a.m.k. þrjá mánuði og sem samsvara einkalyklunum sem nota má til að undirrita rafrænt tölvutæka útgáfu áreiðanlega listans,

d) allar breytingar á upplýsingunum í a-, b- og c-lið.“

d) Eftirfarandi 3. mgr. a bætist við:

„3a. Ef aðildarríki birtir útgáfu af áreiðanlega listanum sem er læsileg mönnum skal einnig veita upplýsingarnar, sem um getur í 3. mgr., fyrir þá útgáfu.“

2) Viðaukinn við þessa ákvörðun komi í stað viðaukans.

2. gr.

**Beiting**

Ákvörðun þessari skal beitt frá 1. febrúar 2014.

3. gr.

**Viðtakendur**

Ákvörðun þessari er beint til aðildarríkjanna.

Gjört í Brussel 14. október 2013.

*Fyrir hönd framkvæmdastjórnarinnar,*

Michel BARNIER

*framkvæmdastjóri.*

## VIÐAUKI

## TÆKNIFORSKRIFTIR FYRIR SAMEIGINLEGT SNIÐMÁT FYRIR 'ÁREIÐANLEGAN LISTA YFIR EFTIRLITSSKYLDA/FAGGILTA VOTTUNARAÐILA'

## ALMENNAR KRÖFUR

## 1. Inngangur

Tilgangurinn með sameiginlegu sniðmáti fyrir 'áreiðanleg lista aðildarríkja yfir eftirlitsskylda/faggilta vottunaraðila' er að koma á fót sameiginlegri aðferð sem sérhvert aðildarríki notar við að veita upplýsingar um eftirlits-/faggildingarstöðu vottunaraðila af hálfu vottunaraðila <sup>(1)</sup> sem það hefur eftirlit með/veitir faggildingu með tilliti til þess að farið sé að viðeigandi ákvæðum í tilskipun 1999/93/EB. Undir þetta fellur að veita eldri upplýsingar um eftirlits-/faggildingarstöðu eftirlitsskyldu/faggiltu vottunaraðilastunnar.

Þessum upplýsingum er einkum ætlað að styðja staðfestingu fullgildra rafræna undirskrifa (QES) og útfærðra rafræna undirskrifa (AdES) <sup>(2)</sup> sem eru studdar fullgildum vottorðum <sup>(3)</sup> <sup>(4)</sup>.

Skyldubundnu upplýsingarnar í áreiðanlega listanum verða að lágmarki að innihalda upplýsingar um eftirlitsskylda/faggilta vottunaraðila (CSP) sem gefa út fullgild vottorð (QC) <sup>(5)</sup> í samræmi við ákvæðin sem mælt er fyrir um í tilskipun 1999/93/EB (2. og 3. mgr. 3. gr. og a-lið 1. mgr. 7. gr.), þ.m.t., ef þær eru ekki hluti af fullgildu vottorðunum, upplýsingar um fullgild vottorð sem styðja rafræna undirskrift og hvort undirskriftin er gerð með öruggum undirskriftarbúnaði (SSCD) eður ei <sup>(6)</sup>.

Valfrjálst er að bæta á áreiðanlegan lista hvers aðildarríkis fyrir sig viðbótarupplýsingum um aðra vottunaraðila sem gefa ekki út fullgild vottorð en veita þjónustu í tengslum við rafrænar undirskriftir (t.d. vottunaraðila sem veita tímastimplunarþjónustu og gefa út tímastimplunartóka, vottunaraðila sem gefa út vottorð sem eru ekki fullgild o.s.frv.) að því tilskildu að þeir séu annaðhvort eftirlitsskyldir/faggiltir á sambærilegan hátt og þeir vottunaraðilar sem gefa út fullgild vottorð eða samþykktir samkvæmt öðru landsbundnu samþykktarkerfi (e. national approval scheme). Landsbundin samþykktarkerfi sumra aðildarríkja geta verið frábrugðin eftirlitskerfum eða valfrjálsum faggildingarkerfum sem gilda fyrir vottunaraðila sem gefa út fullgild vottorð að því er varðar gildandi kröfur og/eða ábyrga stofnun. Hugtökin 'faggiltur' og/eða 'eftirlitsskyldur' í þessum forskriftum ná einnig yfir landsbundin samþykktarkerfi en aðildarríki munu veita viðbótarupplýsingar um eðli landsbundinna kerfa í áreiðanlegum listum sínum, þ.m.t. skýringu á því í hverju þau kunna að vera frábrugðin faggildingar-/eftirlitskerfum sem gilda um vottunaraðila sem gefa út fullgild vottorð.

Sameiginlega sniðmátið byggist á tækniforskrift Fjarskiptastaðlastofnunar Evrópu (ETSI TS) 119 612 v1.1.1 <sup>(7)</sup> (hér á eftir nefnt ETSI TS 119 612), sem fjallar um að semja og birta slíkar skrár og um staðsetningu þeirra, aðgang að þeim, sannvottun þeirra og heilleika.

## 2. Skipan sameiginlega sniðmátsins fyrir áreiðanlega listann

Sameiginlega sniðmátið fyrir áreiðanlegan lista aðildarríkis er byggt upp samkvæmt ETSI TS 119 612 og greinist í eftirfarandi flokka upplýsinga:

1. Tag áreiðanlega listans (e. trusted list tag) sem auðveldar að bera kennsl á hann við rafræna leit.
2. Upplýsingar um áreiðanlega listann og útgáfukerfi hans.
3. Runu svæða sem innihalda ótvíræðar auðkennisupplýsingar um sérhvern eftirlitsskyldan/faggiltan vottunaraðila í kerfinu (þessi runa er valkvæð, þ.e. þegar hún er ekki notuð telst listinn ekki hafa neitt innihald, sem merkir að ekki sé neinn eftirlitsskyldur/faggiltur vottunaraðili í viðkomandi aðildarríki að því er varðar áreiðanlega listann).
4. Ítarlegar upplýsingar um sérstaka traustþjónustu hvers skráðs vottunaraðila – en núverandi staða hennar er færð inn í áreiðanlega listann – eru veittar sem runa svæða, sem auðkenna á ótvíræðan hátt þá eftirlitsskyldu/faggiltu vottunaraðilastöðu, sem vottunaraðilinn veitir og núverandi stöðu hennar (þessi runa verður að innihalda a.m.k. eina færslu).

<sup>(1)</sup> Eins og skilgreint er í 11. mgr. 2. gr. tilskipunar 1999/93/EB.

<sup>(2)</sup> Eins og skilgreint er í 2. mgr. 2. gr. tilskipunar 1999/93/EB.

<sup>(3)</sup> Upphafsstafaorðið 'AdES<sub>QC</sub>' er notað alls staðar í þessu skjali fyrir útfærða rafræna undirskrift (AdES) sem studd er fullgildu vottorði (QC).

<sup>(4)</sup> Ath. að þetta myndi einnig greiða fyrir nýtingu ýmissar rafrænnar þjónustu, sem byggð er á einfaldri útfærðri rafrænni undirskrift (AdES), yfir landamæri, að því tilskildu að stuðningsþjónusta vegna vottunar (t.d. útgáfa vottorða sem eru ekki fullgild) væri hluti af eftirlitsskyldri/faggiltri þjónustu sem aðildarríki tilgreinir undir valfrjálsum upplýsingum í áreiðanlegum lista sínum.

<sup>(5)</sup> Eins og skilgreint er í 10. mgr. 2. gr. tilskipunar 1999/93/EB.

<sup>(6)</sup> Eins og skilgreint er í 6. mgr. 2. gr. tilskipunar 1999/93/EB.

<sup>(7)</sup> ETSI TS 119 612 v1.1.1 (2013-06) – Electronic Signatures and Infrastructures (ESI); Trusted Lists.

5. Upplýsingar um sögu þessarar stöðu fyrir hverja skráða eftirlitsskylda/faggilta vottunarþjónustu, ef við á.
6. Undirskrift sem notuð er á áreiðanlega listann.

Að því er varðar vottunaraðila sem gefur út fullgild vottorð leyfir skipan áreiðanlega listans, einkum sá hluti sem inniheldur þjónustupplýsingar (sbr. 4. lið hér að framan), viðbótarupplýsingar í viðskeytum þjónustupplýsinga (e. service information extensions) til að bæta upp aðstæður þar sem ófullnægjandi (tölvutækar) upplýsingar liggja fyrir í fullgilda vottorðinu um „fullgilda“ stöðu þess, mögulegan stuðning þess af öruggum undirskriftarbúnaði (SSCD) og ekki síst til að taka tillit til þess að flestir vottunaraðilar (sem starfa á viðskiptagrundvelli) nota aðeins eina vottunarstöð (CA) til að gefa út mismunandi tegundir endaskilríkja, jafnt fullgild sem ekki fullgild.

Að því er varðar þjónustu (vottunarstöðvar) við gerð vottorða má draga úr fjölda þjónustufærslna í skránni fyrir hvern vottunaraðila þegar þjónusta einnar eða fleiri vottunarstöðva á efra stigi er fyrir hendi innan dreifilyklaskipulags (PKI) vottunaraðilans (t.d. í tengslum við stigveldi vottunarstöðva frá röturvottunarstöð niður í nokkrar vottunarstöðvar sem gefa út vottorð) með því að telja upp þessar vottunarstöðvar á efra stigi en ekki þær sem gefa út endaskilríki (t.d. með því að tilgreina aðeins röturvottunarstöð (e. Root CA) vottunaraðilans). Í slíkum tilvikum gilda þó stöðupplýsingarnar um allt stigveldi vottunarstöðva fyrir neðan þjónustuna sem er skráð og viðhalda skal og tryggja meginregluna um að sjá skuli til þess að ótvíræð tengsl séu milli vottunarþjónustu af hálfu vottunaraðila sem gefur út fullgild vottorð (CSPQC) og þess mengis vottorða sem ætlunin er að auðkenna sem fullgild vottorð.

