Den Europæiske Unions
Tidende

DA
L-udgaven

2025/1942

30.9.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/1942

af 29. september 2025

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår kvalificerede valideringstjenester for kvalificerede elektroniske signaturer og kvalificerede valideringstjenester for 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 33, stk. 2, og artikel 40, og

ud fra følgende betragtninger:

(1) Kvalificerede valideringstjenester for kvalificerede elektroniske signaturer og for kvalificerede elektroniske segl sikrer integriteten, ægtheden og korrektheden af processen og resultaterne af valideringen af henholdsvis kvalificerede elektroniske signaturer og kvalificerede elektroniske segl. Disse kvalificerede tillidstjenester spiller en afgørende rolle i det digitale erhvervsmiljø ved at fremme overgangen fra traditionelle papirbaserede processer til elektroniske tilsvarende processer.

(2) Den formodning om overensstemmelse, der er fastsat i artikel 33, stk. 2, og artikel 40 i forordning (EU) nr. 910/2014, bør kun finde anvendelse, hvis kvalificerede valideringstjenester for kvalificerede elektroniske signaturer og kvalificerede elektroniske segl overholder de tekniske standarder, der er fastsat i nærværende forordning. Nævnte 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 samt muligheden for at kontrollere kvalificerede elektroniske signaturers og kvalificerede elektroniske segls kvalificerede status og tekniske gyldighed.

(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 33, 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 for kvalificerede valideringstjenester for kvalificerede elektroniske signaturer og for kvalificerede valideringstjenester for kvalificerede elektroniske segl

Standard ETSI TS 119 441 V1.2.1 (2023-10) ([1]) (»ETSI TS 119 441«) og ETSI TS 119 172-4 V1.1.1 (2021-05) ([2]) (»ETSI TS 119 172-4«) finder anvendelse med følgende tilpasninger:

1. For ETSI TS 119 441

   1) 2.1 Normative references

   — [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] udgår.

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

   — [7] Kommissionens gennemførelsesforordning (EU) 2024/482 ([3])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).

   — [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] Den Europæiske Cybersikkerhedscertificeringsgruppe, undergruppe Kryptografi: »Agreed Cryptographic Mechanisms«, offentliggjort af Den Europæiske Unions Agentur for Cybersikkerhed (»ENISA«) ([4]).

   — [11] Kommissionens gennemførelsesforordning (EU) 2024/3144 ([5]) om ændring af gennemførelsesforordning (EU) 2024/4822 for så vidt angår gældende internationale standarder og om berigtigelse af nævnte gennemførelsesforordning.

   — [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]) EUT 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]) EUT L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

2) 2.2 Informative references

— [i.11] udgår.

3) 3.3 Abbreviations

— EUCC Den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier

4) 4.3.3 Process

— NOTE 10 Se ETSI EN 319 102-1 [3] for vejledning og ETSI TS 119 172-4 [8] for yderligere vejledning vedrørende EU-kvalificerede signaturer eller segl.

5) 6.1 Signature Validation Service practice statement

— OVR-6.1-02 Erklæringen om praksis vedrørende signaturvalideringstjenesten skal struktureres som angivet i bilag A.

— OVR-6.1-03 Erklæringen om praksis vedrørende signaturvalideringstjenesten skal opregne eller henvise til de understøttede politikker for signaturvalideringstjenesten (f.eks. via OID'er) og kort beskrive dem.

6) 6.3 Information security policy

— OVR-6.3-02 Sikkerhedspolitikken skal dokumentere de sikkerheds- og privatlivskontroller, der er gennemført for at beskytte personoplysninger.

7) 7.2 Human resources

— OVR-7.2-02 Personale i betroede roller hos signaturvalideringstjenesteudbydere (SVSP'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.

8) 7.5 Cryptographic controls

— OVR-7.5-02 [BETINGET] Når valideringsrapporter signeres, udstedes et offentligt SVSP-signeringscertifikat, der svarer til den private SVSP-signeringsnøgle, af en betroet certificeringsmyndighed i overensstemmelse med NCP+-certifikatpolitikken som specificeret i ETSI EN 319 411-1 [12]. Den bør udstedes i overensstemmelse med en relevant certifikatpolitik, der er specificeret i ETSI EN 319 411-2 [i.17].

