Euroopan unionin
virallinen lehti

FI
L-sarja

2025/1942

30.9.2025

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2025/1942,

annettu 29 päivänä syyskuuta 2025,

Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 soveltamissäännöistä hyväksyttyjen sähköisten allekirjoitusten hyväksyttyjen validointipalvelujen ja hyväksyttyjen sähköisten leimojen hyväksyttyjen validointipalvelujen osalta

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta 23 päivänä heinäkuuta 2014 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 ([1]) ja erityisesti sen 33 artiklan 2 kohdan ja 40 artiklan,

sekä katsoo seuraavaa:

(1) Hyväksyttyjen sähköisten allekirjoitusten ja hyväksyttyjen sähköisten leimojen hyväksytyillä validointipalveluilla varmistetaan hyväksyttyjen sähköisten allekirjoitusten ja hyväksyttyjen sähköisten leimojen validointiprosessin ja validointitulosten eheys, aitous ja oikeellisuus. Näillä hyväksytyillä luottamuspalveluilla on keskeinen rooli digitaalisessa liiketoimintaympäristössä, sillä ne edistävät siirtymistä perinteisistä paperipohjaisista prosesseista vastaaviin sähköisiin prosesseihin.

(2) Asetuksen (EU) N:o 910/2014 33 artiklan 2 kohdassa ja 40 artiklassa säädettyä vaatimustenmukaisuusolettamaa olisi sovellettava ainoastaan, jos hyväksyttyjen sähköisten allekirjoitusten ja hyväksyttyjen sähköisten leimojen hyväksytyt validointipalvelut ovat tässä asetuksessa vahvistettujen teknisten standardien mukaisia. Näiden standardien olisi heijastettava vakiintuneita käytäntöjä, ja niiden olisi oltava laajasti tunnustettuja kyseessä olevilla aloilla. Niitä olisi mukautettava siten, että niihin sisällytetään lisätarkastuksia, joilla varmistetaan hyväksyttyjen luottamuspalvelujen turvallisuus ja luotettavuus sekä mahdollisuus tarkistaa hyväksyttyjen sähköisten allekirjoitusten ja hyväksyttyjen sähköisten leimojen hyväksytty asema ja tekninen pätevyys.

(3) Jos luottamuspalvelun tarjoaja noudattaa tämän asetuksen liitteessä vahvistettuja vaatimuksia, valvontaelinten olisi oletettava, että asetuksen (EU) N:o 910/2014 asiaankuuluvia vaatimuksia on noudatettu, ja otettava tällainen olettamus asianmukaisesti huomioon luottamuspalvelun hyväksytyn aseman myöntämiseksi tai vahvistamiseksi. Hyväksytty luottamuspalvelun tarjoaja voi kuitenkin edelleen tukeutua muihin käytäntöihin osoittaakseen, että asetuksen (EU) N:o 910/2014 vaatimuksia noudatetaan.

(4) Komissio arvioi säännöllisesti uusia teknologioita, käytäntöjä, standardeja tai teknisiä eritelmiä. Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/1183 ([2]) johdanto-osan 75 kappaleen mukaan komission olisi tarkasteltava uudelleen ja tarvittaessa päivitettävä tätä asetusta sen pitämiseksi maailmanlaajuisen kehityksen ja uusien teknologioiden, standardien tai teknisten eritelmien mukaisena sekä sisämarkkinoiden parhaiden käytäntöjen noudattamiseksi.

([1]) EUVL L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Euroopan parlamentin ja neuvoston asetus (EU) 2024/1183, annettu 11 päivänä huhtikuuta 2024, asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen vahvistamisen osalta (EUVL L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(5) Tämän asetuksen mukaisiin henkilötietojen käsittelytoimiin sovelletaan Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679 ([3]) ja tarvittaessa Euroopan parlamentin ja neuvoston direktiiviä 2002/58/EY ([4]).

(6) Euroopan tietosuojavaltuutettua on kuultu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725 ([5]) 42 artiklan 1 kohdan mukaisesti, ja hän antoi lausuntonsa 6 päivänä kesäkuuta 2025.

(7) Tässä asetuksessa säädetyt toimenpiteet ovat asetuksen (EU) N:o 910/2014 48 artiklalla perustetun komitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

1 artikla

Viitestandardit ja eritelmät

Asetuksen (EY) N:o 910/2014 33 artiklan 2 kohdassa ja 40 artiklassa tarkoitetut viitestandardit ja eritelmät esitetään tämän asetuksen liitteessä.