### 2.1. Lýsing á upplýsingum í hverjum flokki

1. Tag áreiðanlega listans
2. Upplýsingar um áreiðanlega listann og útgáfukerfi hans

Eftirfarandi upplýsingar falla í þennan flokk:

- **útgáfuaðkenni fyrir snið (e. format version identifier)** áreiðanlega listans,
- **raðnúmer (eða birtingarnúmer)** áreiðanlega listans,
- **upplýsingar um gerð** áreiðanlega listans (t.d. um að þessi áreiðanlegi listi veiti upplýsingar um eftirlits-/faggildingarstöðu vottunarþjónustu af hálfu vottunaraðila sem aðildarríkið, sem vísað er til, hefur eftirlit með/veitir faggildingu með tilliti til þess að farið sé að ákvæðum sem mælt er fyrir um í tilskipun 1999/93/EB),
- **upplýsingar um rekstraraðila (eiganda) kerfisins** fyrir áreiðanlega listann (t.d. nafn, heimilisfang, samskiptaupplýsingar o.s.frv. þess aðila aðildarríkisins, sem sér um að semja áreiðanlega listann, birta hana á öruggan hátt og viðhalda henni),
- **upplýsingar um undirliggjandi eftirlits-/faggildingarkerfi** sem áreiðanlegi listinn tengist, þ.m.t. en ekki eingöngu:
  - landið sem hún gildir fyrir,
  - upplýsingar um eða tilvísun í stað þar sem finna má upplýsingar um kerfið/kerfin (kerfislikan, reglur, viðmiðanir, viðeigandi samfélag, gerð o.s.frv.),
  - varðveislutíma (eldri) upplýsinga,
- **stefna og/eða lagatilkynning, skuldbindingar og ábyrgðarsvið** í tengslum við áreiðanlega listann,
- **útgáfudagur og -tími** áreiðanlega listans,
- **næsta fyrirhugaða uppfærsla** áreiðanlega listans.

### 3. Ótvíræðar auðkennisupplýsingar um sérhvern eftirlitsskyldan/faggiltan vottunaraðila í kerfinu

Í þessu mengi upplýsinga skal a.m.k. eftirfarandi koma fram:

- Heiti stofnunar eða fyrirtækis vottunaraðilans eins og það er notað í formlegri lagalegri skráningu (þ.m.t. einkvæmt auðkenni (e. unique identifier (UID)) stofnunar eða fyrirtækis vottunaraðilans samkvæmt venjum aðildarríkisins).
- Heimilisfang og samskiptaupplýsingar vottunaraðilans.
- Viðbótarupplýsingar um vottunaraðilann, annaðhvort beint eða með vísun í stað þar sem hægt er að hala niður slíkum viðbótarupplýsingum.

4. Runa svæða fyrir hvern skráðan vottunaraðila með ótvíræðri auðkenningu á vottunarþjónustu sem vottunaraðilinn veitir og er eftirlitsskyld/faggilt innan ramma tilskipunar 1999/93/EB

Í þessu mengi upplýsinga skal a.m.k. eftirfarandi koma fram fyrir hverja tegund vottunarþjónustu af hálfu skráðs vottunaraðila:

- Tegundarauðkenni þjónustunnar (e. Service type identifier): Tegundarauðkenni vottunarþjónustunnar (t.d. auðkenni sem gefur til kynna að eftirlitsskyld/faggilt vottunarþjónusta vottunaraðilans sé vottunarstöð sem gefur út fullgild vottorð).
- (Viðskipta-)heiti þjónustunnar (e. Service (trade) name): (viðskipta-)heiti viðkomandi vottunarþjónustu.
- Stafrænt auðkenni þjónustunnar (e. Service digital identity): Ótvírætt, einkvæmt auðkenni vottunarþjónustunnar.
- Núverandi staða þjónustunnar (e. Service current status): Auðkenni fyrir núverandi stöðu þjónustunnar.
- Upphafsdagur og -tími núverandi stöðu.
- Viðskeyti þjónustuuplýsinga (e. Service information extension), ef við á: Frekari upplýsingar um þjónustuna (t.d. veittar beint eða með tilvísun í stað þar sem hægt er að hala niður upplýsingum): upplýsingar um skilgreiningu á þjónustunni, veittar af rekstraraðila kerfisins, upplýsingar um aðgang að þjónustunni, upplýsingar um skilgreiningu á þjónustunni, veittar af vottunaraðilanum og viðskeyti þjónustuuplýsinga. T.d. fyrir þjónustu vottunarstöðvar sem gefur út fullgild vottorð (e. CA/QC services) valkvæð runa upplýsingalína (e. tuples of information), þar sem hver lína gefur:
  - viðmiðanir sem nota skal til að auðkenna frekar (sía út), innan viðkomandi traustþjónustu, nákvæmlega þá veittu þjónustu (t.d. fullgild vottorð) þar sem krafist er viðbótarupplýsinga eða þær veittar að því er varðar stöðu þess, stuðning af öruggum undirskriftarbúnaði (SSCD) og/eða útgáfu til handa lögaðila og
  - tengda „sérgreina“ (e. qualifiers) sem veita upplýsingar um hvort vottorð innan veittrar þjónustu séu auðkennd sem fullgild og/eða hvort auðkennd, fullgild vottorð þessarar þjónustu séu studd öruggum undirskriftarbúnaði eður ei og/eða upplýsingar um hvort slík fullgild vottorð séu gefin út til handa lögaðila (þau teljast sjálfkrafa vera gefin út til handa einstaklingum).

5. Eldri upplýsingar um stöðu hverrar skráðrar vottunarþjónustu

6. Tölvuunnin undirskrift til sannvottunar á öllum svæðum áreiðanlegu skrárinnar að undanskildu undirskriftargildinu sjálfu

### 3. Leiðbeiningar um ritstjórn færslna í áreiðanlega listanum

#### 3.1. Stöðuuplýsingar um eftirlitsskylda/faggilta vottunarþjónustu og veitendur hennar í einni skrá

Áreiðanlegur listi aðildarríkis merkir „Listi yfir eftirlits-/faggildingarstöðu vottunarþjónustu af hálfu vottunaraðila, sem aðildarríkið, sem vísað er til, hefur eftirlit með eða veitir faggildingum með tilliti til þess að farið sé að viðeigandi ákvæðum í tilskipun 1999/93/EB“.

Slíkur áreiðanlegur listi er eina tækið sem viðkomandi aðildarríki ber að nota til að veita upplýsingar um eftirlits-/faggildingarstöðu vottunarþjónustu og veitendur hennar:

- **allir vottunaraðilar**, skv. skilgreiningu í 11. mgr. 2. gr. tilskipunar 1999/93/EB, þ.e. „aðili eða lögpersóna eða einstaklingur sem gefur út skilríki eða veitir aðra þjónustu sem tengist rafrænum undirskriftum“,
- **sem eru eftirlitsskyldir/faggiltir** með tilliti til þess að farið sé að viðeigandi ákvæðum í tilskipun 1999/93/EB.

Að því er varðar skilgreiningar og ákvæði sem mælt er fyrir um í tilskipun 1999/93/EB, einkum með tilliti til viðkomandi vottunaraðila og eftirlitskerfa/valfrjálsra faggildingarkerfa þeirra, er greint á milli tvenns konar vottunaraðila, þ.e. vottunaraðila sem gefa út fullgild vottorð almenningi til handa (CSP<sub>QC</sub>) og vottunaraðila sem gefa ekki út fullgild vottorð til almennings, en sem veita „aðra (stöð-)þjónustu í tengslum við rafrænar undirskriftir“:

- **Vottunaraðilar sem gefa út fullgild vottorð:**
  - Þeir verða að sæta eftirliti aðildarríkisins þar sem þeir hafa staðfestu (ef þeir hafa staðfestu í aðildarríki) og geta einnig hlotið faggildingum fyrir að fara að viðeigandi ákvæðum, sem mælt er fyrir um í tilskipun 1999/93/EB, þ.m.t. kröfum I. viðauka (kröfur viðvíkjandi fullgildum vottorðum) og II. viðauka (kröfur viðvíkjandi vottunaraðilum sem gefa út fullgild vottorð). Vottunaraðilar sem gefa út fullgild vottorð og hafa fengið faggildingum í aðildarríki þurfa samt að falla undir viðeigandi eftirlitskerfi þess aðildarríkis, nema þeir hafi ekki staðfestu þar.

- Viðeigandi ,eftirlits'-kerfi (eða ,valfrjálst faggildingar'-kerfi, eftir því sem við á) er skilgreint og þarf að fullnægja viðeigandi kröfum tilskipunar 1999/93/EB, einkum þeim sem mælt er fyrir um í 3. gr. (3. mgr.), 8. gr. (1. mgr.), 11. gr. og 13. forsendu (eða 2. gr. (13. mgr.), 3. gr. (2. mgr.), 7. gr. (a-lið 1. mgr.), 8. gr. (1. mgr.), 11. gr. og 4., 11., 12. og 13. forsendu, eftir því sem við á).
- **Vottunaraðilar sem gefa ekki út fullgild vottorð:**
  - Þeir geta fallið undir ,valfrjálst faggildingarkerfi' (eins og skilgreint er í tilskipun 1999/93/EB og í samræmi við hana) og/eða undir ,viðurkennt samþykktarkerfi' samkvæmt landsbundinni skilgreiningu, sem tekið er upp á landsvísu til eftirlits með því að farið sé að ákvæðunum sem mælt er fyrir um í þeirri tilskipun og hugsanlega að landsbundnum ákvæðum að því er varðar veitingu vottunarþjónustu (í skilningi 11. mgr. 2. gr. tilskipunar 1999/93/EB).
  - Sumir þeirra hlutrænu eða tvíundar- (röklegu) hluta (e. physical or binary (logical) objects) sem verða til eða eru sendir sem afrakstur vottunarþjónustu geta átt rétt á sérstakri ,fullgildingu' (e. qualification) á grundvelli þess að þeir uppfylla ákvæði og kröfur sem mælt er fyrir um á landsvísu, en þýðing slíkrar ,fullgildingar' myndi líklega takmarkast eingöngu við landsstigið.

