Europeiska unionens
officiella tidning

SV
L-serien

2025/1943

30.9.2025

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/1943

av den 29 september 2025

om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller referensstandarder för kvalificerade certifikat för elektroniska underskrifter och kvalificerade certifikat elektroniska stämplar

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG ([1]), särskilt artiklarna 28.6 och 38.6, och

av följande skäl:

(1) Kvalificerade certifikat för elektroniska underskrifter och kvalificerade certifikat för elektroniska stämplar spelar en avgörande roll i den digitala affärsmiljön genom att främja övergången från traditionella pappersbaserade processer till motsvarande elektroniska processer. Genom att koppla valideringsuppgifter för en elektronisk underskrift eller valideringsuppgifter för en elektronisk stämpel till en fysisk respektive en juridisk person och genom att bekräfta den personens namn ger kvalificerade certifikat säkrare identifiering av undertecknare och stämpelskapare.

(2) Den presumtion om överensstämmelse som fastställs i artiklarna 28.6 och 38.6 i förordning (EU) nr 910/2014 bör endast tillämpas när kvalificerade betrodda tjänster för utfärdande av kvalificerade certifikat för elektroniska underskrifter och kvalificerade betrodda tjänster för utfärdande av elektroniska stämplar uppfyller de standarder som fastställs i den här förordningen. Dessa standarder bör återspegla etablerad praxis och vara allmänt erkända inom de relevanta sektorerna. De bör anpassas så att de omfattar ytterligare kontroller som säkerställer säkerheten och tillförlitligheten hos de kvalificerade betrodda tjänsterna och innehållet i de kvalificerade certifikaten.

(3) Om en tillhandahållare av betrodda tjänster uppfyller kraven i bilagan till denna förordning bör tillsynsorganen presumera att de relevanta kraven i förordning (EU) nr 910/2014 är uppfyllda och vederbörligen överväga denna presumtion för att bevilja en betrodd tjänst status som kvalificerad eller för att bekräfta sådan status. Det är dock fortfarande tillåtet för en kvalificerad tillhandahållare av betrodda tjänster att använda andra metoder för att visa att kraven i förordning (EU) nr 910/2014 är uppfyllda.

(4) Kommissionen utvärderar regelbundet ny teknik samt nya metoder, standarder eller tekniska specifikationer. I enlighet med skäl 75 i Europaparlamentets och rådets förordning (EU) 2024/1183 ([2]) bör kommissionen vid behov se över och uppdatera denna förordning för att hålla den i linje med den globala utvecklingen, ny teknik samt nya standarder eller tekniska specifikationer och för att följa bästa praxis på den inre marknaden.

(5) Europaparlamentets och rådets förordning (EU) 2016/679 ([3]) och, i förekommande fall, Europaparlamentets och rådets direktiv 2002/58/EG ([4]) är tillämpliga på all behandling av personuppgifter i enlighet med denna förordning.

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

([2]) Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet (EUT L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([3]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter, om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(6) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([5]) och avgav ett yttrande den 6 juni 2025.

(7) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som inrättats genom artikel 48 i förordning (EU) nr 910/2014.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Referensstandarder och specifikationer för kvalificerade certifikat för elektroniska underskrifter och elektroniska stämplar

1. De referensstandarder och specifikationer som avses i artikel 28.6 i förordning (EU) nr 910/2014 anges i bilaga I till den här förordningen.

2. De referensstandarder och specifikationer som avses i artikel 38.6 i förordning (EU) nr 910/2014 anges i bilaga II till den här förordningen.

Artikel 2

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 29 september 2025.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

([5]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

BILAGA I

Förteckning över referensstandarder och specifikationer för kvalificerade certifikat för elektroniska underskrifter

Standarderna Etsi EN 319 411-2 V2.6.1 (*Etsi EN 319 411-2*), Etsi EN 319 412-1 V1.6.1 (*Etsi EN 319 412-1*), Etsi EN 319 412-2 V2.4.1 (*Etsi EN 319 412-2*) och Etsi EN 319 412-5 V2.5.1 (*Etsi EN 319 412-5*) gäller med följande anpassningar:

1. För Etsi EN 319 411-2

(1) 2.1 Normativa hänvisningar

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

— [2] Etsi EN 319 411-1 V1.5.1 (2025-04) *Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements*, med följande anpassningar:

Klausul 2.1 Normativa hänvisningar i Etsi EN 319 411-1 V1.5.1 ska ändras på följande sätt:

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

— [10] Etsi EN 319 412-2 V2.4.1 *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons*.

