Europeiska unionens
officiella tidning

SV
L-serien

2026/1735

22.7.2026

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2026/1735

av den 15 juli 2026

om ändring av genomförandeförordning (EU) 2025/1569 vad gäller tillämpliga standarder och specifikationer

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 45d.5, 45e.2, 45f.6 och 45f.7, och

av följande skäl:

(1) För att säkerställa största möjliga harmonisering bland medlemsstaterna vid utvecklingen av europeiska digitala identitetsplånböcker bygger de tekniska specifikationerna för dessa på det arbete som utförts på grundval av kommissionens rekommendation (EU) 2021/946 ([2]), i synnerhet när det gäller arkitekturen och referensramen. Eftersom arkitekturen och referensramen har utvecklats avsevärt sedan antagandet av kommissionens genomförandeförordning (EU) 2025/1569 ([3]) bör genomförandeförordning (EU) 2025/1569 nu ändras i enlighet med detta för att anpassas till de nya standarderna, specifikationerna och förfarandena.

(2) I enlighet med målen i förordning (EU) nr 910/2014 har ett antal standarder valts ut för att uppfylla de krav som är tillämpliga på utfärdande, förvaltning och kontroll av elektroniska attributsintyg. Dessa standarder bör återspegla etablerad praxis och vara allmänt erkända inom de berörda sektorerna. När så är nödvändigt bör dessa standarder anpassas eller kompletteras för att säkerställa en hög nivå av säkerhet och integritet för elektroniska attributsbetyg och samtidigt främja gränsöverskridande interoperabilitet och en välfungerande inre marknad. I linje med detta mål uppdateras genom denna förordning de krav som är tillämpliga på utfärdandet och återkallandet av kvalificerade elektroniska attributsbetyg och elektroniska attributsintyg som utfärdats av, eller på uppdrag av, ett offentligt organ som ansvarar för en autentisk källa, och det införs krav för undertecknande och stämpling av kontrollresultat mot autentiska källor.

(3) Europaparlamentets och rådets förordning (EU) 2016/679 ([4]) och, i förekommande fall, Europaparlamentets och rådets direktiv 2002/58/EG ([5]) 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]) Kommissionens rekommendation (EU) 2021/946 av den 3 juni 2021 om en unionsgemensam verktygslåda för en samordnad strategi för en europeisk ram för digital identitet (EUT L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Kommissionens genomförandeförordning (EU) 2025/1569 av den 29 juli 2025 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller kvalificerade elektroniska attributsintyg och elektroniska attributsintyg som tillhandahålls av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa (EUT L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) 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 (den allmänna dataskyddsförordningen) (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) 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).

(4) Europeiska datatillsynsmannen har rådfrågats i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([6]) och avgav ett yttrande den 17 april 2026 ([7]).

(5) 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

Ändringar av genomförandeförordning (EU) 2025/1569

Genomförandeförordning (EU) 2025/1569 ska ändras på följande sätt:

1. Artikel 3.2 ska ersättas med följande:

”2. Om tillhandahållare av kvalificerade elektroniska attributsintyg och tillhandahållare av elektroniska attributsintyg som utfärdats av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa utfärdar elektroniska attributsintyg som ingår i system som är registrerade i katalogen med system för attributsintyg, ska de uppfylla kraven i motsvarande system för attributsintyg. De policyer och förfaranden som utfärdarna av intyg fastställer för att uppfylla kraven i systemen för attributsintyg ska ingå i den bedömning av överensstämmelse som fastställs i förordning (EU) nr 910/2014.”

2. Artikel 4 ska ändras på följande sätt:

a) Punkt 1 ska utgå.

b) Punkt 3 ska ersättas med följande:

”3. Tillhandahållare av kvalificerade elektroniska attributsintyg och tillhandahållare av elektroniska attributsintyg som utfärdats av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska, när dessa intyg utfärdas med en giltighetstid på mer än 24 timmar, återkalla dem under åtminstone följande omständigheter:

a) På begäran av den person till vilken det elektroniska attributsintyget utfärdades eller, i tillämpliga fall, av föremålet för intyget.

b) Om tillhandahållaren får kännedom om att säkerheten eller tillförlitligheten har äventyrats för de kvalificerade elektroniska attributsintyg eller elektroniska attributsintyg som utfärdats av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa.

c) I andra situationer, i enlighet med kraven i unionsrätten eller nationell rätt.”

c) Punkt 4 ska ersättas med följande:

”4. Tillhandahållare av kvalificerade elektroniska attributsintyg och tillhandahållare av elektroniska attributsintyg, som utfärdats av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa, ska inrätta tekniker och förvaltningsmetoder för återkallande som bevarar integriteten och förhindrar länkbarhet och spårbarhet. Teknikerna för återkallande ska uppfylla kraven i bilaga II.”

([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]) *EDPS Formal comments on the draft Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties* |,Europeiska datatillsynsmannen.

3. Artikel 9 ska ändras på följande sätt:

   a) Följande punkt ska införas som punkt 2a efter punkt 2:

      ”2a. Kontrollmekanismen ska överensstämma med specifikationerna i bilaga IV.”

   b) Punkt 4 ska ersättas med följande:

      ”4. Kontrollresultatet ska ange om attributet har kontrollerats eller inte och specificera det offentliga organ som ansvarar för den autentiska källa eller, i tillämpliga fall, det offentliga organ som utsetts att agera på den autentiska källans vägnar, som attributet har kontrollerats mot.

      Kontrollresultaten ska undertecknas eller stämplas av det offentliga organ som ansvarar för den autentiska källan eller av den utsedda mellanhand som erkänts på nationell nivå, med användning av åtminstone en avancerad elektronisk underskrift som är baserad på ett kvalificerat certifikat för elektroniska underskrifter eller en avancerad elektronisk stämpel som är baserad på ett kvalificerat certifikat för elektroniska stämplar.”

4. Bilaga I ska ersättas med texten i bilaga I till den här förordningen.

5. Bilaga II ska ersättas med texten i bilaga II till den här förordningen.

6. Texten i bilaga III till den här förordningen ska läggas till som bilaga IV.

Artikel 2

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 1.3 ska tillämpas från och med den 1 januari 2027.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 15 juli 2026.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA I

”BILAGA I

Förteckning över referensstandarder och specifikationer som avses i artikel 3

ETSI TS 119 471 V1.1.1 (2025-05) ska tillämpas med följande anpassningar:

1. 2.1 Normative references (normativa referenser):

   [1] ETSI EN 319 401 V3.2.1 (2026-01): ’Electronic Signatures and Trust Infrastructures (ESI)’ (Elektroniska underskrifter och infrastrukturer), ’General Policy Requirements for Trust Service Providers’ (allmänna policykrav för tillhandahållare av betrodda tjänster).

   [2] Europeiska gruppen för cybersäkerhetscertifiering, undergruppen för kryptografi: ’Agreed Cryptographic Mechanisms’ (överenskomna kryptografiska mekanismer), offentliggjord av Europeiska unionens cybersäkerhetsbyrå (Enisa).

   [3] FIPS PUB 140-3 (2019) ’Security Requirements for Cryptographic Modules’ (säkerhetskrav för kryptografiska moduler).

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

   [5] Kommissionens genomförandeförordning (EU) 2024/3144 ([2]).

   [6] ISO/IEC 15408:2022 (delarna 1–5): ’Information security, cybersecurity and privacy protection – Evaluation criteria for IT security’ (informationssäkerhet, cybersäkerhet och integritetsskydd – utvärderingskriterier för IT-säkerhet).

2. 3.1 Terms (termer):
   Följande term läggs till:

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

3. 4. EAA trust services (Betrodda EAA-tjänster)

   — Avsnitt 4.2.2.2 ’Verification of attributes against authentic sources’ (kontroll av attribut mot autentiska källor) ska inte tillämpas.

   — REQ-EAASP-4.2.2.3-02: EAASP ska autentisera sig för den EUDIW-instans (instans för den europeiska digitala identitetsplånboken) som genomför ömsesidiga autentiseringsmekanismer som använder ett giltigt åtkomstcertifikat.

   — REQ-EAASP-4.2.2.3-03: EAASP ska validera EUDIW-enheten, och *kontrollera om EUDIW-instansen återkallas.*

   — Avsnitt *4.3.2 ’EUDIW Specific’ (specifikt för EUDIW) ska inte tillämpas.*

4. 6.1 EAAS practice statement (EAAS-förklaring om praxis):

   — REQ-EAASP-6.1-02: EAASP ska dokumentera återkallelsemekanismen i EAAS-förklaringen om praxis

5. 6.3 Information security policy (informationssäkerhetspolicy):

   — REQ-EAASP-6.3-02: EAASP ska fastställa förfaranden för att underrätta tillsynsorganet om alla ändringar av tillhandahållandet av den betrodda tjänsten för elektroniska attributsintyg och om avsikter att upphöra med denna verksamhet, i enlighet med verksamhetskraven och relevanta lagar och andra författningar, inbegripet kraven i genomförandeakter som antagits i enlighet med artikel 24.5 i förordning (EU) nr 910/2014. EAASP ska till tillsynsorganet sända en anmälan senast

     — en månad innan någon ändring genomförs,

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

([1]) 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/oj).

([2]) 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).

6. 7.5 Cryptographic controls (kryptografiska kontroller):

   — REQ-EAASP-7.5.2-05: inget värde.

   — REQ-EAASP-7.5.2-06: inget värde.

   — REQ-EAASP-7.5.3-01A: 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-EAASP-7.5.3-01B: EAASP 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 [2].

   — REQ-EAASP-7.5.3-02: EAASP ska säkerställa att den säkra kryptogafiska enhet som EAASP använder för digital signatur för EAA är en kvalificerad underskrift, eller en kvalificerad anordning för skapande av stämplar, och att alla andra digitala signaturer eller stämplar som används för att tillhandahålla den motsvarande betrodda tjänsten för elektroniska attributsintyg, eller en del av denna, skapats med en säker krypteringshårdvara som är ett tillförlitligt system som certifierats i enlighet med

      a) Common Criteria for Information Technology Security Evaluation, såsom dessa anges i Common Criteria for Information Technology Security Evaluation, version 3.1 (CC3.1) till och med den 31 augusti 2027 eller i 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, eller såsom dessa anges i ISO/IEC 15408 [6], och som certifierats på nivå EAL 4 eller högre, eller

      b) den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) [4][5] och som certifierats på nivå EAL 4 eller högre, eller

      c) FIPS-140-2 nivå 3 som ska användas till och med den 31 augusti 2027 för befintliga certifierade system eller FIPS PUB 140-3 [3] nivå 3 till och med den 31 december 2030.

      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.

   — REQ-EAASP-7.5.5-01: inget värde.

   — REQ-EAASP-7.5.5-02: inget värde.

   — REQ-EAASP-7.5.5-04: inget värde.

7. 7.9 Vulnerabilities and Incident management (sårbarheter och incidenthantering):

   — REQ-EAASP-7.9-02: Övervakningsverksamheten ska ta hänsyn till känsligheten hos all information som samlas in eller analyseras.

8. 7.12 EAASP and EAAS termination and termination plans (EAASP och EAAS – avslutande och planer för avslutande):

   — REQ-EAASP-7.12-04: EAASP: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].”

BILAGA II

”BILAGA II

Tekniska specifikationer som avses i artikel 3 och artikel 4

Tillhandahållare av kvalificerade elektroniska attributsintyg och tillhandahållare av elektroniska attributsintyg som utfärdats av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska utfärda intygen i enlighet med åtminstone en av de standarder som förtecknas i bilaga II till kommissionens genomförandeförordning (EU) 2024/2979 ([1]) och tillämpa de relevanta teknikerna för återkallelse, som också anges i bilaga II till kommissionens genomförandeförordning (EU) 2024/2979.”

([1]) Kommissionens genomförandeförordning (EU) 2024/2979 av den 28 november 2024 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller integritet och centrala funktioner hos EU:s digitala identitetsplånböcker (EUT L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

BILAGA III

”BILAGA IV

Förteckning över standarder och tekniska specifikationer som avses i artikel 9

De kontrollmekanismer som avses i artikel 9 ska överensstämma med en eller båda av följande med följande ändringar:

a) De tekniska specifikationer som anges i avsnitt 6.1.1 i ETSI TS 119 478 V1.1.1 (2026-01) – Electronic Signatures and Trust Infrastructures (ESI) (Elektroniska underskrifter och infrastrukturer), Specification of interfaces related to Authentic Sources (specifikation för gränssnitt relaterade till autentiska källor).

— REQ-ASIP-6.1.1.2-04-01 [VILLKORAD]: I fall attributeVerificationResult är antingen http://uri.etsi.org/19478/VerificationResult/Match eller http://uri.etsi.org/19478/VerificationResult/MatchWithVariation kan attributeVerificationResult innehålla ett attributeValue-element.

— REQ-ASIP-6.1.1.2-04-02 [VILLKORAD]: Om returnerat attributeVerificationResult är http://uri.etsi.org/19478/VerificationResult/Match och attributeVerificationResult innehåller ett attributeValue-element, ska attributeValue-elementet innehålla det värde som anges i begäran.

— REQ-ASIP-6.1.1.2-04-03 [VILLKORAD]: Om returnerat attributeVerificationResult är http://uri.etsi.org/19478/VerificationResult/MatchWithVariation och attributeVerificationResult innehåller ett attributeValue-element, ska attributeValue-elementet innehålla det värde på attributet som lagras i den autentiska källan.

— REQ-ASIP-6.1.1.2-06-04-01 [VILLKORAD]: Ifall fragmentVerificationResult är antingen http://uri.etsi.org/19478/VerificationResult/Match eller http://uri.etsi.org/19478/VerificationResult/MatchWithVariation the får attributeVerificationResult innehålla ett fragmentValue-element.

— REQ-ASIP-6.1.1.2-06-04-02 [VILLKORAD]: Om returnerat fragmentVerificationResult är http://uri.etsi.org/19478/VerificationResult/Match, och attributeVerificationResult innehåller ett fragmentValue-element, ska fragmentValue-elementet innehålla det värde som anges i begäran.

— REQ-ASIP-6.1.1.2-06-04-03 [VILLKORAD]: Om returnerat fragmentVerificationResult är http://uri.etsi.org/19478/VerificationResult/MatchWithVariation och attributeVerificationResult innehåller ett fragmentValue-element, ska fragmentValue-elementet innehålla det värde på attributet som lagras i den autentiska källan.

b) De tekniska specifikationer som anges i avsnitt 6.2.3 i ETSI TS 119 478 V1.1.1 (2026-01) – Electronic Signatures and Trust Infrastructures (ESI) (Elektroniska underskrifter och infrastrukturer), Specification of interfaces related to Authentic Sources (specifikation för gränssnitt relaterade till autentiska källor).

— REQ-ASIP-6.2.3.2.1-08-04: Elementet AttributeVerificationResponse kan innehålla exakt ett underordnat element (child element) av typerna TextValue, XMLValue eller AttributeProperties.”