2 artikla

Voimaantulo

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 29 päivänä syyskuuta 2025.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN

([3]) Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) (EYVL L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta (EUVL L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

LIITE

Luettelo hyväksyttyjen sähköisten allekirjoitusten hyväksyttyjä validointipalveluja ja hyväksyttyjen sähköisten leimojen hyväksyttyjä validointipalveluja koskevista viitestandardeista ja eritelmistä

Standardeja ETSI TS 119 441 V1.2.1 (2023-10) ([1]) ('ETSI TS 119 441') ja ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) ('ETSI TS 119 172-4') sovelletaan seuraavin mukautuksin:

1. ETSI TS 119 441

1) 2.1 Velvoittavat viittaukset

— [1] ETSI TS 119 101 V1.1.1 (2016-03) "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".

— [2] ETSI EN 319 401 V3.1.1 (2024-06) "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

— [3] ETSI EN 319 102-1 V1.4.1 (2024-06) "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

— [4] ISO/IEC 15408-1:2022 – Information security, cybersecurity and privacy protection – Evaluation criteria for IT security.

— [5] Tyhjä.

— [6] FIPS PUB 140-3 (2019) "Security Requirements for Cryptographic Modules".

— [7] Komission täytäntöönpanoasetus (EU) 2024/482 ([3]) Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC) hyväksymisestä.

— [8] ETSI TS 119 172-4 V1.1.1 (2021-05) "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists".

— [9] ETSI TS 119 102-2 V1.4.1 (2023-06) "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report".

— [10] Euroopan kyberturvallisuuden sertifiointiryhmä, Salausta käsittelevä alaryhmä: Euroopan kyberturvallisuusviraston (ENISA) julkaisema asiakirja "Agreed Cryptographic Mechanisms" ([4]).

— [11] Komission täytäntöönpanoasetus (EU) 2024/3144 ([5]) täytäntöönpanoasetuksen (EU) 2024/4822 muuttamisesta sovellettavien kansainvälisten standardien osalta ja kyseisen täytäntöönpanoasetuksen oikaisemisesta.

— [12] ETSI EN 319 411-1 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

([1]) ETSI TS 119 441 – Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services, V1.2.1 (2023-10).
([2]) ETSI TS 119 172-4 – Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists, V1.1.1 (2021-05).
([3]) EUVL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([4]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([5]) EUVL L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2 Lähdeviitteet

— [i.11] Tyhjä.

3) 3.3 Lyhenteet

— EUCC Yhteisiin kriteereihin perustuva eurooppalainen kyberturvallisuuden sertifiointijärjestelmä

4) 4.3.3 Prosessi

— HUOMAUTUS 10 Ks. ohjeita standardista ETSI EN 319 102-1 [3] ja EU:n hyväksyttyä allekirjoitusta tai leimaa koskevia lisäohjeita standardista ETSI TS 119 172-4 [8].

5) 6.1 Allekirjoituksen validointipalvelun käytäntöselostus

— OVR-6.1-02 Allekirjoitusten validointipalvelun (SVS) käytäntöselostus on jäsenneltävä liitteen A mukaisesti.

— OVR-6.1-03 SVS:n käytäntöselostuksessa on lueteltava tuetut SVS-politiikat tai viitattava niihin (esim. OID-tunnisteiden avulla) ja kuvattava niitä lyhyesti.

6) 6.3 Tietoturvapolitiikka

— OVR-6.3-02 Turvallisuuspolitiikassa on dokumentoitava henkilötietojen suojaamiseksi toteutetut turvallisuuden ja yksityisyyden suojatoimenpiteet.

7) 7.2 Henkilöresurssit

— OVR-7.2-02 Allekirjoitusten validointipalvelun tarjoajan (SVSP) luotetuissa rooleissa olevan henkilöstön ja tarvittaessa luotetuissa rooleissa olevien alihankkijoiden, on pystyttävä täyttämään vaatimus, joka koskee ”asiantuntemusta, kokemusta ja pätevyyttä”, joka on osoitettu virallisen koulutuksen ja suositusten, työkokemuksen tai näiden yhdistelmän kautta.

— OVR-7.2-03 Kohdan OVR-7.2-02 noudattamiseen on sisällyttävä säännöllisesti (vähintään 12 kuukauden välein) tehtäviä päivityksiä uusista uhkista ja nykyisistä turvakäytännöistä.

8) 7.5 Salaustekniikka koskevat tarkastukset

— OVR-7.5-02 [EHDOLLINEN] Kun validointiraportteja allekirjoitetaan, SVSP:n yksityistä allekirjoitusavainta vastaavan SVSP:n julkisen allekirjoitusvarmenteen myöntää luotettava varmentaja (CA) standardissa ETSI EN 319 411-1 [12] määritellyn laajennetun normalisoidun varmennepolitiikan (NCP+) mukaisesti. Se olisi myönnettävä standardissa ETSI EN 319 411-2 [i.17] määritellyn asianmukaisen varmennepolitiikan mukaisesti.