Semja þarf og viðhalda einum áreiðanlegum lista fyrir hvert aðildarríki, sem tilgreinir eftirlits- og/eða faggildingarstöðu vottunarþjónustu sem þeir vottunaraðilar veita sem eru undir eftirliti/faggiltir af hálfu aðildarríkisins. Áreiðanlegi listinn skal innihalda a.m.k. þá vottunaraðila sem gefa út fullgild vottorð. Áreiðanlegi listinn getur einnig tilgreint stöðu annarrar vottunarþjónustu sem er eftirlitsskyld eða faggilt undir samþykktarkerfi samkvæmt landbundinni skilgreiningu.

### 3.2. *Stakt mengi gilda fyrir eftirlits-/faggildingarstöðu*

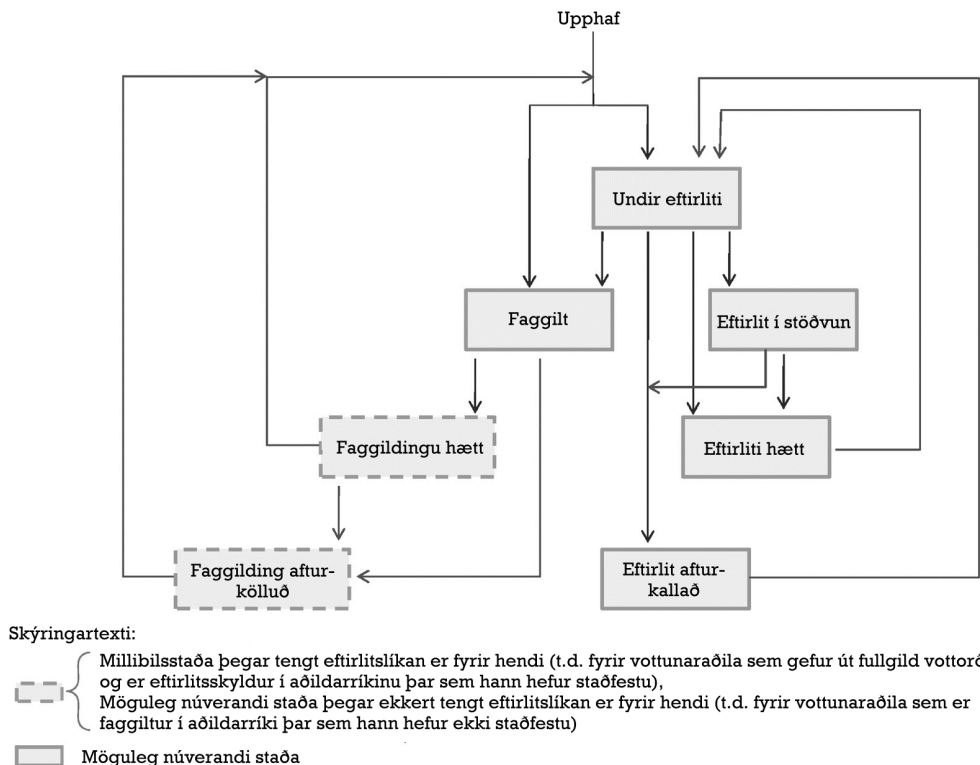
Í áreiðanlega listanum sýnir gildi núverandi stöðu hvort tiltekin þjónusta er nú annaðhvort ,eftirlitsskyld' eða ,faggilt'. Þar að auki getur eftirlits- eða faggildingarstaða verið jákvæð (,undir eftirliti', ,faggilt', ,eftirlit í stöðvun'), hætt (,eftirliti hætt', ,faggildingu hætt') eða jafnvel afturkölluð (,eftirlit afturkallað', ,faggilding afturkölluð') og tilgreind með samsvarandi gildi. Staða sömu vottunarþjónustu getur breyst á líftíma hennar frá því að vera undir eftirliti yfir í að vera faggilt og öfugt<sup>(8)</sup>.

Í mynd 1 hér á eftir er lýst hvernig vænta má að flæði verði milli mögulegrar eftirlits-/faggildingarstöðu fyrir staka þjónustu vottunaraðila:

<sup>(8)</sup> T.d. getur vottunaraðili með staðfestu í aðildarríki sem veitir vottunarþjónustu sem er upphaflega undir eftirliti aðildarríkisins (eftirlitsstofnunar) að nokkrum tíma liðnum ákveðið að gangast undir valfrjálsa faggildingu fyrir vottunarþjónustuna sem nú er undir eftirliti. Á hinn bóginn getur vottunaraðili í öðru aðildarríki ákveðið að hætta ekki með faggilta vottunarþjónustu heldur færa hana úr faggildingarstöðu yfir í eftirlitstöðu, t.d. af viðskiptalegum og/eða fjárhagslegum ástæðum.

Mynd 1

## Flæði sem vænta má milli eftirlits-/faggildingarstöðu fyrir staka þjónustu vottunaraðila



Þegar vottunarþjónusta sem gefur út fullgild vottorð hefur staðfestu í aðildarríki verður hún að sæta eftirliti (aðildarríkisins sem hún hefur staðfestu í) og getur fengið valfrjálsa faggildinguna. Þegar slík þjónusta er skráð í áreiðanlegan lista verður gildið fyrir stöðu hennar að vera eitt af þeim sem sýnt er hér að framan sem „gildi fyrir núverandi stöðu“ í samræmi við raunverulega stöðu hennar og því verður að breyta, eftir því sem við á, í samræmi við stöðufærðir hér að framan. Þó verða bæði „faggilding hætt“ og „faggilding afturkölluð“ að vera gildi fyrir „millibilisstöðu“ þegar samsvarandi þjónusta vottunaraðila sem gefur út fullgild vottorð er tilgreind í áreiðanlegum lista aðildarríkisins þar sem hann hefur staðfestu, þar sem slík þjónusta verður sjálfkrafa að vera undir eftirliti (jafnvel þegar hún er ekki eða ekki lengur faggilt). Þessi gildi geta verið endanleg gildi þegar samsvarandi þjónusta er skráð (faggilt) í öðru aðildarríki en því sem hún hefur staðfestu í.

Aðildarríki, sem koma á fót eða hafa komið á fót „viðurkenndu samþykktarkerfi/-kerfum“ samkvæmt landsbundinni skilgreiningu, sem tekið er upp á landsvisu til eftirlits með því að þjónusta vottunaraðila, sem gefa *ekki* út fullgild vottorð, samrýmist ákvæðunum sem mælt er fyrir um í tilskipun 1999/93/EB og mögulegum landsbundnum ákvæðum að því er varðar veitingu vottunarþjónustu (í skilningi 11. mgr. 2. gr. tilskipunar 1999/93/EB), verða að flokka slík samþykktarkerfi í eftirfarandi tvo flokka:

— „valfrjáls faggilding“ í samræmi við skilgreiningu og ákvæði tilskipunar 1999/93/EB (2. gr. (13. mgr.), 3. gr. (2. mgr.), 7. gr. (a-liður 1. mgr.), 8. gr. (1. mgr.), 11. gr. og 4., 11., 12. og 13. forsendu),

— „eftirlit“ eins og krafist er í tilskipun 1999/93/EB og framkvæmt með ákvæðum landslaga og kröfum í samræmi við landslög.

Samkvæmt því getur vottunarþjónusta sem gefur ekki út fullgild vottorð verið undir eftirliti eða haft valfrjálsa faggildinguna. Þegar slík þjónusta er skráð í áreiðanlegan lista verður gildið fyrir stöðu hennar að vera eitt af þeim sem sýnt er hér að framan sem „gildi fyrir núverandi stöðu“ (sjá mynd 1) í samræmi við raunverulega stöðu hennar og því verður að breyta, eftir því sem við á, í samræmi við stöðufærðir hér að framan.

Áreiðanlegi listinn verður að innihalda upplýsingar um undirliggjandi eftirlits-/faggildingarkerfi, einkum:



- upplýsingar um eftirlitskerfið sem gildir um hvern og einn vottunaraðila sem gefur út fullgild vottorð,
- upplýsingar, ef við á, um landsbundna ‚valfrjálsa faggildingarkerfið‘, sem gildir um hvern og einn vottunaraðila sem gefur út fullgild vottorð,
- upplýsingar, ef við á, um eftirlitskerfið sem gildir um hvern og einn vottunaraðila sem gefur ekki út fullgild vottorð,
- upplýsingar, ef við á, um landsbundna ‚valfrjálsa faggildingarkerfið‘, sem gildir um hvern og einn vottunaraðila sem gefur ekki út fullgild vottorð.

Tvö síðustu upplýsingamengin hafa afgerandi þýðingu til að treystendur (e. relying parties) geti metið gæða- og öryggisstig slíkra eftirlits-/faggildingarkerfa sem gilda á landsvísi um vottunaraðila sem gefa ekki út fullgild vottorð. Þegar upplýsingar um eftirlits-/faggildingarstöðu eru veittar í áreiðanlega listanum að því er varðar þjónustu vottunaraðila sem gefa ekki út fullgild vottorð skal veita framangreindar upplýsingar á vettvangi áreiðanlega listans með því að nota ‚Scheme information URI‘ (liður 5.3.7 — upplýsingar sem aðildarríkin veita), ‚Scheme type/community/rules‘ (liður 5.3.9 — með því að nota texta sem er sameiginlegur fyrir öll aðildarríki og valkvæðar sértækar upplýsingar sem aðildarríki veitir) og ‚TSL policy/legal notice‘ (liður 5.3.11 — texti sem er sameiginlegur fyrir öll aðildarríki og vísar í tilskipun 1999/93/EB auk þess sem hvert aðildarríki getur bætt við texta/tilvísunum sem eru sértækar fyrir það ríki).

Frekari ‚fullgildingar‘-upplýsingar (e. ‚qualification‘ information) sem eru skilgreindar á vettvangi landsbundinna eftirlits-/faggildingarkerfa fyrir vottunaraðila sem gefa ekki út fullgild vottorð má veita á þjónustustiginu þegar við á og þörf er á (t.d. til að greina á milli nokkurra mismunandi gæða-/öryggisstiga) með því að nota ‚additionalServiceInformation Extension‘ (liður 5.5.9.4) sem hluta af ‚Service information extensions‘ (liður 5.5.9). Frekari upplýsingar um samsvarandi tækniforskriftir er að finna í ítarlegu forskriftunum í I. kafla.