— [14] Etsi EN 319 412-1 V1.6.1 *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*.

— [3] Etsi EN 319 412-5 V2.5.1 *Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*.

— [5] Etsi EN 319 412-1 V1.6.1 *Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*.

— [6] CEN/TS 419261:2015 *Security requirements for trustworthy systems managing certificates and time-stamps*.

— [7] Europeiska gruppen för cybersäkerhetscertifiering, undergruppen för kryptografi: *Agreed Cryptographic Mechanisms*, offentliggjord av Europeiska unionens cybersäkerhetsbyrå (Enisa) ([1]).

— [8] Kommissionens genomförandeförordning (EU) 2024/482 ([2]) om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC).

— [9] Kommissionens genomförandeförordning (EU) 2024/3144 om ändring av genomförandeförordning (EU) 2024/482 vad gäller tillämpliga internationella standarder och om rättelse av den genomförandeförordningen ([3]).

— [10] ISO/IEC 15408:2022 (delarna 1–5): *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security*.

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

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([3]) EUT L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

(2) 5.2 Krav på förklaringar om certifieringspraxis

— OVR-5.2-02 I de certifikatpolicyer som anges i dokumentationen från tillhandahållaren av betrodda tjänster ska kraven på de certifikatprofiler som ska användas specifieras.

(3) 5.3 Certifikatpolicyns benämning och identifiering

— OVR-5.3-01 Om en certifikatpolicy enligt beskrivningen i klausul 4.2.2 ändras på ett sätt som påverkar tillämpligheten ska policyns identifierare ändras.

(4) 6.1 Ansvar för offentliggörande och datakatalog

— OVR-6.1-02 Den information som anges i DIS-6.1-04 i Etsi EN 319 411-1 [2] ska vara offentligt och internationellt tillgänglig.

(5) 6.2.2 Initial identitetsvalidering

— REG-6.2.2-01A Insamling av attribut och bevis för certifikatinnehavarens identitet samt validering av dessa ska ske i enlighet med vad som anges i de genomförandeakter som antagits i enlighet med artikel 24.1c i förordning (EU) nr 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] och [QCP-n-qscd] Den fysiska personens identitet och, i tillämpliga fall, eventuella särskilda attribut för personen, ska kontrolleras i enlighet med de genomförandeakter som antagits i enlighet med artikel 24.1c i förordning (EU) nr 910/2014 [i.1].

— ANMÄRKNING 1 ogiltig.

(6) 6.3.3 Utfärdande av certifikat

— GEN-6.3.3-01 Kraven GEN-6.3.3-01 till GEN-6.3.3-10 som anges i Etsi EN 319 411-1 [2], klausul 6.3.3 ska tillämpas.

— GEN-6.3.3-02 [CONDITIONAL] Om ett certifikat utfärdas till en fysisk person som identifierats tillsammans med den juridiska personen ska de attribut för certifikatinnehavare som identifierar organisationen i certifikatet representera den juridiska personen, alternativt underenheten inom den juridiska personen, medan identifieraren för certifikatinnehavare i certifikatet ska hänvisa till den fysiska personen.

— GEN-6.3.3-03 Identifieraren för certifikatpolicyn ska vara [CHOICE]:

(a) [QCP-n]

— såsom anges i klausul 5.3 a och/eller

— ett OID som tilldelats av tillhandahållaren av betrodda tjänster, annan berörd part eller ytterligare standardisering för en certifikatpolicy som förbättrar de tillämpliga krav på policyer som anges i detta dokument.

(b) [QCP-n-qscd]

— såsom anges i klausul 5.3 c och/eller

— ett OID som tilldelats av tillhandahållaren av betrodda tjänster, annan berörd part eller ytterligare standardisering för en certifikatpolicy som förbättrar de tillämpliga krav på policyer som anges i detta dokument.