— OVR-7.5-03 [EHDOLLINEN] Kun validointiraportteja allekirjoitetaan, SVSP:n yksityistä allekirjoitusavainta on säilytettävä ja käytettävä suojatussa salauslaitteessa, joka on seuraavien mukaisesti sertifioitu luotettava järjestelmä:

a) tietoteknologian turvallisuuden arviointia koskevat yhteiset kriteerit, sellaisina kuin ne on esitetty standardissa ISO/IEC 15408 [4] tai asiakirjassa ”Common Criteria for Information Technology Security Evaluation”, versio CC:2022, osat 1–5, jotka yhteisten kriteerien mukaisten sertifikaattien tunnustamista tietotekniikan turvallisuuden alalla koskevan järjestelyn (Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security) osallistujat ovat julkaisseet ja jotka on sertifioitu vähintään tasolle EAL 4; tai

b) EUCC [7][11], ja sertifioitu vähintään tasolle EAL 4; tai

c) 31.12.2030 saakka FIPS PUB 140-3 [6] taso 3.

Sertifioinnin on koskettava turvatavoitetta tai suojausprofiilia tai moduulin suunnittelua ja turva-asiakirjoja, jotka täyttävät tämän asiakirjan vaatimukset, riskianalyysin perusteella ja ottaen huomioon fyysiset ja muut ei-tekniset turvatoimenpiteet.

Jos suojatulla salauslaitteella on EUCC [7][11]-sertifiointi, laite on konfiguroitava ja sitä on käytettävä kyseisen sertifioinnin mukaisesti.

— OVR-7.5-04 Tyhjä.

— OVR-7.5-06 SVSP:n yksityisen allekirjoitusavaimen saa viedä ja tuoda toiseen suojattuun salauslaitteeseen ainoastaan, jos kyseinen vienti ja tuonti toteutetaan turvallisesti ja kyseisten laitteiden sertifioinnin mukaisesti.

9) 7.7 Toimintaturvallisuus

— OVR-7.7-02 Sen varmistamiseksi, että järjestelmissä, joihin sovellus on kehitetty, sovelletaan asianmukaisia turvatoimenpiteitä ja ne mukautuvat erityisiin sovellusympäristöihin, allekirjoituksen validointisovelluksessa (SVA) on käytettävä sovellusympäristöä, jota ylläpidetään ajantasaisilla turvakorjauksilla.

— OVR-7.7-03 SVA:han sovelletaan seuraavia standardin ETSI TS 119 101 [1] lausekkeessa 5.2 määriteltyjä vaatimuksia: GSM 1.3.

10) 7.8 Verkkoturvallisuus

— OVR-7.8-02 Jos etäpääsy luottamuksellisia tietoja säilyttäviin tai käsitteleviin järjestelmiin on sallittu, on hyväksyttävä virallinen politiikka ja se on kuvattava osana kohdassa OVR-6.3-02 vaadittuja osatekijöitä.

— OVR-7.8-04 Standardin ETSI EN 319 401 [1] kohdassa REQ-7.8-13 edellytetty haavoittuvuus-kartoitus on tehtävä vähintään neljännesvuosittain.

— OVR-7.8-05 Standardin ETSI EN 319 401 [1] kohdassa REQ-7.8-17X edellytetty tunkeutumistesti on tehtävä vähintään neljännesvuosittain.

— OVR-7.8-06 Palomuurit on konfiguroitava siten, että estetään kaikki protokollat ja liittymät, joita ei tarvita SVSP:n toiminnassa.

11) 7.12 Allekirjoitusten validointipalvelun lopettaminen ja lopettamissuunnitelmat

— OVR-7.12-02 TSP:n toiminnan lopettamissuunnitelman on oltava asetuksen (EU) N:o 910/2014 [i.1] 24 artiklan 5 kohdan nojalla hyväksytyissä täytäntöönpanosäädöksissä vahvistettujen vaatimusten mukainen.

12) 7.14 Toimitusketju

— OVR-7.14-01 Sovelletaan standardin ETSI EN 319 401 [2] lausekkeessa 7.14 määriteltyjä vaatimuksia.

13) 8.1 Allekirjoituksen validointiprosessi

— VPR-8.1-07 Validointisovelluksen (SVA) on oltava standardin ETSI TS 119 101 [1] lausekkeen 7.4 kohtien SIA 1 – SIA 4 vaatimusten mukainen.

