Europeiska unionens
officiella tidning

SV
L-serien

2025/1942

30.9.2025

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/1942

av den 29 september 2025

om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller referensstandarder för kvalificerade tjänster för validering av kvalificerade elektroniska underskrifter och av kvalificerade elektroniska stämplar

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 33.2 och 40, och

av följande skäl:

(1) Kvalificerade valideringstjänster för kvalificerade elektroniska underskrifter och kvalificerade elektroniska stämplar säkerställer integritet, äkthet och korrekthet hos processen för och resultatet av valideringen av kvalificerade elektroniska underskrifter respektive kvalificerade elektroniska stämplar. Dessa kvalificerade betrodda tjänster spelar en avgörande roll i den digitala miljön genom att främja övergången från traditionella pappersbaserade processer till motsvarande elektroniska processer.

(2) Den presumtion om överensstämmelse som fastställs i artiklarna 33.2 och 40 i förordning (EU) nr 910/2014 bör endast tillämpas när kvalificerade tjänster för validering av kvalificerade elektroniska underskrifter och av kvalificerade elektroniska stämplar uppfyller de tekniska 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 samt möjligheten att kontrollera kvalificerade elektroniska underskrifters och kvalificerade elektroniska stämplars status som kvalificerade samt deras tekniska giltighet.

(3) Om en tillhandahållare av betrodda tjänster uppfyller kraven i bilagan 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) 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).

(5) 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.

(6) 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.

(7) 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

De referensstandarder och specifikationer som avses i artiklarna 33.2 och 40 i förordning (EU) nr 910/2014 anges i bilagan till den här förordningen.

Artikel 2

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

Förteckning över referensstandarder och specifikationer för kvalificerade valideringstjänster för kvalificerade elektroniska underskrifter och för kvalificerade valideringstjänster för kvalificerade elektroniska stämplar

Standarderna Etsi TS 119 441 V1.2.1 (2023-10) ([1]) (*Etsi TS 119 441*) och Etsi TS 119 172-4 V1.1.1 (2021-05) ([2]) (*Etsi TS 119 172-4*) gäller med följande anpassningar:

1. För Etsi TS 119 441

   1) 2.1 Normativa hänvisningar

   — [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] Ogiltig.

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

   — [7] Kommissionens genomförandeförordning (EU) 2024/482 ([3]) 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] 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] Europeiska gruppen för cybersäkerhetscertifiering, undergruppen för kryptografi: *Agreed Cryptographic Mechanisms*, offentliggjord av Europeiska unionens cybersäkerhetsbyrå (Enisa) ([4]).

   — [11] Kommissionens genomförandeförordning (EU) 2024/3144 ([5]) om ändring av genomförandeförordning (EU) 2024/4822 vad gäller tillämpliga internationella standarder och om rättelse av den genomförandeförordningen.

   — [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 Informativa hänvisningar

— [i.11] Ogiltig.

3) 3.3 Förkortningar

— EUCC *European Common Criteria-based cybersecurity certification scheme,* den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering.

4) 4.3.3 Process

— ANMÄRKNING 10 Se Etsi EN 319 102-1 [3] för vägledning och Etsi TS 119 172-4 [8] för ytterligare vägledning om fall med EU-kvalificerade underskrifter eller stämplar.

5) 6.1 Förklaring om praxis för valideringstjänst för underskrifter

— OVR-6.1-02 Förklaringen om praxis för valideringstjänsten för underskrifter ska ha den uppbyggnad som anges i bilaga A.

— OVR-6.1-03 Förklaringen om praxis för valideringstjänsten för underskrifter ska innehålla en förteckning över eller hänvisningar till de policyer för valideringstjänster för underskrifter som stöds (t.ex. med hjälp av OID:n) och kortfattade beskrivningar av dessa.

6) 6.3 Informationssäkerhetspolicy

— OVR-6.3-02 I säkerhetspolicyn ska de säkerhets- och integritetskontroller som används för att skydda personuppgifter dokumenteras.