(7) 6.3.5 Användning av nyckelpar och certifikat

— SDP-6.3.5-02A [CONDITIONAL] Om tillhandahållaren av betrodda tjänster förvaltar anordningen för skapande av kvalificerade underskrifter för certifikatinnehavaren ska tillhandahållaren vara en kvalificerad tillhandahållare av betrodda tjänster som tillhandahåller en kvalificerad betrodd tjänst för förvaltningen av en kvalificerad anordning för skapande av elektroniska underskrifter på distans, i enlighet med förordning (EU) nr 910/2014 [i.1].

— SDP-6.3.5-11A Om certifikatmottagaren eller certifikatinnehavaren genererar certifikatinnehavarens nycklar ska certifikatmottagarens skyldigheter (se klausul 6.3.4) innefatta

(a) en skyldighet att generera nycklar för certifikatinnehavaren med hjälp av en algoritm som överensstämmer med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering [7] och offentliggjorts av Enisa för användning av den certifierade nyckeln i enlighet med certifikatpolicyn och

(b) en skyldighet att använda en längd och en algoritm för nycklarna som överensstämmer med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering [7] och offentliggjorts av Enisa för användning av den certifierade nyckeln i enlighet med certifikatpolicyn under certifikatets giltighetstid.

(8) 6.3.10 Certifikatstatustjänster

— CSS-6.3.10-08 [CONDITIONAL] Om förteckningar över återkallade certifikat tillhandahålls ska tillhandahållaren av betrodda tjänster se till att den senaste förteckningen är intakt och tillgänglig som minst under den period som anges i certifikatpolicyn, i enlighet med kraven i CSS-6.3.10-12.

(9) 6.4.4 Personalkontroller

— OVR-6.4.4-02 Den personal i betrodda roller som arbetar för tillhandahållaren av betrodda tjänster och, i tillämpliga fall, underleverantörer i betrodda roller, ska kunna uppfylla kravet på expertkunskap, erfarenhet och kvalifikationer genom formell utbildning och meriter, eller faktisk erfarenhet, eller en kombination av dessa.

— OVR-6.4.4-03 Överensstämmelse med OVR-6.4.4-02 ska omfatta regelbundna (minst var tolfte månad) uppdateringar om nya hot och aktuella säkerhetsrutiner.

— OVR-6.4.4-04 Utöver de betrodda roller som anges i Etsi EN 319 401 [1], (klausul 7.2-15), ska de betrodda rollerna för registrerings- och återkallandetjänstemän med ansvar enligt definitionen i TS 419261 [6] stödjas. I fall där tillhandahållaren av kvalificerade betrodda tjänster förvaltas direkt av, alternativt drivs på uppdrag av, en medlemsstat eller ett offentligt organ får dessa ytterligare betrodda roller fullgöras av en eller flera formella representanter som agerar för och på uppdrag av de registrerings- och återkallandetjänstemän som tjänstgör vid lokala eller regionala förvaltningar.

(10) 6.4.9 Certifikatutfärdares eller registreringsinstans avveckling

— OVR-6.4.9-02 Tillhandahållarens avvecklingsplan ska uppfylla kraven i de genomförandeakter som antagits i enlighet med artikel 24.5 i förordning (EU) nr 910/2014.

(11) 6.5.1 Generering och installation av nyckelpar

— OVR-6.5.1-01A Certifikatutfärdares generering av nyckelpar ska utföras med en algoritm som överensstämmer med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [7] för certifikatutfärdarens underteckningsändamål.

— OVR-6.5.1-01B Den längd och algoritm som används för certifikatutfärdarens underskriftsnyckel ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [7] för certifikatutfärdarens underteckningsändamål.

— OVR-6.5.1-01C [CONDITIONAL] Om certifikatutfärdaren genererar certifikatinnehavarens nycklar ska dessa nycklar överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [7] för de ändamål som anges i certifikatpolicyn under certifikatets giltighetstid.

(12) 6.5.2 Skydd av privata nycklar och tekniska kontrollåtgärder för kryptografiska moduler

— GEN-6.5.2-01 Alla de krav som anges i Etsi EN 319 411-1 [2], klausul 6.5.2 ska tillämpas med undantag för kraven OVR-6.5.2-01, OVR-6.5.2-03 och OVR-6.5.2-04.

