

**FRAMKVÆMDARÁKVÖRÐUN FRAMKVÆMDASTJÓRNARINNAR
(ESB) 2015/1505****2019/EES/101/05****frá 8. september 2015****um tækniforskriftir og snið fyrir traustlista skv. 5. mgr. 22. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 910/2014 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti á innri markaðinum (*)**

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) nr. 910/2014 frá 23. júlí 2014 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti á innri markaðinum og um niðurfellingu á tilskipun 1999/93/EB ⁽¹⁾, einkum 5. mgr. 22. gr.,*og að teknu tilliti til eftirfarandi:*

- 1) Traustlistar eru nauðsynlegir til að byggja upp traust á milli markaðsaðila þar sem þeir sýna fram á stöðu þjónustu-veitanda þegar eftirlit fór fram.
- 2) Notkun rafrænna undirskrifta yfir landamæri hefur verið auðvelduð með ákvörðun framkvæmdastjórnarinnar 2009/767/EB ⁽²⁾ sem lagði þá skyldu á aðildarríkin að semja, viðhalda og birta traustlista (e. trusted lists) með upplýsingum um þá vottunaraðila sem gefa út fullgild vottorð til handa almenningi í samræmi við tilskipun Evrópuþingsins og ráðsins 1999/93/EB ⁽³⁾ og sem aðildarríkin hafa eftirlit með og veita faggildingu.
- 3) Með 22. gr. reglugerðar (EB) nr. 910/2014/ESB er sú skylda lögð á aðildarríkin að koma á, viðhalda og birta, með öruggum hætti, rafrænt undirritaða eða innsiglaða traustlista á formi sem hentar fyrir sjálfvirka vinnslu og að tilkynna framkvæmdastjórninni um þá aðila sem bera ábyrgð á að koma landsbundnu traustlistunum á.
- 4) Líta ætti svo á að traustþjónustuveitandi og traustþjónustan sem hann veitir séu fullgild ef veitandinn hefur fullgilda stöðu á traustlistanum. Til þess að tryggja að þjónustuveitendur geti auðveldlega uppfyllt aðrar skyldur sem leiðir af reglugerð (ESB) nr. 910/2014, einkum þær sem settar eru fram í 27. og 37. gr., með fjarmiðlun og með rafrænum hætti, og til að uppfylla réttmætar væntingar annarra vottunaraðila, sem ekki gefa út fullgild vottorð en láta í té þjónustu í tengslum við rafrænar undirskriftir samkvæmt tilskipun 1999/93/EB og eru á skrá þann 30. júní 2016, ættu aðildarríkin að hafa þann möguleika að bæta annari traustþjónustu en bara fullgildri inn á traustlista sína, kjósi þau það, að því tilskildu að það komi skýrt fram að hún sé ekki fullgild samkvæmt reglugerð (ESB) nr. 910/2014.
- 5) Í samræmi við 25. forsendu reglugerðar (ESB) nr. 910/2014 er aðildarríkjunum heimilt að bæta við öðrum tegundum traustþjónustu, sem skilgreindar eru sem slíkar á landsvísu, en þeim sem skilgreindar eru í 16. mgr. 3. gr. reglugerðar (ESB) nr. 910/2014 að því tilskildu að það komi skýrt fram að þær séu ekki fullgildar samkvæmt reglugerð (ESB) nr. 910/2014.
- 6) Ráðstafanirnar, sem kveðið er á um í þessari ákvörðun, eru í samræmi við álit nefndarinnar sem komið var á fót með 48. gr. reglugerðar (EB) nr. 910/2014.

SAMÞYKKT ÁKVÖRÐUN ÞESSA:

1. gr.

Aðildarríkin skulu taka saman, birta og viðhalda traustlistum með upplýsingum um fullgilda traustþjónustuveitendur sem þau hafa eftirlit með, ásamt upplýsingum um fullgilda traustþjónustu sem þeir veita. Listarnir skulu vera í samræmi við tækniforskriftirnar sem settar eru fram í I. viðauka.