Enda þótt aðskildar stofnanir aðildarríkis geti haft með höndum eftirlit og faggilding vottunarþjónustu í því aðildarríki er gert ráð fyrir aðeins einni færslu fyrir hverja einstaka vottunarþjónustu og að eftirlits-/faggildingarstaða hennar sé uppfærð í samræmi við það.

### 3.3. Færslur í áreiðanlega listanum sem miða að því að auðvelda staðfestingu á fullgildum rafrænum undirskriftum (QES) og útfærðum rafrænum undirskriftum sem studdar eru fullgildu vottorði (AdES<sub>QC</sub>)

Mikilvægasti þátturinn í gerð áreiðanlegs lista er að setja saman skyldubundinn hluta hans, þ.e. ‚skrá yfir þjónustu‘ (‚List of services‘) fyrir hvern vottunaraðila sem gefur út fullgild vottorð, svo að hún endurspegli nákvæma stöðu hverrar vottunarþjónustu, sem gefur út fullgild vottorð, á réttan hátt og til að tryggja að upplýsingarnar sem veittar eru í hverri færslu séu fullnægjandi til að auðvelda staðfestingu á fullgildum rafrænum undirskriftum (QES) og útfærðum rafrænum undirskriftum sem eru studdar fullgildu vottorði (AdES<sub>QC</sub>) (þegar þær tengjast innihaldi fullgildra endaskilríkja sem vottunaraðilinn gefur út innan ramma vottunarþjónustunnar sem er tilgreind í þessari færslu).

Á meðal upplýsinganna sem krafist er geta verið aðrar upplýsingar en stafrænt auðkenni þjónustu (‚Service digital identity‘) stakrar (rótár-)vottunarstöðvar, einkum upplýsingar sem sýna fullgildingarstöðu (e. QC status) vottorða sem slík vottunarstöð gefur út og hvort studdar undirskriftir eru gerðar með öruggum undirskriftarbúnaði eður ei. Sú stofnun í aðildarríki, sem er tilnefnd til að semja, ritstýra og viðhalda áreiðanlega listanum, verður því að taka tillit til núverandi lýsingar (e. profile) og innihalds hvers útgefins fullgilds vottorðs fyrir hvern einstakan vottunaraðila sem gefur út fullgild vottorð, sem áreiðanlega skráin tekur til.

Helst ætti hvert útgefið fullgilt vottorð að innihalda QcCompliance-yfirlýsingu samkvæmt skilgreiningu ETSI <sup>(9)</sup> þegar fullyrt er að um fullgilt vottorð sé að ræða og QcSSCD-yfirlýsingu samkvæmt skilgreiningu ETSI þegar fullyrt er að það sé stutt af öruggum undirskriftarbúnaði til að mynda rafrænar undirskriftir og/eða að hvert útgefið fullgilt vottorð innihaldi eitt af kennimörkum viðfangs (OIDs) fyrir QCP/QCP+ vottunarstefnur (e. QCP/QCP+ certificate policy Object Identifiers (OIDs)) samkvæmt skilgreiningu í ETSI EN 319 411-2 <sup>(10)</sup>. Vottunaraðilar sem gefa út fullgild vottorð nota mismunandi staðla sem viðmiðun, túlkun þessara staðla er mismunandi og það skortir vitund um tilvist og forgang ýmissa staðlaðra tækniforskrifta eða staðla og þetta hefur leitt af sér að mismunur er á raunverulegu innihaldi fullgildra vottorða sem nú eru gefin út (t.d. hvort þessar Qc-yfirlýsingar, sem ETSI hefur skilgreint, eru notaðar eða ekki) og hindrar þar af leiðandi að viðtakendur geti einfaldlega treyst vottorði undirritunaraðila (og tengdri keðju/slóð) og þannig lagt mat á, a.m.k. með tölvulesanlegum aðferðum, hvort staðhæft er að vottorðið sem styður rafræna undirskrift sé fullgilt vottorð eður ei og hvort það er tengt öruggum undirskriftarbúnaði sem rafræna undirskriftin var gerð með.

<sup>(9)</sup> Sjá ETSI EN 319 412-5 (Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile) varðandi skilgreiningu á slíkri yfirlýsingu.

<sup>(10)</sup> ETSI EN 319 411-2 — Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.



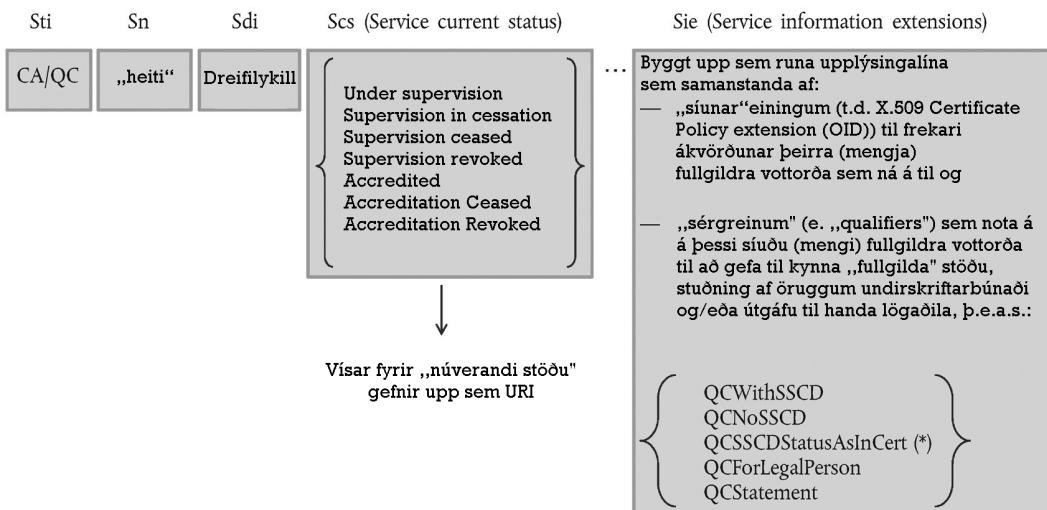
Með því að fylla út svæðin „Service type identifier“ („Sti“), „Service name“ („Sn“) og „Service digital identity“ („Sdi“) í færslunni fyrir þjónustuna í áreiðanlega listanum með upplýsingum sem veittar eru á svæðinu „Service information extensions“ („Sie“) er hægt að ákvarða fyllilega hvern gerðar fullgilt vottorð er, sem er gefið út af vottunarbýðingunni skráðs vottunaraðila sem gefur út fullgild vottorð, og veita upplýsingar um hvort það sé stutt af öryggum undirskriftarbúnaði (þegar þessar upplýsingar koma ekki fram í útgefna fullgilda vottorðinu). Sérstakar upplýsingar, „Service current status“ („Scs“), tengjast þessari færslu. Þetta er sýnt á mynd 2 hér á eftir.

Ef þjónusta væri skráð einungis með stafrænu auðkenni þjónustu („Sdi“) (rótar-)vottunarstöðvar þýddi það að tryggð væri (af hálfu vottunaraðilans sem gefur út fullgild vottorð, en einnig af hálfu eftirlits-/faggildingarstofnunarinnar sem sér um eftirlit/faggildingu þessa vottunaraðila) að sérhver endaskilríki sem eru gefin út innan (stígveldis) þessarar (rótar-)vottunarstöðvar innihaldi nægar upplýsingar, skilgreindar af ETSI og á tölvutæku formi, til að meta hvort um fullgilt vottorð er að ræða og hvort það er stutt af öryggum undirskriftarbúnaði eður ei. Ef síðarnefnda fullyrðingin er t.d. ekki rétt (t.d. ef ekki er nein vísbending á tölvutæku formi samkvæmt ETSI-staðli í fullgilda vottorðinu um hvort það sé stutt af öryggum undirskriftarbúnaði) er einungis hægt að álykta að fullgild vottorð, sem eru gefin út innan þessa stígveldis (rótar-)vottunarstöðvar séu ekki studd af öryggum undirskriftarbúnaði, ef aðeins „Sdi“ viðkomandi (rótar-)vottunarstöðvar er skráð. Til að gefa til kynna að líta verði svo á að þessi fullgildu vottorð séu studd af öryggum undirskriftarbúnaði ætti að nota „Sie“-svæðið (þetta gefur einnig til kynna að upplýsingarnar séu tryggðar af vottunaraðilanum sem gefur út fullgild vottorð og undir eftirliti/faggiltar af eftirlits- eða faggildingarstofnuninni, eftir því sem við á).

### Mynd 2

#### Þjónustufærsla í áreiðanlega listanum um þjónustu skráðs vottunaraðila sem gefur út fullgild vottorð Almennar meginreglur — reglur um ritstjórn — færslur um vottunaraðila sem gefa út fullgild vottorð (skráð þjónusta)

Þjónustufærsla um skráðan vottunaraðila sem gefur út fullgild vottorð:



(\*) merkir að tryggð sé að sérhvert fullgilt vottorð innihaldi slíkar upplýsingar í Sdi-[Sie]-skilgreiningu vottunarstöðvar sem gefur út fullgild vottorð (CA/QC) (ef ekkert er skráð á svæðið fyrir fullgilt vottorð (QC) merkir það að ekki sé um öryggan undirskriftarbúnað að ræða (NoSSCD))

Þessar tækniforskriftir fyrir sameiginlegt sniðmát fyrir áreiðanlega listann gera mögulegt að nota samsetningu fimm meginþátta upplýsinga í þjónustufærslunni:

— „Service type identifier“ („Sti“), sem t.d. auðkennir vottunarstöð sem gefur út fullgild vottorð („CA/QC“).

— „Service name“ („Sn“).

— „Service digital identity“ („Sdi“)-upplýsingar, sem auðkenna skráða þjónustu, t.d. (að lágmarki) dreifilykill vottunarstöðvar sem gefur út fullgild vottorð.