7) 7.2 Personalresurser

— OVR-7.2-02 Den personal i betrodda roller som arbetar för tillhandahållaren av valideringstjänster för underskrifter och, i tillämpliga fall, underleverantörer i betrodda roller, ska kunna uppfylla kravet på expertkunskap, erfarenhet och kvalifikationer genom formell utbildning och meriter, eller faktisk erfarenhet, eller en kombination av dessa.

— OVR-7.2-03 Överensstämmelse med OVR-7.2-02 ska omfatta regelbundna (minst var tolfte månad) uppdateringar om nya hot och aktuella säkerhetsrutiner.

8) 7.5 Kryptografiska kontroller

— OVR-7.5-02 [CONDITIONAL] När valideringsrapporter undertecknas ska det öppna underskriftscertifikat för tillhandahållaren av valideringstjänster för underskrifter som motsvarar den privata underskriftsnyckeln för tillhandahållaren utfärdas av en tillförlitlig certifikatutfärdare i enlighet med NCP+-certifikatpolicyn enligt Etsi EN 319 411-1 [12]. Det bör utfärdas i enlighet med en lämplig certifikatpolicy som anges i Etsi EN 319 411-2 [i.17].

— OVR-7.5-03 [CONDITIONAL] När valideringsrapporter undertecknas ska den privata underskriftsnyckeln för tillhandahållaren av valideringstjänster 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 [4] eller i *Common Criteria for Information Technology Security Evaluation*, version CC:2022, 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) EUCC [7][11] och certifierats på nivå EAL 4 eller högre eller

c) till och med den 31.12.2030, FIPS PUB 140-3 [6] 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][11]-certifiering ska hårdvaran konfigureras och användas i enlighet med den certifieringen.

— OVR-7.5-04 ogiltig.

— OVR-7.5-06 En privat underskriftsnyckel för en tillhandahållare av valideringstjänster för underskrifter får endast exporteras och importeras till en annan krypteringshårdvara om denna export och import genomförs på ett säkert sätt och i enlighet med certifieringen av de aktuella hårdvaruenheterna.

9) 7.7 Driftsäkerhet

— OVR-7.7-02 För att säkerställa att de system som används för att utveckla tillämpningen för validering av underskrifter har lämpliga säkerhetsåtgärder och anpassas till specifika tillämpningsmiljöer ska en tillämpningsmiljö som underhålls med aktuella säkerhetskorrigeringar användas.

— OVR-7.7-03 Följande krav som anges i Etsi TS 119 101 [1], klausul 5.2 ska tillämpas på tillämpningen för validering av underskrifter: GSM 1.3.

10) 7.8 Nätverkssäkerhet

— OVR-7.8-02 Om fjärråtkomst till system där konfidentiella uppgifter lagras eller behandlas är tillåtet ska en formell policy antas och beskrivas som en del i uppfyllandet av de krav som ställs i OVR-6.3-02.

— OVR-7.8-04 Den sårbarhetsskanning som krävs enligt REQ-7.8-13 i Etsi EN 319 401 [1] ska utföras minst en gång per kvartal.

— OVR-7.8-05 Det penetrationstest som krävs enligt REQ-7.8-17X i Etsi EN 319 401 [1] ska utföras minst en gång om året.

— OVR-7.8-06: Brandväggar ska konfigureras så att de förhindrar alla protokoll och åtkomster som inte krävs för driften av tillhandahållaren av valideringstjänster för underskrifter.

11) 7.12 Avveckling och avvecklingsplaner för tillhandahållande av valideringstjänster för underskrifter

— OVR-7.12-02 Tillhandahållarens avvecklingsplan ska uppfylla kraven i de genomförandeakter som antagits i enlighet med artikel 24.5 i förordning (EU) nr 910/2014 [i.1].

12) 7.14 Leveranskedja

— OVR-7.14-01 De krav som anges i Etsi EN 319 401 [2], klausul 7.14 ska tillämpas.