— OVR-7.5-03 [BETINGET] Når valideringsrapporter signeres, skal den private SVSP-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 [4] 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 [7][11] og certificeret til EAL 4 eller højere eller

c) indtil den 31.12.2030, FIPS PUB 140-3 [6] 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 [7][11], skal enheden konfigureres og anvendes i overensstemmelse med denne certificering.

— OVR-7.5-04 udgår.

— OVR-7.5-06 En SVSP'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 enhederne.

9) 7.7 Operation security

— OVR-7.7-02 For at sikre, at de systemer, som applikationen udvikles på grundlag af, anvender passende sikkerhedsforanstaltninger og tilpasses specifikke applikationsmiljøer, skal signaturvalideringsapplikationen anvende et applikationsmiljø, der vedligeholdes med opdaterede sikkerhedsrettelser.

— OVR-7.7-03 Følgende krav, der er specificeret i ETSI TS 119 101 [1], punkt 5.2, skal gælde for signaturvalideringsapplikationen: GSM 1.3.

10) 7.8 Network security

— OVR-7.8-02 Hvis fjernadgang til systemer, der lagrer eller behandler fortrolige data, er tilladt, skal en formel politik vedtages og beskrives som en del af de elementer, der kræves i henhold til OVR-6.3-02.

— OVR-7.8-04 Den sårbarhedsscanning, der kræves i henhold til REQ-7.8-13 i ETSI EN 319 401 [1], skal udføres mindst én gang pr. kvartal.

— OVR-7.8-05 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-7.8-06 Firewalls skal være konfigurerede til at forhindre alle protokoller og al adgang, der ikke er nødvendige for tillidstjenesteudbyderens (SVSP'ens) drift.

11) 7.12 Signature Validation Service provisioning termination and termination plans

— OVR-7.12-02 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].

12) 7.14 Supply chain

— OVR-7.14-01 De krav, der er angivet i ETSI EN 319 401 [2], afsnit 7.14, finder anvendelse.

13) 8.1 Signature validation process

— VPR-8.1-07 Valideringsapplikationen skal opfylde kravene i ETSI TS 119 101 [1], afsnit 7.4 SIA 1 til SIA 4.

— VPR-8.1-11 [BETINGET] Når signaturvalideringstjenesten har til formål at validere kvalificerede elektroniske signaturer eller kvalificerede elektroniske segl i overensstemmelse med artikel 32, stk. 1 (henholdsvis artikel 40) i forordning (EU) nr. 910/2014 [i.1], skal valideringsprocessen følge kravene i ETSI TS 119 172-4 [8].

14) 8.2 Signature validation protocol

— SVP-8.2-03 Signaturvalideringssvaret skal indeholde OID for signaturvalideringspolitikken.

15) 8.4 Signature validation report

— SVR-8.4-02 Valideringsrapporten skal være i overensstemmelse med ETSI TS 119 102-2 [9].

— SVR-8.4-07 [BETINGET] Når en signaturvalideringspolitik ikke er behandlet fuldt ud af signaturvalideringstjenesten, skal rapporten, ud over validerede begrænsninger, også omhandle begrænsninger, der er blevet ignoreret eller tilsidesat.

— SVR-8.4-15 Valideringsrapporten skal klart angive oprindelsen af hvert indgangssted (PoE) (fra signaturen, fra klienten og fra serveren).

— SVR-8.4-16 Valideringsrapporten skal være forsynet med en valideringsrapportsignatur, som skal være signaturvalideringstjenesteudbyderens digitale signatur.

— SVR-8.4-17 [BETINGET] Når valideringsrapporter signeres, skal formatet og målet for signaturen være i overensstemmelse med ETSI TS 119 102-2 [9].

16) 9 Framework for definition of validation service policies built on a trust service policy defined in the present document:

— OVR-9-05 [BETINGET] Når der udarbejdes en signaturvalideringstjenestepolitik på grundlag af en tillidstjenestepolitik, der er defineret i dette dokument, skal der foretages en risikovurdering for at evaluere forretningsmæssige krav og fastlægge, hvilke sikkerhedskrav der skal indgå i politikken for det pågældende fællesskab og anvendelsesområde.

