Europeiska unionens
officiella tidning

SV
L-serien

2025/2531

17.12.2025

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/2531

av den 16 december 2025

om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller referensstandarder och specifikationer för kvalificerade elektroniska liggare

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 artikel 45l.3, och

av följande skäl:

(1) Genom Europaparlamentets och rådets förordning (EU) 2024/1183 ([2]) infördes en förteckning över nya betrodda tjänster och kvalificerade betrodda tjänster, inbegripet registreringen av data i en kvalificerad elektronisk liggare, i förordning (EU) nr 910/2014. Kommissionen ska upprätta en förteckning över referensstandarder och, vid behov, fastställa specifikationer för sådana tjänster.

(2) En elektronisk liggare är en sekvens av elektroniska dataloggar som ska säkerställa dataintegriteten och riktigheten i dessa dataloggars kronologiska ordning. För att säkerställa att registreringen av data i en kvalificerad elektronisk liggare är kronologiskt ordnad, konsekvent och tillförlitlig är det nödvändigt att fastställa en gemensam uppsättning specifikationer för registreringen av elektroniska uppgifter i en kvalificerad elektronisk liggare.

(3) Den presumtion om överensstämmelse som fastställs i artikel 42.1a i förordning (EU) nr 910/2014 bör endast tillämpas när kvalificerade betrodda tjänster för registrering av data i en kvalificerad elektronisk liggare 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.

(4) 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.

(5) Kommissionen utvärderar regelbundet ny teknik, nya metoder, standarder eller tekniska specifikationer. I enlighet med skäl 75 i förordning (EU) 2024/1183 bör kommissionen vid behov se över och, vid behov, uppdatera denna tillämpningsförordning för att hålla den i linje med den globala utvecklingen, ny teknik, nya metoder samt nya standarder eller tekniska specifikationer och för att följa bästa praxis på den inre marknaden.

([1]) OJ 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 behandlingen av personuppgifter enligt denna förordning, och även med beaktande av Europeiska dataskyddsstyrelsens 'Guidelines 02/2025 on processing of personal data through blockchain technologies' ([5]).

(7) Samråd med Europeiska datatillsynsmannen har skett i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([6]) och avgav ett yttrande den 21 oktober 2025 ([7]).

(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

De referensstandarder och specifikationer som avses i artikel 45l.3 i förordning (EU) nr 910/2014 anges, för kvalificerade elektroniska liggare, 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 16 december 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 och 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]) edpb_guidelines_202502_blockchain_en.pdf.

([6]) 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).

([7]) Europeiska datatillsynsmannens formella synpunkter på utkastet till genomförandeförordning om tillämpningsföreskrifter för förordning (EU) nr 910/2014 vad gäller referensstandarder och specifikationer för kvalificerade elektroniska liggare.

BILAGA

Förteckning över tekniska specifikationer och referensstandarder för kvalificerade distribuerade elektroniska liggare

1. I denna förordning gäller följande definitioner:

   a) *slutgilitighet*: status för en datalogg i en elektronisk liggare i vilken dataloggen har blivit irreversibel och inte kan modifieras eller tas bort.

   b) *distribuerad elektronisk liggare*: en elektronisk liggare som delas av en uppsättning noder för de distribuerade elektroniska liggarna och som synkroniseras mellan noderna för de distribuerade elektroniska liggarna med hjälp av en konsensusmekanism.

   c) *nod för en distribuerad elektronisk liggare*: en anordning eller process som är en del av ett nätverk av distribuerade elektroniska liggare och som lagrar en fullständig eller partiell kopia av en elektronisk liggares dataloggar.

   d) *nätverk av distribuerade elektroniska liggare*: ett nätverk av noder för distribuerade elektroniska liggare vilket utgör ett system för distribuerade elektroniska liggare.

   e) *system för distribuerad elektronisk liggare*: ett system som genomför en distribuerad elektronisk liggare.

   f) *konsensus*: det att noderna för distribuerade elektroniska liggare är överens om giltigheten av transaktioner och bibehållandet av ett enhetligt och ordnat antal validerade transaktioner i hela systemet för den distribuerade elektroniska liggaren.

