Europeiska unionens
officiella tidning

SV
L-serien

2025/1944

30.9.2025

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/1944

av den 29 september 2025

om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller referensstandarder för processer för sändning och mottagning av uppgifter genom kvalificerade elektroniska tjänster för rekommenderad leverans och vad gäller sådana tjänsters interoperabilitet

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 44.2 och 44.2b, och

av följande skäl:

(1) Kvalificerade elektroniska tjänster för rekommenderad leverans utgör säkra kanaler för överföring av handlingar, som också tillhandahåller bevis på att uppgifterna har sänts och mottagits. Tjänsterna syftar till att tillhandahålla säker identifiering av adressaten och säkerställa en hög tillförlitlighetsnivå för identifieringen av avsändaren.

(2) Den presumtion om överensstämmelse som fastställs i artikel 44.1a i förordning (EU) nr 910/2014 bör endast tillämpas när kvalificerade betrodda tjänster för tillhandahållande av kvalificerade elektroniska tjänster för rekommenderad leverans 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.

(3) Om en tillhandahållare av betrodda tjänster uppfyller kraven i bilaga I 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) I enlighet med artikel 44.2a i förordning (EU) nr 910/2014 är det, när kvalificerade tillhandahållare av betrodda tjänster kommer samtycker till att göra sina tjänster interoperabla, viktigt att de följer de lämpliga standarder och specifikationer som fastställs i bilaga II till denna genomförandeförordning, i syfte att enkelt överföra elektroniska rekommenderade uppgifter mellan två eller flera kvalificerade tillhandahållare av betrodda tjänster och främja god sed på den inre marknaden.

(5) 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.

([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).

(6) 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.

(7) 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.

(8) 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 elektroniska tjänster för rekommenderad leverans

De referensstandarder och specifikationer som avses i artikel 44.2 i förordning (EU) nr 910/2014 anges i bilaga I till den här förordningen.

Artikel 2

Referensstandarder och specifikationer för interoperabilitet mellan kvalificerade elektroniska tjänster för rekommenderad leverans

De referensstandarder och specifikationer som avses i artikel 44.2b i förordning (EU) nr 910/2014 anges i bilaga II till den här förordningen.

Artikel 3

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

([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).

([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 som avses i artikel 1

Standarden Etsi EN 319 521 V1.1.1 (2019-02) (*Etsi EN 319 521*) gäller med följande anpassningar:

1. För Etsi EN 319 521

(1) 2.1 Normativa hänvisningar:

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

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

— [7] 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).

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

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

(2) 3.1 Termer

— *avancerad elektronisk stämpel*: Enligt definitionen i förordning (EU) nr 910/2014 [i.1].

— *avancerad elektronisk underskrift*: Enligt definitionen i förordning (EU) nr 910/2014 [i.1].

— *kvalificerad elektronisk stämpel*: Enligt definitionen i förordning (EU) nr 910/2014 [i.1].

— *kvalificerad elektronisk underskrift*: Enligt definitionen i förordning (EU) nr 910/2014 [i.1].

— *krypteringshårdvara*: enhet som innehåller användarens privata nyckel, skyddar denna nyckel från att utsättas för skada och utför underskrifts- eller dekrypteringsfunktioner för användarens räkning.

([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 Gemensamma bestämmelser

— REQ-ERDS-5.1.1-01 Den elektroniska tjänsten för rekommenderad leverans ska säkerställa att användarinnehållets tillgänglighet, integritet och konfidentialitet garanteras under tjänstens hantering av detta innehåll genom att välja lämpliga kryptografiska tekniker för integritet och konfidentialitet som överensstämmer med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [5].

(4) 5.2.1.1 Allmänt

— REQ-QERDS-5.2.1.1-01 Tillhandahållaren av den kvalificerade elektroniska tjänsten för rekommenderad leverans ska med en mycket hög tillförlitlighetsnivå, antingen direkt eller med hjälp av en tredje part, kontrollera mottagarens identitet på grundval av en av följande metoder eller vid behov en kombination av dessa:

(a) Genom fysisk närvaro av den fysiska personen eller av en behörig företrädare för den juridiska personen, med hjälp av lämpliga bevis och förfaranden och i enlighet med nationell rätt.

(b) På distans, med hjälp av ett medel för elektronisk identifiering som uppfyller kraven i artikel 8 i förordning (EU) nr 910/2014 [i.1] vad gäller tillitsnivå hög, eller genom europeiska digitala identitetsplånboken.

(c) Genom ett certifikat för en kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel.

(d) Genom användning av andra identifieringsmetoder som säkerställer identifiering av den fysiska personen eller den behöriga företrädaren för den juridiska personen med en mycket hög tillförlitlighetsnivå. Försäkran om att denna identifiering utförs med en mycket hög tillförlitlighetsnivå ska bekräftas av ett organ för bedömning av överensstämmelse.