— GEN-6.5.2-02 Den generering av nyckelpar, inklusive nycklar som används av återkallande- och registreringstjänster, som utförs av tillhandahållaren av betrodda tjänster ska utföras inom en krypteringshårdvara som utgör ett tillförlitligt system som certifierats i enlighet med

— de gemensamma kriterierna för utvärdering av informationsteknologisk säkerhet, såsom dessa anges i ISO/IEC 15408 [10] eller i *Common Criteria for Information Technology Security Evaluation*, version CC:2002, delarna 1–5, som offentliggjorts av deltagarna i *Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security* och certifierats på nivå EAL 4 eller högre eller

— den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) [8][9] och certifierats på nivå EAL 4 eller högre eller

— till och med den 31.12.2030, FIPS PUB 140-3 [11] nivå 3.

Denna certifiering ska avse ett säkerhetsmål eller en skyddsprofil, eller en modulkonstruktion och säkerhetsdokumentation, som uppfyller kraven i detta dokument, på grundval av en riskanalys och med beaktande av fysiska och andra icke-tekniska säkerhetsåtgärder.

Om krypteringshårdvaran omfattas av en EUCC [8][9]-certifiering ska hårdvaran konfigureras och användas i enlighet med den certifieringen.

— GEN-6.5.2-03 Certifikatutfärdarens privata underskriftsnyckel ska lagras och användas inom en krypteringshårdvara som uppfyller kraven i GEN-6.5.2-01 och GEN-6.5.2-02.

(13) 6.5.7 Nätverkssäkerhetskontroller

— OVR-6.5.7-02 Den sårbarhetsskanning som krävs enligt REQ-7.8-13 i Etsi EN 319 401 [1] ska utföras minst en gång per kvartal.

— OVR-6.5.7-03 Det penetrationstest som krävs enligt REQ-7.8-17X i Etsi EN 319 401 [1] ska utföras minst en gång om året.

— OVR-6.5.7-04 Brandväggar ska konfigureras så att de förhindrar alla protokoll och åtkomster som inte krävs för driften av tillhandahållaren av betrodda tjänster.

(14) 6.6.1 Certifikatprofil

— GEN-6.6.1-05 Certifikatet ska innehålla en av de policyidentifieringar som anges i GEN-6.3.3-03 [CHOICE]. Certifikatet får innehålla andra OID:n som tilldelats av tillhandahållaren av betrodda tjänster.

2. För Etsi EN 319 412-2

(1) 2.1 Normativa hänvisningar

— [2] Etsi EN 319 412-5 V2.5.1 *Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*.

— [9] Europeiska gruppen för cybersäkerhetscertifiering, undergruppen för kryptografi, *Agreed Cryptographic Mechanisms*, offentligjord av *ENISA*.

(2) 4.2.2 Underskrift

— GEN-4.2.2-2 Valet av underskriftsalgoritm ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [9].

— ANMÄRKNING ogiltig.

(3) 4.2.3.1 Utfärdare som är juridiska personer

— GEN-4.2.3.1-3 Om det är känt att det finns ett lämpligt registreringsnummer, ska utfärdarens identitet innehålla attributet *organizationIdentifier* med det registreringsnumret, såsom det anges i det officiella register genom vilket numret upprättats.

(4) 4.2.5 Information om öppen nyckel för certifikatinnehavare

— GEN-4.2.5-2 Valet av öppen nyckel för certifikatinnehavare ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [9].

— ANMÄRKNING ogiltig.

(5) 4.2.6 Serienummer

— GEN-4.2.6-01 Certifikatets serienummer (enligt IETF RFC 5280 [1] klausul 4.1.2.2) ska vara unikt för varje certifikat som utfärdas av tillhandahållaren av betrodda tjänster.

