2026/1731

22.7.2026

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2026/1731

af 15. juli 2026

om ændring af gennemførelsesforordning (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 og (EU) 2024/2982 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 5a, stk. 23, 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 Kommissionens gennemførelsesforordning (EU) 2024/2977 ([3]), (EU) 2024/2979 ([4]), (EU) 2024/2980 ([5]) og (EU) 2024/2982 ([6]), bør disse gennemførelsesforordninger nu ændres, så de bringes i overensstemmelse med nye standarder, specifikationer og procedurer.

I overensstemmelse med målene i forordning (EU) nr. 910/2014 er der udvalgt en række standarder med henblik på opfyldelse af disse specifikke krav. Disse standarder bør afspejle etableret praksis og være bredt anerkendte inden for de relevante sektorer. F.eks. anvendes W3C VCDM-formatet som referenceformat for attesteringer i navnlig uddannelsessektoren, og de europæiske digitale identitetstegnebøger bør derfor også understøtte dette format, når de nye profiler i W3C VCDM-formatet er tilgængelige. Hvor det er nødvendigt, bør standarderne tilpasses eller suppleres for at garantere de europæiske digitale identitetstegnebøgers sikkerhed og pålidelighed og samtidig fremme interoperabilitet på tværs af grænserne og et velfungerende indre marked.

(2) I forbindelse med enhver anvendelse af tegnebogen, som kræver fremlæggelse af tegnebogsbrugerens ID-billede, skal tegnebogsløsningerne understøtte funktionen selektiv videregivelse, og videregivelsen skal være under brugerens fulde kontrol. For at garantere muligheden for at træffe beslutning om videregivelse og for at beskytte ID-billedet mod utilsigtede eller uautoriserede anmodninger om videregivelse bør den strukturmæssige udformning af de europæiske digitale identitetstegnebøger omfatte advarselsmekanismer, og alle transaktioner vedrørende anvendelse af ID-billedet bør logges. For at sikre, at tegnebogsbrugeren er opmærksom på deling af biometriske data, bør

([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) 2024/2977 af 28. november 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår personidentifikationsdata og elektronisk attestering af attributter udstedt til europæiske digitale identitetstegnebøger (EUT L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).
([4]) 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).
([5]) Kommissionens gennemførelsesforordning (EU) 2024/2980 af 28. november 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår anmeldelser til Kommissionen vedrørende økosystemet for europæiske digitale identitetstegnebøger (EUT L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).
([6]) Kommissionens gennemførelsesforordning (EU) 2024/2982 af 28. november 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår protokoller og grænseflader, der skal understøttes af den europæiske ramme for digital identitet (EUT L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

advarslerne angive, at anmodningen indebærer deling af biometriske data, og specifikt kræve, at brugeren bekræfter videregivelsen. Når en modtagerpart behandler ID-billedet med det formål entydigt at identificere en fysisk person eller bekræfte den pågældende persons påståede identitet, finder artikel 6 og 9 i Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([7]) anvendelse sammen med alle andre krav i nævnte forordning, herunder at modtagerparters behandling af ID-billedet bør begrænses til, hvad der er nødvendigt for den tilsigtede anvendelse. Den tilsigtede anvendelse bør meddeles tegnebogsbrugeren sammen med anmodningen om videregivelse på et klart og forståeligt sprog. For at tage behørigt hensyn til følsomheden af biometriske data bør tegnebogsbrugeren udtrykkeligt og specifikt bekræfte videregivelsen af ID-billedet. Tavshed eller forudafkrydsede felter bør ikke betragtes som en bekræftelse fra tegnebogsbrugerens side. Tegnebogsbrugerens udtrykkelige bekræftelse bør være en teknisk sikkerhedsforanstaltning og ikke i sig selv udgøre et retsgrundlag for behandling. Som fastsat i artikel 9, stk. 4, i forordning (EU) 2016/679, kan medlemsstaterne opretholde eller indføre yderligere betingelser, herunder begrænsninger, for behandling af genetiske data, biometriske data eller helbredsoplysninger.

