Europeiska unionens
officiella tidning

SV
L-serien

2025/1946

30.9.2025

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/1946

av den 29 september 2025

om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller referensstandarder för kvalificerade tjänster för bevarande 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 34.2 och 40, och

av följande skäl:

(1) Kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter och av kvalificerade elektroniska stämplar säkerställer långsiktig integritet, äkthet, bevis på förekomst av och tillgänglighet till bevarandebevis för dessa elektroniska underskrifter och elektroniska stämplar. Detta gör det möjligt att styrka den rättsliga giltigheten hos elektroniska underskrifter och elektroniska stämplar över längre tidsperioder och garantera att de kan valideras oavsett kommande tekniska förändringar. Dessa tjänster tillhandahålls separat eller som en del av en annan kvalificerad betrodd tjänst, såsom kvalificerade elektroniska arkiveringstjänster.

(2) Den presumtion om överensstämmelse som fastställs i artiklarna 34.1a och 40 i förordning (EU) nr 910/2014 bör endast tillämpas när kvalificerade tjänster för bevarande av kvalificerade elektroniska underskrifter och av kvalificerade elektroniska stämplar 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 den kvalificerade betrodda tjänsten samt möjligheten att kontrollera underskrifternas och stämplarnas status som kvalificerade och deras giltighet över tid.

(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 34.2 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 som avses i artikel 2

Standarderna Etsi TS 119 511 V1.1.1 (2019-06) (*Etsi TS 119 511*) och Etsi TS 119 172-4 V1.1.1 (2021-05) (*Etsi TS 119 172-4*) gäller med följande anpassningar:

1. För Etsi TS 119 511

   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 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 genomförandeförordning (EU) 2024/482 ([1]) 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).

      — [7] Kommissionens genomförandeförordning (EU) 2024/3144 ([2]) om ändring av genomförandeförordning (EU) 2024/482 vad gäller tillämpliga internationella standarder och om rättelse av den genomförandeförordningen.

      — [8] Europeiska gruppen för cybersäkerhetscertifiering, undergruppen för kryptografi: *Agreed Cryptographic Mechanisms*, offentliggjord av Europeiska unionens cybersäkerhetsbyrå (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 (delarna 1–5) *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security*.

   2) 3.1 Termer

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

   3) 6.4 Bevarandeprofiler

      — OVR-6.4-08A [WTS][WOS] Den förväntade giltighetstiden för bevis ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [8].

      — ANMÄRKNING 3 ogiltig.

   4) 6.5 Policy för bevarandebevis

      — OVR-6.5-04A De kryptografiska algoritmer som används ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [8].

      — ANMÄRKNING 1 ogiltig.

([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 Personalresurser

— OVR-7.2-02 Den personal i betrodda roller som arbetar för tillhandahållaren av tjänster för bevarande 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.

6) 7.5 Kryptografiska kontroller

— OVR-7.5-05 [CONDITIONAL] När en tillhandahållare av tjänster för bevarande undertecknar (en del av) ett bevarandebevis ska tillhandahållarens privata underskriftsnyckel 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 [10] 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 [6][7] och certifierats på nivå EAL 4 eller högre eller

c) till och med den 31.12.2030, FIPS PUB 140-3 [5] 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 [6][7]-certifiering ska hårdvaran konfigureras och användas i enlighet med den certifieringen.

— OVR-7.5-06 [CONDITIONAL] ogiltig.

— OVR-7.5-07 [CONDITIONAL] När en tillhandahållare av tjänster för bevarande undertecknar (en del av) ett bevarandebevis ska alla eventuella säkerhetskopior av tillhandahållarens privata underskriftsnycklar skyddas med avseende på integritet och konfidentialitet med hjälp av krypteringshårdvaran innan kopiorna lagras någon annanstans än på denna hårdvara.

— OVR-7.5-08 En privat underskriftsnyckel från en tillhandahållare av tjänster för bevarande 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.

7) 7.8 Nätverkssäkerhet

— OVR-7.8-03 Den sårbarhetsskanning som krävs enligt REQ-7.8-13 i Etsi EN 319 401 [1] ska utföras minst en gång per kvartal.

— OVR-7.8-04 Det penetrationstest som krävs enligt REQ-7.8-17X i Etsi EN 319 401 [1] ska utföras minst en gång om året.

— OVR-7.8-05 Brandväggar ska konfigureras så att de förhindrar alla protokoll och åtkomster som inte krävs för driften av tillhandahållaren av tjänster för bevarande.

8) 7.14 Kryptografisk övervakning

— OVR-7.14-03A Utvärderingen av de kryptografiska algoritmerna i OVR-7.14.01 och OVR-7.14.02 ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [8].

— ANMÄRKNING ogiltig.

9) 7.12 Avveckling av och avvecklingsplaner för tillhandahållare av betrodda tjänster

— OVR-7.12-01A Tillhandahållarens avvecklingsplan ska uppfylla kraven i de genomförandeakter som antagits i enlighet med artikel 24.5 i förordning (EU) nr 910/2014 [i.2].

10) 7.17 Leveranskedja

— OVR-7.17-01 De krav som anges i Etsi EN 319 401 [1], klausul 7.14 ska tillämpas.

11) Bilaga A (normativ): Kvalificerad tjänst för bevarande av kvalificerade elektroniska underskrifter enligt definitionen i artikel 34 i förordning (EU) nr 910/2014

— OVR-A-02 [PDS][PDS+PGD]

a) Tjänsten för bevarande ska omfatta bevarande av all information som behövs för att kontrollera den elektroniska underskriftens eller stämpelns status som kvalificerad och som inte skulle vara offentligt tillgänglig förrän efter bevarandeperiodens slut.

b) Bevarandetjänsten ska säkerställa att den information som bevaras, vid varje given tidpunkt under bevarandeperioden, är sådan att den process som anges i klausul 4.4 i Etsi TS 119 172-4 [9] när informationen som bevaras används som indata ger ett resultat som tydligt indikerar huruvida den digitala underskriften eller stämpeln vid tidpunkten för bevarandet var tekniskt lämplig för genomförande av en EU-kvalificerad elektronisk underskrift eller en EU-kvalificerad elektronisk stämpel.

— OVR-A-03 [PDS][PDS+PGD] Tidsstämpling som används i bevarandebeviset ska vara kvalificerad tidsstämpling i enlighet med förordning (EU) nr 910/2014 [i.2].

2. För Etsi TS 119 172-4

1) 2.1 Normativa hänvisningar:

— [1] Etsi EN 319 102-1 V1.4. (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) *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 högsta värde på 0 för underskriftscertifikatet, vilket säkerställer att återkallandeinformationen endast godtas om den har utfärdats efter bästa tidpunkt för underskrift. Inget värde ska anges för *ReclocationFreshnessConstraints* för andra certifikat än underskriftscertifikatet, inklusive certifikat som stöder tidsstämpling.

3) 4.3 Krav på metoder för validering av underskrifter och kontroll av regler för tillämplighet

— REQ-4.3-02 Tillämpningar för validering av underskrifter ska överensstämma med Etsi TS 119 101 [13].

4) 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:

— Processen stoppas.

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

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