- Að því er varðar þjónustu vottunarstöðva sem gefa út fullgild vottorð (CA/QC), valkvæðar ‚Service information extension‘ (‚Sie‘)-upplýsingar sem gera kleift að bæta inn ýmsum sértekum, þjónustutengdum upplýsingaþáttum sem varða afturköllunarstöðu útrunninna vottorða, viðbótareinkenni fullgildra vottorða, yfirtöku vottunaraðila af hálfu annars vottunaraðila og aðrar þjónustuupplýsingar til viðbótar. Sem dæmi eru viðbótareinkenni fullgildra vottorða táknuð með runu einnar eða fleiri upplýsingalína þar sem hver lína gefur:
  - viðmiðanir sem nota skal til að auðkenna frekar (sía út), undir vottunarþjónustunni sem er auðkennd undir ‚Sdi‘, nákvæmlega það mengi fullgildra vottorða þar sem krafist er viðbótarupplýsinga eða þær veittar að því er varðar stöðu þeirra sem ‚fullgildra‘, stuðning af öruggum undirskriftarbúnaði (SSCD) og/eda útgáfu til handa lögaðila og
  - tengdar upplýsingar (‚ségreina‘) um hvort þetta mengi fullgildra vottorða skuli teljast ‚fullgilt‘, sé stutt af öruggum undirskriftarbúnaði eður ei eða hvort þessar viðbótarupplýsingar eru hluti af fullgilda vottorðinu á stöðluðu tölvutæku formi og/eda upplýsingar sem varða útgáfu slíkra fullgildra vottorða til handa lögaðilum (þau skulu sjálfkrafa aðeins teljast gefin út til handa einstaklingum).
- Upplýsingar um ‚núverandi stöðu‘ fyrir þessa þjónustufærslu þar sem veittar eru upplýsingar um:
  - hvort þjónustan er eftirlitsskyld eða faggilt og
  - eftirlits-/faggildingarstöðuna sjálfa.

### 3.4. Leiðbeiningar um ritstjórn og notkun CSP<sub>QC</sub>-þjónustufærslu

#### Almennar leiðbeiningar um ritstjórn eru:

1. Ef tryggt er, fyrir skráða þjónustu sem er auðkennd með ‚Sdi‘, (með ábyrgð vottunaraðila sem gefur út fullgild vottorð og eftirliti/faggildingunni eftirlits-/faggildingarstofnunar) að fullgild vottorð, sem eru studd af öruggum undirskriftarbúnaði, innihaldi QcCompliance-yfirlýsingu samkvæmt skilgreiningu ETSI og innihaldi QcSSCD-yfirlýsingu og/eda kennimark viðfangs fyrir QCP+ (e. QCP+ Object Identifier (OID)), nægir að viðeigandi ‚Sdi‘ sé notað, en ‚Sie‘-svæðið er valfrjálst og þarf ekki að innihalda upplýsingar um stuðning af öruggum undirskriftarbúnaði.
2. Ef tryggt er, fyrir skráða þjónustu sem er auðkennd með ‚Sdi‘, (með ábyrgð vottunaraðila sem gefur út fullgild vottorð og eftirliti/faggildingunni eftirlits-/faggildingarstofnunar) að fullgild vottorð, sem eru ekki studd af öruggum undirskriftarbúnaði, innihaldi QcCompliance-yfirlýsingu og/eda kennimark viðfangs fyrir fullgildar vottunarkröfur (e. QCP OID) og innihaldi ekki QcSSCD-yfirlýsingu eða kennimark viðfangs fyrir QCP+ (QCP+ OID), nægir að viðeigandi ‚Sdi‘ sé notað, en ‚Sie‘-svæðið er valfrjálst og þarf ekki að innihalda upplýsingar um stuðning af öruggum undirskriftarbúnaði (sem þýðir að það er ekki stutt af öruggum undirskriftarbúnaði).
3. Ef tryggt er, fyrir skráða þjónustu sem er auðkennd með ‚Sdi‘, (með ábyrgð vottunaraðila sem gefur út fullgild vottorð og eftirliti/faggildingunni eftirlits-/faggildingarstofnunar) að fullgild vottorð innihaldi QcCompliance-yfirlýsingu og ætlunin er að sum þessara fullgildu vottorða séu studd af öruggum undirskriftarbúnaði en önnur ekki (þetta má t.d. aðgreina með mismunandi kennimörkum viðfangs fyrir vottunarfærslu, sem er sértekur fyrir tiltekna vottunaraðila, eða með annars konar upplýsingum í fullgilda vottorðinu sem eru sértekur fyrir tiltekna vottunaraðila, beint eða óbeint, hvort heldur er á tölvutæku formi eður ei), en vottorð sem er stutt af öruggum undirskriftarbúnaði inniheldur HVORKI QcSSCD-yfirlýsingu NE QCP(+) OID samkvæmt skilgreiningu ETSI, er hugsanlega ekki nægilegt að viðeigandi ‚Sdi‘ sé notað OG nota verður ‚Sie‘-svæðið til að sýna afdráttarlausar upplýsingar um stuðning af öruggum undirskriftarbúnaði ásamt hugsanlegu upplýsingaviðskeyti til að auðkenna það mengi vottorða sem um er að ræða. Þess vegna er líklegt að færa þurfi inn mismunandi upplýsingagildi fyrir stuðning af öruggum undirskriftarbúnaði (‚SSCD support information values‘) fyrir sama ‚Sdi‘ þegar ‚Sie‘-svæðið er notað.
4. Ef tryggt er, fyrir skráða þjónustu sem er auðkennd með ‚Sdi‘, (með ábyrgð vottunaraðila sem gefur út fullgild vottorð og eftirliti/faggildingunni eftirlits-/faggildingarstofnunar) að fullgild vottorð innihaldi hvorki QcCompliance-yfirlýsingu, kennimark viðfangs fyrir QCP (QCP OID), QcSSCD-yfirlýsingu eða kennimark viðfangs fyrir QCP+ (QCP+ OID), en tryggt er að ætlunin sé að sum þessara endaskilríkja sem eru gefin út undir þessu ‚Sdi‘ eigi að vera fullgild vottorð og/eda studd af öruggum undirskriftarbúnaði en önnur ekki (þetta má t.d. aðgreina með mismunandi kennimörkum viðfangs fyrir vottunarfærslu, sem er sértekur fyrir tiltekna vottunaraðila sem gefa út fullgild vottorð, eða með annars konar upplýsingum í fullgilda vottorðinu sem eru sértekur fyrir tiltekna vottunaraðila sem gefa út fullgild vottorð, beint eða óbeint, hvort heldur er á tölvutæku formi eður ei), þá er ekki nægilegt að viðeigandi ‚Sdi‘ sé notað OG nota verður ‚Sie‘-svæðið til að sýna afdráttarlausar upplýsingar um fullgildingunni. Þess vegna er líklegt að færa þurfi inn mismunandi upplýsingagildi fyrir SSCD-stuðning fyrir sama ‚Sdi‘ þegar ‚Sie‘-svæðið er notað.

Það skal vera almenn meginregla að fyrir skráðan vottunaraðila í áreiðanlega listanum verði að vera ein þjónustufærsla fyrir hvern einstakan dreiflykil fyrir vottunarþjónustu af CA/QC-gerð, þ.e.a.s. fyrir hverja vottunarstöð sem gefur (beint) út fullgild vottorð. Í undantekningartilvikum og við aðstæður sem er vandlega stjórnað getur eftirlits-/faggildingarstofnun

aðildarríkisins ákveðið að nota dreifilykil vottunarstöðvar á rótarstigi eða efra stigi innan dreifilyklaskipulags (PKI) vottunaraðilans sem „Sdi“ stakrar færslu í upptalningu á þjónustu þessa skráða vottunaraðila (t.d. í tengslum við stigveldi vottunarstöðva vottunaraðilans frá rótarvottunarstöð niður í nokkrar vottunarstöðvar sem gefa út vottorð) í stað þess að telja upp allar undirskipaðar vottunarstöðvar sem gefa út skilríki (t.d. tilgreina vottunarstöð sem er ekki beinn útgefandi fullgildra vottorða fyrir endaskilríki heldur vottar stigveldi vottunarstöðva niður í vottunarstöðvar sem gefa út fullgild vottorð til endaaðila). Aðildarríki sem nota slíkan dreifilykil vottunarstöðvar á rótarstigi eða efra stigi sem „Sdi“-gildi í þjónustufærslu í áreiðanlega listanum þurfa að íhuga vandlega afleiðingar þess (kosti og galla). Enn fremur verður aðildarríkið að leggja fram nauðsynleg gögn til að auðvelda gerð vottunarslóðar og sannprófun (e. certification path building and verification) þegar það nýtir sér þessa heimiluðu undantekningu frá almennu meginreglunni. Til dæmis, þegar vottunaraðili, sem gefur út fullgild vottorð, notar eina rótarvottunarstöð og undir henni eru nokkrar vottunarstöðvar sem gefa út bæði fullgild vottorð og vottorð sem eru ekki fullgild, en fullgildu vottorðin innihalda aðeins QcCompliance-yfirlýsinguna og ekki er tilgreint hvort þau séu studd af öruggum undirskriftarbúnaði, myndi það að tilgreina aðeins „Sdi“ rótarvottunarstöðvarinnar þýða, samkvæmt reglunum sem eru útskýrðar hér að framan, að ekkert af fullgildu vottorðunum sem eru gefin út undir þessari rótarvottunarstöð sé stutt af öruggum undirskriftarbúnaði. Ef um er að ræða fullgild vottorð sem eru í raun studd af öruggum undirskriftarbúnaði, en yfirlýsing á tölvutæku formi sem tilgreinir slíkan stuðning er ekki felld inn í vottorðin, er sterklega mælt með því að nota QcSSCD-yfirlýsinguna í fullgild vottorð sem gefin eru út framvegis. Í millitíðinni (þar til síðasta fullgilda vottorðið sem inniheldur ekki þessar upplýsingar er útrunnið) ætti að nota „Sie“-svæðið og tengt „Qualifications Extension“-svæði í áreiðanlega listanum, t.d. til að láta í té siunarupplýsingar til að auðkenna mengi vottorða með því að nota sérstök kennimörk viðfangs, skilgreind af vottunaraðila sem gefur út fullgild vottorð, sem eru hugsanlega notuð af vottunaraðila sem gefur út fullgild vottorð til að greina á milli mismunandi gerða fullgildra vottorða (sem sum eru studd af öruggum undirskriftarbúnaði og sum ekki) og tengja afráttarlausar upplýsingar um stuðning af öruggum undirskriftarbúnaði við þessi auðkenndu (síuðu) mengi vottorða með notkun „sérgreina“.

