2025/1943

30.9.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/1943

af 29. september 2025

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår referencestandarder for kvalificerede certifikater for elektroniske signaturer og kvalificerede certifikater for elektroniske segl

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF ([1]), særlig artikel 28, stk. 6, og artikel 38, stk. 6, og

ud fra følgende betragtninger:

(1) Kvalificerede certifikater for elektroniske signaturer og kvalificerede certifikater for elektroniske segl spiller en afgørende rolle i det digitale erhvervsmiljø ved at fremme overgangen fra traditionelle papirbaserede processer til tilsvarende elektroniske processer. Ved at knytte valideringsdata for elektroniske signaturer eller elektroniske segl til henholdsvis en fysisk eller juridisk person og ved at bekræfte denne persons navn øger kvalificerede certifikater sikkerheden med hensyn til underskriverens og den forseglende parts identitet.

(2) Den formodning om overholdelse, der er fastsat i artikel 28, stk. 6, og artikel 38, stk. 6, i forordning (EU) nr. 910/2014, bør kun finde anvendelse, hvis kvalificerede tillidstjenester til udstedelse af kvalificerede certifikater for elektroniske signaturer og kvalificerede tillidstjenester til udstedelse af kvalificerede certifikater for elektroniske segl overholder de standarder, der er fastsat i denne forordning. Disse standarder bør afspejle etableret praksis og være bredt anerkendt inden for de relevante sektorer. De bør tilpasses, så de omfatter yderligere kontrol, der sikrer de kvalificerede tillidstjenesters sikkerhed og troværdighed og indholdet af de kvalificerede certifikater.

(3) Hvis en tillidstjenesteudbyder overholder kravene i bilaget til denne forordning, bør tilsynsorganerne antage, at de relevante krav i forordning (EU) nr. 910/2014 er opfyldt, og tage behørigt hensyn til en sådan formodning i forbindelse med tildeling eller bekræftelse af tillidstjenestens status som kvalificeret. En kvalificeret tillidstjenesteudbyder kan dog stadig anvende anden praksis til at påvise overholdelse af kravene i forordning (EU) nr. 910/2014.

(4) Kommissionen vurderer regelmæssigt nye teknologier, praksisser, standarder eller tekniske specifikationer. I overensstemmelse med betragtning 75 til Europa-Parlamentets og Rådets forordning (EU) 2024/1183 ([2]) bør Kommissionen efter behov revidere og ajourføre denne forordning for at sikre dens overensstemmelse med den globale udvikling, nye teknologier, standarder eller tekniske specifikationer og for at følge bedste praksis på det indre marked.

(5) Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([3]) og, hvor det er relevant, Europa-Parlamentets og Rådets direktiv 2002/58/EF ([4]) finder anvendelse på alle behandlingsaktiviteter vedrørende personoplysninger i henhold til nærværende forordning.

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

([2]) Europa-Parlamentets og Rådets forordning (EU) 2024/1183 af 11. april 2024 om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af den europæiske ramme for digital identitet (EUT L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([3]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(6) Den Europæiske Tilsynsførende for Databeskyttelse blev hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([5]) og afgav udtalelse den 6. juni 2025.

(7) Foranstaltningerne i nærværende forordning er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 48 i forordning (EU) nr. 910/2014 —

VEDTAGET DENNE FORORDNING:

Artikel 1

Referencestandarder og specifikationer for kvalificerede certifikater for elektroniske signaturer og elektroniske segl

1. De referencestandarder og specifikationer, der er omhandlet i artikel 28, stk. 6, i forordning (EU) nr. 910/2014, er fastsat i bilag I til nærværende forordning.

2. De referencestandarder og specifikationer, der er omhandlet i artikel 38, stk. 6, i forordning (EU) nr. 910/2014, er fastsat i bilag II til nærværende forordning.