(*) Þessi ESB-gerð birtist í Stjttíð. ESB L 235, 9.9.2015, bls. 26. Hennar var getið í ákvörðun sameiginlegu EES-nefndarinnar nr. 167/2019 frá 13. júní 2019 um breytingu á XI. viðauka (Rafræn fjarskipti, hljóð- og myndmiðlun og upplýsingasamfélagið) við EES-samninginn (bíður birtingar).

(1) Stjttíð. ESB L 257, 28.8.2014, bls. 73.

(2) 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 (Stjttíð. ESB L 274, 20.10.2009, bls. 36).

(3) Tilskipun Evrópuþingsins og ráðsins 1999/93/EB frá 13. desember 1999 um ramma Bandalagsins varðandi rafrænar undirskriftir (Stjttíð. EB L 13, 19.1.2000, bls. 12).

2. gr.

Aðildarríkjunum er heimilt að bæta við traustlistana upplýsingum um traustþjónustuveitendur sem eru ekki fullgildir, ásamt upplýsingum um traustþjónustuna sem þeir veita og sem ekki er fullgild. Í listanum skal koma skýrt fram hvaða traustþjónustuveitendur og traustþjónusta, sem þeir veita, eru ekki fullgild.

3. gr.

1) Skv. 2. mgr. 22. gr. reglugerðar (ESB) nr. 910/2014 skulu aðildarríkin undirrita eða innsigla rafrænt traustlista sinn á formi sem hentar fyrir sjálfvirka vinnslu, í samræmi við tækniforskriftirnar í I. viðauka.

2) Ef aðildarríki birtir rafrænt útgáfu af traustlistanum sem er læsileg mönnum skal það tryggja að sú útgáfa traustlistans innihaldi sömu upplýsingar og útgáfan fyrir sjálfvirka vinnslu og undirrita hana eða innsigla rafrænt í samræmi við tækniforskriftirnar í I. viðauka.

4. gr.

1) Aðildarríkin skulu senda framkvæmdastjórninni upplýsingarnar, sem um getur í 3. mgr. 22. gr. reglugerðar (ESB) nr. 910/2014 og nota til þess sniðmátið í II. viðauka.

2) Upplýsingarnar sem um getur í 1. mgr. skulu innihalda tvenn eða fleiri dreifilyklaskilríki rekstraraðila kerfisins, með gildistíma sem eru hliðraðir um a.m.k. þrjú mánuði og sem samsvara einkalyklunum sem nota má til að undirrita eða innsigla rafrænt útgáfu traustlistans sem hentar fyrir sjálfvirka vinnslu og útgáfu hans sem er læsileg mönnum þegar þær eru birtar.

3) Skv. 4. mgr. 22. gr. reglugerðar (ESB) nr. 910/2014 skal framkvæmdastjórnin gera upplýsingarnar, sem um getur í 1. og 2. mgr. og aðildarríkin hafa veitt, aðgengilegar almenningi um örugga tengingu við sannvottaðan vefþjón, í undirritaðri eða innsiglaðri útgáfu sem hentar fyrir sjálfvirka vinnslu.

4) Framkvæmdastjórninni er heimilt að gera upplýsingarnar, sem um getur í 1. og 2. mgr. og aðildarríkin hafa veitt, aðgengilegar almenningi um örugga tengingu við sannvottaðan vefþjón, í undirritaðri eða innsiglaðri útgáfu sem er læsileg mönnum.

5. gr.

Ákvörðun þessi öðlast gildi á tuttugasta degi eftir að hún birtist í *Stjórnartíðindum Evrópusambandsins*.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 8. september 2015.

Fyrir hönd framkvæmdastjórnarinnar,

Jean-Claude JUNCKER

forseti.

I. VIÐAUKI

TÆKNIFORSKRIFTIR FYRIR SAMEIGINLEGT SNIÐMÁT FYRIR TRAUSTLISTA

I. KAFLI

ALMENNAR KRÖFUR

Traustlistar skulu innihalda bæði gildandi upplýsingar og allar eldri upplýsingar um stöðu traustþjónustu á listunum, allt frá því að traustþjónustuveitandanum var bætt á listann.

