Den Europæiske Unions
Tidende

DA
L-udgaven

2025/1944

30.9.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/1944

af 29. september 2025

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår referencestandarder for processer for afsendelse og modtagelse af data i kvalificerede elektroniske registrerede leveringstjenester og for så vidt angår disse tjenesters interoperabilitet

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 44, stk. 2, og artikel 44, stk. 2b, og

ud fra følgende betragtninger:

(1) Kvalificerede elektroniske registrerede leveringstjenester udgør en sikker kanal til fremsendelse af dokumenter, herunder bevis for afsendelse og modtagelse af data. De har til formål at skabe sikkerhed med hensyn til at identificere adressaten og opretholde en høj grad af tillid til identifikationen af afsenderen.

(2) Den formodning om overholdelse, der er fastsat i artikel 44, stk. 1a, i forordning (EU) nr. 910/2014, bør kun finde anvendelse, hvis kvalificerede tillidstjenester til levering af kvalificerede elektroniske registrerede leveringstjenester overholder de standarder, der er fastsat i nærværende forordning. Disse standarder bør afspejle etableret praksis og være bredt anerkendt inden for de relevante sektorer. De bør tilpasses, så de omfatter yderligere kontroller, der sikrer den kvalificerede tillidstjenestes sikkerhed og troværdighed.

(3) Hvis en tillidstjenesteudbyder overholder kravene i bilag I 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 ved 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. æ910/2014.

(4) I henhold til artikel 44, stk. 2a, i forordning (EU) nr. 910/2014 er det, hvis kvalificerede tillidstjenesteudbydere indvilliger i at gøre deres tjenester interoperable, vigtigt, at de overholder de relevante standarder og specifikationer, der er fastsat i bilag II til nærværende gennemførelsesforordning, med henblik på let at overføre elektroniske registrerede data mellem to eller flere kvalificerede tillidstjenesteudbydere og fremme fair praksis på det indre marked.

(5) 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).

(6) 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 denne forordning.

(7) 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.

(8) 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 elektroniske registrerede leveringstjenester

De referencestandarder og specifikationer, der er omhandlet i artikel 44, stk. 2, i forordning (EU) nr. 910/2014, er fastsat i bilaget til nærværende forordning.

Artikel 2

Referencestandarder og specifikationer for interoperabilitet mellem kvalificerede elektroniske registrerede leveringstjenester

De referencestandarder og specifikationer, der er omhandlet i artikel 44, stk. 2b, i forordning (EU) nr. 910/2014 er anført i bilag II til nærværende forordning.

Artikel 3

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 I

Liste over referencestandarder og specifikationer, jf. artikel 1

Standarden ETSI EN 319 521 V1.1.1 (2019-02) (»ETSI EN 319 521«) finder anvendelse med følgende tilpasninger:

1. For ETSI EN 319 521:

   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 EN 319 411-1 V1.5.1 (2025-04) »Electronic Signatures and Infrastructures (ESI) Policy and security requirements for trust service providers issuing certificates Part 1: General requirements«.

   — [3] ETSI EN 319 522-1 V1.2.1 (2024-01) »Electronic Signatures and Infrastructures (ESI) Electronic Registered Delivery Services; Part 1: Framework and Architecture«.

   — [4] ETSI EN 319 522-2 V1.2.1 (2024-01) »Electronic Signatures and Infrastructures (ESI) Electronic Registered Delivery Services; Part 2: Semantic content«.

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

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

   — [7] 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).

   — [8] 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.

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

   2) 3.1 Terms

   — avanceret elektronisk segl: som defineret i forordning (EU) nr. 910/2014 [i.1].

   — avanceret elektronisk signatur: som defineret i forordning (EU) nr. 910/2014 [i.1].

   — kvalificeret elektronisk segl: som defineret i forordning (EU) nr. 910/2014 [i.1].

   — kvalificeret elektronisk signatur: som defineret i forordning (EU) nr. 910/2014 [i.1].

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

([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.

3) 5.1.1 Common provisions

— REQ-ERDS-5.1.1-01 Den elektroniske registrerede leveringstjeneste skal sikre, at tilgængeligheden, integriteten og fortroligheden af brugerindholdet er tilstrækkeligt garanteret, mens det håndteres af den elektroniske registrerede leveringstjeneste, idet der vælges passende kryptografiske teknikker til integritet og fortrolighed, som er i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [5].

4) 5.2.1.1 General

— REQ-QERDS-5.2.1.1-01 Udbyderen af kvalificerede elektroniske registrerede leveringstjenester skal med en meget høj grad af sikkerhed verificere modtagerens identitet enten direkte eller ved at benytte en tredjepart og ved hjælp af en af følgende metoder eller en kombination heraf, alt efter hvad der er nødvendigt:

a) ved fysisk tilstedeværelse af den fysiske person eller af en bemyndiget repræsentant for den juridiske person, ved hjælp af passende dokumentation og procedurer, i overensstemmelse med national ret

b) på afstand ved hjælp af et elektronisk identifikationsmiddel, der opfylder kravene i artikel 8 i forordning (EU) nr. 910/2014 [i.1] med hensyn til sikringsniveauet »høj«, eller ved hjælp af den europæiske digitale identitetstegnebog

c) ved hjælp af et certifikat for en kvalificeret elektronisk signatur eller et kvalificeret elektronisk segl

d) ved at anvende andre identifikationsmetoder, der sikrer, at den fysiske person eller den bemyndigede repræsentant for den juridiske person kan identificeres med en meget høj grad af sikkerhed. Garantien for, at denne identifikation foretages med en meget høj grad af sikkerhed, skal bekræftes af et overensstemmelsesvurderingsorgan.

— REQ-QERDS-5.2.1.1-01A Udbyderen af kvalificerede elektroniske registrerede leveringstjenester skal verificere afsenderens identitet på passende vis, enten direkte eller ved at benytte en tredjepart, på grundlag af en af følgende metoder eller en kombination heraf:

a) ved fysisk tilstedeværelse af den fysiske person eller af en bemyndiget repræsentant for den juridiske person, ved hjælp af passende dokumentation og procedurer, i overensstemmelse med national ret

b) på afstand ved hjælp af den europæiske digitale identitetstegnebog eller et anmeldt elektronisk identifikationsmiddel, der opfylder kravene i artikel 8 i forordning (EU) nr. 910/2014 [i.1] med hensyn til sikringsniveauet »betydelig«, forudsat at det er udstedt på grundlag af forudgående fysisk tilstedeværelse af den fysiske person eller en bemyndiget repræsentant for den juridiske person

c) ved hjælp af et certifikat for en avanceret elektronisk signatur eller et avanceret elektronisk segl, forudsat at certifikatet er udstedt til den fysiske person eller til en bemyndiget repræsentant for den juridiske person i overensstemmelse med normaliseret certifikatpolitik (NCP-politik) som defineret i ETSI EN 319 411-1 [2], eller

d) ved at anvende andre identifikationsmetoder, der sikrer, at den fysiske person eller den bemyndigede repræsentant for den juridiske person kan identificeres med en meget høj grad af sikkerhed. Det skal bekræftes af et overensstemmelsesvurderingsorgan, at denne identifikation foretages med en høj grad af sikkerhed.

— BEMÆRK Den tredjepart, der verificerer afsenderens og modtagerens identitet, kan være en anden udbyder af kvalificerede elektroniske registrerede leveringstjenester, hvis afsenderen og modtageren er tilknyttet forskellige udbydere af kvalificerede elektroniske registrerede leveringstjenester.

5) 5.2.1.2 Recipient identification and handover of user content

— REQ-QERDS-5.2.1.2-03 Hvis identifikationen af modtageren er baseret på en intern proces for kvalificerede elektroniske registrerede leveringstjenester, skal udbyderen af kvalificerede elektroniske registrerede leveringstjenester gennemføre hele processen i et sikkert og kontrolleret miljø.