13) 8.1 Process för validering av underskrifter

— VPR-8.1-07 Valideringstillämpningen ska uppfylla kraven i Etsi TS 119 101 [1], klausulerna 7.4 SIA 1–SIA 4.

— VPR-8.1-11 [CONDITIONAL] När valideringstjänsten för underskrifter syftar till att validera kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplar i enlighet med artikel 32.1 (respektive artikel 40) i förordning (EU) nr 910/2014) [i.1] ska valideringsprocessen uppfylla kraven i Etsi TS 119 172-4 [8].

14) 8.2 Protokoll för validering av underskrifter

— SVP-8.2-03 Svaret på underskriftsvalideringen ska innehålla OID:t för policyn för validering av underskrifter.

15) 8.4 Rapport för validering av underskrifter

— SVR-8.4-02 Valideringsrapporten ska överensstämma med Etsi TS 119 102-2 [9].

— SVR-8.4-07 [CONDITIONAL] När en policy för validering av underskrifter inte behandlas fullständigt av tjänsten för validering av underskrifter ska rapporten, utöver uppgifter om validerade begränsningar innehålla uppgifter om begränsningar som har ignorerats eller åsidosatts.

— SVR-8.4-15 Valideringsrapporten ska tydligt ange varifrån varje existensbevis kommer (från själva underskriften, från klienten, från servern).

— SVR-8.4-16 Valideringsrapporten ska vara försedd med en valideringsrapportsunderskrift som ska utgöras av den digitala underskriften för tillhandahållaren av valideringstjänster för underskrifter.

— SVR-8.4-17 [CONDITIONAL] När valideringsrapporter undertecknas ska formatet och målet för underskriften överensstämma med Etsi TS 119 102-2 [9].

16) 9 Ram för fastställande av policyer för valideringstjänster med en policy för betrodda tjänster som fastställs i detta dokument som grund:

— OVR-9-05 [CONDITIONAL] När en policy för en valideringstjänst för underskrifter utformas med en policy för betrodda tjänster som fastställs i detta dokument som grund ska en riskbedömning utföras för att utvärdera verksamhetskraven och fastställa vilka säkerhetskrav som ska ingå i policyn för den angivna gruppen och tillämpligheten.

— OVR-9-06 [CONDITIONAL] När en policy för en valideringstjänst för underskrifter utformas med en policy för betrodda tjänster som fastställs i detta dokument som grund ska policyn godkännas och ändras i enlighet med en fastställd översynsprocess, inklusive fördelning av ansvaret för att upprätthålla policyn.

— OVR-9-07 [CONDITIONAL] När en policy för en valideringstjänst för underskrifter utformas med en policy för betrodda tjänster som fastställs i detta dokument som grund ska det finnas en fastställd översynsprocess för att säkerställa att policyn stöds av förklaringarna om praxis.

— OVR-9-08 [CONDITIONAL] När en policy för en valideringstjänst för underskrifter utformas med en policy för betrodda tjänster som fastställs i detta dokument som grund ska tillhandahållaren av betrodda tjänster göra de policyer som tillhandahållaren stöder tillgängliga för sin användargrupp.

— OVR-9-09 [CONDITIONAL] När en policy för en valideringstjänst för underskrifter utformas med en policy för betrodda tjänster som fastställs i detta dokument som grund ska ändringar som tillhandahållaren av betrodda tjänster gör i policyerna göras tillgängliga för mottagarna.

17) Bilaga B (normativ) Kvalificerad valideringstjänst för kvalificerade elektroniska underskrifter enligt definitionen i artikel 33 i förordning (EU) nr 910/2014.

— VPR-B-02 [CONDITIONAL] Om tillhandahållaren av valideringstjänsten för underskrifter är en tillhandahållare av kvalificerade valideringstjänster ska genomförandet överensstämma med Etsi TS 119 172-4 [8].

— ANMÄRKNING 2 ogiltig.

— OVR-B-04 [CONDITIONAL] Om tillhandahållaren av valideringstjänster för underskrifter är en kvalificerad tillhandahållare av valideringstjänster för underskrifter ska testerna i OVR-B-03 utföras för olika användningsfall, positiva och negativa.