Hugtökin „samþykktur“, „faggiltur“ og/eða „eftirlitsskyldur“ í þessum forskriftum ná einnig yfir landsbundin samþykktarkerfi en aðildarríki munu veita viðbótarupplýsingar um eðli slíkra landsbundinna kerfa í traustlista sínum, þ.m.t. skýringu á því í hverju þau kunna að vera frábrugðin eftirlitskerfum sem gilda um fullgilda traustþjónustuveitendur og þá fullgildu traustþjónustu sem þeir veita.

Upplýsingarnar, sem veittar eru í traustlistanum, miða fyrst og fremst að því að styðja við staðfestingu á fullgildum traustþjónustutökum, þ.e. hlutrænum eða tvíundar- (röklegum) hlutum, sem verða til eða eru sendir sem afrakstur fullgildrar traustþjónustu, svo sem t.d. fullgildar rafrænar undirskriftir/innsigli, útfærðar rafrænar undirskriftir/innsigli studd fullgildu vottorði, fullgildir tímastimplar, fullgild rafræn sönnunargögn um afhendingu, o.s.frv.

II. KAFLI

ÍTARLEGAR FORSKRIFTIR FYRIR SAMEIGINLEGT SNIÐMÁT FYRIR TRAUSTLISTANA

Forskriftir þessar byggjast á forskriftunum og kröfunum sem tilgreindar eru í tækniforskriftum Fjarskiptastaðlastofnunar Evrópu ETSI TS 119 612 v2.1.1. (hér á eftir nefndar ETSI TS 119 612).

Ef engin sértæk krafa er tilgreind í þessum forskriftum skulu kröfurnar í 5. og 6. lið ETSI TS 119 612 gilda í heild sinni. Ef sértækar kröfur eru settar fram 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 skulu þessar forskriftir ganga frammar.

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“ = „Traustlisti með upplýsingum um fullgilda traustþjónustuveitendur sem eru eftirlitsskyldir í útgáfu-aðildarríkinu ásamt upplýsingum um fullgilda traustþjónustu sem þeir veita, í samræmi við viðeigandi ákvæði sem mælt er fyrir um í reglugerð Evrópuþingsins og ráðsins (ESB) nr. 910/2014 frá 23. júlí 2014 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti á innri markaðinum og um niðurfellingu á tilskipun 1999/93/EB.“

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 traustlistans, undirliggjandi eftirlitskerfi og, ef við á, gildandi landsbundið/landsbundin samþykktar- (þ.e. faggildingar-)kerfi. Sameiginlegi textinn sem nota skal er sá sem fer hér á eftir, þar sem heiti viðkomandi aðildarríkis skal koma í stað stafastrengsins „(heiti viðeigandi aðildarríkis)“:

„Þessi listi er traustlisti með upplýsingum um fullgilda traustþjónustuveitendur sem eru eftirlitsskyldir í (heiti viðeigandi aðildarríkis) ásamt upplýsingum um fullgilda traustþjónustu sem þeir veita, í samræmi við viðeigandi ákvæði sem mælt er fyrir um í reglugerð Evrópuþingsins og ráðsins (ESB) nr. 910/2014 frá 23. júlí 2014 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti á innri markaðinum og um niðurfellingu á tilskipun 1999/93/EB.“

Notkun rafrænna undirskrifa yfir landamæri hefur verið auðvelduð með ákvörðun framkvæmdastjórnarinnar 2009/767/EB frá 16. október 2009 sem lagði þá skyldu á aðildarríkin að semja, viðhalda og birta traustlista með upplýsingum um þá 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 fyrir rafrænar undirskriftir og sem aðildarríkin hafa eftirlit með eða veita faggildingu. Traustlisti þessi er framhald af traustlistanum sem komið var á með ákvörðun 2009/767/EB.“

Traustlistar eru mikilvægur þáttur í því að byggja upp traust á milli rafrænna markaðsaðila því þeir gera notendum kleift að ákvarða fullgilda stöðu traustþjónustuveitenda og þjónustu þeirra og sögu þeirra að því er varðar stöðu.

Í traustlistum aðildarríkjanna koma fram, að lágmarki, upplýsingarnar sem tilgreindar eru í 1. og 2. gr. framkvæmdar-ákvörðunar framkvæmdastjórnarinnar (ESB) 2015/1505.