*Almennar leiðbeiningar um notkun* hugbúnaðar, þjónustu eða vara fyrir rafrænar undirskriftir, sem byggjast á áreiðanlegum lista í samræmi við þessar tækniforskriftir, eru sem hér segir:

„Sti“-færsla fyrir vottunarstöð sem gefur út fullgild vottorð („CA/QC“) (sömuleiðis CA/QC-færsla sem að auki flokkast sem „rótar-CA/QC“ með því að nota „Sie“- „additionalServiceInformation Extension“)

- Þýðir að öll útgefin endaskilríki frá vottunarstöð sem er auðkennd með „Sdi“ (sömuleiðis innan stigveldis vottunarstöðva þar sem byrjað er á rótarvottunarstöð sem er auðkennd með „Sdi“) eru fullgild vottorð, *ad því tilskildu* að staðhæft sé í vottorðinu að svo sé með því að nota viðeigandi Qc-yfirlýsingu á tölvutæku formi (þ.e. QcCompliance-yfirlýsingu) og/eða kennimark viðfangs fyrir QCP(+) samkvæmt skilgreiningu ETSI (og þetta er tryggt af eftirlits-/faggildingarstofnun, sjá hér að framan undir „Almennar leiðbeiningar um ritstjórn“)

*Aths:* ef engar „Sie“, „Qualifications Extension“-upplýsingar eru til staðar eða ef endaskilríki, sem staðhæft er að sé fullgilt vottorð, er ekki auðkennt frekar með hjálp tengdrar „Sie“, „Qualifications Extension“ skulu tölvutæku upplýsingarnar í fullgilda vottorðinu sæta eftirliti/faggildingu með tilliti til nákvæmni þeirra. Það merkir að tryggt sé að notkun (eða ekki notkun) viðeigandi Qc-yfirlýsinga (þ.e. QcCompliance, QcSSCD) og/eða kennimarks viðfangs fyrir QCP(+) samkvæmt skilgreiningu ETSI sé í samræmi við staðhæfingu vottunaraðila sem gefur út fullgild vottorð,

- **og EF** „Sie“, „Qualifications Extension“-upplýsingar eru fyrir hendi, verður, til viðbótar við ofangreinda almenna túlkunarreglu, að skoða þau vottorð sem eru auðkennd með notkun þessara „Sie“, „Qualifications Extension“-upplýsinga, sem byggjast á meginreglunni um röð af síum til frekari auðkenningar á mengi vottorða, með tilliti til tengdra sérgreina sem veita viðbótarupplýsingar um fullgilda stöðu, „SSCD-stuðning“ og/eða „lögaðila sem vottorðshafa“ (t.d. þau vottorð sem innihalda sérstakt kennimark viðfangs í viðskeyti vottunarstefunnar og/eða hafa sértækt „lykilnotkunar“ mynstur og/eða eru síuð með því að nota sértækt gildi sem kemur fram í einu tilteknu svæði vottorðs eða viðskeyti o.s.frv.). Þessir sérgreinar eru hluti af eftirfarandi mengi „sérgreina“ sem notaðir eru til að bæta upp skort á upplýsingum í samsvarandi innihaldi fullgildra vottorða og sem eru notaðir:

- til að tilgreina fullgilda stöðu: „QCStatement“ sem merkir að auðkennd vottorð, eitt eða fleiri, séu fullgild,

OG/EDA

- til að tilgreina hvers eðlis stuðningur af öruggum undirskriftarbúnaði er:

- „QCWithSSCD“-sérgreinisgildið merkir „fullgilt vottorð stutt af öruggum undirskriftarbúnaði“ eða

- „QCNoSSCD“-sérgreinisgildið merkir „fullgilt vottorð, ekki stutt af öruggum undirskriftarbúnaði“ eða

- „QCSSCDStatusAsInCert“-sérgreinisgildið merkir að tryggt sé að upplýsingar um stuðning af öruggum undirskriftarbúnaði séu fyrir hendi í sérhverju fullgildu vottorði undir „Sdi“- „Sie“-upplýsingum þessara CA/QC-færslu,

OG/EDA

- til að tilgreina að vottorðið sé gefið út til handa lögaðila:
- ‚QCForLegalPerson‘-sérgræinisgildið merkir ‚vottorð gefið út til handa lögaðila‘.

3.5. Þjónusta sem styður við þjónustu vottunarstöðva sem gefa út fullgild vottorð (‚CA/QC‘) en er ekki hluti af ‚Sdi‘ vottunarstöðvar sem gefur út fullgild vottorð

Þjónusta í tengslum við gildisstöðu vottorða (e. certificate validity status services) í sambandi við fullgild vottorð og þar sem upplýsingar um gildi vottorða (t.d. afturköllunarlistar (CRLs) og svör þegar notaður er samskiptaháttur til að kalla eftir upplýsingum um stöðu vottorða yfir nettengingar (OCSP responses)) eru undirritaðar af aðila sem hefur einkalykil sem er ekki vottaður á vottunarslóð sem leiðir að skráðri vottunarstöð sem gefur út fullgild vottorð (‚CA/QC‘) skal tekin með í áreiðanlega listann með því að skrá þessa þjónustu í tengslum við gildisstöðu vottorða sem slíka í áreiðanlega listanum (t.d. sem ýmist þjónustutegund ‚OCSP/QC‘ eða ‚CRL/QC‘) þar sem líta má á þessa þjónustu sem hluta af eftirlitsskyldu/faggiltu ‚fullgildu‘ þjónustunni í tengslum við veitingu vottunarþjónustu vegna fullgildra vottorða. Að sjálfsgöðu ber að líta svo á að OCSP-svarendur eða útgefendur afturköllunarlista séu ‚gildir‘ og í samræmi við gildi stöðu skráðu CA/QC-þjónustunnar þegar vottorð þeirra eru undirrituð af vottunarstöðvum sem falla undir stigveldi skráðu CA/QC-þjónustunnar.

Svipað ákvæði getur gilt um vottunarþjónustu sem gefur út vottorð sem eru ekki fullgild (‚CA/PKC‘-þjónustutegund).

Þjónusta í tengslum við gildisstöðu vottorða skal tilgreina í áreiðanlega listanum þegar tilheyrandi upplýsingar um staðsetningu slíkrar þjónustu eru ekki fyrir hendi í endaskilríkjunum sem þjónustan í tengslum við gildisstöðu vottorða tekur til.

#### 4. Skilgreiningar og skammstafanir

Í þessu skjali gilda eftirfarandi skilgreiningar og upphafsstaforð:

| Heiti   | Upphafsstafaforð  | Skilgreining  |
|---|-------------------|---|
| Vottunaraðili (Certification Service Provider)  | CSP               | Eins og skilgreint er í 11. mgr. 2. gr. tilskipunar 1999/93/EB.   |
| Vottunarstöð (Certification Authority)  | CA                | 1) vottunaraðili sem býr til og úthlutar dreifilyklaskilríkjum eða<br>2) tækniþjónusta við gerð vottorða sem er notuð af vottunaraðila sem býr til og úthlutar dreifilyklaskilríkjum.<br><i>ATHS:</i> Frekari útskýringar á hugtakinu vottunarstöð er að finna í lið 4 í EN 319 411-2 <sup>(1)</sup> .  |
| Vottunarstöð sem gefur út fullgild vottorð (Certification Authority issuing Qualified Certificates) | CA/QC             | Vottunarstöð sem fullnægir þeim kröfum sem mælt er fyrir um í II. viðauka við tilskipun 1999/93/EB og gefur út fullgild vottorð sem fullnægja kröfum sem mælt er fyrir um í I. viðauka við tilskipun 1999/93/EB.  |
| Vottorð (Certificate)   | Vottorð           | Eins og skilgreint er í 9. mgr. 2. gr. tilskipunar 1999/93/EB.  |
| Fullgild vottorð (Qualified Certificate)  | QC                | Eins og skilgreint er í 10. mgr. 2. gr. tilskipunar 1999/93/EB.   |
| Undirritunaraðili (Signatory)   | Undirritunaraðili | Eins og skilgreint er í 3. mgr. 2. gr. tilskipunar 1999/93/EB.  |
| Eftirlit (Supervision)  | Eftirlit          | Vísar til eftirlits sem kveðið er á um í 3. mgr. 3. gr. tilskipunar 1999/93/EB. Samkvæmt tilskipun 1999/93/EB er aðildarríkjum skylt að koma á fót viðeigandi kerfi til að unnt sé að hafa eftirlit með vottunaraðilum sem hafa staðfestu á yfirráðasvæði þeirra og gefa út viðurkennd skilríki almenningi til handa, til að tryggja eftirlit með því að farið sé að ákvæðum sem mælt er fyrir um í þeirri tilskipun. |
| Valfrjáls faggilding (Voluntary Accreditation)  | Faggilding        | Eins og skilgreint er í 13. mgr. 2. gr. tilskipunar 1999/93/EB.   |
| Áreiðanlegur listi (Trusted List)   | TL                | Táknar skrána sem sýnir eftirlits-/faggildingarstöðu vottunarþjónustu vottunaraðila, sem aðildarríkið, sem vísað er til, hefur eftirlit með/veitir faggildingum með tilliti til þess að farið sé að ákvæðum sem mælt er fyrir um í tilskipun 1999/93/EB.  |