— VPR-8.1-11 [EHDOLLINEN] Kun SVS:n tarkoituksena on validoida hyväksyttyjä sähköisiä allekirjoituksia tai hyväksyttyjä sähköisiä leimoja asetuksen (EU) N:o 910/2014 [i.1] 32 artiklan 1 kohdan (tai 40 artiklan) mukaisesti, validointiprosessissa on noudatettava standardin ETSI TS 119 172-4 [8] vaatimuksia.

14) 8.2 Allekirjoituksen validointiprotokolla

— SVP-8.2-03 Allekirjoituksen validointivastauksessa on oltava SVS-politiikan OID-tunniste.

15) 8.4 Allekirjoituksen validointiraportti

— SVR-8.4-02 Allekirjoituksen validointiraportin on oltava standardin ETSI TS 119 102-2 [9] mukainen.

— SVR-8.4-07 [EHDOLLINEN] Jos SVS ei noudata allekirjoitusten validointipolitiikkaa kokonaisuudessaan, raportissa on validoitujen rajoitusten lisäksi raportoitava rajoituksista, jotka on jätetty huomiotta tai ohitettu.

— SVR-8.4-15 Validointiraportissa on ilmoitettava selvästi kunkin olemassaolotodisteen (PoE) alkuperä (allekirjoituksesta, asiakkaalta, palvelimelta).

— SVR-8.4-16 Validointiraportissa on oltava validointiraportin allekirjoitus, jonka on oltava SVSP:n digitaalinen allekirjoitus.

— SVR-8.4-17 [EHDOLLINEN] Kun validointiraportit allekirjoitetaan, allekirjoituksen muodon ja kohteen on oltava standardin ETSI TS 119 102–2 [9] mukaisia.

16) 9 Tässä asiakirjassa määriteltyyn luottamuspalvelupolitiikkaan perustuvien validointipalvelupolitiikkojen määrittelypuitteet:

— OVR-9-05 [EHDOLLINEN] Kun laaditaan tässä asiakirjassa määriteltyyn luottamuspalvelupolitiikkaan perustuvaa SVS-politiikkaa, on tehtävä riskinarviointi, jossa arvioidaan toimintavaatimukset ja määritetään turvallisuusvaatimukset, jotka on sisällytettävä ilmoitettua yhteisöä ja sovellettavuutta koskevaan politiikkaan.

— OVR-9-06 [EHDOLLINEN] Kun laaditaan tässä asiakirjassa määriteltyyn luottamuspalvelupolitiikkaan perustuvaa SVS-politiikkaa, politiikka on hyväksyttävä ja sitä on muutettava määritellyn tarkistusprosessin mukaisesti, mukaan lukien politiikan ylläpitämiseen liittyvät vastuut.

— OVR-9-07 [EHDOLLINEN] Kun laaditaan tässä asiakirjassa määriteltyyn luottamuspalvelupolitiikkaan perustuvaa SVS-politiikkaa, käytössä on oltava määritelty tarkistusprosessi, jolla varmistetaan, että politiikkaa tuetaan käytäntöselostuksilla.

— OVR-9-08 [EHDOLLINEN] Kun laaditaan tässä asiakirjassa määriteltyyn luottamuspalvelupolitiikkaan perustuvaa SVS-politiikkaa, TSP:n on asetettava TSP:n tukemat politiikat käyttäjäyhteisönsä saataville.

— OVR-9-09 [EHDOLLINEN] Kun laaditaan tässä asiakirjassa määriteltyyn luottamuspalvelupolitiikkaan perustuvaa SVS-politiikkaa, TSP:n tukemiin politiikkoihin tehdyt tarkistukset on asetettava tilaajien saataville.

17) Liite B (velvoittava) Asetuksen (EU) N:o 910/2014 33 artiklassa määritelty QES:n hyväksytty validointipalvelu

— VPR-B-02 [EHDOLLINEN] Jos SVSP on QSVSP, toteutuksessa on noudatettava standardia ETSI TS 119 172-4 [8].

— HUOMAUTUS 2 Tyhjä.

— OVR-B-04 [EHDOLLINEN] Jos SVSP on QSVSP, kohdan OVR-B-03 mukaisissa testeissä on tarkastettava erilaiset positiiviset ja negatiiviset käyttötapaukset.

— VPR-B-11 [EHDOLLINEN] Jos SVSP on QSVSP, SVSP:n on ohjattava hajautuslaskentaa (joko suoritettava laskenta palvelimen puolella tai ohjattava asiakasta, jos se on sallittua asiakaspuolella).