Aðildarríkjunum er heimilt að bæta við traustlistana upplýsingum um traustþjónustuveitendur sem eru ekki fullgildir, ásamt upplýsingum um traustþjónustuna sem þeir veita og sem ekki er fullgild. Það skal koma skýrt fram að þeir séu ekki fullgildir samkvæmt reglugerð (ESB) nr. 910/2014.

Aðildarríkjunum er heimilt að bæta við á traustlistana upplýsingum um traustþjónustu, sem skilgreind er sem slík á landsvísu en er annarrar tegundar en sú sem skilgreind er í 16. mgr. 3. gr. reglugerðar (ESB) nr. 910/2014. Það skal koma skýrt fram að hún sé ekki fullgild samkvæmt reglugerð (ESB) nr. 910/2014.

b) Sértekjar upplýsingar um undirliggjandi eftirlitskerfi og, ef við á, gildandi landsbundið/landsbundin samþykktar- (þ.e. faggildingar-)kerfi, einkum ⁽¹⁾:

- 1) Upplýsingar um landsbundna eftirlitskerfið sem fullgildir traustþjónustuveitendur og traustþjónustuveitendur sem ekki eru fullgildir heyra undir, sem og fullgild traustþjónusta og traustþjónusta, sem ekki er fullgild, sem þeir veita í samræmi við reglugerð (ESB) nr. 910/2014.
- 2) Upplýsingar, eftir atvikum, um landsbundin valfrjáls faggildingarkerfi sem gilda um vottunaraðila sem gefið hafa út fullgild vottorð samkvæmt tilskipun 1999/93/EB.

Eftirfarandi skal a.m.k. vera í þessum sértæku upplýsingum fyrir hvert undirliggjandi kerfi sem er talið upp hér að framan:

- 1) Almenn lýsing.
- 2) Upplýsingar um ferlið sem fylgt er innan landsbundna eftirlitskerfisins og, ef við á, við samþykki samkvæmt landsbundna samþykkiskerfinu.
- 3) Upplýsingar um viðmiðanir sem notaðar eru við eftirlit með traustþjónustuveitendum eða, eftir atvikum, þegar þeir eru samþykktir.
- 4) Upplýsingar um viðmiðanir og reglur sem eru notaðar við val á eftirlits-/úttektaraðilum og til að skilgreina hvernig þeir meta traustþjónustuveitendur og traustþjónustuna sem þeir veita.
- 5) Ef við á, 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.

Það skal aðeins innihalda vefföng á breskri ensku.

⁽¹⁾ Þessar upplýsingar hafa afgerandi þýðingu til að treystendur geti metið gæða- og öryggisstig slíkra kerfa. Veita skal þessar upplýsingar á vettvangi traustlistans með því að nota fyrirliggjandi „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, jafnframt því sem hvert aðildarríki getur bætt við texta/tilvísunum sem eru sértekjar fyrir það ríki). Frekari upplýsingar um slík kerfi fyrir traustþjónustu sem er ekki fullgild og traustþjónustu sem er skilgreind sem slík á landsvísu (fullgild) 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 „Scheme service definition URI“ (liður 5.5.6).

Það skal a.m.k. innihalda tvö vefföng:

- 1) sameiginlegt veffang fyrir traustlista allra aðildarríkja, sem vísar á lýsandi texta sem skal gilda um alla traustlista, sem hér segir:

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

Lýsandi texti:

„Participation in a scheme

Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

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

Policy/rules for the assessment of the listed services

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (EU) 2015/1505.

The trusted lists include both current and historical information about the status of listed trust services.

Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

Interpretation of the Trusted List

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows:

The “qualified” status of a trust service is indicated by the combination of the “Service type identifier” (“Sti”) value in a service entry and the status according to the “Service current status” field value as from the date indicated in the “Current status starting date and time”. Historical information about such a qualified status is similarly provided when applicable.

Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

A “CA/QC” “Service type identifier” (“Sti”) entry (possibly further qualified as being a “RootCA-QC” through the use of the appropriate “Service information extension” (“Sie”) `additionalServiceInformationExtension`)

— indicates that any end-entity certificate issued by or under the CA represented by the “Service digital identifier” (“Sdi”) CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:

- the `id-etsi-qcs-QcCompliance` ETSI defined statement (`id-etsi-qcs 1`),
- the `0.4.0.1456.1.1` (QCP+) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. “under-supervision”, “supervisionincessation”, “accredited” or “granted”) for that entry.

— **and IF** “Sie” “Qualifications Extension” information is present, then in addition to the above default rule, those certificates that are identified through the use of “Sie” “Qualifications Extension” information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the “SSCD support” and/or “Legal person as subject” (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific “Key usage” pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of “Qualifiers” used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:

— to indicate the qualified certificate nature:

— “QCStatement” meaning the identified certificate(s) is(are) qualified under Directive 1999/93/EC;

— “QCForESig” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is(are) qualified certificate(s) for electronic signature under Regulation (EU) No 910/2014;

— “QCForESeal” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is(are) qualified certificate(s) for electronic seal under Regulation (EU) No 910/2014;

— “QCForWSA” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is(are) qualified certificate(s) for web site authentication under Regulation (EU) No 910/2014.

— to indicate that the certificate is not to be considered as qualified:

— “NotQualified” meaning the identified certificate(s) is(are) not to be considered as qualified; and/or

— to indicate the nature of the SSCD support:

— “QCWithSSCD” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or

— “QCNoSSCD” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or

— “QCSSCDStatusAsInCert” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD;

— to indicate the nature of the QSCD support:

— “QCWithQSCD” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

— “QCNoQSCD” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or

— “QCQSCDStatusAsInCert” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD;

— “QCQSCDManagedOnBehalf” indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; and/or

— to indicate issuance to Legal Person:

- “QCForLegalPerson” meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under Directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

- if none of the id-etsi-qcs 1 statement, QCP OID or QCP + OID information is included in an end-entity certificate, and
- if no “Sie”“Qualifications Extension” information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a “QCStatement” qualifier, or
- an “Sie”“Qualifications Extension” information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a “NotQualified” qualifier,

then the certificate is not to be considered as qualified.

“Service digital identifiers” are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other “Sti” type entry is that, for that “Sti” identified service type, the listed service named according to the “Service name” field value and uniquely identified by the “Service digital identity” field value has the current qualified or approval status according to the “Service current status” field value as from the date indicated in the “Current status starting date and time”.

Specific interpretation rules for any additional information with regard to a listed service (e.g. “Service information extensions” field) may be found, when applicable, in the Member State specific URI as part of the present “Scheme type/community/rules” field.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists.“

2) Sérþækt veffang fyrir traustlista hvers aðildarríkis, sem vísar á lýsandi texta sem skal gilda um traustlista þess aðildarríkis:

<http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC> þar sem CC = ISO 3166-1 ⁽¹⁾ 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 traustþjónustu á listanum í samræmi við viðeigandi eftirlitskerfi og, eftir atvikum, samþykktarkerfi aðildarríkisins,
- þar sem notendur geta nálgast sértæka lýsingu aðildarríkisins sem vísað er til á því hvernig skuli nota og túlka innihald traustlistans með tilliti til traustþjónustu sem ekki er fullgild og/eða traustþjónustu sem skilgreind er sem slík á landsvísi, sem eru á listanum. Þetta má nota til að tilgreina hugsanlegan sundurgreinanleika (e. granularity) í landsbundna samþykktarkerfinu að því er varðar vottunaraðila sem gefa ekki út fullgild vottorð og hvernig svæðin fyrir „Scheme service definition URI“ (liður 5.5.6) og „Service information extension“ (liður 5.5.9) eru notuð í þessum tilgangi.