Artikel 2

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 29. september 2025.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

([5]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

BILAG I

Liste over referencestandarder og specifikationer for kvalificerede certifikater for elektroniske signaturer

Standard 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«) og ETSI EN 319 412-5 V2.5.1 (»ETSI EN 319 412-5«) finder anvendelse med følgende tilpasninger:

1. For ETSI EN 319 411-2:

   1) 2.1 Normative references

      — [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 følgende tilpasninger:

         I punkt 2.1 Normative references i ETSI EN 319 411-1 V1.5.1 foretages følgende ændringer:

         — [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] Den Europæiske Cybersikkerhedscertificeringsgruppe, undergruppen om kryptografi: »Agreed Cryptographic Mechanisms«, offentliggjort af Den Europæiske Unions Agentur for Cybersikkerhed (»ENISA«) ([1]).

      — [8] Kommissionens gennemførelsesforordning (EU) 2024/482 ([2]) om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2019/881 for så vidt angår vedtagelsen af den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (EUCC).

      — [9] Kommissionens gennemførelsesforordning (EU) 2024/3144 ([3]) om ændring af gennemførelsesforordning (EU) 2024/482 for så vidt angår gældende internationale standarder og om berigtigelse af nævnte gennemførelsesforordning.

      — [10] ISO/IEC 15408:2022 (del 1 til 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 Certification Practice Statement Requirements

— OVR-5.2-02 De certifikatpolitikker, der er identificeret i tillidstjenesteudbyderens dokumentation, skal angive kravene til de certifikatprofiler, der skal anvendes.

3) 5.3 Certificate Policy name and identification

— OVR-5.3-01 Hvis der foretages ændringer af en certifikatpolitik som beskrevet i punkt 4.2.2, der påvirker anvendeligheden, skal politikidentifikatoren ændres.

4) 6.1 Publication and repository responsibilities

— OVR-6.1-02 Oplysningerne i DIS-6.1-04 i ETSI EN 319 411-1 [2] skal være offentligt og internationalt tilgængelige.

5) 6.2.2 Initial identity validation

— REG-6.2.2-01A Indsamlingen af attributter og dokumentation for emnets identitet samt valideringen heraf skal ske som angivet i overensstemmelse med de gennemførelsesretsakter, der er vedtaget i henhold til artikel 24, stk. 1c, i forordning (EU) nr. 910/2014 [i.1].

— REG-6.2.2-02 [QCP-n] og [QCP-n-qscd] Identiteten af og, hvis det er relevant, attributter knyttet til en fysisk person skal verificeres i overensstemmelse med de gennemførelsesretsakter, der er vedtaget i henhold til artikel 24, stk. 1c, i forordning (EU) nr. 910/2014 [i.1].

— NOTE 1 udgår.

6) 6.3.3 Certificate issuance

— GEN-6.3.3-01 Kravene GEN-6.3.3-01 til GEN-6.3.3-10 i ETSI EN 319 411-1 [2], afsnit 6.3.3, finder anvendelse.

— GEN-6.3.3-02 [BETINGET] Hvis et certifikat udstedes til en fysisk person, der identificeres i tilknytning til den juridiske person, skal de emneattributter, der identificerer organisationen i certifikatet, repræsentere den juridiske person eller en underenhed af nævnte juridiske person, og emneidentifikatoren i certifikatet skal være den fysiske person.

— GEN-6.3.3-03 CP-identifikatoren skal være [CHOICE]:

a) [QCP-n]

— som angivet i punkt 5.3, litra a), og/eller

— en OID, der er tildelt af tillidstjenesteudbyderen, en anden relevant interessent eller gennem yderligere standardisering, for en certifikatpolitik, der udbygger de tilsvarende gældende politikkrav, som er defineret i dette dokument.

b) [QCP-n-qscd]

— som specificeret i punkt 5.3, litra c), og/eller

— en OID, der er tildelt af tillidstjenesteudbyderen, en anden relevant interessent eller gennem yderligere standardisering, for en certifikatpolitik, der udbygger de tilsvarende gældende politikkrav, som er defineret i dette dokument.

