2025/1946

30.9.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/1946

af 29. september 2025

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår kvalificerede tjenester til bevaring af kvalificerede elektroniske signaturer og kvalificerede 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 34, stk. 2, og artikel 40, og

ud fra følgende betragtninger:

(1) Kvalificerede tjenester til bevaring af kvalificerede elektroniske signaturer og kvalificerede elektroniske segl sikrer disse elektroniske signaturers og elektroniske segls integritet, ægthed, opbevaringsdokumentation og tilgængelighed på lang sigt. Dette gør det muligt at påvise deres juridiske gyldighed over længere perioder og garanterer, at de kan valideres uanset fremtidige teknologiske ændringer. Disse tjenester leveres uafhængigt eller som en del af en anden kvalificeret tillidstjeneste såsom kvalificerede elektroniske arkiveringstjenester.

(2) Formodningen om overholdelse i artikel 34, stk. 1a, og artikel 40 i forordning (EU) nr. 910/2014 bør kun finde anvendelse, hvis kvalificerede tjenester til bevaring af kvalificerede elektroniske signaturer og kvalificerede 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 den kvalificerede tillidstjenestes sikkerhed og troværdighed samt evnen til at kontrollere signaturernes og seglenes status som kvalificeret og tekniske gyldighed over tid.

(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.

([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).

(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.

(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

De referencestandarder og specifikationer, der er omhandlet i artikel 34, stk. 2, og artikel 40 i forordning (EU) nr. 910/2014, er fastsat i bilaget 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

([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).

([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

Liste over referencestandarder og specifikationer, jf. artikel 2

Standard ETSI TS 119 511 V1.1.1 (2019-06) (»ETSI TS 119 511«) og ETSI TS 119 172-4 V1.1.1 (2021-05) (»ETSI TS 119 172-4«) finder anvendelse med følgende tilpasninger:

1. For ETSI TS 119 511:

   1) 2.1 Normative references:

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

      — [2] ETSI TS 119 612 (V2.3.1) »Electronic Signatures and Infrastructures (ESI) Trusted Lists«.

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

      — [6] Kommissionens gennemførelsesforordning (EU) 2024/482 ([1]) 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).

      — [7] Kommissionens gennemførelsesforordning (EU) 2024/3144 ([2]) om ændring af gennemførelsesforordning (EU) 2024/482 for så vidt angår gældende internationale standarder og om berigtigelse af nævnte gennemførelsesforordning.

      — [8] Den Europæiske Cybersikkerhedscertificeringsgruppe, undergruppen om kryptografi: »Agreed Cryptographic Mechanisms«, offentliggjort af Den Europæiske Unions Agentur for Cybersikkerhed (»ENISA«) ([3]).

      — [9] 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«.

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

   2) 3.1 Terms

      — sikker kryptografisk enhed: enhed, der opbevarer brugerens private nøgle, beskytter denne nøgle mod kompromittering og udfører signerings- eller dekrypteringsfunktioner på brugerens vegne.

   3) 6.4 Preservation profiles

      — OVR-6.4-08A [WTS][WOS] Den forventede dokumentationsvarighed skal være i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [8].

      — NOTE 3 udgår.

   4) 6.5 Preservation evidence policy

      — OVR-6.5-04A De anvendte kryptografiske algoritmer skal være i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [8].

      — NOTE 1 udgår.

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

5) 7.2 Human resources

— OVR-7.2-02 Personale i betroede roller hos PSP'ere og, hvis det er relevant, disses 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-7.2-03 Overholdelse af OVR-7.2-02 skal omfatte regelmæssige (mindst hver 12. måned) opdateringer om nye trusler og aktuel sikkerhedspraksis.

6) 7.5 Cryptographic controls

— OVR-7.5-05 [BETINGET] Når en PSP signerer (en del af et stykke) opbevaringsdokumentation, skal PSP'ens private signeringsnøgle opbevares og anvendes i en sikker kryptografisk enhed, som er et pålideligt system, der er certificeret i overensstemmelse med:

a) Fælles kriterier for evaluering af informationsteknologisikkerhed, jf. ISO/IEC 15408 [10] eller Fælles kriterier for evaluering af informationsteknologisikkerhed, version CC:2022, 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

b) EUCC [6][7] og certificeret til EAL 4 eller højere eller

c) indtil den 31.12.2030, FIPS PUB 140-3 [5] 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 [6][7], skal enheden konfigureres og anvendes i overensstemmelse med denne certificering.

— OVR-7.5-06 [BETINGET] udgår.

— OVR-7.5-07 [BETINGET] Når PSP'en signerer (en del af et stykke) opbevaringsdokumentation, skal eventuelle sikkerhedskopier af PSP'ens private signeringsnøgler beskyttes for at sikre integriteten og fortroligheden af den sikre kryptografiske enhed, inden de lagres steder, der ikke er en del af nævnte enhed.