— OVR-9-06 [BETINGET] Når der udarbejdes en signaturvalideringstjenestepolitik på grundlag af en tillidstjenestepolitik, der er defineret i dette dokument, skal politikken godkendes og ændres i overensstemmelse med en fastlagt revisionsproces, herunder med angivelse af ansvar for vedligeholdelse af politikken.

— OVR-9-07 [BETINGET] Når der udarbejdes en signaturvalideringstjenestepolitik på grundlag af en tillidstjenestepolitik, der er defineret i dette dokument, skal der være fastlagt en revisionsproces for at sikre, at politikken understøttes af erklæringerne om praksis.

— OVR-9-08 [BETINGET] Når der udarbejdes en signaturvalideringstjenestepolitik på grundlag af en tillidstjenestepolitik, der er defineret i dette dokument, skal tillidstjenesteudbyderen stille de politikker, som tillidstjenesteudbyderen understøtter, til rådighed for sit brugerfællesskab.

— OVR-9-09 [BETINGET] Når der udarbejdes en signaturvalideringstjenestepolitik på grundlag af en tillidstjenestepolitik, der er defineret i dette dokument, skal de revisioner af politikker, som tillidstjenesteudbyderen understøtter, stilles til rådighed for abonnenterne.

17) Annex B (normative) Qualified Validation Service for QES as defined by Article 33 of Regulation (EU) No 910/2014:

— VPR-B-02 [BETINGET] Hvis signaturvalideringstjenesteudbyderen er en kvalificeret signaturvalideringstjenesteudbyder, skal gennemførelsen være i overensstemmelse med ETSI TS 119 172-4 [8].

— NOTE 2 udgår.

— OVR-B-04 [BETINGET] Hvis signaturvalideringstjenesteudbyderen er en kvalificeret signaturvalideringstjenesteudbyder, skal prøvningerne i OVR-B-03 teste forskellige anvendelsestilfælde, både positive og negative.

— VPR-B-11 [BETINGET] Hvis signaturvalideringstjenesteudbyderen er en kvalificeret signaturvalideringstjenesteudbyder, skal denne kontrollere hashberegningen (enten udføre beregningen på serversiden eller kontrollere klienten, hvis dette er tilladt på klientsiden).

— NOTE 5 udgår.

— NOTE 6 udgår.

— VPR-B-15 [BETINGET] Hvis signaturvalideringstjenesteudbyderen er en kvalificeret signaturvalideringstjenesteudbyder, skal valideringsrapporten, for at opfylde VPR-B-13 til VPR-B-14, være i overensstemmelse med ETSI TS 119 102-2 [9].

— VPR-B-16 [BETINGET] Hvis signaturvalideringstjenesteudbyderen er en kvalificeret signaturvalideringstjenesteudbyder, skal gennemførelsen være i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [10], til brug af egnede kryptografiske teknikker ved levering af kvalificerede valideringstjenester for kvalificerede elektroniske signaturer.

18) Annex C (informative) Mapping of requirements to Regulation (EU) No 910/2014, afsnittet »Providing validation in compliance with Article 32(1)«, andet afsnit:

— For at sikre, at alle betingelser, der kræves i henhold til artikel 32, stk. 1, og artikel 40 i forordning (EU) nr. 910/2014 [i.1], er opfyldt, er der behov for en korrekt valideringsalgoritme. Den giver det samme deterministiske resultat for en signatur eller et segl, der indsendes til validering. Signaturvalideringspolitikken er afgørende for dette formål. ETSI TS 119 172-4 [8], der er baseret på den valideringsalgoritme, der er specificeret i ETSI EN 319 102-1 [3], er udstedt med dette formål for øje.

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 (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 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 24 timer for signeringscertifikatet. Der fastsættes ingen værdi for RevocationFreshnessConstraints for andre certifikater end signeringscertifikatet, herunder certifikater, der understøtter tidsstempler.

3) 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,

a) stopper processen

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

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