7) 6.3.5 Key Pair and Certificate Usage

— SDP-6.3.5-02A [BETINGET] Hvis tillidstjenesteudbyderen forvalter det kvalificerede elektroniske signatur-/seglgenereringssystem for emnet, skal tillidstjenesteudbyderen være en kvalificeret tillidstjenesteudbyder, der udbyder en kvalificeret tillidstjeneste til forvaltning af et kvalificeret elektronisk signaturgenereringssystem på afstand i overensstemmelse med forordning (EU) nr. 910/2014 [i.1].

— SDP-6.3.5-11A Abonnentens forpligtelser (se punkt 6.3.4) skal, hvis abonnenten eller emnet genererer emnets nøgler, omfatte:

a) en forpligtelse til at generere emnets nøgler ved hjælp af en algoritme, der er i overensstemmelse med de aftalte kryptografiske mekanismer, som er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe [7] og offentliggjort af ENISA, til de anvendelser af den certificerede nøgle, der er identificeret i certifikatpolitikken

b) en forpligtelse til at anvende en nøglelængde og algoritme, der er i overensstemmelse med de aftalte kryptografiske mekanismer, som er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe [7] og offentliggjort af ENISA, til de anvendelser af den certificerede nøgle, der er identificeret i certifikatpolitikken, i certifikatets gyldighedsperiode.

8) 6.3.10 Certificate Status Services

— CSS-6.3.10-08 [BETINGET] Hvis der stilles CRL'er til rådighed, skal tillidstjenesteudbyderen opretholde integriteten og tilgængeligheden af den seneste CRL som minimum i den periode, der er angivet i certifikatpolitikerklæringen, som krævet i CSS-6.3.10-12.

9) 6.4.4 Personnel Controls

— OVR-6.4.4-02 Tillidstjenesteudbyderens personale i betroede roller og, hvis det er relevant, dennes underleverandører i betroede roller skal kunne opfylde kravet om at have opnået »ekspertviden, erfaring og kvalifikation« gennem formel uddannelse og eksaminer eller faktisk erfaring eller en kombination af de to.

— OVR-6.4.4-03 Overholdelse af OVR-6.4.4-02 skal omfatte regelmæssige (mindst hver 12. måned) opdateringer om nye trusler og aktuel sikkerhedspraksis.

— OVR-6.4.4-04 Ud over de betroede roller, der er identificeret i ETSI EN 319 401 [1] (punkt 7.2-15), skal betroede roller for medarbejdere, der beskæftiger sig med registrering og tilbagekaldelser, og som har ansvar som defineret i TS 419261 [6], understøttes. I tilfælde, hvor den kvalificerede tillidstjenesteudbyder forvaltes direkte af eller drives på vegne af en medlemsstat eller en offentlig myndighed, kan disse yderligere betroede roller varetages af en eller flere formelle repræsentanter, der handler for og på vegne af de registrerings- og tilbagekaldelsesmedarbejdere, der fungerer i lokale eller regionale forvaltninger.

10) 6.4.9 CA or RA Termination

— OVR-6.4.9-02 Tillidstjenesteudbyderens plan i tilfælde af virksomhedsafbrydelse skal opfylde kravene i de gennemførelsesretsakter, der er vedtaget i henhold til artikel 24, stk. 5, i forordning (EU) nr. 910/2014 [i.1].

11) 6.5.1 Key Pair Generation and Installation

— OVR-6.5.1-01A Certificeringsmyndigheders generering af nøglepar skal ske ved hjælp af en algoritme, der er i overensstemmelse med de aftalte kryptografiske mekanismer, som er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [7] til certificeringsmyndighedens signeringsformål.

— OVR-6.5.1-01B Den valgte nøglelængde og algoritme for certificeringsmyndighedens signeringsnøgle skal være i overensstemmelse med de aftalte kryptografiske mekanismer, som er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [7] til certificeringsmyndighedens signeringsformål.

— OVR-6.5.1-01C [BETINGET] Hvis certificeringsmyndigheden genererer emnets nøgler, skal nøgler genereret af certificeringsmyndigheden være i overensstemmelse med de aftalte kryptografiske mekanismer, som er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [7], til de formål, der er angivet i certificeringspolitikken i certifikatets gyldighedsperiode.