Aðildarríki MEGA skilgreina og nota fleiri vefköng til viðbótar út frá fyrrgreinda veffanginu sem er sérþækt fyrir aðildarríkið (t.d. vefköng 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 traustlistans skal vera runa margmála stafastrengja (sjá

⁽¹⁾ ISO 3166-1:2006: ‘Codes for the representation of names of countries and their subdivisions – Part 1: Country codes’.

lið 5.1.4) með raunverulegum texta slíkrar stefnu eða tilkynningar sem skylt er að hafa á breskri ensku og má hafa á einni eða fleiri þjóðtungum, uppbyggt sem hér segir:

- 1) Fyrst er skyldubundinn hluti, sem er sameiginlegur fyrir traustlista allra aðildarríkja þar sem tilgreindur er gildandi lagarammi og sem hljóðar svo á ensku:

The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Texti á einni eða fleiri þjóðtungum aðildarríkis:

Gildandi lagarammi fyrir traustlista þennan er reglugerð Evrópuþingsins og ráðsins (ESB) nr. 910/2014 frá 23. júlí 2014 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti á innri markaðinum og um niðurfellingu á tilskipun 1999/93/EB.

- 2) Annar hluti, sem er valkvæður, er sértækur fyrir hvern traustlista með tilvísunum í tiltekna gildandi lagaramma einstakra aðildarríkja.

Service current status (liður 5.5.4)

Þetta svæði skal vera til staðar og skal vera í samræmi við forskriftirnar í lið 5.5.4. í TS 119 612.

Flutningur á „Service current status“-gildi þjónustu, sem er að finna á traustlista aðildarríkja Evrópusambandsins daginn fyrir þann dag sem reglugerð (ESB) nr. 910/2014 kemur til framkvæmda (þ.e. 30. júní 2016), skal fara fram á þeim degi sem reglugerðin kemur til framkvæmda (þ.e. 1. júlí 2016) eins og tilgreint er í viðauka J við ETSI TS 119 612.

III. KAFLI

SAMFELLA TRAUSTLISTA

Skilríki sem tilkynna á framkvæmdastjórninni um samkvæmt 2. mgr. 4. gr. þessarar ákvörðunar skulu uppfylla kröfur liðar 5.7.1 í ETSI TS 119 612 og skulu gefin út þannig að:

- minnst þrjú mánuðir séu á milli síðasta gildisdags þeirra („ekki eftir“),
- þau séu gerð á nýjum lyklapörum. Ekki má endurvotta áður notuð lyklapör.

Ef ein af dreifilyklaskilríkjunum, sem mætti nota til að staðfesta undirskrift eða innsigli traustlistans og sem hafa verið tilkynnt til framkvæmdastjórnarinnar og birt í miðlægum tenglaskráum framkvæmdastjórnarinnar, eru útrunnin skulu aðildarríkin:

- endurútgefa án tafar nýjan traustlista, sem er undirritaður eða innsiglaður með einkalykli þar sem dreifilyklaskilríkin eru ekki útrunnin, hafi fyrirliggjandi traustlisti verið undirritaður eða innsiglaður með einkalykli og dreifilyklaskilríki hans eru útrunnin,
- búa til, ef þörf er á, ný lyklapör sem má nota til að undirrita eða innsigla traustlistann og útbúa samsvarandi dreifilyklaskilríki þeirra,
- tilkynna framkvæmdastjórninni án tafar um nýja listann yfir dreifilyklaskilríki sem samsvara einkalyklunum sem mætti nota til að undirrita eða innsigla traustlistann.

Ef einn af einkalyklunum sem samsvara einum af dreifilyklaskilríkjunum, sem mætti nota til að staðfesta undirskrift eða innsigli traustlistans og sem hafa verið tilkynnt til framkvæmdastjórnarinnar og birt í miðlægum tenglaskráum framkvæmdastjórnarinnar, hefur verið ranglega notaður eða ónýttur skulu aðildarríkin:

- endurútgefa án tafar nýjan traustlista, sem er undirritaður eða innsiglaður með einkalykli sem hefur ekki verið ranglega notaður, hafi útgefni traustlistinn verið undirritaður eða innsiglaður með einkalykli sem hefur verið ranglega notaður eða ónýttur,

- búa til, ef þörf er á, ný lyklopör sem má nota til að undirrita eða innsigla traustlistann og útbúa samsvarandi dreifilyklaskilríki þeirra,
- tilkynna framkvæmdastjórninni án tafar um nýja listann yfir dreifilyklaskilríki sem samsvara einkalyklunum sem mætti nota til að undirrita eða innsigla traustlistann.