   g) *konsensusmekanism*: den uppsättning regler och förfaranden genom vilken konsensus nås..

   h) *styrregler*: en uppsättning protokoll, policyer och mekanismer som styr hur systemet för den distribuerade elektroniska liggaren används, hur data valideras och läggs till i en elektronisk liggare, och hur deltagarna interagerar.

   i) *transaktion*: det minsta momentet i en arbetsprocess inom en elektronisk liggare.

   j) *arbetsprocess*: en eller flera sekvenser av åtgärder som krävs för att producera ett resultat som är förenligt med styrreglerna för en elektronisk liggare.

   k) *validerad transaktion*: en transaktion för vilken den integritet, den autenticitet och de protokoll-specifika villkor som krävs har kontrollerats i enlighet med styrreglerna för systemet för den distribuerade elektroniska liggaren.

   l) *kryptografisk koppling*: referensdata som upprättas med hjälp av passande krypteringstekniker för att säkerställa integriteten, autenticiteten eller spårheten hos referensdata och den rätta sekvensen hos dataloggarna.

   m) *liggarerapport*: strukturerad presentation av verifierbar information som hämtats från dataloggar i en liggare, och som ger insyn i specifika aktiviteter, statusar eller överensstämmelser med fördefinierade regler.

   n) *tillhandahållare av kvalificerad elektronisk liggare*: kvalificerade tillhandahållaren av betrodda tjänster som tillhandahåller en kvalificerad betrodd tjänst bestående i registrering av data i en kvalificerad elektroniska liggare.

   o) *kvalificerad distribuerad elektronisk liggare*: distribuerad elektronisk liggare som uppfyller kraven på en kvalificerad elektronisk liggare.

2. Om den kvalificerade tillhandahållaren av betrodda tjänster behöver tillhandahålla en liggarerapport, ska denna utarbetas på ett automatiserat sätt.

3. Tillhandahållare av kvalificerad elektronisk liggare ska skapa, föra in elektroniska uppgifter i, uppdatera och upprätthålla en kvalificerad elektronisk liggare i överensstämmelse med de specifikationer som fastställs i

   a) för alla tillhandahållare av kvalificerad elektronisk liggare, Etsi EN 319 401 v3.1.1 (2024–06) med följande anpassningar:

      — 2.1 Normativa referenser:

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

[2] IETF RFC 7515 (maj 2015): *JSON Web Signature (JWS)*.

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

[4] Kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 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).

[5] Kommissionens genomförandeförordning (EU) 2024/3144 av den 18 december 2024 om ändring av genomförandeförordning (EU) 2024/482 vad gäller tillämpliga internationella standarder och om rättelse av den genomförandeförordningen.

[6] ISO/IEC 15408:2022 (delarna 1 till 5): *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security*.

— 6.1 Förklaring om praxis för betrodd tjänst:

  — REQ-6.1–12 Förklaringen om praxis för elektronisk liggare ska omfatta åtminstone följande information:

    — Den funktionella och tekniska kapaciteten hos den elektroniska liggarplattformen och dess användning under hela tillhandahållandet av registrering av data i en kvalificerad elektornisk liggare som en kvalificerad betrodd tjänst.

    — De specifika mekanismer för autentisering av datas ursprung som används vid tillhandahållandet av tjänsten.

    — De specifika mekanismer för sekventiell kronologisk ordning som används vid tillhandahållandet av tjänsten.

    — I förekommande fall, den kryptografiska koppling som används för att säkerställa sekvensen hos dataloggarna.

    — I förekommande fall, den konsensusmekanism som säkerställer slutgiltigheten och integriteten hos de dataloggar och transaktioner som lagras i liggaren, inbegripet eventuell tid som läggs till av försiktighetsskäl fram till dess att slutgiltigheten och integriteten uppnås.

    — De specifika dataintegritetsmekanismer som används vid tillhandahållandet av tjänsten.