BILAGA II

Förteckning över referensstandarder och specifikationer för kvalificerade certifikat för elektroniska stämplar

Standarderna Etsi EN 319 411-2 V2.6.1 (*Etsi EN 319 411-2*), Etsi EN 319 412-1 V1.6.1 (*Etsi EN 319 412-1*), Etsi EN 319 412-3 V1.3.1 (*Etsi EN 319 412-3*), Etsi EN 319 412-2 V2.4.1 (*Etsi EN 319 412-2*) och Etsi EN 319 412-5 V2.5.1 (*Etsi EN 319 412-5*) gäller med följande anpassningar:

1. För Etsi EN 319 411-2

(1) 2.1 Normativa hänvisningar

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

— [2] Etsi EN 319 411-1 V1.5.1 (2025-04) *Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements*, med följande anpassningar:

Klausul 2.1 Normativa hänvisningar i Etsi EN 319 411-1 V1.5.1 ska ändras på följande sätt:

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

— [10] Etsi EN 319 412-2 V2.4.1 *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.*

— [14] Etsi EN 319 412-1 V1.6.1 *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.*

— [3] Etsi EN 319 412-5 V2.5.1 *Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.*

— [5] Etsi EN 319 412-1 V1.6.1 *Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.*

— [6] CEN/TS 419261:2015 *Security requirements for trustworthy systems managing certificates and time-stamps* (framtagen av CEN).

— [7] Europeiska gruppen för cybersäkerhetscertifiering, undergruppen för kryptografi: *Agreed Cryptographic Mechanisms*, offentliggjord av Enisa.

— [8] Kommissionens genomförandeförordning (EU) 2024/482 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC).

— [9] Genomförandeförordning (EU) 2024/3144 om ändring av genomförandeförordning (EU) 2024/482 vad gäller tillämpliga internationella standarder och om rättelse av den genomförandeförordningen.

— [10] ISO/IEC 15408:2022 (delarna 1–5) *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security.*

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

(2) 5.2 Krav på förklaringar om certifieringspraxis

— OVR-5.2-02 I de certifikatpolicyer som anges i dokumentationen från tillhandahållaren av betrodda tjänster ska kraven på de certifikatprofiler som ska användas specificeras.

(3) 5.3 Certifikatpolicyns benämning och identifiering

— OVR-5.3-01 Om en certifikatpolicy enligt beskrivningen i klausul 4.2.2 ändras på ett sätt som påverkar tillämpligheten ska policyns identifierare ändras.

(4) 6.1 Ansvar för offentliggörande och datakatalog

— OVR-6.1-02 Den information som anges i DIS-6.1-04 i Etsi EN 319 411-1 [2] ska vara offentligt och internationellt tillgänglig.

(5) 6.2.2 Initial identitetsvalidering

— REG-6.2.2-01A Insamling av attribut och bevis för certifikatinnehavarens identitet samt validering av dessa ska ske i enlighet med vad som anges i de genomförandeakter som antagits i enlighet med artikel 24.1c i förordning (EU) nr 910/2014 [i.1].

— REG-6.2.2-03 [QCP-n] och [QCP-n-qscd] Den juridiska personens identitet och, i tillämpliga fall, eventuella särskilda attribut, ska kontrolleras i enlighet med de genomförandeakter som antagits i enlighet med artikel 24.1c i förordning (EU) nr 910/2014 [i.1].

— ANMÄRKNING 3, se anmärkning 2.

(6) 6.3.3 Utfärdande av certifikat

— GEN-6.3.3-01 Kraven GEN-6.3.3-01 till GEN-6.3.3-10 som anges i Etsi EN 319 411-1 [2], klausul 6.3.3 ska tillämpas.

— GEN-6.3.3-02 Identifieraren för certifikatpolicyn ska vara [CHOICE]:

(a) [QCP-l]

— såsom anges i klausul 5.3 b och/eller

— ett OID som tilldelats av tillhandahållaren av betrodda tjänster, annan berörd part eller ytterligare standardisering för en certifikatpolicy som förbättrar de tillämpliga krav på policyer som anges i detta dokument.

(b) [QCP-l-qscd]

— såsom anges i klausul 5.3 d och/eller

— ett OID som tilldelats av tillhandahållaren av betrodda tjänster, annan berörd part eller ytterligare standardisering för en certifikatpolicy som förbättrar de tillämpliga krav på policyer som anges i detta dokument.

(7) 6.3.5 Användning av nyckelpar och certifikat

— SDP-6.3.5-02A [CONDITIONAL] Om tillhandahållaren av betrodda tjänster förvaltar anordningen för skapande av kvalificerade underskrifter för certifikatinnehavaren ska tillhandahållaren vara en kvalificerad tillhandahållare av betrodda tjänster som tillhandahåller en kvalificerad betrodd tjänst för förvaltningen av en kvalificerad anordning för skapande av elektroniska stämplar på distans, i enlighet med förordning (EU) nr 910/2014 [i.1].

— SDP-6.3.5-11A Om certifikatmottagaren eller certifikatinnehavaren genererar certifikatinnehavarens nycklar ska certifikatmottagarens skyldigheter (se klausul 6.3.4) innefatta

(a) en skyldighet att generera nycklar för certifikatinnehavaren med hjälp av en algoritm som överensstämmer med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [7] för användning av den certifierade nyckeln i enlighet med certifikatpolicyn och

(b) en skyldighet att använda en längd och en algoritm för nycklarna som överensstämmer med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhets-certifiering och offentliggjorts av Enisa [7] för användning av den certifierade nyckeln i enlighet med certifikatpolicyn under certifikatets giltighetstid.

(8) 6.3.10 Certifikatstatustjänster

— CSS-6.3.10-08 [CONDITIONAL] Om förteckningar över återkallade certifikat tillhandahålls ska tillhandahållaren av betrodda tjänster se till att den senaste förteckningen är intakt och tillgänglig som minst under den period som anges i certifikatpolicyn, i enlighet med kraven i CSS-6.3.10-12.

(9) 6.4.4 Personalkontroller

— OVR-6.4.4-02 Den personal i betrodda roller som arbetar för tillhandahållaren av betrodda tjänster och, i tillämpliga fall, underleverantörer i betrodda roller, ska kunna uppfylla kravet på expertkunskap, erfarenhet och kvalifikationer genom formell utbildning och meriter, eller faktisk erfarenhet, eller en kombination av dessa.

— OVR-6.4.4-03 Överensstämmelse med OVR-6.4.4-02 ska omfatta regelbundna (minst var tolfte månad) uppdateringar om nya hot och aktuella säkerhetsrutiner.

— OVR-6.4.4-04 Utöver de betrodda roller som anges i Etsi EN 319 401 [1], (klausul 7.2-15), ska de betrodda rollerna för registrerings- och återkallandetjänstemän med ansvar enligt definitionen i TS 419261 [6] stödjas. I fall där tillhandahållaren av kvalificerade betrodda tjänster förvaltas direkt av, alternativt drivs på uppdrag av, en medlemsstat eller ett offentligt organ får dessa ytterligare betrodda roller fullgöras av en eller flera formella representanter som agerar för och på uppdrag av de registrerings- och återkallandetjänstemän som tjänstgör vid lokala eller regionala förvaltningar.

(10) 6.4.9 Certifikatutfärdares eller registreringsinstans avveckling

— OVR-6.4.9-02 Tillhandahållarens avvecklingsplan ska uppfylla kraven i de genomförandeakter som antagits i enlighet med artikel 24.5 i förordning (EU) nr 910/2014 [i.1]].

(11) 6.5.1 Generering och installation av nyckelpar

— OVR-6.5.1-01A Certifikatutfärdares generering av nyckelpar ska utföras med en algoritm som överensstämmer med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [7] för certifikatutfärdarens underteckningsändamål.

— OVR-6.5.1-01B Den längd och algoritm som används för certifikatutfärdarens underskriftsnyckel ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [7] för certifikatutfärdarens underteckningsändamål.

— OVR-6.5.1-01C [CONDITIONAL] Om certifikatutfärdaren genererar certifikatinnehavarens nycklar ska dessa nycklar överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [7] för de ändamål som anges i certifikatpolicyn under certifikatets giltighetstid.

(12) 6.5.2 Skydd av privata nycklar och tekniska kontrollåtgärder för kryptografiska moduler

— GEN-6.5.2-01 Alla de krav som anges i Etsi EN 319 411-1 [2], klausul 6.5.2 ska tillämpas med undantag för kraven OVR-6.5.2-01, OVR-6.5.2-03 och OVR-6.5.2-04.