— HUOMAUTUS 5 Tyhjä.

— HUOMAUTUS 6 Tyhjä.

— VPR-B-15 [EHDOLLINEN] Jos SVSP on QSVSP, validointiraportin on vaatimusten VPR-B-13 ja VPR-B-14 noudattamiseksi oltava standardin ETSI TS 119 102-2 [9] mukainen.

— VPR-B-16 [EHDOLLINEN] Jos SVSP on QSVSP, toteutuksessa on noudatettava Euroopan kyberturvallisuuden sertifiointiryhmän hyväksymiä ja ENISAn julkaisemia sovittuja salausmekanismeja [10], jotta voidaan käyttää sopivia salaustekniikoita, kun tarjotaan hyväksyttyjä validointipalveluja QES:ää varten.

18) Liite C (informatiivinen) Vaatimusten sovittaminen asetukseen (EU) N:o 910/2014, jakso ”Validoinnin tarjoaminen 32 artiklan 1 kohdan mukaisesti”, toinen kohta:

— Sen varmistamiseksi, että kaikki asetuksen (EU) N:o 910/2014 [i.1] 32 artiklan 1 kohdassa ja 40 artiklassa vaaditut edellytykset todennetaan, tarvitaan oikea validointialgoritmi. Se antaa saman deterministisen tuloksen validoitavaksi toimitetulle allekirjoitukselle tai leimalle. Allekirjoitusten validointipolitiikka on tässä tarkoituksessa olennaisen tärkeä. Standardi ETSI TS 119 172-4 [8], joka perustuu standardissa ETSI EN 319 102-1 [3] määriteltyyn validointialgoritmiin, on annettu tätä silmällä pitäen.

2. ETSI TS 119 172-4

1) 2.1 Velvoittavat viittaukset

— [1] ETSI EN 319 102-1 V1.4.1 (2024-06) ”Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation”.

— Kaikkia viittauksia standardiin ”ETSI TS 119 102-1 [1]” pidetään viittauksina standardiin ”ETSI EN 319 102-1 [1]”.

— [2] ETSI TS 119 612 V2.3.1 (2024-11) ”Electronic Signatures and Infrastructures (ESI); Trusted Lists”.

— [13] ETSI TS 119 101 V1.1.1 (2016-03) ”Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation”.

2) 4.2 Validointirajoitukset ja validointimenettelyt, vaatimus REQ-4.2-03, kohta ”X.509 Validointirajoitukset”, c alakohta:

— i) Jos loppukäyttäjän varmenne muodostaa luottamusankkurin, rajoitusta ”RevocationChecking-Constraints” ei käytetä.

— ii) Jos loppukäyttäjän varmenne ei muodosta luottamusankkuria, rajoituksen ”RevocationChecking-Constraints” arvoksi asetetaan ”eitherCheck”, siten kuin määritellään standardin ETSI TS 119 172-1 [3] lausekkeessa A.4.2.1 olevan taulukon A.2 riveillä (m)2.1.

— iii) Jos loppukäyttäjän varmenne muodostaa luottamusankkurin, standardin ETSI TS 119 172-1 [3] lausekkeessa A.4.2.1 olevan taulukon A.2 riveillä (m)2.2 määriteltyä rajoitusta ”RevocationFreshness-Constraints” ei käytetä.

— iv) Jos loppukäyttäjän varmenne ei muodosta luottamusankkuria, standardin ETS TS 119 172-1 [3] lausekkeessa A.4.2.1 olevan taulukon A.2 riveillä (m)2.2 määriteltyä rajoitusta ”RevocationFreshness-Constraints” käytetään allekirjoitusvarmenteen osalta enimmäisarvolla 24 tuntia. Rajoitukselle ”RevocationFreshnessConstraints” ei aseteta arvoa muille varmenteille kuin allekirjoitusvarmenteelle, aikaleimaa tukevat varmenteet mukaan luettuina.

3) 4.4 Teknisen sovellettavuuden (sääntöjen) tarkastusprosessi

— REQ-4.4.2-03 Jos jokin kohdassa REQ-4.4.2-01 määritellyistä tarkastuksista epäonnistuu,

a) prosessi pysähtyy;

b) allekirjoitus määritellään teknisesti määrittelemättömäksi eli ei EU:n hyväksytyksi sähköiseksi allekirjoitukseksi eikä EU:n hyväksytyksi sähköiseksi leimaksi;

c) edellä esitetty tulos ja kaikkien väliprosessien tulokset on otettava huomioon allekirjoituksen sovellettavuussääntöjä koskevassa tarkastusraportissa.