  — 6.2. Villkor:

    — REQ-6.2–03 Abonnenter på och parter som förlitar sig på tjänsten ska informeras på ett tydligt, begripligt och lättillgängligt sätt, på en allmänt tillgänglig plats och enskilt, om de exakta villkoren, inbegripet de punkter som förtecknas ovan, innan de ingår ett avtalsförhållande.

  — 6.3. Informationssäkerhetspolicy:

    — REQ-6.3–04X Tillhandahållaren av betrodda tjänster ska upprätta förfaranden för att meddela ändringar i den betrodda tjänsten till tillsynsorganet, i enlighet med verksamhetskraven och relevanta lagar och andra författningar. TSP ska till tillsynsorganet sända en anmälan åtminstone

      — en månad innan någon ändring genomförs,

      — tre månader före det planerade upphörandet av tillhandahållandet av betrodda tjänster.

  — 7.2. Personalresurser:

    — REQ-7.2–04X TSP:s personal i betrodd roll 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-7.2–05X Detta ska omfatta regelbundna (minst var tolfte månad) uppdateringar om nya hot och aktuella säkerhetsrutiner.

— 7.5 Kryptografiska kontroller:

— REQ-7.5–01X Lämpliga säkerhetskontroller ska finnas för hantering av kryptografiska nycklar, kryptografiska algoritmer och kryptografiska enheter under hela deras livscykel, med kryptoföljsamhet när så är lämpligt.

— REQ-7.5–02 TSP ska för tillhandahållandet av sina betrodda tjänster välja och använda lämpliga kryptografiska tekniker som överensstämmer med Agreed Cryptographic Mechanisms som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [1].

Särskilt gäller följande:

— REQ-7.5–03 Leverantörer av kvalificerade elektroniska liggare ska fastställa ursprunget för dataloggarna i den elektroniska liggaren. I detta syfte ska de använda avancerade elektroniska underskrifter baserade på kvalificerade certifikat eller avancerade elektroniska stämplar baserade på kvalificerade certifikat som skapats av användarna av tjänsten i enlighet med följande standarder och specifikationer:

a) Etsi EN 319 122–1 V1.3.1 (2023–06). Elektroniska underskrifter och infrastrukturer (Electronic Signatures and Infrastructures, ESI). CAdES digitala underskrifter. Del 1: Byggstenar och CAdES -basunderskrifter (Building blocks and CAdES baseline signatures).

b) Etsi EN 319 132–1 V1.3.1 (2024–07). Elektroniska underskrifter och infrastrukturer (Electronic Signatures and Infrastructures, ESI). XAdES digitala underskrifter. Del 1: Byggstenar och XAdES-basunderskrifter (Building blocks and XAdES baseline signatures).

c) Etsi TS 119 182–1 V1.2.1 (2024–07). Elektroniska underskrifter och infrastrukturer (Electronic Signatures and Infrastructures, ESI). JAdES digitala underskrifter. Del 1: Byggstenar och JAdES-basunderskrifter (Building blocks and JAdES baseline signatures), med följande anpassning:

— 5.1.8 x5c-header-parametern (X.509 certifikatkedja)

— x5c-header-parametern enligt definitionen i avsnitt 4.1.6 i IETF RFC 7515 [2] ska finnas med i JAdES-underskriften, antingen som signerad eller osignerad header-parameter.

— x5c-header-parametern ska ha den semantik som specificeras i IETF RFC 7515 [2], avsnitt 4.1.6.

— x5c-header-parametern ska ha den syntax som specificeras i IETF RFC 7515 [2], avsnitt 4.1.6.

— REQ-7.5–04: Leverantörerna av kvalificerade elektroniska liggare ska fastställa den unika sekventiella kronologiska ordningen för dataloggarna i den elektroniska liggaren. För detta ska de använda kryptografiska kopplingar, baserade i hashlistor eller hashträd, med användning av kryptografiska hashfunktioner, i enlighet med följande specifikationer och standarder:

a) SHA-256 eller större hash-storlek på output, i överensstämmelse med Agreed Cryptographic Mechanisms som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [1].

b) SHA3-256 eller större hash-storlek på output, i överensstämmelse med Agreed Cryptographic Mechanisms som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [1].