— GEN-6.5.2-02 Den generering av nyckelpar, inklusive nycklar som används av återkallande- och registreringstjänster, som utförs av tillhandahållaren av betrodda tjänster ska utföras inom en krypteringshårdvara som utgör ett tillförlitligt system som certifierats i enlighet med

  — de gemensamma kriterierna för utvärdering av informationsteknologisk säkerhet, såsom dessa anges i ISO/IEC 15408 [10] eller i *Common Criteria for Information Technology Security Evaluation*, version CC:2002, delarna 1–5, som offentliggjorts av deltagarna i *Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security* och certifierats på nivå EAL 4 eller högre eller

  — den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) [8][9] och certifierats på nivå EAL 4 eller högre eller

  — till och med den 31.12.2030, FIPS PUB 140-3 [11] nivå 3.

Denna certifiering ska avse ett säkerhetsmål eller en skyddsprofil, eller en modulkonstruktion och säkerhetsdokumentation, som uppfyller kraven i detta dokument, på grundval av en riskanalys och med beaktande av fysiska och andra icke-tekniska säkerhetsåtgärder.

Om krypteringshårdvaran omfattas av en EUCC [8][9]-certifiering ska hårdvaran konfigureras och användas i enlighet med den certifieringen.

— GEN-6.5.2-03 Certifikatutfärdarens privata underskriftsnyckel ska lagras och användas inom en krypteringshårdvara som uppfyller kraven i GEN-6.5.2-01 och GEN-6.5.2-02.

(13) 6.5.7 Nätverkssäkerhetskontroller

— OVR-6.5.7-02 Den sårbarhetsskanning som krävs enligt REQ-7.8-13 i Etsi EN 319 401 [1] ska utföras minst en gång per kvartal.

— OVR-6.5.7-03 Det penetrationstest som krävs enligt REQ-7.8-17X i Etsi EN 319 401 [1] ska utföras minst en gång om året.

— OVR-6.5.7-04 Brandväggar ska konfigureras så att de förhindrar alla protokoll och åtkomster som inte krävs för driften av tillhandahållaren av betrodda tjänster.

(14) 6.6.1 Certifikatprofil

— GEN-6.6.1-05 Certifikatet ska innehålla en av de policyidentifieringar som anges i GEN-6.3.3-02 [CHOICE].

2. För Etsi EN 319 412-3

(1) 2.1 Normativa hänvisningar

— [2] Etsi EN 319 412-2 V2.4.1 *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons*.

(2) 4.2.1 Certifikatinnehavare

— LEG-4.2.1-6 Attributet organizationIdentifier ska innehålla en annan identifiering än organisationsnamnet för den organisation som är certifikatinnehavare. Om det är känt att det finns ett lämpligt registreringsnummer, ska attributet organizationIdentifier innehålla det registreringsnumret, såsom det anges i det officiella register genom vilket numret upprättats.

3. För Etsi EN 319 412-2:

(1) 2.1 Normativa hänvisningar

— [2] Etsi EN 319 412-5 V2.5.1 *Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*.

— [9] Europeiska gruppen för cybersäkerhetscertifiering, undergruppen för kryptografi: *Agreed Cryptographic Mechanisms*, offentliggjord av Enisa.

(2) 2.2 Informativa hänvisningar

— [i.7] ogiltig.

(3) 4.2.2 Underskrift

— GEN-4.2.2-2 Valet av underskriftsalgoritm ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [9].

— ANMÄRKNING ogiltig.

(4) 4.2.3.1 Utfärdare som är juridiska personer

— GEN-4.2.3.1-3 Om det är känt att det finns ett lämpligt registreringsnummer, ska utfärdarens identitet innehålla attributet *organizationIdentifier* med det registreringsnumret, såsom det anges i det officiella register genom vilket numret upprättats.

(5) 4.2.5 Information om öppen nyckel för certifikatinnehavare

— GEN-4.2.5-2 Valet av öppen nyckel för certifikatinnehavare ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [9].

— ANMÄRKNING ogiltig.

(6) 4.2.6 Serienummer

— GEN-4.2.6-01 Certifikatets serienummer (enligt IETF RFC 5280 [1] klausul 4.1.2.2) ska vara unikt för varje certifikat som utfärdas av tillhandahållaren av betrodda tjänster.