(3) For at give medlemsstaterne tilstrækkelig tid til at tilpasse deres nationale procedurer må tegnebogsbrugerens ID-billede først være en del af de obligatoriske personidentifikationsdata for fysiske personer fra den 11. august 2028. Når disse billeder hentes fra eksisterende identitetsdokumenter såsom identitetskort eller pas, finder de relevante krav i henholdsvis Rådets forordning (EU) 2025/1208 ([8]) eller forordning (EF) nr. 2252/2004 ([9]) anvendelse.

(4) I henhold til forordning (EU) nr. 910/2014 skal tegnebøger kunne fremvise et EU-tillidsmærke for europæiske digitale identitetstegnebøger som en kontrollerbar, simpel og genkendelig angivelse af, at en tegnebog er udstedt i overensstemmelse med forordningen. Anvendelsen af et sådant tillidsmærke vil bidrage til et velfungerende indre marked, sikre fair konkurrence og beskytte forbrugernes interesser. For at gøre det muligt at anvende et sådant tillidsmærke bør tillidsmærkets visuelle og tekniske karakteristika fastlægges.

(5) Som fastsat i artikel 12b i forordning (EU) nr. 910/2014 skal gatekeepere give udbydere af europæiske digitale identitetstegnebøger og udstedere af anmeldte elektroniske identifikationsmidler effektiv interoperabilitet med og, med henblik på interoperabilitet, adgang til det samme styresystem eller de samme hardware- eller softwarefunktioner. Sådan effektiv interoperabilitet og adgang skal gives gratis, og uanset om hardware- eller softwarefunktionerne er en del af styresystemet, er tilgængelige for eller anvendes af den pågældende gatekeeper, når denne udbyder sådanne tjenester. Da alle tegnebogsløsninger bør understøtte et fælles sæt protokoller og grænseflader for at sikre anvendelighed, sikkerhed og interoperabilitet på tværs af medlemsstaterne, bør gatekeepere muliggøre de styresystems-, hardware- eller softwarefunktioner, der er nødvendige for at gennemføre de protokoller og grænseflader, der er fastsat i bilag XII til nærværende forordning. I den forbindelse bør en lokal kommunikationskanal som muliggjort af specifikationen vedrørende Client To Authenticator Protocol (CTAP), version 2.3 ([10]), foretrækkes af gatekeepere i onlinestrømme på tværs af anordninger til både fysisk nærhedskontrol og dataoverførsel mellem de to enheder frem for anvendelse af CTAP-hybridtunneltjenester.

(6) For at give medlemsstaterne, udbydere af registreringscertifikater for tegnebogsmodtagere og tegnebogsudbydere tilstrækkelig tid til at gøre tegnebogsenhederne i stand til at autentificere og validere registreringscertifikater for tegnebogsmodtagere bør dette krav først finde anvendelse fra den 11. august 2028.

(7) Forordning (EU) 2016/679 og, i det omfang det er relevant, Europa-Parlamentets og Rådets direktiv 2002/58/EF ([11]) finder anvendelse på alle behandlingsaktiviteter vedrørende personoplysninger i henhold til nærværende forordning.

([7]) 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).

([8]) Rådets forordning (EU) 2025/1208 af 12. juni 2025 om styrkelse af sikkerheden af unionsborgeres identitetskort og af opholdsdokumenter, der udstedes til unionsborgere og deres familiemedlemmer, som udøver deres ret til fri bevægelighed (EUT L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Rådets forordning (EF) nr. 2252/2004 af 13. december 2004 om standarder for sikkerhedselementer og biometriske identifikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder (EUT L 385 af 29.12.2004, s. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Fido Alliance proposed standard, Client to Authenticator Protocol (CTAP), 26. februar 2026.

([11]) 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).

(8) Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([12]) og afgav udtalelse den 17. april 2026 ([13]).

(9) 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) 2024/2977

I gennemførelsesforordning (EU) 2024/2977 foretages følgende ændringer:

1) Som artikel 3a indsættes:

»*Artikel 3a*

Beskyttelse af ID-billedet

1. Foruden oplysningskrav i henhold til forordning (EU) 2016/679 sikrer tegnebogsudbydere, at de tegnebogsløsninger, som de leverer, udsender advarsler til tegnebogsbrugere, når tegnebogsmodtagere anmoder om videregivelse af ID-billedet, med angivelse af, at anmodningen indebærer deling af biometriske data og kræver bekræftelse af den selektive videregivelse af ID-billedet.

