Europeiska unionens
officiella tidning

SV
L-serien

2025/1929

30.9.2025

# KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2025/1929

## av den 29 september 2025

## om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller bindningen av datum och tidpunkt till uppgifter och fastställande av korrektheten hos tidskällor för tillhandahållande av kvalificerade elektroniska tidsstämplingar

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 42.2, och

av följande skäl:

(1) Kvalificerade elektroniska tidsstämplingar spelar en avgörande roll i den digitala miljön genom att främja övergången från traditionella pappersbaserade processer till motsvarande elektroniska processer. Kvalificerade elektroniska tidsstämplingar binder information om datum och tidpunkt till elektroniska uppgifter, vilket bidrar till att säkerställa korrektheten hos de datum och tidpunkter som stämplingarna indikerar samt integriteten hos de digitala dokument till vilka datumen och tidpunkterna är bundna.

(2) Den presumtion om överensstämmelse som fastställs i artikel 42.1a i förordning (EU) nr 910/2014 bör endast tillämpas när kvalificerade betrodda tjänster för utfärdande av kvalificerade tidsstämplingar uppfyller de standarder som fastställs i den här förordningen. Dessa standarder bör återspegla etablerad praxis och vara allmänt erkända inom de relevanta sektorerna. Dessa standarder bör anpassas så att de omfattar ytterligare kontroller som säkerställer säkerheten och tillförlitligheten för den kvalificerade betrodda tjänsten och bindningen av datum och tidpunkter till uppgifter samt korrektheten för tidskällan.

(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 genomförordning 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.

(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.

([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).

([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.

(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*

De referensstandarder och specifikationer som avses i artikel 42.2 i förordning (EU) nr 910/2014 anges i bilagan till den här förordningen.

*Artikel 2*

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*

([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 tjänster för tidsstämpling**

Standarderna Etsi EN 319 421 V1.3.1 ([1]) (*Etsi EN 319 421*) och Etsi EN 319 422 V1.1.1 ([2]) (*Etsi EN 319 422*) gäller med följande anpassningar:

1. För Etsi EN 319 421

(1) 2.1 Normativa hänvisningar:

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

— [4] Etsi EN 319 401 V3.1.1 (2024–06) *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*.

— [5] Etsi EN 319 422 V1.1.1 (2016–03) *Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles*.

— [6] ogiltig.

— [9] Europeiska gruppen för cybersäkerhetscertifiering, undergruppen för kryptografi: *Agreed Cryptographic Mechanisms*, offentliggjord av Europeiska unionens cybersäkerhetsbyrå (Enisa) ([3]).

— [10] Kommissionens genomförandeförordning (EU) 2024/482 ([4]) 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).

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

(2) 3.1 Termer

— *giltighetsperiod för certifikat*: tidsintervall från *notBefore* till och med *notAfter*, under vilket certifikatutfärdaren garanterar att denne kommer att lagra information om certifikatets status.

(3) 3.3 Förkortningar

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

(4) 6.2 Förklaring om praxis för betrodd tjänst

— OVR-6.2–03 Utfärdaren av tidsstämplingar ska i sin informationsförklaring ange tillgänglighetsuppgifter för sin tjänst för tidsstämpling.

(5) 7.3 Personalsäkerhet

— OVR-7.3–02 Den personal i betrodda roller som arbetar för utfärdaren av tidsstämplingar 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-7.3–03 Överensstämmelse med OVR-7.3–02 ska omfatta regelbundna (minst var tolfte månad) uppdateringar om nya hot och aktuella säkerhetsrutiner.

([1]) EN 319 421 - *Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers issuing Time Stamps*, V1.3.1.
([2]) EN 319 422 - *Electronic Signatures and Infrastructures (ESI) - Time-stamping protocol and time-stamp token profiles*, V1.1.1 (2016–03) https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([4]) EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) EUT L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

(6) 7.6.2 Tidsstämplingsenhetens nyckelgenerering

— TIS-7.6.2–03 Tidsstämplingsenhetens nyckelgenerering ska ske 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 [3] 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 [10][11] och certifierats på nivå EAL 4 eller högre eller

c) till och med den 31.12.2030, FIPS PUB 140–3 [7] 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 [10][11]-certifiering ska hårdvaran konfigureras och användas i enlighet med den certifieringen.

— TIS-7.6.2–04 ogiltig.

— ANMÄRKNING 3 ogiltig.

— TIS-7.6.2–05A Tidsstämplingsenhetens algoritm för nyckelgenerering, längden på de underskriftsnycklar som genereras samt underskriftsalgoritmen som används för att underteckna tidsstämplingarna respektive för att underteckna tidsstämplingsenhetens certifikat för öppna nycklar ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering [9] och offentliggjorts av Enisa.

— ANMÄRKNING 4 ogiltig.

— TIS-7.6.2–06 En underskriftsnyckel från en tidsstämplingsenhet 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) 7.6.3 Skydd av privat nyckel från tidsstämplingsenhet

— TIS-7.6.3–02 Tidsstämplingsenhetens privata nyckel 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 [3] 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) [10][11] och certifierats på nivå EAL 4 eller högre eller

c) till och med den 31.12.2030, FIPS PUB 140–3 [7] 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 [10][11]-certifiering ska hårdvaran konfigureras och användas i enlighet med den certifieringen.