12) 6.5.2 Private key protection and cryptographic module engineering controls

— GEN-6.5.2-01 Alle krav i ETSI EN 319 411-1 [2], afsnit 6.5.2, finder anvendelse, undtagen krav OVR-6.5.2-01, OVR-6.5.2-03 og OVR-6.5.2-04.

— GEN-6.5.2-02 Tillidstjenesteudbyderens generering af nøglepar, herunder nøgler, der anvendes af tilbagekaldelses- og registreringstjenester, skal foretages i en sikker kryptografisk enhed, som er et pålideligt system, der er certificeret i overensstemmelse med:

— Fælles kriterier for evaluering af informationsteknologisikkerhed, jf. ISO/IEC 15408 [10] eller Fælles kriterier for evaluering af informationsteknologisikkerhed, version CC:2002, del 1-5, der er offentliggjort af deltagerne i ordningen vedrørende anerkendelse af certifikater for fælles kriterier inden for IT-sikkerhed og certificeret til EAL 4 eller højere, eller

— den europæiske ordning for cybersikkerhedscertificering baseret på fælles kriterier (EUCC) [8][9] og certificeret til EAL 4 eller højere eller

— indtil den 31.12.2030, FIPS PUB 140-3 [11] niveau 3.

Denne certificering skal omfatte et sikkerhedsmål eller en beskyttelsesprofil eller et moduldesign og sikkerhedsdokumentation, der opfylder kravene i dette dokument, på grundlag af en risikoanalyse og under hensyntagen til fysiske og andre ikketekniske sikkerhedsforanstaltninger.

Hvis den sikre kryptografiske enhed er omfattet af en certificering under EUCC [8][9], skal enheden konfigureres og anvendes i overensstemmelse med denne certificering.

— GEN-6.5.2-03 Certificeringsmyndighedens private signeringsnøgle skal opbevares og anvendes i en sikker kryptografisk enhed, der opfylder kravene i GEN-6.5.2-01 og GEN-6.5.2-02.

13) 6.5.7 Network Security Controls

— OVR-6.5.7-02 Den sårbarhedsscanning, der kræves i REQ-7.8-13 i ETSI EN 319 401 [1], skal udføres mindst én gang pr. kvartal.

— OVR-6.5.7-03 Den penetrationstest, der kræves i henhold til REQ-7.8-17X i ETSI EN 319 401 [1], skal udføres mindst én gang om året.

— OVR-6.5.7-04 Firewalls skal være konfigurerede til at forhindre alle protokoller og al adgang, der ikke er nødvendige for TSP'ens drift.

14) 6.6.1 Certificate Profile

— GEN-6.6.1-05 Certifikatet skal indeholde en af de politikidentifikatorer, der er angivet i GEN-6.3.3-03 [CHOICE]. Certifikatet kan indeholde andre OID'er, der er tildelt af tillidstjenesteudbyderen.

2. For ETSI EN 319 412-2:

1) 2.1 Normative references

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

— [9] Den Europæiske Cybersikkerhedscertificeringsgruppe, undergruppe om kryptografi »Agreed Cryptographic Mechanisms«, offentliggjort af ENISA.

2) 4.2.2 Signature

— GEN-4.2.2-2 Signaturalgoritmen skal vælges i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [9].

— NOTE udgår.

3) 4.2.3.1 Legal person issuers

— GEN-4.2.3.1-3 Hvis der er kendskab til, at der findes et behørigt registreringsnummer, skal udstederens identitet indeholde organizationIdentifier med en værdi for dette registreringsnummer som anført i det pågældende officielle register, hvoraf registreringsnummeret fremgår.

4) 4.2.5 Subject public key info

— GEN-4.2.5-2 Den offentlige emnenøgle skal vælges i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [9].

— NOTE udgår.

5) 4.2.6 Serial number

— GEN-4.2.6-01 Certifikatets serienummer (som angivet i IETF RFC 5280 [1], afsnit 4.1.2.2) skal være unikt for hvert certifikat, der udstedes af tillidstjenesteudbyderen.