| Heiti  | Upphafsstafaorð    | Skilgreining   |
|--|--------------------|--|
| Stöðuskrá traustþjónustu (Trust-service Status List)   | TSL                | Tegund undirritaðrar skrár sem notuð er sem grunnur fyrir framsetningu á upplýsingum um stöðu traustþjónustu í samræmi við forskriftir sem settar eru fram í ETSI TS 119 612.  |
| Traustþjónusta (Trust Service)   |                    | Þjónusta sem eykur tiltrú og traust á rafrænum viðskiptum (felur venjulega, en ekki nauðsynlega, í sér notkun dulkóðunartækni eða meðferð trúnaðarupplýsinga) (ETSI TS 119 612).<br><i>ATHS:</i> Þetta hugtak er notað í víðari merkingu en vottunarþjónusta sem gefur út vottorð eða veitir aðra þjónustu í tengslum við rafrænar undirskriftir.        |
| Veitandi traustþjónustu (Trust Service Provider)   | TSP                | Aðili sem starfrækir eina eða fleiri tegundir (rafrænnar) traustþjónustu (þetta hugtak er notað í víðari merkingu en vottunaraðili).   |
| Tóki fyrir traustþjónustu (Trust Service Token)  | TrST               | Hlutrænn eða tviundar- (röklegur) hlutur, sem verður til eða er sendur sem afrakstur traustþjónustu. Dæmi um tviundartóka fyrir traustþjónustu (e. binary TrSTs) eru vottorð, afturköllunarlistar (CRLs), tímastimplunartókar (TSTs) og svör þegar notaður er samskiptaháttur til að kalla eftir upplýsingum um stöðu vottorða yfir nettengingar (OCSP). |
| Fullgild rafræn undirskrift (Qualified Electronic Signature)   | QES                | Útfærð rafræn undirskrift sem studd er fullgildu vottorði og er gerð með öruggum undirskriftarbúnaði eins og skilgreint er í 2. gr. tilskipunar 1999/93/EB.  |
| Útfærð rafræn undirskrift (Advanced Electronic Signature)  | AdES               | Eins og skilgreint er í 2. mgr. 2. gr. tilskipunar 1999/93/EB.   |
| Útfærð rafræn undirskrift sem studd er fullgildu vottorði (Advanced Electronic Signature supported by a Qualified Certificate) | AdES <sub>QC</sub> | Merkir rafræna undirskrift sem fullnægir kröfum um útfærða rafræna undirskrift og er studd fullgildu vottorði eins og skilgreint er í 2. gr. tilskipunar 1999/93/EB.   |
| Öruggur undirskriftarbúnaður (Secure Signature Creation Device)  | SSCD               | Eins og skilgreint er í 6. mgr. 2. gr. tilskipunar 1999/93/EB.   |

(<sup>1</sup>) EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

Í eftirfarandi köflum skulu eftirfarandi lykilorð túlkuð eins og lýst er í RFC 2119 (<sup>11</sup>): ‚VERÐUR‘ (MUST), ‚MÁ EKKI‘ (MUST NOT), ‚SKYLDUBUNDIÐ‘ (REQUIRED), ‚SKAL‘ (SHALL), ‚SKAL EKKI‘ (SHALL NOT), ‚ÆTTI‘ (SHOULD), ‚ÆTTI EKKI‘ (SHOULD NOT), ‚MÆLT MEÐ‘ (RECOMMENDED), ‚MÁ‘ (MAY), og ‚VALKVÆTT‘ (OPTIONAL).

## I. KAFLI

### ÍTARLEGAR FORSKRIFTIR FYRIR SAMEIGINLEGT SNIÐMÁT FYRIR ‚ÁREIÐANLEGAN LISTA YFIR EFTIRLITSSKYLDA/FAGGILTA VOTTUNARAÐILA‘

Forskriftir þessar byggjast á forskriftunum og kröfunum sem tilgreindar eru í tækniforskriftum Fjarskiptastaðlastofnunar Evrópu ETSI TS 119 612 v1.1.1. (hér á eftir nefndar ETSI TS 119 612).

Ef engar sértækar kröfur eru tilgreindar í þessum forskriftum SKULU kröfurnar í 5. og 6. lið ETSI TS 119 612 gilda í heild sinni. Ef sértækar kröfur eru tilgreindar í þessum forskriftum SKULU þær ganga frammar samsvarandi kröfum í ETSI TS 119 612. Komi misræmi í ljós milli forskrifa þessara og forskriftanna í ETSI TS 119 612 SKAL fara að núverandi forskriftum.

#### Scheme operator name (liður 5.3.4)

Þetta svæði SKAL vera til staðar og SKAL vera í samræmi við forskriftirnar í lið 5.3.4. í TS 119 612.

(<sup>11</sup>) IETF RFC 2119: „Key words for use in RFCs to indicate Requirements Levels“

Land MÁ hafa aðskildar stofnanir fyrir eftirlit og faggildingu og jafnvel fleiri stofnanir fyrir annars konar rekstrartengda starfsemi. Það er á ábyrgð hvers aðildarríkis að tilnefna rekstraraðila kerfisins (e. Scheme operator) fyrir áreiðanlegan lista aðildarríkisins. Gert er ráð fyrir því að eftirlitsstofnunin, faggildingarstofnunin og rekstraraðili kerfisins (þegar þeir eru aðskildir aðilar) hafi sín eigin ábyrgðarsvið og skuldbindingar.

Hverjar þær aðstæður þar sem fleiri en einn aðili ber ábyrgð á þáttum sem snerta eftirlit, faggildingu eða rekstur SKULU endurspeglast með samræmdum hætti og vera auðkenndar sem slíkar í upplýsingunum um kerfið (e. Scheme information), sem eru hluti af áreiðanlega listanum, þ.m.t. í upplýsingum sem eru sértækar fyrir kerfið og er að finna í ‚Scheme information URI‘ (liður 5.3.7).

#### **Scheme name** (liður 5.3.6)

Þetta svæði SKAL vera til staðar og SKAL vera í samræmi við forskriftirnar í lið 5.3.6 í TS 119 612 þar sem nota SKAL eftirfarandi heiti fyrir kerfið:

‘EN\_name\_value’ = ‘Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Scheme Operator’s Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.’

#### **Scheme information URI** (liður 5.3.7)

Þetta svæði SKAL vera til staðar og SKAL vera í samræmi við forskriftirnar í lið 5.3.7 í TS 119 612 þar sem ‚viðeigandi upplýsingar um kerfið‘ SKULU innihalda að lágmarki:

- Inngangsupplýsingar sem eru sameiginlegar fyrir öll aðildarríki að því er varðar gildissvið og samhengi áreiðanlega listans og undirliggjandi eftirlits-/faggildingarkerfi. Sameiginlegi textinn sem nota skal er sá sem fer hér á eftir, þar sem heiti viðkomandi aðildarríkis SKAL koma í stað stafastrengsins ‚*[name of the relevant Member State]*‘:

„The present list is the ‘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,
- allowing for a trusted validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)), including, when this is not part of the QCs, 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 compliance 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 Article 3(3), Article 8(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 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 at a national level on a voluntary basis.“



- Sértekur upplýsingar um undirliggjandi eftirlits-/faggildingarkerfi, einkum <sup>(12)</sup>:
    - upplýsingar um eftirlitskerfið sem gildir um hvern og einn vottunaraðila sem gefur út fullgild vottorð,
    - upplýsingar, ef við á, um landsbundna valfrjálsa faggildingarkerfið sem gildir um hvern og einn vottunaraðila sem gefur út fullgild vottorð,
    - upplýsingar, ef við á, um eftirlitskerfið sem gildir um hvern og einn vottunaraðila sem gefur ekki út fullgild vottorð,
    - upplýsingar, eftir því sem við á, um landsbundna valfrjálsa faggildingarkerfið, sem gildir um hvern og einn vottunaraðila sem gefur ekki út fullgild vottorð.
- Eftirfarandi SKAL a.m.k. vera í þessum sérteknu upplýsingum fyrir hvert undirliggjandi kerfi sem er talið upp hér að framan:
- almenn lýsing,
  - upplýsingar um ferlið sem eftirlits-/faggildingarstofnunin fylgir við eftirlit sitt/faggildingu og sem vottunaraðilar fylgja vegna eftirlitsskyldu sinnar/faggildingar,
  - upplýsingar um viðmiðanir sem notaðar eru við eftirlit með/faggildingu vottunaraðila.
- Ef við á, sérstakar upplýsingar um sérstakar ‚fullgildingar‘ sem sumir þeirra hlutrænu eða tviundar- (röklegu) hluta, sem til verða eða eru sendir sem afrakstur vottunarþjónustu, eiga rétt á að fá á grundvelli þess að þau uppfylla ákvæði og kröfur sem mælt er fyrir um á landsvisu, þ.m.t. merking slíkrar ‚fullgildingar‘ og tengd ákvæði landslaga og kröfur.

Veita MÁ valkvæðar viðbótarupplýsingar um kerfið, sem eru sértekur fyrir aðildarríkið, s.s.:

- upplýsingar um viðmiðanir og reglur sem eru notaðar við val á eftirlits-/úttektaraðilum og til að skilgreina hvernig þeir hafa eftirlit með (fylgjast með)/faggilda (taka út) vottunaraðila,
- aðrar samskiptaupplýsingar og almennar upplýsingar sem varða starfrækslu kerfisins.

#### **Scheme type/community/rules** (liður 5.3.9)

Þetta svæði SKAL vera til staðar og SKAL vera í samræmi við forskriftirnar í lið 5.3.9. í TS 119 612 og SKAL innihalda a.m.k. tvö vefböng (URIs):

- sameiginlegt veffang fyrir áreiðanlega lista allra aðildarríkja, sem vísar á lýsandi texta sem SKAL gilda um alla áreiðanlega lista, sem hér segir:

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

Lýsandi texti:

*„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 implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State’s Trusted List, compiled by the European Commission.

*Policy/rules for the assessment of the listed services*

The Trusted List of a Member State must provide, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 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.

<sup>(12)</sup> Tvö síðustu upplýsingamengin hafa afgerandi þýðingu til að treystendur geti metið gæða- og öryggisstig slíkra eftirlits-/faggildingarkerfa sem gilda um vottunaraðila sem gefa ekki út fullgild vottorð. Veita skal þessi upplýsingamengi á vettvangi áreiðanlega listans með því að nota fyrirliðgjandi ‚Scheme information URI‘ (liður 5.3.7 — upplýsingar sem aðildarríkin veita), ‚Scheme type/community/rules‘ (liður 5.3.9 — með því að nota texta sem er sameiginlegur fyrir öll aðildarríkin) og ‚TSL policy/legal notice‘ (liður 5.3.11 — texti sem er sameiginlegur fyrir öll aðildarríki og vísar í tilskipun 1999/93/EB, jafnframt því sem hvert aðildarríki getur bætt við texta/tilvísunum sem eru sértekur fyrir það ríki). Frekari upplýsingar um landsbundin eftirlits-/faggildingarkerfi fyrir vottunaraðila sem gefa ekki út fullgild vottorð má veita á þjónustustiginu þegar við á og þörf er á (t.d. til að greina á milli nokkurra mismunandi gæða- eða öryggisstiga) með því að nota ‚Scheme service definition URI‘ (liður 5.5.6).