6) 5.2.2 Provisions for EU QERDS authentication

— REQ-QERDS-5.2.2-03 [BETINGET] Når udbyderen af kvalificerede elektroniske registrerede leveringstjenester knytter autentifikationsmidler til en afsenderidentitet, der er verificeret i henhold til punkt 5.2.1, skal de være en af følgende:

a) tofaktorautentifikationsmekanismer

b) en europæisk digital identitetstegnebog eller et anmeldt elektronisk identifikationsmiddel, der opfylder kravene i artikel 8 i forordning (EU) nr. 910/2014 [i.1] med hensyn til sikringsniveauet »høj« eller »betydelig«

c) en gensidig TLS-autentifikation, som omfatter det certifikat, der er udstedt til afsenderen i overensstemmelse med NCP-politikken som defineret i ETSI EN 319 411-1 [2]

d) en digital signatur understøttet af et certifikat, der er udstedt i overensstemmelse med NCP-politikken som defineret i ETSI EN 319 411-1 [2]

e) andre midler, der sikrer autentifikationen af den identificerede afsender. Overensstemmelsen af tilknytningen skal bekræftes af et overensstemmelsesvurderingsorgan. Eksempel: Dette kan omfatte brugen af et af ovennævnte midler i litra a), b) og d) for at registrere et Transport Layer Security-klientcertifikat (TLS-klientcertifikat) til automatisk afsendelse via gensidig TLS eller for at registrere et digitalt seglcertifikat, der bruges til at forsegle påstande for at autentificere med elektroniske registrerede leveringstjenester. Andre mekanismer, i tilfælde hvor de identificerede afsendere gør brug af delegerede tredjepartstjenester, kan også finde anvendelse.

— REQ-QERDS-5.2.2-03A [BETINGET] Når udbyderen af kvalificerede elektroniske registrerede leveringstjenester knytter autentifikationsmidler til en modtageridentitet, der er verificeret i henhold til punkt 5.2.1, skal de være et af følgende, forudsat at midlerne eller en kombination af midler sikrer et meget højt tillidsniveau med hensyn til den autentificerede modtagers identitet:

a) en flerfaktorautentifikationsmekanisme

b) en europæisk digital identitetstegnebog eller et anmeldt elektronisk identifikationsmiddel, der opfylder kravene i artikel 8 i forordning (EU) nr. 910/2014 [i.1] med hensyn til sikringsniveauet »høj« eller »betydelig«

c) et certifikat for en kvalificeret elektronisk signatur eller for et kvalificeret elektronisk segl

d) andre midler, der sikrer autentifikationen af den identificerede modtager. Overensstemmelsen af tilknytningen skal bekræftes af et overensstemmelsesvurderingsorgan. Eksempel: Dette kan omfatte brugen af et af ovennævnte midler i litra a)-c) for at registrere et Transport Layer Security-klientcertifikat (TLS-klientcertifikat) til automatisk afsendelse via gensidig TLS eller for at registrere et digitalt seglcertifikat, der bruges til at forsegle påstande for at autentificere med elektroniske registrerede leveringstjenester. Andre mekanismer, i tilfælde hvor de identificerede afsendere gør brug af delegerede tredjepartstjenester, kan også finde anvendelse.

— REQ-QERDS-5.2.2-04 [BETINGET] Hvis afsenderen opretter forbindelse til den kvalificerede elektroniske registrerede leveringstjeneste via en sikker forbindelse, der kræver gensidig maskine-til-maskine-autentifikation mellem afsenderens maskine og den kvalificerede elektroniske registrerede leveringstjenestes server på grundlag af certifikater udstedt i overensstemmelse med NCP-politikken som defineret i ETSI EN 319 411-1 [2], kan der, efter at denne sikre forbindelse er etableret, anvendes enkeltfaktorautentifikationsmekanismer i en anden fase af afsenderens autentifikation, hvis de organisatoriske procedurer og sikkerhedsforanstaltninger, der er indført, sikrer tillid til autentifikationen af afsenderen.