BILAG II

Liste over referencestandarder og specifikationer for kvalificerede certifikater for elektroniske segl

Standard 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«) og ETSI EN 319 412-5 V2.5.1 (»ETSI EN 319 412-5«) finder anvendelse med følgende tilpasninger:

1. For ETSI EN 319 411-2:

   1) 2.1 Normative references

      — [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 følgende tilpasninger:

         I punkt 2.1 Normative references i ETSI EN 319 411-1 V1.5.1 foretages følgende ændringer:

         — [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«, (udarbejdet af CEN).

      — [7] Den Europæiske Cybersikkerhedscertificeringsgruppe, undergruppen om kryptografi: »Agreed Cryptographic Mechanisms« offentliggjort af ENISA.

      — [8] Kommissionens gennemførelsesforordning (EU) 2024/482 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2019/881 for så vidt angår vedtagelsen af den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (EUCC).

      — [9] Kommissionens gennemførelsesforordning (EU) 2024/3144 om ændring af gennemførelsesforordning (EU) 2024/482 for så vidt angår gældende internationale standarder og om berigtigelse af nævnte gennemførelsesforordning.

      — [10] ISO/IEC 15408:2022 (del 1-5) »Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse — Evalueringskriterier for IT-sikkerhed«.

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

   2) 5.2 Certification Practice Statement Requirements

      — OVR-5.2-02 De certifikatpolitikker, der er identificeret i tillidstjenesteudbyderens dokumentation, skal angive kravene til de certifikatprofiler, der skal anvendes.

3) 5.3 Certificate Policy name and identification

— OVR-5.3-01 Hvis der foretages ændringer af en certifikatpolitik som beskrevet i punkt 4.2.2, der påvirker anvendeligheden, skal politikidentifikatoren ændres.

4) 6.1 Publication and repository responsibilities

— OVR-6.1-02 Oplysningerne i DIS-6.1-04 i ETSI EN 319 411-1 [2] skal være offentligt og internationalt tilgængelige.

5) 6.2.2 Initial identity validation

— REG-6.2.2-01A Indsamlingen af attributter og dokumentation for emnets identitet samt valideringen heraf skal ske som angivet i overensstemmelse med de gennemførelsesretsakter, der er vedtaget i henhold til artikel 24, stk. 1c, i forordning (EU) nr. 910/2014 [i.1].

— REG-6.2.2-03 [QCP-n] og [QCP-n-qscd] Identiteten af og, hvis det er relevant, attributter knyttet til den juridiske person skal verificeres i overensstemmelse med de gennemførelsesretsakter, der er vedtaget i henhold til artikel 24, stk. 1c, i forordning (EU) nr. 910/2014 [i.1].

— NOTE 3 Se note 2.

6) 6.3.3 Certificate issuance

— GEN-6.3.3-01 Kravene GEN-6.3.3-01 til GEN-6.3.3-10 i ETSI EN 319 411-1 [2], afsnit 6.3.3, finder anvendelse.

— GEN-6.3.3-02 CP-identifikatoren skal være [CHOICE]:

a) [QCP-l]

— som specificeret i punkt 5.3, litra b), og/eller

— en OID, der er tildelt af tillidstjenesteudbyderen, en anden relevant interessent eller gennem yderligere standardisering, for en certifikatpolitik, der udbygger de tilsvarende gældende politikkrav, som er defineret i dette dokument.

b) [QCP-l-qscd]

— som specificeret i punkt 5.3, litra d), og/eller

— en OID, tildelt af tillidstjenesteudbyderen, en anden relevant interessent eller gennem yderligere standardisering, for en certifikatpolitik, der supplerer de gældende politikkrav, som er defineret i dette dokument.

7) 6.3.5 Key Pair and Certificate Usage

— SDP-6.3.5-02A [BETINGET] Hvis tillidstjenesteudbyderen forvalter det kvalificerede elektroniske signatur-/seglgenereringssystem for emnet, skal tillidstjenesteudbyderen være en kvalificeret tillidstjenesteudbyder, der udbyder en kvalificeret tillidstjeneste til forvaltning af et kvalificeret elektronisk seglgenereringssystem på afstand i overensstemmelse med forordning (EU) nr. 910/2014 [i.1].

— SDP-6.3.5-11A Abonnentens forpligtelser (se punkt 6.3.4) skal, hvis abonnenten eller emnet genererer emnets nøgler, omfatte:

a) en forpligtelse til at generere emnets nøgler ved hjælp af en algoritme, der er i overensstemmelse med de aftalte kryptografiske mekanismer, som er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [7], til de anvendelser af den certificerede nøgle, der er identificeret i certifikatpolitikken og

b) en forpligtelse til at anvende nøglelængde og algoritme, der er i overensstemmelse med de aftalte kryptografiske mekanismer, som er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA[7], til de anvendelser af den certificerede nøgle, der er identificeret i certifikatpolitikken, i certifikatets gyldighedsperiode.

8) 6.3.10 Certificate Status Services

— CSS-6.3.10-08 [BETINGET] Hvis der stilles CRL'er til rådighed, skal tillidstjenesteudbyderen opretholde integriteten og tilgængeligheden af den seneste CRL som minimum i den periode, der er angivet i certifikatpolitikerklæringen, som krævet i CSS-6.3.10-12.

9) 6.4.4 Personnel Controls

— OVR-6.4.4-02 Tillidstjenesteudbyderens personale i betroede roller og, hvis det er relevant, dennes underleverandører i betroede roller skal kunne opfylde kravet om at have opnået »ekspertviden, erfaring og kvalifikation« gennem formel uddannelse og eksaminer eller faktisk erfaring eller en kombination af de to.

— OVR-6.4.4-03 Overholdelse af OVR-6.4.4-02 skal omfatte regelmæssige (mindst hver 12. måned) opdateringer om nye trusler og aktuel sikkerhedspraksis.

— OVR-6.4.4-04 Ud over de betroede roller, der er identificeret i ETSI EN 319 401 [1] (punkt 7.2-15), skal betroede roller for medarbejdere, der beskæftiger sig med registrering og tilbagekaldelser, og som har ansvar som defineret i TS 419261 [6], understøttes. I tilfælde, hvor den kvalificerede tillidstjenesteudbyder forvaltes direkte af eller drives på vegne af en medlemsstat eller en offentlig myndighed, kan disse yderligere betroede roller varetages af en eller flere formelle repræsentanter, der handler for og på vegne af de registrerings- og tilbagekaldelsesmedarbejdere, der fungerer i lokale eller regionale forvaltninger.

10) 6.4.9 CA or RA Termination

— OVR-6.4.9-02 Tillidstjenesteudbyderen af elektroniske registrerede leveringstjenesters plan i tilfælde af virksomhedsafbrydelse skal opfylde kravene i de gennemførelsesretsakter, der er vedtaget i henhold til artikel 24, stk. 5, i forordning (EU) nr. 910/2014 [i.1].

11) 6.5.1 Key Pair Generation and Installation

— OVR-6.5.1-01A Certificeringsmyndigheders generering af nøglepar skal ske ved hjælp af en algoritme, der er i overensstemmelse med de aftalte kryptografiske mekanismer, som er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [7] til certificeringsmyndighedens signeringsformål.

— OVR-6.5.1-01B Den valgte nøglelængde og algoritme for certificeringsmyndighedens signeringsnøgle skal være i overensstemmelse med de aftalte kryptografiske mekanismer, som er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [7] til certificeringsmyndighedens signeringsformål.

— OVR-6.5.1-01C [BETINGET] Hvis certificeringsmyndigheden genererer emnets nøgler, skal nøgler genereret af certificeringsmyndigheden være i overensstemmelse med de aftalte kryptografiske mekanismer, som er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [7], til de formål, der er angivet i certificeringspolitikken i certifikatets gyldighedsperiode.

12) 6.5.2 Private key protection and cryptographic module engineering controls

— GEN-6.5.2-01 Alle krav i ETSI EN 319 411-1 [2], afsnit 6.5.2, finder anvendelse, undtagen krav OVR-6.5.2-01, OVR-6.5.2-03 og OVR-6.5.2-04.

— GEN-6.5.2-02 Tillidstjenesteudbyderens generering af nøglepar, herunder nøgler, der anvendes af tilbagekaldelses- og registreringstjenester, skal foretages i en sikker kryptografisk enhed, som er et pålideligt system, der er certificeret i overensstemmelse med:

  — Fælles kriterier for evaluering af informationsteknologisikkerhed, jf. ISO/IEC 15408 [10] eller Fælles kriterier for evaluering af informationsteknologisikkerhed, version CC:2002, del 1-5, der er offentliggjort af deltagerne i ordningen vedrørende anerkendelse af certifikater for fælles kriterier inden for IT-sikkerhed og certificeret til EAL 4 eller højere, eller

  — den europæiske ordning for cybersikkerhedscertificering baseret på fælles kriterier (EUCC) [8][9] og certificeret til EAL 4 eller højere eller

  — indtil den 31.12.2030, FIPS PUB 140-3 [11] niveau 3.

Denne certificering skal omfatte et sikkerhedsmål eller en beskyttelsesprofil eller et moduldesign og sikkerhedsdokumentation, der opfylder kravene i dette dokument, på grundlag af en risikoanalyse og under hensyntagen til fysiske og andre ikketekniske sikkerhedsforanstaltninger.

Hvis den sikre kryptografiske enhed er omfattet af en certificering under EUCC [8][9], skal enheden konfigureres og anvendes i overensstemmelse med denne certificering.

— GEN-6.5.2-03 Certificeringsmyndighedens private signeringsnøgle skal opbevares og anvendes i en sikker kryptografisk enhed, der opfylder kravene i GEN-6.5.2-01 og GEN-6.5.2-02.

13) 6.5.7 Network Security Controls

— OVR-6.5.7-02 Den sårbarhedsscanning, der kræves i REQ-7.8-13 i ETSI EN 319 401 [1], skal udføres mindst én gang pr. kvartal.

— OVR-6.5.7-03 Den penetrationstest, der kræves i henhold til REQ-7.8-17X i ETSI EN 319 401 [1], skal udføres mindst én gang om året.

— OVR-6.5.7-04 Firewalls skal være konfigurerede til at forhindre alle protokoller og al adgang, der ikke er nødvendige for TSP'ens drift.

14) 6.6.1 Certificate Profile

— GEN-6.6.1-05 Certifikatet skal indeholde en af de politikidentifikatorer, der er angivet i GEN-6.3.3-02 [CHOICE].

2. For ETSI EN 319 412-3:

1) 2.1 Normative references

— [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 Subject

— LEG-4.2.1-6 organizationIdentifier skal indeholde en identifikation af organisationsemnet, som er forskellig fra organisationens navn. Hvis der er kendskab til, at der findes et behørigt registreringsnummer, skal attributten organizationIdentifier indeholde en værdi for dette registreringsnummer som anført i det pågældende officielle register, hvoraf registreringsnummeret fremgår.

3. For ETSI EN 319 412-2:

1) 2.1 Normative references

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

— [9] Den Europæiske Cybersikkerhedscertificeringsgruppe, undergruppen om kryptografi: »Agreed Cryptographic Mechanisms« offentliggjort af ENISA.

2) 2.2 Informative references

— [i.7] udgår.

3) 4.2.2 Signature

— GEN-4.2.2-2 Signaturalgoritmen skal vælges i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [9].

— NOTE udgår.

4) 4.2.3.1 Legal person issuers

— GEN-4.2.3.1-3 Hvis der er kendskab til, at der findes et behørigt registreringsnummer, skal udstederens identitet indeholde organizationIdentifier med en værdi for dette registreringsnummer som anført i det pågældende officielle register, hvoraf registreringsnummeret fremgår.

5) 4.2.5 Subject public key info

— GEN-4.2.5-2 Den offentlige emnenøgle skal vælges i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [9].

— NOTE udgår.

6) 4.2.6 Serial number

— GEN-4.2.6-01 Certifikatets serienummer (som angivet i IETF RFC 5280 [1], afsnit 4.1.2.2) skal være unikt for hvert certifikat, der udstedes af tillidstjenesteudbyderen.