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 compliance 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 Article 3(3), Article 8(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 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 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 Article 2(11) of Directive 1999/93/EC). 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 Trusted List*

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

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

- indicates that from the 'Service digital identifier' ('Sdi') identified CA (similarly within the CA hierarchy starting from the 'Sdi' identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) *provided* that it is claimed as such in the certificate through the use of appropriate EN 319 412-5 defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or EN 319 411-2 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

*Note:* if no 'Sie' 'Qualifications Extension' information is present or if an end-entity certificate that is claimed to be a QC is not further identified through a related 'Sie' 'Qualifications Extension' information, 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. QcCompliance, QcSSCD, etc.) 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' 'Qualifications Extension' information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this 'Sie' 'Qualifications Extension' information, 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 the qualified status, the '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 qualified status: 'QCStatement' meaning the identified certificate(s) is(are) qualified,

AND/OR

- 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 ‘Ses’ 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 Member States’ Trusted Lists.“

- sértækt veffang fyrir áreiðanlegan lista hvers aðildarríkis, sem vísar á lýsandi texta sem SKAL gilda um áreiðanlegan lista þessa aðildarríkis:

<http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC> þar sem CC = ISO 3166-1 <sup>(13)</sup> alpha-2 landskóðinn sem notaður er í ‚Scheme territory’-svæðinu (liður 5.3.10)

- þar sem notendur geta nálgast sértæka stefnu/reglur aðildarríkisins sem vísað er til, sem leggja SKAL til grundvallar mati á þjónustu í skránni í samræmi við viðeigandi eftirlitskerfi og valfrjáls faggildingarkerfi aðildarríkisins,
- þar sem notendur geta nálgast sértæka lýsingu aðildarríkisins sem vísað er til á því hvernig skuli nota og túlka innihald áreiðanlega listans með tilliti til vottunarþjónustu sem ekki varðar útgáfu fullgilda vottorða. Þennan texta má nota til að tilgreina hugsanlegan sundurgreinaleika (e. granularity) í landsbundnum eftirlits-/faggildingarkerfum að því er varðar vottunaraðila sem gefa ekki út fullgild vottorð og hvernig ‚Scheme service definition URI’ (liður 5.5.6) og svæðið fyrir ‚Service information extension’ (liður 5.5.9) eru notuð í þessum tilgangi.

Aðildarríki MEGA skilgreina og nota fleiri vefböng til viðbótar út frá fyrrgreinda veffanginu sem er sértækt fyrir aðildarríkið (t.d. vefböng sem eru skilgreind út frá þessu stigveldissértæka veffangi).

#### **TSL policy/legal notice** (liður 5.3.11)

Þetta svæði SKAL vera til staðar og SKAL vera í samræmi við forskriftirnar í lið 5.3.11 í TS 119 612, þar sem stefnan/lagatilkynningin um réttarstöðu kerfisins eða lagaskilyrði sem kerfið uppfyllir innan þeirrar lögsögu sem það heyrir undir og/eða hvers konar takmarkanir á og skilyrði fyrir viðhaldi og birtingu áreiðanlega listans SKAL vera margmála stafastrengur (án sniðtákna) í tveimur hlutum:

1. Fyrst er skyldubundinn hluti, sem er sameiginlegur fyrir áreiðanlega lista allra aðildarríkja (þar sem skylt er að nota breska ensku og hugsanlega eina eða fleiri þjóðtungur) þar sem fram kemur að gildandi lagarammi sé tilskipun 1999/93/EB og samsvarandi framkvæmd í lögum aðildarríkisins sem er tilgreint undir svæðinu ‚Scheme Territory’.

Sameiginlegi textinn í enskri útgáfu:

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 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.

<sup>(13)</sup> ISO 3166-1:2006: „Codes for the representation of names of countries and their subdivisions – Part 1: Country codes“.

Texti á einni eða fleiri þjóðtungum aðildarríkis: [opinber þýðing á enska textanum hér að framan].

2. Annar hlutinn, sem er valkvæður, er sértækur fyrir hvern áreiðanlegan lista (þar sem skylt er að nota breska ensku og mögulega eina eða fleiri þjóðtungur), með tilvísunum í tiltekna, gildandi lagamma einstakra aðildarríkja (t.d. einkum í tengslum við landsbundin eftirlits-/faggildingarkerfi fyrir vottunaraðila sem gefa ekki út fullgild vottorð).

## II. KAFLI

### SAMFELLA ÁREIÐANLEGRA LISTA

Skilríki sem tilkynna á framkvæmdastjórninni um samkvæmt c-lið 3. gr. þessarar ákvörðunar SKULU gefin út þannig að:

- minnst þrjú mánuðir séu á milli gildistökudagsetninga þeirra,
- þau séu gerð á nýjum lykilorðum þar sem ekki á að endurvotta lykilorð sem hafa verið notuð áður.

Ef EINN af einkalyklunum sem samsvara dreifilyklinum, sem mætti nota til að staðfesta undirskrift áreiðanlega listans og sem hefur verið tilkynntur til framkvæmdastjórnarinnar og birtur í miðlægum tenglaskráum framkvæmdastjórnarinnar, hefur verið ranglega notaður eða ónýttur SKULU aðildarríkin:

- endurútgefa án tafar nýjan áreiðanlegan lista, sem er undirritaður með einkalykli sem hefur ekki verið ranglega notaður, hafi útgefni, áreiðanlegi listinn verið undirritaður með einkalykli sem hefur verið ranglega notaður eða ónýttur,
- tilkynna framkvæmdastjórninni án tafar um nýjan lista yfir dreifilyklaskilríki sem samsvara einkalyklunum sem mætti nota til að undirrita áreiðanlega listann.

Ef ALLIR einkalyklarnir sem samsvara dreifilyklunum, sem mætti nota til að staðfesta undirskrift áreiðanlega listans og sem hafa verið tilkynntir til framkvæmdastjórnarinnar og birtir í miðlægum tenglaskráum framkvæmdastjórnarinnar, hafa verið ranglega notaðir eða ónýttir SKULU aðildarríkin:

- búa til ný lykilorð sem má nota til að undirrita áreiðanlega listann og samsvarandi dreifilyklaskilríki þeirra,
- endurútgefa án tafar nýjan áreiðanlegan lista, sem er undirritaður með einum þessara nýju einkalykla og tilkynna samsvarandi dreifilyklaskilríki,
- tilkynna framkvæmdastjórninni án tafar um nýja listann yfir dreifilyklaskilríki sem samsvara einkalyklunum sem mætti nota til að undirrita áreiðanlega listann.

## III. KAFLI

### FORSKRIFTIR FYRIR ÚTGÁFU ÁREIÐANLEGA LISTANS SEM ER LÆSILEG MÖNNUM

Ef útbúin er og birt útgáfa af áreiðanlega listanum sem er læsileg mönnum ÆTTI hún að vera á PDF-skjalsniði samkvæmt ISO 32000 <sup>(14)</sup> sem VERÐUR vera í samræmi við PDF/A-snið samkvæmt ISO 19005 <sup>(15)</sup>.

Innihald áreiðanlega listans í útgáfu sem er læsileg mönnum og byggð á PDF/A-skjalsniði ÆTTI að uppfylla eftirfarandi kröfur:

- Skipan útgáfunnar sem er læsileg mönnum ÆTTI að endurspeglar röklegu fyrirmyndina sem lýst er í TS 119 612.
- Sérhvert fyrirliggjandi gagnasvæði ÆTTI að sjást og þar ætti að koma fram:
  - heiti svæðisins (t.d. ‚Service type identifier‘),
  - gildið fyrir svæðið (t.d. ‚CA/QC‘)
  - merking (lýsing) gildisins fyrir svæðið, ef við á (t.d. ‚Vottunaraðili sem gefur út dreifilyklaskilríki‘),
  - fleiri útgáfur á náttúrulegum tungumálum (e. natural languages) eins og gert er ráð fyrir í áreiðanlega listanum, ef við á.

<sup>(14)</sup> ISO 32000-1:2008: Document management – Portable document format – Part 1: PDF 1.7

<sup>(15)</sup> ISO 19005-2:2011: Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2)

- 
- Eftirfarandi svæði og samsvarandi gildi fyrir stafrænu vottorðin sem er að finna á „Service digital identity“-svæðinu ÆTTU, að lágmarki, að vera sýnileg í útgáfunni sem er læsileg mönnum:
    - Útgáfa (Version)
    - Raðnúmer (Serial number)
    - Algrím fyrir undirskrift (Signature algorithm)
    - Útgefandi (Issuer)
    - Gildir frá
    - Gildir til
    - Vottorðshafi (Subject)
    - Dreifilykill (Public key)
    - Vottunarstefnur (Certificate Policies)
    - Lykilauðkenni vottorðshafa (Subject Key Identifier)
    - Dreifingarstaðir fyrir afturköllunarlista (CRL Distribution Points)
    - Lykilauðkenni vottunarstöðvar (Authority Key Identifier)
    - Notkun lykilsins (Key Usage)
    - Grundvallartakmarkanir (Basic constraints)
    - Algrím fyrir þumalfar (Thumbprint algorithm)
    - Þumalfar (Thumbprint)
  - Útgáfan sem er læsileg mönnum ÆTTI að vera auðþrenganleg
  - Útgáfan sem er læsileg mönnum VERÐUR að vera undirrituð af rekstraraðila kerfisins samkvæmt PAdES-grunnsmiði fyrir undirskriftir <sup>(16)</sup>.

---

<sup>(16)</sup> ETSI TS 103 172 (Mars 2012) - Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile