2025/1929

30.9.2025

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2025/1929

af 29. september 2025

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår binding af dato og klokkeslæt til data og om fastlæggelse af nøjagtigheden af tidskilderne til levering af kvalificerede elektroniske tidsstempler

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF ([1]), særlig artikel 42, stk. 2, og

ud fra følgende betragtninger:

(1) Kvalificerede elektroniske tidsstempler spiller en afgørende rolle i det digitale miljø ved at fremme overgangen fra traditionelle papirbaserede processer til tilsvarende elektroniske processer. Ved at binde dato- og klokkeslætsoplysninger til elektroniske data bidrager kvalificerede elektroniske tidsstempler til at sikre nøjagtigheden af den dato og det klokkeslæt, de angiver, og integriteten af digitale dokumenter, som dato og klokkeslæt er bundet til.

(2) Den formodning om overholdelse, der er fastsat i artikel 42, stk. 1a„ i forordning (EU) nr. 910/2014, bør kun finde anvendelse, hvis kvalificerede tillidstjenester til udstedelse af kvalificerede tidsstempler overholder de standarder, der er fastsat i nærværende forordning. Disse standarder bør afspejle etableret praksis og være bredt anerkendt inden for de relevante sektorer. Disse standarder bør tilpasses, så de omfatter yderligere kontrol, der sikrer den kvalificerede tillidstjenestes sikkerhed og troværdighed og bindingen af dato og klokkeslæt til data og nøjagtigheden af tidskilden.

(3) Hvis en tillidstjenesteudbyder overholder kravene i bilaget til denne forordning, bør tilsynsorganerne antage, at de relevante krav i forordning (EU) nr. 910/2014 er opfyldt, og tage behørigt hensyn til en sådan formodning i forbindelse med tildeling eller bekræftelse af tillidstjenestens status som kvalificeret. En kvalificeret tillidstjenesteudbyder kan dog stadig anvende anden praksis til at påvise overholdelse af kravene i forordning (EU) nr. 910/2014.

(4) Kommissionen vurderer regelmæssigt nye teknologier, praksisser, standarder eller tekniske specifikationer. I overensstemmelse med betragtning 75 til Europa-Parlamentets og Rådets forordning (EU) 2024/1183 ([2]) bør Kommissionen efter behov revidere og ajourføre denne gennemførelsesforordning for at sikre dens overensstemmelse med den globale udvikling, nye teknologier, standarder eller tekniske specifikationer og for at følge bedste praksis på det indre marked.

(5) Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([3]) og, hvor det er relevant, Europa-Parlamentets og Rådets direktiv 2002/58/EF ([4]) finder anvendelse på alle behandlingsaktiviteter vedrørende personoplysninger i henhold til nærværende forordning.

([1]) EUT L 257 af 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Europa-Parlamentets og Rådets forordning (EU) 2024/1183 af 11. april 2024 om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af den europæiske ramme for digital identitet (EUT L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([3]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj.

(6) Den Europæiske Tilsynsførende for Databeskyttelse blev hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([5]) og afgav udtalelse den 6. juni 2025.

(7) Foranstaltningerne i nærværende forordning er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 48 i forordning (EU) nr. 910/2014 —

VEDTAGET DENNE FORORDNING:

Artikel 1

De referencestandarder og specifikationer, der er omhandlet i artikel 42, stk. 2, i forordning (EU) nr. 910/2014, er anført i bilaget til nærværende forordning.

Artikel 2

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 29. september 2025.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

([5]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

BILAG

Liste over referencestandarder og specifikationer for kvalificerede tidsstempeltjenester

Standard ETSI EN 319 421 V1.3.1 ([1]) (»ETSI EN 319 421«) og ETSI EN 319 422 V1.1.1 ([2]) (»ETSI EN 319 422«) finder anvendelse med følgende tilpasninger:

1. For ETSI EN 319 421:

   1) 2.1 Normative references:

      — [3] ISO/IEC 15408:2022 (del 1-5) »Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse — Evalueringskriterier for IT-sikkerhed«.

      — [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] udgår.

      — [9] Den Europæiske Cybersikkerhedscertificeringsgruppe, undergruppen om kryptografi: »Agreed Cryptographic Mechanisms«, offentliggjort af Den Europæiske Unions Agentur for Cybersikkerhed (»ENISA«) ([3]).

      — [10] Kommissionens gennemførelsesforordning (EU) 2024/482 ([4]) af 31. januar 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2019/881 for så vidt angår vedtagelsen af den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (EUCC).

      — [11] Kommissionens gennemførelsesforordning (EU) 2024/3144 ([5]) af 18. december 2024 om ændring af gennemførelsesforordning (EU) 2024/482 for så vidt angår gældende internationale standarder og om berigtigelse af nævnte gennemførelsesforordning

   2) 3.1 Terms

      — certifikatgyldighedsperiode: tidsinterval fra notBefore til og med notAfter, hvor certificeringsmyndigheden garanterer, at den vil opbevare oplysninger om certifikatets status.

   3) 3.3 Abbreviations

      — EUCC Den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier

   4) 6.2 Trust Service Practice Statement

      — OVR-6.2-03 TSA'en skal medtage erklæringer om tilgængeligheden af sin tidsstemplingstjeneste i sin TSA-oplysningserklæring.

   5) 7.3 Personnel security

      — OVR-7.3-02 TSA'ens personale i betroede roller og, hvis det er relevant, dennes underleverandører i betroede roller skal kunne opfylde kravet om at have opnået »ekspertviden, erfaring og kvalifikation« gennem formel uddannelse og eksaminer eller faktisk erfaring eller en kombination af de to.

      — OVR-7.3-03 Overholdelse af OVR-7.3-02 skal omfatte regelmæssige (mindst hver 12. måned) opdateringer om nye trusler og aktuel sikkerhedspraksis.

([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 TSU key generation

— TIS-7.6.2-03 Genereringen af TSU'ens nøgle(r) skal foretages i en sikker kryptografisk enhed, som er et pålideligt system, der er certificeret i overensstemmelse med:

a) Fælles kriterier for evaluering af informationsteknologisikkerhed, jf. ISO/IEC 15408 [3] eller Fælles kriterier for evaluering af informationsteknologisikkerhed, version CC:2022, del 1-5, der er offentliggjort af deltagerne i ordningen vedrørende anerkendelse af certifikater for fælles kriterier inden for IT-sikkerhed og certificeret til EAL 4 eller højere, eller

b) EUCC [10][11] og certificeret til EAL 4 eller højere, eller

c) indtil den 31.12.2030, FIPS PUB 140-3 [7] niveau 3.

Denne certificering skal omfatte et sikkerhedsmål eller en beskyttelsesprofil eller et moduldesign og sikkerhedsdokumentation, der opfylder kravene i dette dokument, på grundlag af en risikoanalyse og under hensyntagen til fysiske og andre ikketekniske sikkerhedsforanstaltninger.

Hvis den sikre kryptografiske enhed er omfattet af en certificering under EUCC [10][11], skal enheden konfigureres og anvendes i overensstemmelse med denne certificering.

— TIS-7.6.2-04 udgår.

— NOTE 3 udgår.

— TIS-7.6.2-05A TSU-nøglegenereringsalgoritmen, den deraf følgende signeringsnøglelængde og signaturalgoritme, der anvendes til signering af henholdsvis tidsstempler og TSU-certifikater for offentlige nøgler, skal være i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe [9] og offentliggjort af ENISA.

— NOTE 4 udgår.

— TIS-7.6.2-06 En TSU's signeringsnøgle må kun eksporteres og importeres til en anden sikker kryptografisk enhed, hvis denne eksport og import gennemføres sikkert og i overensstemmelse med certificeringen af disse enheder.

7) 7.6.3 TSU private key protection

— TIS-7.6.3-02 TSU'ens private nøgle opbevares og anvendes i en sikker kryptografisk enhed, som er et pålideligt system, der er certificeret i overensstemmelse med:

a) Fælles kriterier for evaluering af informationsteknologisikkerhed, jf. ISO/IEC 15408 [3] eller Fælles kriterier for evaluering af informationsteknologisikkerhed, version CC:2002, del 1-5, der er offentliggjort af deltagerne i ordningen vedrørende anerkendelse af certifikater for fælles kriterier inden for IT-sikkerhed og certificeret til EAL 4 eller højere, eller

b) den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (EUCC) [10][11] og certificeret til EAL 4 eller højere, eller

c) indtil den 31.12.2030, FIPS PUB 140-3 [7] niveau 3.

Denne certificering skal omfatte et sikkerhedsmål eller en beskyttelsesprofil eller et moduldesign og sikkerhedsdokumentation, der opfylder kravene i dette dokument, på grundlag af en risikoanalyse og under hensyntagen til fysiske og andre ikketekniske sikkerhedsforanstaltninger.

Hvis den sikre kryptografiske enhed er omfattet af en certificering under EUCC [10][11], skal enheden konfigureres og anvendes i overensstemmelse med denne certificering.

— TIS-7.6.3-03 udgår.

— NOTE 2 udgår.

8) 7.6.7 End of TSU key life cycle

— TIS-7.6.7-03A Udløbsdatoen for TSU's private nøgler skal være i overensstemmelse med de aftalte kryptografiske mekanismer [9].

— NOTE 1 udgår.

9) 7.10 Network security

— OVR-7.10-05 Den sårbarhedsscanning, der kræves i henhold til REQ-7.8-13 i ETSI EN 319 401 [1], skal udføres mindst én gang pr. kvartal.

— OVR-7.10-06 Den penetrationstest, der kræves i henhold til REQ-7.8-17X i ETSI EN 319 401 [1], skal udføres mindst én gang om året.

— OVR-7.10-07 Firewalls skal være konfigurerede til at forhindre alle protokoller og al adgang, der ikke er nødvendige for TSA'ens drift.

10) 7.14 TSA termination and termination plans

— OVR-7.14-01A Tillidstjenesteudbyderens plan i tilfælde af virksomhedsafbrydelse skal opfylde kravene i de gennemførelsesretsakter, der er vedtaget i henhold til artikel 24, stk. 5, i forordning (EU) nr. 910/2014 [i.4].

2. For ETSI EN 319 422:

(1) 2.1 Normative references

— [5] udgår.

— [6] udgår.

— [8] Den Europæiske Cybersikkerhedscertificeringsgruppe, undergruppen om kryptografi: »Agreed Cryptographic Mechanisms«.

— [9] RFC 9110 HTTP Semantics.

2) 4.1.3 Hash algorithms to be used

— Følgende bestemmelse finder anvendelse:

Hashalgoritmer, der anvendes til at mærke oplysninger, der skal tidsstemples, den forventede varighed af tidsstemplet og de valgte hashfunktioner i forhold til tid skal være i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [8].

— NOTE udgår.

3) 4.2.3 Algorithms to be supported

— Følgende bestemmelse finder anvendelse:

De signaturalgoritmer til tidsstempeltokens, der skal understøttes, skal være i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [8].

— NOTE udgår.

4) 4.2.4 Key lengths to be supported

— Følgende bestemmelse finder anvendelse:

Signaturalgoritmens nøglelængder for den valgte signaturalgoritme skal være i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA.

— NOTE udgår.

5) 5.1.3 Algorithms to be supported

— Følgende bestemmelse finder anvendelse:

Hashalgoritmer for tidsstempeldata, der skal understøttes, den forventede varighed af tidsstemplet og de valgte hashfunktioner i forhold til tid skal være i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [8].

— NOTE udgår.

6) 5.2.3 Algorithms to be used

— Følgende bestemmelse finder anvendelse:

Hashalgoritmer, der anvendes til at mærke oplysninger, der skal tidsstemples, og signaturalgoritmer til tidsstempeltokens, skal være i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [8].

— NOTE udgår.

7) 6.3 Key lengths requirements

— Følgende bestemmelse finder anvendelse:

Nøglelængden for den valgte signaturalgoritme i TSU-certifikatet skal være i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [8].

— NOTE udgår.

8) 6.5 Algorithm requirements

— Følgende bestemmelse finder anvendelse:

Den offentlige TSU-nøgle og TSU-certifikatsignaturen skal anvende de algoritmer, der er i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [8].

— NOTE udgår.

9) 7 Profiles for the transport protocols to be supported

— Tidsstemplingsklienten og tidsstemplingsserveren skal understøtte tidsstemplingsprotokollen via HTTPS [9] som defineret i afsnit 3.4 i IETF RFC 3161 [1].

10) 8 Object identifiers of the cryptographic algorithms

— Følgende bestemmelse finder anvendelse:

Den offentlige TSU-nøgle og TSU-certifikatsignaturen skal anvende algoritmer i overensstemmelse med de aftalte kryptografiske mekanismer, der er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [8].

11) 9.1 Regulation compliance statement

— Hvis et tidsstempeltoken af TSA'en erklæres for at være et kvalificeret elektronisk tidsstempel i overensstemmelse med forordning (EU) nr. 910/2014 [i.2], skal det indeholde en forekomst af udvidelsen qcStatements i feltet til udvidelse af tidsstempeltokenet med syntaks som defineret i IETF RFC 3739 [i.3], afsnit 3.2.6.

— Udvidelsen af qcStatements skal indeholde en forekomst af angivelsen »esi4-qtstStatement-1« som defineret i bilag B.

— Udvidelsen qcStatements må ikke markeres som kritisk.