— TIS-7.6.3–03 ogiltig.

— ANMÄRKNING 2 ogiltig.

(8) 7.6.7 Utlöpande av tidsstämplingsenhetens nycklar

— TIS-7.6.7–03A Utgångsdatumet för tidsstämplingsenhetens privata nycklar ska överensstämma med *Agreed Cryptographic Mechanisms* [9].

— ANMÄRKNING 1 ogiltig.

(9) 7.10 Nätverkssäkerhet

— OVR-7.10–05 Den sårbarhetsskanning som krävs enligt REQ-7.8–13 i Etsi EN 319 401 [1] ska utföras minst en gång per kvartal.

— OVR-7.10–06 Det penetrationstest som krävs enligt REQ-7.8–17X i Etsi EN 319 401 [1] ska utföras minst en gång om året.

— OVR-7.10–07 Brandväggar ska konfigureras så att de förhindrar alla protokoll och åtkomster som inte krävs för utfärdaren av tidsstämplingars drift.

(10) 7.14 Avveckling och avvecklingsplaner för utfärdare av tidsstämplingar

— OVR-7.14–01A Tillhandahållarens avvecklingsplan ska uppfylla kraven i de genomförandeakter som antagits i enlighet med artikel 24.5 i förordning (EU) nr 910/2014 [i.4].

2. För Etsi EN 319 422

(1) 2.1 Normativa hänvisningar

— [5] ogiltig.

— [6] ogiltig.

— [8] Europeiska gruppen för cybersäkerhetscertifiering, undergruppen för kryptografi: *Agreed Cryptographic Mechanisms.*

— [9] RFC 9110 HTTP-semantik.

(2) 4.1.3 Hashalgoritmer som ska användas

— Följande klausul ska tillämpas:

De hashalgoritmer som används för att hasha den information som ska tidsstämplas, förväntad varaktighet för tidsstämplingen och valda hashfunktioner kontra tid ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [8].

— ANMÄRKNING ogiltig.

(3) 4.2.3 Algoritmer som ska stödjas

— Följande klausul ska tillämpas:

De underskriftsalgoritmer för tidsstämplingstoken som ska stödjas ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [8].

— ANMÄRKNING ogiltig.

(4) 4.2.4 Nyckellängder som ska stödjas

— Följande klausul ska tillämpas:

Nyckellängderna för den valda underskriftsalgoritmen ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa.

— ANMÄRKNING ogiltig.

(5) 5.1.3 Algoritmer som ska stödjas

— Följande klausul ska tillämpas:

De hashalgoritmer för tidsstämplingsuppgifter som ska stödjas, förväntad varaktighet för tidsstämplingen och valda hashfunktioner kontra tid ska överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [8].

— ANMÄRKNING ogiltig.

(6) 5.2.3 Algoritmer som ska användas

— Följande klausul ska tillämpas:

De hashalgoritmer som används för att hasha den information som ska tidsstämplas och underskriftsalgoritmerna för tidsstämplingstoken överensstämma med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [8].

— ANMÄRKNING ogiltig.

(7) 6.3 Krav på nyckellängder

— Följande klausul ska tillämpas:

Den valda underskriftsalgoritmen för tidsstämplingsenhetscertifikatet ska ha en nyckellängd som överensstämmer med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [8].

— ANMÄRKNING ogiltig.

(8) 6.5 Algoritmkrav

— Följande klausul ska tillämpas:

Tidsstämplingsenhetens öppna nycklar och certifikatunderskrift ska använda algoritmer som överensstämmer med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [8].

— ANMÄRKNING ogiltig.

(9) 7 Profiler för de transportprotokoll som ska stödjas

— Tidsstämplingsklienten och tidsstämplingsservern ska stödja tidsstämplingsprotokollet via HTTPS [9] i enlighet med vad som anges i klausul 3.4 i IETF RFC 3161 [1].

(10) 8 Objektidentifierare för kryptografiska algoritmer

— Följande klausul ska tillämpas:

Tidsstämplingsenhetens öppna nycklar och certifikatunderskrift ska använda algoritmer som överensstämmer med *Agreed Cryptographic Mechanisms* som godkänts av den europeiska gruppen för cybersäkerhetscertifiering och offentliggjorts av Enisa [8].

(11) 9.1 Förklaring om överensstämmelse med förordningen

— Om utfärdaren av tidsstämplingar anger att en tidsstämplingstoken är en kvalificerad elektronisk tidsstämpling i enlighet med förordning (EU) nr 910/2014 [i.2] ska den innehålla en förekomst av *qcStatements*-tillägget i tilläggsfältet för tidsstämplingstoken med den syntax som anges i IETF RFC 3739 [i.3], klausul 3.2.6.

— *qcStatements*-tillägget ska innehålla en förekomst av *"esi4-qtstStatement-1"* i enlighet med bilaga B.

— *qcStatements*-tillägget ska inte markeras som kritiskt.