2. Med henblik på gennemførelsen af selektiv videregivelse af ID-billedet til en tegnebogsmodtager sikrer tegnebogsudbydere, at tegnebogsløsningerne kræver, at tegnebogsbrugeren udtrykkeligt og specifikt bekræfter fremlæggelsen af ID-billedet.

3. ID-billedet må ikke opbevares af tegnebogsmodtagere, medmindre behandling af billedet er nødvendig med henblik på identifikation og autentifikation i overensstemmelse med EU's databeskyttelseslovgivning, eller dette er fastsat i EU-retten eller national ret i overensstemmelse med EU's databeskyttelseslovgivning. ID-billedet må ikke overføres til tredjelande eller internationale organisationer, medmindre dette er tilladt i henhold til EU's databeskyttelseslovgivning.«

2) Artikel 4, stk. 1, affattes således:

»1. Elektroniske attesteringer af attributter udstedt til tegnebogsenheder skal opfylde mindst én af de standarder, der er anført i bilag II til gennemførelsesforordning (EU) 2024/2979.«

3) I artikel 5, stk. 4, litra b), affattes således:

»b) hvis tegnebogsenhedsattesteringen af den tegnebogsenhed, som personidentifikationsdataene blev udstedt til, er blevet tilbagekaldt«

4) Bilaget erstattes af teksten i bilag I til nærværende forordning.

([12]) 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).

([13]) EDPS Formal comments on the draft Implementing Regulation as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980 | Den Europæiske Tilsynsførende for Databeskyttelse.

Artikel 2

Ændring af gennemførelsesforordning (EU) 2024/2979

I gennemførelsesforordning (EU) 2024/2979 foretages følgende ændringer:

1) Artikel 3, stk. 2, udgår.

2) Artikel 5, stk. 1, litra a), affattes således:

»a) kun udfører kryptografiske tegnebogsoperationer, der involverer kritiske aktiver, der er lagret i en sikker kryptografisk tegnebogsanordning og ikke er nødvendige for autentifikationen af tegnebogsbrugeren, i tilfælde, hvor disse applikationer har godkendt tegnebogsbrugere«

3) Som artikel 5a indsættes:

»*Artikel 5a*

Kryptografiske mekanismer

Tegnebogsudbydere anvender med henblik på artikel 4, stk. 2, kun de kryptografiske mekanismer, der er omhandlet i bilag Ia.«

4) I artikel 6 foretages følgende ændringer:

a) Stk. 1 affattes således:

»1. Tegnebogsudbydere udsteder tegnebogsenhedsattesteringer for hver tegnebogsenhed. Tegnebogsudbyderne underskriver eller forsegler tegnebogsenhedsattesteringerne på en sådan måde, at signaturerne eller seglene kan valideres ved hjælp af et certifikat, der er opført i overensstemmelse med afsnit 2, punkt 1), litra h), i bilag II til gennemførelsesforordning (EU) 2024/2980.«

b) Stk. 2 affattes således:

»2. Tegnebogsudbydere sikrer, at de tegnebogsenhedsattesteringer, der er omhandlet i stk. 1, opfylder de tekniske specifikationer, der er anført i bilag Ib.«

c) Stk. 3, litra b), affattes således:

»b) sørge for sikre identifikations- og autentifikationsmekanismer for tegnebogsbrugere, som er uafhængige af tegnebogsenheder«.

5) Artikel 9, stk. 2, litra b), affattes således:

»b) navn, kontaktoplysninger og den entydige identifikator for den tilsvarende tegnebogsmodtager og den medlemsstat, hvor den pågældende tegnebogsmodtager er etableret«

6) Artikel 10, stk. 1, affattes således:

»1. Tegnebogsudbydere sikrer, at elektroniske attesteringer af attributter, der er udstedt i overensstemmelse med de tekniske specifikationer, der gælder for fælles indlejrede offentliggørelsespolitikker, jf. i bilag III, kan behandles af de tegnebogsenheder, som de stiller til rådighed.«

7) I artikel 12 foretages følgende ændringer:

a) Stk. 2, litra c), affattes således:

»c) generering af signaturer eller segl i overensstemmelse med som minimum det obligatoriske format for signaturer og segl, der er omhandlet i bilag IV«.

b) Stk. 3 affattes således:

»3. Signaturgenereringsapplikationerne kan være integreret i eller være eksterne i forhold til tegnebogsforekomster.«

c) Følgende stykke indsættes:

»4. De signaturgenereringsapplikationer, der anvendes af tegnebogsenheder, skal som minimum understøtte den API-grænseflade, der er omhandlet i bilag IV.«

8) Artikel 14, stk. 1, udgår.

9) Som artikel 14a indsættes:

»*Artikel 14a*

EU-tillidsmærke for europæiske digitale identitetstegnebøger

1. Tegnebogsudbydere sikrer, at tegnebogsenhederne fremviser EU-tillidsmærket for europæiske digitale identitetstegnebøger. EU-tillidsmærket for europæiske digitale identitetstegnebøger skal være udformet som anført i bilag VI og VII.

2. Tegnebogsudbydere sikrer, at tegnebogsenhederne sætter tegnebogsbrugerne i stand til at få adgang til oplysninger, der gør det muligt for dem at verificere tegnebogsløsningens certificeringsstatus. Med henblik herpå sikrer tegnebogsudbyderne, at efter registrering af en tegnebogsløsning indeholder de tilsvarende tegnebogsenheder de URL'er, som Europa-Kommissionen har stillet til rådighed for en sådan verifikation. Tegnebogsudbyderne sikrer, at deres tegnebogsenheder har adgang til data fra EU-tillidsmærket for europæiske digitale identitetstegnebøger, der opfylder de tekniske specifikationer i bilag VIII.

3. Referencefarverne for EU-tillidsmærket for europæiske digitale identitetstegnebøger er Pantone nr. 661 og 116 eller, hvis der anvendes firefarvetryk, blå (100 % cyan + 67 % magenta + 0 % gul + 40 % sort) og gul (0 % cyan + 20 % magenta + 100 % gul + 0 % sort), og hvis der anvendes RGB-farver, skal referencefarverne være blå (0 rød + 51 grøn + 153 blå) og gul (255 rød + 204 grøn + 0 blå).

4. Kun hvis det ikke er praktisk muligt at benytte farve, må EU-tillidsmærket for europæiske digitale identitetstegnebøger anvendes i sort-hvid som angivet i bilag VII.

5. Hvis EU-tillidsmærket for europæiske digitale identitetstegnebøger anvendes på en mørk baggrund, kan det anvendes i negativt format med samme baggrundsfarve. Hvis EU-tillidsmærket for europæiske digitale identitetstegnebøger anvendes i farve på en farvet baggrund, der gør det vanskeligt at se mærket, kan der benyttes en afgrænsende ydre linje omkring EU-tillidsmærket for europæiske digitale identitetstegnebøger for at gøre kontrasten med baggrundsfarverne større.

6. EU-tillidsmærket for europæiske digitale identitetstegnebøger skal have en minimumsstørrelse på 64×85 pixels med 150 dpi.

7. Tegnebogsudbydere sikrer, at EU-tillidsmærket for europæiske digitale identitetstegnebøger anvendes på en måde, der muliggør en klar angivelse af den tegnebogsenhed, som EU-tillidsmærket for europæiske digitale identitetstegnebøger hører til. EU-tillidsmærket for europæiske digitale identitetstegnebøger kan knyttes til grafiske elementer eller tekstelementer, der klart angiver den tegnebogsenhed, som mærket anvendes for, forudsat at de ikke ændrer mærkets genkendelighed som et EU-tillidsmærke for europæiske digitale identitetstegnebøger eller forbindelsen til listen over certificerede europæiske digitale identitetstegnebøger, jf. artikel 5d i forordning (EU) nr. 910/2014.