Alternativt när tillhandahållarna av kvalificerade elektroniska liggare använder tidsregistrering för att säkerställa den unika sekventiella kronologiska ordningen för dataloggarna i den elektroniska liggaren, ska de använda kvalificerade tidsstämplar.

— REQ-7.5–05 Leverantörer av kvalificerade elektroniska liggare ska säkerställa integriteten hos de dataloggar som registreras i en kvalificerad elektronisk liggare. I detta syfte ska de använda avancerade elektroniska underskrifter baserade på kvalificerade certifikat eller avancerade elektroniska stämplar baserade på kvalificerade certifikat, i enlighet med följande standarder och specifikationer:

  a) Sådana underskrift- eller stämpelformat som överensstämmer med Agreed Cryptographic Mechanisms som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [1].

  b) SHA-256 eller större hash-storlek på output, i överensstämmelse med Agreed Cryptographic Mechanisms som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [1].

  c) SHA3-256 eller större hash-storlek på output, i överensstämmelse med Agreed Cryptographic Mechanisms som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [1].

  d) Tillhandahållarna av kvalificerade elektroniska liggare ska säkerställa att alla efterföljande ändringar av data som registrerats i en kvalificerad elektronisk liggare omedelbart kan upptäckas.

— REQ-7.5–06 Om mekanismer för digital signatur används, ska privata underskriftsnycklar för tillhandahållaren av den ´kvalificerade elektroniska liggaren 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 ([1]) [6] 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) den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) ([2]) ([3]) [4][5] och certifierats på nivå EAL 4 eller högre eller

  c) till och med den 31.12.2030, FIPS PUB 140–3 ([4]) [3] 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-certifiering[4][5], ska hårdvaran konfigureras och användas i enlighet med den certifieringen.

([1]) ISO/IEC 15408:2022 (delarna 1–5): *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security*.

([2]) kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 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) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).

([3]) Kommissionens genomförandeförordning (EU) 2024/3144 av den 18 december 2024 om ändring av genomförandeförordning (EU) 2024/482 vad gäller tillämpliga internationella standarder och om rättelse av den genomförandeförordningen (EUT L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

([4]) FIPS PUB 140–3 (2019): *Säkerhetskrav för kryptografiska moduler* (Security Requirements for Cryptographic Modules").

— 7.8 Nätverkssäkerhet:

— REQ-7.8–14X Den sårbarhetsskanning som krävs enligt REQ-7.8–13 i Etsi EN 319401 ska utföras minst en gång per kvartal.

— REQ-7.8–18X Det penetrationstest som krävs enligt REQ-7.8–17X ska utföras minst en gång om året.

— REQ-7.8–21X: Brandväggar ska också konfigureras så att de förhindrar alla protokoll och åtkomster som inte krävs för driften av TSP.

— 7.9.1 Övervakning och loggning:

— REQ-7.9.1–02X Övervakningsverksamheten ska ta hänsyn till känsligheten hos all information som samlas in eller analyseras.

— 7.12 TSP:s avslutande och planer för avslutande:

— REQ-7.12–02A TSP:s plan för avslutande ska uppfylla kraven i de genomförandeakter som antagits i enlighet med artikel 24.5 i förordning (EU) nr 910/2014 [i.1].

b) För alla leverantörer av kvalificerade elektroniska liggare som använder teknik för distribuerade elektroniska liggare gäller dessutom följande:

(1) ISO 23257:2022 Blockkedjeteknik och teknik för distribuerade liggare – Referensarkitektur, avsnitt 9, med en fullständig beskrivning av systemet för distribuerade elektroniska liggare, motsvarande nätverk för teknik för distribuerade elektroniska liggare och noder för teknik för distribuerade elektroniska liggare.

(2) ISO/TS 23635:2022. Blockkedjeteknik och teknik för distribuerade liggare – Riktlinjer för styrning, med avseende på skriftliga och allmänt tillgängliga policyer och metoder som rör styrningsstrukturen för den elektroniska liggare som de tillhandahåller.