— VPR-B-11 [CONDITIONAL] Om tillhandahållaren av valideringstjänster för underskrifter är en kvalificerad tillhandahållare av valideringstjänster för underskrifter ska tillhandahållaren kontrollera hashberäkningen (antingen utföra beräkningen på serversidan eller kontrollera klienten om beräkning på klientsidan tillåts).

— ANMÄRKNING 5 ogiltig.

— ANMÄRKNING 6 ogiltig.

— VPR-B-15 [CONDITIONAL] Om tillhandahållaren av valideringstjänster för underskrifter är en kvalificerad tillhandahållare av valideringstjänster för underskrifter ska valideringsrapporten för att uppfylla kraven i VPR-B-13–VPR-B-14 överensstämma Etsi TS 119 102-2 [9].

— VPR-B-16 [CONDITIONAL] Om tillhandahållaren av valideringstjänster för underskrifter är en kvalificerad tillhandahållare av valideringstjänster för underskrifter ska genomförandet överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [10] för användning av lämpliga kryptografiska tekniker vid tillhandahållandet av kvalificerade valideringstjänster för kvalificerade elektroniska underskrifter.

18) Bilaga C (informativ) *Mapping of requirements to Regulation (EU) No 910/2014*, avsnittet *Providing validation in compliance with Article 32(1)*, andra stycket:

— För att säkerställa att samtliga villkor i artiklarna 32.1 och 40 i förordning (EU) nr 910/2014 [i.1] kontrolleras krävs en korrekt valideringsalgoritm. Den ger samma deterministiska resultat för underskrifter som för stämplar som ska valideras. Policyn för validering av underskrifter är avgörande för denna uppgift. Etsi TS 119 172-4 [8], baserad på den valideringsalgoritm som anges i Etsi EN 319 102-1 [3], har utfärdats med detta i åtanke.

2. För Etsi TS 119 172-4

1) 2.1 Normativa hänvisningar:

— [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*.

— Alla hänvisningar till ”Etsi TS 119 102-1 [1]” ska förstås som hänvisningar till ”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 Valideringsbegränsningar och valideringsförfaranden, krav REQ-4.2-03, avsnitt *X.509 validation constraints*, punkt c):

— i) Om ett slutmottagarcertifikat representerar ett tillitsankare ska *RevocationCheckingConstraints* inte användas.

— ii) Om ett slutmottagarcertifikat inte representerar ett tillitsankare ska *eitherCheck* anges för *RevocationCheckingConstraints* i enlighet med vad som anges i Etsi TS 119 172-1 [3], klausul A.4.2.1, tabell A.2 rad m2.1.

— iii) Om ett slutmottagarcertifikat representerar ett tillitsankare ska *RevocationFreshnessConstraints* enligt Etsi TS 119 172-1 [3], klausul A.4.2.1, tabell A.2 rad m2.2 inte användas.

— iv) Om ett slutmottagarcertifikat inte representerar ett tillitsankare ska *RevocationFreshnessConstraints* enligt Etsi TS 119 172-1 [3], klausul A.4.2.1, tabell A.2 rad (m)2.2 användas, med ett maximalt värde på 24 timmar för underskriftscertifikatet. Inget värde ska anges för *ReclocationFreshnessConstraints* för andra certifikat än underskriftscertifikatet, inklusive certifikat som stöder tidsstämpling.

3) 4.4 Process för kontroll av (regler för) teknisk tillämplighet

— REQ-4.4.2-03 Om någon av de kontroller som anges i REQ-4.4.2-01 ger negativt resultat gäller följande:

a) Processen stoppas.

b) Underskriften har på teknisk väg fastställts vara obestämd, dvs. den utgör varken en EU-kvalificerad elektronisk underskrift eller en EU-kvalificerad elektronisk stämpel.

c) Resultaten ovan och resultaten av samtliga mellanliggande processer ska avspeglas i rapporten om kontrollen av reglerna för underskriftens tillämplighet.