2026/1735

22.7.2026

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2026/1735

af 15. juli 2026

om ændring af gennemførelsesforordning (EU) 2025/1569 for så vidt angår gældende standarder og specifikationer

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 45d, stk. 5, artikel 45e, stk. 2, artikel 45f, stk. 6, og artikel 45f, stk. 7, og

ud fra følgende betragtninger:

(1) For at sikre den højeste grad af harmonisering mellem medlemsstaterne med hensyn til udviklingen af europæiske digitale identitetstegnebøger er de tekniske specifikationer for tegnebøgerne baseret på det arbejde, der er udført på grundlag af Kommissionens henstilling (EU) 2021/946 ([2]) og navnlig den tekniske struktur og referencerammen. Da den tekniske struktur og referencerammen har udviklet sig betydeligt siden vedtagelsen af Kommissionens gennemførelsesforordning (EU) 2025/1569 ([3]), bør gennemførelsesforordning (EU) 2025/1569 nu ændres for at bringe den i overensstemmelse med de nye standarder og specifikationer.

(2) I overensstemmelse med målene i forordning (EU) nr. 910/2014 er en række standarder blevet udvalgt med henblik på opfyldelse af de krav, der gælder for udstedelse, forvaltning og verifikation af elektroniske attesteringer af attributter. Disse standarder bør afspejle etableret praksis og være bredt anerkendte inden for de relevante sektorer. Hvor det er nødvendigt, bør standarderne tilpasses eller suppleres for at garantere en høj grad af sikkerhed og integritet af elektroniske attesteringer af attributter og samtidig fremme grænseoverskridende interoperabilitet og et velfungerende indre marked. I tråd med denne målsætning ajourfører nærværende forordning de krav, der gælder for udstedelse og tilbagekaldelse af kvalificerede elektroniske attesteringer af attributter og elektroniske attesteringer af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, og indfører krav til underskrift og forsegling af kontrolresultater i forhold til autentiske kilder.

(3) Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([4]) og, i det omfang det er relevant, Europa-Parlamentets og Rådets direktiv 2002/58/EF ([5]) 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]) Kommissionens henstilling (EU) 2021/946 af 3. juni 2021 om en fælles EU-værktøjskasse for en koordineret tilgang til en ramme for en europæisk digital identitet (EUT L 210 af 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Kommissionens gennemførelsesforordning (EU) 2025/1569 af 29. juli 2025 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår kvalificerede elektroniske attesteringer af attributter og elektroniske attesteringer af attributter, der leveres af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde (EUT L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) 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).

([5]) 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 (direktivet 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).

(4) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([6]) og afgav udtalelse den 17. april 2026 ([7]).

(5) Foranstaltningerne i denne 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

Ændring af gennemførelsesforordning (EU) 2025/1569

I gennemførelsesforordning (EU) 2025/1569 foretages følgende ændringer:

1. (vedrører ikke den danske udgave)

2. I artikel 4 foretages følgende ændringer:

a) Stk. 1 udgår.

b) Stk. 3 affattes således:

»3. Udbydere af kvalificerede elektroniske attesteringer af attributter og udbydere af elektroniske attesteringer af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, tilbagekalder disse attesteringer, når de er udstedt med en gyldighedsperiode på mere end 24 timer, som minimum i følgende tilfælde:

a) efter anmodning fra den person, til hvem den elektroniske attestering af attributter er udstedt, eller fra genstanden for attesteringen

b) hvis udbyderen bliver bekendt med, at der er sket en kompromittering af sikkerheden eller troværdigheden af de kvalificerede elektroniske attesteringer af attributter eller elektroniske attesteringer af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde

c) i andre situationer som krævet i henhold til EU-retten eller national ret.«

c) Stk. 4 affattes således:

»4. Udbydere af kvalificerede elektroniske attesteringer af attributter og udbydere af elektroniske attesteringer af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, indfører tilbagekaldelsesteknikker og forvaltningsmåder, der beskytter privatlivets fred og hindrer sammenkædelighed og sporbarhed. Tilbagekaldelsesteknikkerne skal opfylde kravene i bilag II.«

([6]) 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 nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) EDPS Formal comments on the draft Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties | European Data Protection Supervisor.

3. I artikel 9 foretages følgende ændringer:

   a) Efter stk. 2 indsættes som stk. 2a:

      »2a: Kontrolmekanismen skal overholde specifikationerne i bilag IV.«

   b) Stk. 4 affattes således:

      »4. Kontrolresultatet skal angive, om attributten er blevet verificeret eller ej, og det skal fremgå, hvilken offentlig myndighed der er ansvarlig for den autentiske kilde, eller, hvis det er relevant, hvilken offentlig myndighed der er udpeget til at handle på vegne af den autentiske kilde, i forhold til hvilken attributten er blevet kontrolleret.

      Kontrolresultatet skal underskrives eller forsegles af den offentlige myndighed med ansvar for en autentisk kilde eller af den udpegede mellemmand, der er anerkendt på nationalt plan, som minimum ved hjælp af henholdsvis en avanceret elektronisk signatur baseret på et kvalificeret certifikat for elektroniske signaturer eller et avanceret elektronisk segl baseret på et kvalificeret certifikat for elektroniske segl.«

4. Bilag I erstattes af teksten i bilag I til nærværende forordning.

5. Bilag II erstattes af teksten i bilag II til nærværende forordning.

6. Teksten i bilag III til nærværende forordning tilføjes som bilag IV.

Artikel 2

Ikrafttræden

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

Artikel 1, stk. 3, finder anvendelse fra den 1. januar 2027.

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

Udfærdiget i Bruxelles, den 15. juli 2026.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG I

»BILAG I

Liste over referencestandarder og specifikationer som omhandlet i artikel 3

ETSI TS 119 471 V1.1.1 (2025-05) finder anvendelse med følgende tilpasninger:

1) 2.1 Normative references:

[1] ETSI EN 319 401 V3.2.1 (2026-01): »Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers«

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

[3] FIPS PUB 140-3 (2019) »Security Requirements for Cryptographic Modules«

[4] Kommissionens gennemførelsesforordning (EU) 2024/482 ([1])

[5] Kommissionens gennemførelsesforordning (EU) 2024/3144 ([2])

[6] ISO/IEC 15408:2022 (del 1-5): »Information security, cybersecurity and privacy protection – Evaluation criteria for IT security«.

2) 3.1 Terms:
Følgende term tilføjes:

— sikker kryptografisk anordning: en anordning, som indeholder brugerens private nøgle, beskytter denne nøgle mod kompromittering og udfører signatur- eller dekrypteringsfunktioner på vegne af brugeren

3) 4. EAA trust services

— Punkt 4.2.2.2 »Verification of attributes against authentic sources« finder ikke anvendelse.

— REQ-EAASP-4.2.2.3-02: EAASP skal autentificere mod den EUDIW-forekomst, som implementerer gensidige autentifikationsmekanismer, der bruger et gyldigt adgangscertifikat.

— REQ-EAASP-4.2.2.3-03: EAASP skal validere EUDIW-enheden, og *om EUDIW-forekomsten er tilbagekaldt*.

— Punkt *4.3.2 »EUDIW Specific« finder ikke anvendelse*.

4) 6.1 EAAS practice statement:

— REQ-EAASP-6.1-02: EAASP skal dokumentere tilbagekaldelsesmekanismen i EAAS-praksiserklæringen

5) 6.3 Information security policy:

— REQ-EAASP-6.3-02: EAASP skal etablere procedurer for underretning af tilsynsorganet om enhver ændring i leveringen af tillidstjenesten til elektronisk attestering af attributter og om intentionen om at indstille disse aktiviteter i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter, herunder i overensstemmelse med kravene i de gennemførelsesretsakter, der er vedtaget i henhold til artikel 24, stk. 5, i forordning (EU) nr. 910/2014. EAASP skal underrette tilsynsorganet mindst:

— en måned før gennemførelsen af en ændring

— tre måneder før den planlagte indstilling af leveringen af en tillidstjeneste.

([1]) Kommissionens gennemførelsesforordning (EU) 2024/482 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) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Kommissionens gennemførelsesforordning (EU) 2024/3144 af 18. december 2024 om ændring af gennemførelsesforordning (EU) 2024/482 for så vidt angår gældende internationale standarder og om berigtigelse af nævnte gennemførelsesforordning (EUT L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

6) 7.5 Cryptographic controls:

— REQ-EAASP-7.5.2-05: udgår

— REQ-EAASP-7.5.2-06: udgår

— REQ-EAASP-7.5.3-01A: Der skal være indført passende sikkerhedskontroller for forvaltningen af alle kryptografiske nøgler, kryptografiske algoritmer og kryptografiske anordninger i hele deres livscyklus ud fra, hvor det er relevant, en kryptografisk fleksibilitetstilgang.

— REQ-EAASP-7.5.3-01B: EAASP skal med henblik leveringen af tillidstjenester udvælge og anvende egnede kryptografiske teknikker, som er i overensstemmelse med de aftalte kryptografiske mekanismer, som er godkendt af Den Europæiske Cybersikkerhedscertificeringsgruppe og offentliggjort af ENISA [2].

— REQ-EAASP-7.5.3-02: EAASP skal sikre, at den sikre kryptografiske anordning, som anvendes til digital underskrift eller forsegling af EAA, er et kvalificeret signatur- eller seglgenereringssystem, og at alle andre digitale signaturer eller segl, der anvendes i leveringen af den pågældende tillidstjeneste til elektronisk attestering af attributter eller dele heraf genereres ved hjælp af en sikker kryptografisk anordning, der er et pålideligt system certificeret i overensstemmelse med:

(a) fælles kriterier for evaluering af informationsteknologisikkerhed som fastsat i Fælles kriterier for evaluering af informationsteknologisikkerhed, version 3.1 (CC3.1), frem til den 31. august 2027 eller version CC:2022, del 1-5, som 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) [4][5] og certificeret til EAL 4 eller højere, eller

(c) FIPS-140-2 niveau 3, som skal anvendes frem til den 31. august 2027 for eksisterende certificerede systemer, eller FIPS PUB 140-3 [3] niveau 3 frem til den 31. december 2030.

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

Hvis den sikre kryptografiske anordning er omfattet af en certificering inden for rammerne af EUCC [4][5], skal anordningen konfigureres og anvendes i overensstemmelse med denne certificering.

— REQ-EAASP-7.5.5-01: udgår

— REQ-EAASP-7.5.5-02: udgår

— REQ-EAASP-7.5.5-04: udgår

7) 7.9 Vulnerabilities and Incident management:

— REQ-EAASP-7.9-02: Overvågningsaktiviteter skal tage hensyn til følsomheden af alle oplysninger, der indsamles eller analyseres.

8) 7.12 EAASP and EAAS termination and termination plans:

— REQ-EAASP-7.12-04: EAASP's plan i tilfælde af virksomhedsafbrydelse skal opfylde kravene i de gennemførelsesretsakter, der er vedtaget i henhold til artikel 24, stk. 5, i forordning (EU) No 910/2014 [i.1].«

BILAG II

»*BILAG II*

Tekniske specifikationer som omhandlet i artikel 3 og artikel 4

Udbydere af kvalificerede elektroniske attesteringer af attributter og udbydere af elektronisk attestering af attributter, der er udstedt af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde, udsteder deres attesteringer i overensstemmelse med mindst én af de standarder, der er anført i bilag II til Kommissionens gennemførelsesforordning (EU) 2024/2979 ([1]), og anvender de relevante tilbagekaldelsesteknikker, som også er anført i bilag II til Kommissionens gennemførelsesforordning (EU) 2024/2979.«

([1]) Kommissionens gennemførelsesforordning (EU) 2024/2979 af 28. november 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår integriteten af og de centrale funktioner i europæiske digitale identitetstegnebøger (EUT L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

BILAG III

»*BILAG IV*

Liste over standarder og tekniske specifikationer som omhandlet i artikel 9

De kontrolmekanismer, der er omhandlet i artikel 9, skal være i overensstemmelse med en eller begge af følgende med følgende tilpasninger:

(a) de tekniske specifikationer i punkt 6.1.1 i ETSI TS 119 478 V1.1.1 (2026-01) - Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources

— REQ-ASIP-6.1.1.2-04-01 [CONDITIONAL]: Hvis attributeVerificationResult er enten http://uri.etsi.org/19478/VerificationResult/Match eller http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, kan attributeVerificationResult indeholde et attributeValue-element.

— REQ-ASIP-6.1.1.2-04-02 [CONDITIONAL]: Hvis det returnerede attributeVerificationResult er http://uri.etsi.org/19478/VerificationResult/Match, og attributeVerificationResult indeholder et attributeValue-element, skal attributeValue-elementet indeholde værdien som i anmodningen.

— REQ-ASIP-6.1.1.2-04-03 [CONDITIONAL]: Hvis det returnerede attributeVerificationResult er http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, og attributeVerificationResult indeholder et attributeValue-element, skal attributeValue-elementet indeholde attributtens værdi som lagret i den autentiske kilde.

— REQ-ASIP-6.1.1.2-06-04-01 [CONDITIONAL]: Hvis fragmentVerificationResult er enten http://uri.etsi.org/19478/VerificationResult/Match eller http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, kan attributeVerificationResult indeholde et fragmentValue-element.

— REQ-ASIP-6.1.1.2-06-04-02 [CONDITIONAL]: Hvis det returnerede fragmentVerificationResult er http://uri.etsi.org/19478/VerificationResult/Match, og attributeVerificationResult indeholder et fragmentValue-element, skal fragmentValue-elementet indeholde værdien som i anmodningen.

— REQ-ASIP-6.1.1.2-06-04-03 [CONDITIONAL]: Hvis det returnerede fragmentVerificationResult er http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, og attributeVerificationResult indeholder et fragmentValue-element, skal fragmentValue-elementet indeholde værdien af fragmentet af attributten som lagret i den autentiske kilde.

(b) de tekniske specifikationer i punkt 6.2.3 i ETSI TS 119 478 V1.1.1 (2026-01) - Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources.«

— REQ-ASIP-6.2.3.2.1-08-04: AttributeVerificationResponse-elementet kan indeholde præcist ét underelement, som skal være enten TextValue, XMLValue eller AttributeProperties.«