7) 5.4.1 Common provisions

— REQ-ERDS-5.4.1-06 Udbyderen af elektroniske registrerede leveringstjenester skal generere og stille dokumentation om hændelser vedrørende elektroniske registrerede leveringer til rådighed for legitime interesserede parter, jf. afsnit 6 i ETSI EN 319 522-1 [3].

— REQ-ERDS-5.4.1-07 Udbyderen af elektroniske registrerede leveringstjenester skal arkivere al dokumentation og/eller sammenfatninger heraf, som denne har udstedt.

— REQ-ERDS-5.4.1-08 Den dokumentation, der genereres af elektroniske registrerede leveringstjenester, skal være i overensstemmelse med den semantik for dokumentation, der er defineret i afsnit 8 i ETSI EN 319 522-2 [4].

8) 7.2.1 Common provisions

— REQ-ERDS-7.2.1-02 Personale i betroede roller hos udbyderen af elektroniske registrerede leveringstjenester 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.

— REQ-ERDS-7.2,1-03 Overholdelse af REQ-ERDS-7.2,1-02 skal omfatte regelmæssige (mindst hver 12. måned) opdateringer om nye trusler og aktuel sikkerhedspraksis.

9) 7.3.2 Media handling

— REQ-ERDS-7.3.1-02 Alle krav fra ETSI EN 319 401 [1], afsnit 7.3.3, finder anvendelse.

10) 7.5 Cryptographic controls

— REQ-ERDS-7.5-01A Udbyderen af elektroniske registrerede leveringstjenester skal udvælge og anvende egnede kryptografiske teknikker i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [5].

— REQ-ERDSP-7.5-03 Den private signeringsnøgle for elektroniske registrerede leveringstjenester skal opbevares og anvendes i en sikker kryptografisk enhed, som er et pålideligt system certificeret i overensstemmelse med:

a) Fælles kriterier for evaluering af informationsteknologisikkerhed, jf. ISO/IEC 15408 [6] 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

b) den europæiske ordning for cybersikkerhedscertificering baseret på fælles kriterier (EUCC) [7][8] og certificeret til EAL 4 eller højere eller

c) indtil den 31.12.2030, FIPS PUB 140-3 [9] 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][8], skal enheden konfigureres og anvendes i overensstemmelse med denne certificering.

11) 7.8 Network security

— REQ-ERDSP-7.8-04 Udbyderen af elektroniske registrerede leveringstjenester skal anvende avancerede protokoller og algoritmer til kryptering på transport layer-niveau i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [5].

— REQ-ERDSP-7.8-06 Den sårbarhedsscanning, der kræves i henhold til REQ-7.8-13 i ETSI EN 319 401 [1], skal udføres mindst én gang pr. kvartal.

— REQ-ERDSP-7.8-07 Den penetrationstest, der kræves i henhold til REQ-7.8-17X i ETSI EN 319 401 [1], skal udføres mindst én gang om året.

— REQ-ERDSP-7.8-08 Firewalls skal være konfigurerede til at forhindre alle protokoller og al adgang, der ikke er nødvendige for tillidstjenesteudbyderens (TSP'ens) drift.

12) 7.12 ERDSP termination and ERDS termination plans

— REQ-ERDS-7.12-03 Udbyderen 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].

13) 7.14 Supply chain

— REQ-ERDS-7.14-01 De krav, der er angivet i ETSI EN 319 401 [1], afsnit 7.14, finder anvendelse.

BILAG II

Liste over referencestandarder og specifikationer, jf. artikel 2

Standard ETSI EN 319 522-1 V1.2.1 (2024-01) (»ETSI EN 319 522-1«), ETSI EN 319 522-2 V1.2.1 (2024-01) (»ETSI EN 319 522-2«), ETSI EN 319 522-3 V1.2.1 (2024-01) (»ETSI EN 319 522-3«), ETSI EN 319 522-4-1 V1.2.1 (2019-01) (»ETSI EN 319 522-4-1«), ETSI EN 319 522-4-2 V1.1.1 (2018-09) (»ETSI EN 319 522-4-2«) og ETSI EN 319 522-4-3 V1.1.1 (2018-09) (»ETSI EN 319 522-4-3«) finder anvendelse.