— REQ-QERDS-5.2.1.1-01A Tillhandahållaren av den kvalificerade elektroniska tjänsten för rekommenderad leverans ska, antingen direkt eller med hjälp av en tredje part, kontrollera avsändarens identitet på grundval av en av följande metoder eller vid behov en kombination av dessa:

(a) Genom fysisk närvaro av den fysiska personen eller av en behörig företrädare för den juridiska personen, med hjälp av lämpliga bevis och förfaranden och i enlighet med nationell rätt.

(b) På distans, genom den europeiska digitala identitetsplånboken eller ett anmält medel för elektronisk identifiering som uppfyller kraven i artikel 8 i förordning (EU) nr 910/2014 [i.1] vad gäller tillitsnivå väsentlig, förutsatt att det har utfärdats på grundval av den fysiska närvaron av den fysiska personen respektive av en behörig företrädare för den juridiska personen.

(c) Genom ett certifikat för en avancerad elektronisk underskrift eller en avancerad elektronisk stämpel, förutsatt att certifikatet har utfärdats till den fysiska personen eller en behörig företrädare för den juridiska personen i enlighet med den normaliserade certifikatpolicy (NCP) som anges i Etsi EN 319 411-1 [2]. eller

(d) Genom användning av andra identifieringsmetoder som säkerställer identifiering av den fysiska personen eller den behöriga företrädaren för den juridiska personen med en mycket hög tillförlitlighetsnivå. Försäkran om att denna identifiering utförs med en hög tillförlitlighetsnivå ska bekräftas av ett organ för bedömning av överensstämmelse.

— ANMÄRKNING Den tredje part som kontrollerar avsändarens och mottagarens identitet kan vara en annan tillhandahållare av kvalificerade elektroniska tjänster för rekommenderad leverans om avsändaren och mottagaren anlitar olika tillhandahållare.

(5) 5.2.1.2 Mottagaridentifiering och överlämning av användarinnehåll

— REQ-QERDS-5.2.1.2-03 Om identifieringen av mottagaren bygger på en process som är intern för den kvalificerade elektroniska tjänsten för rekommenderad leverans ska hela processen utföras i en säkrad och kontrollerad miljö.

(6) 5.2.2 Bestämmelser för autentisering av EU-kvalificerade elektroniska tjänster för rekommenderad leverans

— REQ-QERDS-5.2.2-03 [CONDITIONAL] När tillhandahållaren av den kvalificerade elektroniska tjänsten för rekommenderad leverans binder ett medel för autentisering till en avsändaridentitet i enlighet med klausul 5.2.1 ska det vara ett av följande:

(a) Mekanismer för tvåfaktorsautentisering.

(b) Europeisk digital identitetsplånbok eller ett anmält medel för elektronisk identifiering som uppfyller kraven i artikel 8 i förordning (EU) nr 910/2014 vad gäller tillitsnivå hög eller väsentlig.

(c) Ömsesidig TLS-autentisering, som omfattar det certifikat som utfärdats till avsändaren enligt NCP i enlighet med vad som anges i Etsi EN 319 411-1 [2].

(d) En digital underskrift som stöds av ett certifikat som utfärdats enligt NCP i enlighet med vad som anges i Etsi EN 319 411-1 [2].

(e) Andra medel som säkerställer autentisering av den identifierade avsändaren. Bindningens överensstämmelse med kraven ska bekräftas av ett organ för bedömning av överensstämmelse. Exempel: Detta kan inbegripa användning av något av de medel som anges i leden a, b och d ovan för att registrera ett TLS-klientcertifikat för automatisk sändning via mTLS, eller för att registrera ett certifikat för digital stämpel som används för att stämpla utsagor som ska autentiseras med den elektroniska tjänsten för rekommenderad leverans. Andra mekanismer där de identifierade avsändarna använder delegerade tredjepartstjänster kan också tillämpas.

— REQ-QERDS-5.2.2-03A [CONDITIONAL] När tillhandahållaren av den kvalificerade elektroniska tjänsten för rekommenderad leverans binder ett medel för autentisering till en mottagaridentitet som kontrollerats i enlighet med klausul 5.2.1 ska detta medel vara ett av följande, förutsatt att medlet, eller kombinationen av medel, säkerställer en mycket hög tillförlitlighetsnivå vad gäller den autentiserade mottagarens identitet:

(a) En mekanism för flerfaktorsautentisering.

(b) Europeisk digital identitetsplånbok eller ett anmält medel för elektronisk identifiering som uppfyller kraven i artikel 8 i förordning (EU) nr 910/2014 vad gäller tillitsnivå hög eller väsentlig.

(c) Ett certifikat för en kvalificerad elektronisk underskrift eller en kvalificerad elektronisk stämpel.

(d) Andra medel som säkerställer autentisering av den identifierade mottagaren. Bindningens överensstämmelse med kraven ska bekräftas av ett organ för bedömning av överensstämmelse. Exempel: Detta kan inbegripa användning av något av de medel som anges i led a–c ovan för att registrera ett TLS-klientcertifikat för automatisk sändning via mTLS, eller för att registrera ett certifikat för digital stämpel som används för att stämpla utsagor som ska autentiseras med den elektroniska tjänsten för rekommenderad leverans. Andra mekanismer där de identifierade avsändarna använder delegerade tredjepartstjänster kan också tillämpas.