Ef allir einkalyklarnir sem samsvara dreifilyklaskilríkjunum, sem mætti nota til að staðfesta undirskrift traustlistans og sem hafa verið tilkynnt til framkvæmdastjórnarinnar og birt í miðlægum tenglaskráum framkvæmdastjórnarinnar, hafa verið ranglega notaðir eða ónýttir skulu aðildarríkin:

- búa til ný lyklopör sem má nota til að undirrita eða innsigla traustlistann og útbúa samsvarandi dreifilyklaskilríki þeirra,
- endurútgefa án tafar nýjan traustlista, sem er undirritaður eða innsiglaður 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 eða innsigla traustlistann.

IV. KAFLI

FORSKRIFTIR FYRIR ÚTGÁFU TRAUSTLISTANS SEM ER LÆSILEG MÖNNUM

Ef tekin er saman og birt útgáfa af traustlistanum sem er læsileg mönnum skal hún að vera á PDF-skjalsniði samkvæmt ISO 32000 ⁽¹⁾ sem skal vera í samræmi við PDF/A-snið samkvæmt ISO 19005 ⁽²⁾.

Innihald traustlistans í útgáfu sem er læsileg mönnum og byggð á PDF/A-skjalsniði skal uppfylla eftirfarandi kröfur:

- Skipan útgáfunnar sem er læsileg mönnum skal endurspeglar röklegu fyrirmyndina sem lýst er í TS 119 612.
- Sérhvert fyrirliggjandi gagnasvæði skal sjást og þar skal koma fram:
 - heiti svæðisins (t.d. „*Service type identifier*“),
 - gildið fyrir svæðið (t.d. „<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>“),
 - merking (lýsing) gildisins fyrir svæðið, ef við á (t.d. „*Þjónusta við gerð vottorða sem býr til og undirritar fullgild vottorð á grundvelli kennsla og annarra eiginda sem viðkomandi skráningarþjónusta staðfestir.*“),
 - fleiri útgáfur á náttúrulegum tungumálum (e. natural languages) eins og gert er ráð fyrir í traustlistanum, ef við á.
- Eftirfarandi svæði og samsvarandi gildi fyrir stafrænu vottorðin ⁽³⁾ sem er að finna á „Service digital identity“-svæðinu skulu að lágmarki að vera sýnileg í útgáfunni sem er læsileg mönnum:
 - Útgáfa (Version)
 - Raðnúmer vottorðs (Certificate serial number)
 - Algrím fyrir undirskrift (Signature algorithm)
 - Útgefandi (Issuer) – öll sérstök nafnasvæði sem við eiga
 - Gildistími (Validity period)
 - Vottorðshafi (Subject) – öll sérstök nafnasvæði sem við eiga

⁽¹⁾ ISO 32000-1:2008: Document management — Portable document format — Part 1: PDF 1.7

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

⁽³⁾ Recommendation ITU-T X.509 | ISO/IEC 9594-8: Information technology — Open systems interconnection — The Directory: Public-key and attribute certificate frameworks (see <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>)

- Dreifilykill (Public key)
 - Lykilauðkenni vottunarstöðvar (Authority Key Identifier)
 - Lykilauðkenni vottorðshafa (Subject Key Identifier)
 - Notkun lykilsins (Key Usage)
 - Aukin notkun lykils (Extended key usage)
 - Vottunarstefnur (Certificate Policies) – öll kennimerki stefnu og sérgreinar stefnu
 - Vörpun við stefnur (Policy mappings)
 - Annað heiti vottorðshafa (Subject alternative name)
 - Skráningareiginir vottorðshafa (Subject directory attributes)
 - Grundvallartakmarkanir (Basic constraints)
 - Stefnutakmarkanir (Policy constraints)
 - Dreifingarstaðir fyrir afturköllunarlista (CRL Distribution Points) ⁽¹⁾
 - Aðgangur vottunarstöðvar að upplýsingum (Authority Information Access)
 - Aðgangur vottorðshafa að upplýsingum (Subject Information Access)
 - Yfirlýsingar vegna fullgildra vottorða (Qualified Certificate Statements) ⁽²⁾
 - Tætialgrím (Hash algorithm)
 - Tætigildi vottorðs (Hash value of certificate).
- Útgáfan sem er læsileg mönnum skal vera auðprentanleg.
- Útgáfan sem er læsileg mönnum skal undirrituð eða innsiglið af rekstraraðila kerfisins samkvæmt útfærðri PDF-undirskrift sem tilgreind er í 1. og 3. gr. framkvæmdarákvörðunar framkvæmdastjórnarinnar (ESB) 2015/15015.
-