— OVR-7.5-08 En PSP's private signeringsnøgle må kun eksporteres og importeres til en anden sikker kryptografisk enhed, hvis denne eksport og import gennemføres sikkert og i overensstemmelse med certificeringen af disse enheder.

7) 7.8 Network security

— OVR-7.8-03 Den sårbarhedsscanning, der kræves af REQ-7.8-13 i ETSI EN 319 401 [1], skal udføres mindst én gang pr. kvartal.

— OVR-7.8-04 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-7.8-05 Firewalls skal være konfigurerede til at forhindre alle protokoller og al adgang, der ikke er nødvendige for PSP'ens drift.

8) 7.14 Cryptographic monitoring

— OVR-7.14-03A Evalueringen af de anvendte kryptografiske algoritmer i OVR-7.14.01 og OVR-7.14.02 skal være i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [8].

— NOTE udgår.

9) 7.12 TSP termination and termination plans

— OVR-7.12-01A 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.2].

10) 7.17 Supply chain

— OVR-7.17-01 Kravene i ETSI EN 319 401 [1], afsnit 7.14, finder anvendelse.

11) Annex A (normative): Qualified preservation service for QES as defined by article 34 of the Regulation (EU) No 910/2014

— OVR-A-02 [PDS][PDS+PGD]

a) bevaringstjenesten skal opbevare alle oplysninger, der er nødvendige for at kontrollere den elektroniske signaturs eller det elektroniske segls status som kvalificeret, og som ikke vil være offentligt tilgængelige før udløbet af bevaringsperioden.

b) bevaringstjenesten skal sikre, at de oplysninger, der opbevares, på et hvilket som helst tidspunkt i opbevaringsperioden er af en sådan art, at når de leveres som input til den proces, der er specificeret i punkt 4.4 i ETSI TS 119 172-4 [9], afgør resultatet af denne proces tydeligt, om den digitale signatur eller det digitale segl på tidspunktet for opbevaringen var teknisk egnet til at gennemføre en EU-kvalificeret elektronisk signatur eller et EU-kvalificeret elektronisk segl.

— OVR-A-03 [PDS][PDS+PGD] Tidsstempler, der anvendes som opbevaringsdokumentation, skal være kvalificerede tidsstempler i overensstemmelse med forordning (EU) nr. 910/2014 [i.2].

2. For ETSI TS 119 172-4:

1) 2.1 Normative references:

— [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«.

— Alle henvisninger til »ETSI TS 119 102-1 [1]« skal forstås som henvisninger til »ETSI EN 319 102-1 [1]«.

— [2] ETSI TS 119 612 (V2.3.1) »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 Validation constraints and validation procedures, krav REQ-4.2-03, afsnittet »X.509 valideringsbegrænsninger«, litra c):

— i) Hvis et slutenhedscertifikat repræsenterer et tillidsanker, må RevocationCheckingConstraints ikke anvendes.

— ii) Hvis et slutenhedscertifikat ikke repræsenterer et tillidsanker, skal RevocationCheckingConstraints sættes til »eitherCheck« som defineret i ETSI TS 119 172-1 [3], afsnit A.4.2.1, tabel A.2, række (m)2.1.

— iii) Hvis et slutenhedscertifikat repræsenterer et tillidsanker, må RevocationFreshnessConstraints, som defineret i ETSI TS 119 172-1 [3], afsnit A.4.2.1, tabel A.2, række (m)2.2, ikke anvendes.

— iv) Hvis et slutenhedscertifikat ikke repræsenterer et tillidsanker, skal RevocationFreshnessConstraints, som defineret i ETSI TS 119 172-1 [3], afsnit A.4.2.1, tabel A.2, række (m)2.2, anvendes med en maksimal værdi på 0 for signeringscertifikatet, således at tilbagekaldelsesoplysninger kun accepteres, hvis de er udstedt efter det bedste signaturtidspunkt. Der fastsættes ingen værdi for RevocationFreshnessConstraints for andre certifikater end signeringscertifikatet, herunder certifikater, der understøtter tidsstempler.

3) 4.3 Requirements on signature validation and applicability rules checking practices

— REQ-4.3-02 Signaturvalideringsapplikationer skal være i overensstemmelse med ETSI TS 119 101 [13].

4) 4.4 Technical applicability (rules) checking process

— REQ-4.4.2-03 Hvis nogen af de kontroller, der er angivet i REQ-4.4.2-01, fejler,

— stopper processen

— skal signaturen være teknisk bestemt som ubestemt, dvs. hverken som en EU-kvalificeret elektronisk signatur eller et EU-kvalificeret elektronisk segl

— skal ovennævnte resultat og resultaterne af processer i alle de mellemliggende processer afspejles i rapporten om kontrol af reglerne for anvendelse af signaturer.