— REQ-QERDS-5.2.2-04 [CONDITIONAL] Om avsändaren ansluter till den kvalificerade elektroniska tjänsten för rekommenderad leverans via en säker anslutning som kräver ömsesidig maskin-till-maskin-autentisering mellan avsändarens maskin och tjänstens server på basis av på certifikat som utfärdats enligt NCP i enlighet med Etsi EN 319 411-1 [2] får mekanismer för enfaktorsautentisering användas i en andra fas av autentisering av avsändaren, förutsatt att de organisatoriska förfaranden och säkerhetsåtgärder som tillämpas säkerställer att autentiseringen av avsändaren är tillförlitlig.

(7) 5.4.1 Gemensamma bestämmelser

— REQ-ERDS-5.4.1-06 Den elektroniska tjänsten för rekommenderad leverans ska generera bevis för händelser relaterade till elektronisk rekommenderad leverans och göra dessa bevis tillgängliga för behöriga berörda parter i enlighet med klausul 6 i Etsi EN 319 522-1 [3].

— REQ-ERDS-5.4.1-07 Tillhandahållaren av den elektroniska tjänsten för rekommenderad leverans ska arkivera bevisen och/eller bevissammandragen för varje bevis som utfärdats.

— REQ-ERDS-5.4.1-08 De bevis som den elektroniska tjänsten för rekommenderad leverans genererar ska följa den semantik för bevis som anges i klausul 8 i Etsi EN 319 522-2 [4].

(8) 7.2.1 Gemensamma bestämmelser

— REQ-ERDS-7.2.1-02 Den personal i betrodda roller som arbetar för tillhandahållaren av elektroniska tjänster för rekommenderad leverans ska kunna uppfylla kravet på expertkunskap, erfarenhet och kvalifikationer genom formell utbildning och meriter, eller faktisk erfarenhet, eller en kombination av dessa.

— REQ-ERDS-7.2.1-03 Överensstämmelse med REQ-ERDS-7.2.1-02 ska omfatta regelbundna (minst var tolfte månad) uppdateringar om nya hot och aktuella säkerhetsrutiner.

(9) 7.3.2 Hantering av lagringsmedia

— REQ-ERDS-7.3.1-02 Alla krav i Etsi EN 319 401 [1], avsnitt 7.3.3 ska tillämpas.

(10) 7.5 Kryptografiska kontroller

— REQ-ERDS-7.5-01A Den elektroniska tjänsten för rekommenderad leverans ska välja och använda lämpliga kryptografiska tekniker som överensstämmer med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [5].

— REQ-ERDSP-7.5-03 Den privata underskriftsnyckeln för den elektroniska tjänsten för rekommenderad leverans ska lagras och användas inom en krypteringshårdvara som utgör ett tillförlitligt system som certifierats i enlighet med

(a) de gemensamma kriterierna för utvärdering av informationsteknologisk säkerhet, såsom dessa anges i ISO/IEC 15408 [6] 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

(b) den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) [7][8] och certifierats på nivå EAL 4 eller högre eller

(c) till och med den 31.12.2030, FIPS PUB 140-3 [9] 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 [7][8]-certifiering ska hårdvaran konfigureras och användas i enlighet med den certifieringen.

(11) 7.8 Nätverkssäkerhet

— REQ-ERDSP-7.8-04 Tillhandahållaren av den elektroniska tjänsten för rekommenderad leverans ska använda toppmoderna protokoll och algoritmer för kryptering på transportskiktsnivå som överensstämmer med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [5].

— REQ-ERDSP-7.8-06: Den sårbarhetsskanning som krävs enligt REQ-7.8-13 i Etsi EN 319 401 [1] ska utföras minst en gång per kvartal.

— REQ-ERDSP-7.8-07 Det penetrationstest som krävs enligt REQ-7.8-17X i Etsi EN 319 401 [1] ska utföras minst en gång om året.

— REQ-ERDSP-7.8-08 Brandväggar ska konfigureras så att de förhindrar alla protokoll och åtkomster som inte krävs för driften av tillhandahållaren av betrodda tjänster.

(12) 7.12 Avveckling och avvecklingsplaner för tillhandahållare av elektroniska tjänster för rekommenderad leverans

— REQ-ERDS-7.12-03Tillhandahållarens avvecklingsplan ska uppfylla kraven i de genomförandeakter som antagits i enlighet med artikel 24.5 i förordning (EU) nr 910/2014 [i.1].

(13) 7.14 Leveranskedja

— REQ-ERDS-7.14-01 De krav som anges i Etsi EN 319 401 [1], klausul 7.14 ska tillämpas.

BILAGA II

Förteckning över referensstandarder och specifikationer som avses i artikel 2

Standarderna Etsi EN 319 522-1 V1.2.1 (2024-01) (*Etsi EN 319 522-*), 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*) och Etsi EN 319 522-4-3 V1.1.1 (2018-09) (*Etsi EN 319 522-4-3*) gäller.