⁽¹⁾ RFC 5280: internet X.509 PKI Certificate and CRL Profile

⁽²⁾ RFC 3739: internet X.509 PKI: Qualified Certificates Profile

II. VIÐAUKI

SNIÐMÁT FYRIR TILKYNNINGAR AÐILDARRÍKJANNA

Upplýsingarnar sem aðildarríkjunum ber að tilkynna um skv. 1. mgr. 4. gr. þessarar ákvörðunar skulu innihalda eftirfarandi gögn og allar breytingar á þeim:

- 1) Aðildarríki, nota skal ISO 3166-1 ⁽¹⁾ alpha-2 kóða með eftirfarandi undantekningum:
 - a) Landskóðinn fyrir Bretland skal vera „UK“.
 - b) Landskóðinn fyrir Grikkland skal vera „EL“.
- 2) Þann eða þá aðila sem bera ábyrgð á því að taka saman, viðhalda og birta útgáfu traustlistanna sem hentar til sjálfvirkar vinnslu og útgáfu þeirra sem er læsileg mönnum:
 - a) Heiti rekstraraðila kerfisins: upplýsingar sem veittar eru verða að vera nákvæmlega eins – há-/lágstafir skipta máli – og gildið í „Scheme operator name“ sem fram kemur í traustlistanum og á jafnmörgum tungumálum og þar eru notuð.
 - b) Valkvæðar upplýsingar fyrir framkvæmdastjórnina til eigin nota eingöngu í því tilviki að hafa þurfi samband við viðkomandi aðila (upplýsingarnar verða ekki birtar á samantekinni skrá framkvæmdastjórnar Evrópusambandsins yfir traustlista):
 - heimilisfang rekstraraðila kerfisins,
 - samskiptaupplýsingar ábyrgs eða ábyrgra aðila (nafn, símanúmer, netfang).
- 3) Staðurinn þar sem útgáfa traustlistans sem hentar fyrir sjálfvirka vinnslu er birt (*birtingarstaður gildandi traustlista*).
- 4) Ef við á, staðurinn þar sem traustlistinn sem er læsilegur mönnum er birtur (*birtingarstaður gildandi traustlista*). Ef traustlisti, sem er læsilegur mönnum, er ekki lengur birtur skal það koma fram.
- 5) Dreifilyklaskilríki sem samsvara einkalyklunum sem má nota til að undirrita eða innsigla rafrænt útgáfu traustlistanna sem hentar fyrir sjálfvirka vinnslu og útgáfu þeirra sem er læsileg mönnum: þessi skilríki skulu látin í té sem DER-skilríki kóðuð í Base64 með Privacy Enhanced Mail-sniði. Viðbótarupplýsingar þegar um er að ræða tilkynningar um breytingu ef ný skilríki eiga að koma í stað sérstakra skilríkja á skrá framkvæmdastjórnarinnar og ef bæta á tilkynntu skilríkjunum við þau sem fyrir eru án þess að þau komi í stað annarra.
- 6) Dagsetning framlagningar gagnanna sem tilkynnt er um í 1.–5. lið.

Gögn sem tilkynnt er um skv. 1. lið, 2. lið (a-lið), 3. lið, 4. lið og 5. lið skulu færð inn í samantekna skrá framkvæmdastjórnar Evrópu yfir traustlista í stað áður tilkynnta upplýsinga í þeirri samanteknu skrá.

⁽¹⁾ ISO 3166-1: 'Codes for the representation of names of countries and their subdivisions — Part 1: Country codes'.