8. Hvis tegnebogsudbydere har tilbagekaldt en tegnebogsenhedsattestering, sikrer de, at EU-tillidsmærket for digitale identitetstegnebøger ikke længere fremvises af den pågældende tegnebogsenhed.«

10) Bilag Ia og Ib tilføjes som anført i bilag II og bilag III til nærværende forordning.

11) Bilag II erstattes af bilag IV til nærværende forordning.

12) Bilag III erstattes af bilag V til nærværende forordning.

13) Bilag IV ændres i overensstemmelse med bilag VI til nærværende forordning.

14) Bilag V udgår.

15) Teksten i bilag VII til nærværende forordning indsættes som bilag VI.

16) Teksten i bilag VIII til nærværende forordning indsættes som bilag VII.

17) Teksten i bilag IX til nærværende forordning indsættes som bilag VIII.

Artikel 3

Ændring af gennemførelsesforordning (EU) 2024/2980

I gennemførelsesforordning (EU) 2024/2980 foretages følgende ændringer:

1. Artikel 5, stk. 2, affattes således:

»2. Hvis det er relevant, opretter, vedligeholder og offentliggør Kommissionen en liste over de oplysninger, som medlemsstaterne har anmeldt om udbydere af tegnebøger, udbydere af personidentifikationsdata, udbyder af adgangscertifikater for tegnebogsmodtagere og udbydere af registreringscertifikater for tegnebogsmodtagere, jf. bilag II, afsnit 2, 3, 4 og 5.«

2. Bilag II til gennemførelsesforordning (EU) 2024/2980 ændres som anført i bilag X til nærværende forordning.

Artikel 4

Ændring af gennemførelsesforordning (EU) 2024/2982

I gennemførelsesforordning (EU) 2024/2982 foretages følgende ændringer:

1) Artikel 1, nr. 2), affattes således:

»2) fremlæggelse af attributter for personidentifikationsdata og elektroniske attesteringer af attributter for tegnebogsmodtagere«.

2) I artikel 3 foretages følgende ændringer:

a) Nr. 1) affattes således:

»1) autentificerer og validerer adgangscertifikater for tegnebogsmodtagere, når de interagerer med tegnebogsmodtagere, uden at delegere udførelsen af disse processer til en browser i styresystemet eller en anden mellemliggende applikation«.

b) Nr. 2) udgår.

c) Nr. 3) affattes således:

»3) autentificerer og validerer anmodninger, der er indgivet ved hjælp af adgangscertifikater for tegnebogsmodtagere«

d) Nr. 4) affattes således:

»4) autentificerer og validerer registreringscertifikatet for tegnebogsmodtagere«

e) Nr. 5) affattes således:

»5) viser tegnebogsbrugerne de oplysninger, der er indeholdt i adgangscertifikater for tegnebogsmodtagere«.

f) Nr. 8) udgår.

g) Nr. 9) affattes således:

»9) ikke fremlægger attributter, der anmodes om, for tegnebogsmodtagere, før følgende trin er afsluttet:

a) verifikation af, at indlejrede offentliggørelsespolitikker er blevet behandlet i tegnebogsenheden i overensstemmelse med artikel 10 i gennemførelsesforordning (EU) 2024/2979

b) verifikation af, at tegnebogsbrugerne delvist eller fuldt ud har godkendt fremlæggelsen«.

3) Artikel 4, stk. 1, affattes således:

»1. Tegnebogsudbydere sikrer, at tegnebogsløsningerne understøtter protokollerne og grænsefladerne i bilag I til udstedelse af personidentifikationsdata og elektroniske attesteringer af attributter til tegnebogsenheder.«

4) I artikel 5 foretages følgende ændringer:

   a) Stk. 1 og 2 affattes således:

      »1. Tegnebogsudbydere sikrer, at tegnebogsløsningerne understøtter protokoller og grænseflader til fremlæggelse af attributter for tegnebogsmodtagere på afstand og, hvis det er relevant, i nærheden, i overensstemmelse med de tekniske specifikationer, der er fastsat i bilag II.

      2. Tegnebogsudbydere sikrer, at tegnebogsenhederne efter anmodning fra brugerne besvarer autentificerede og validerede anmodninger fra tegnebogsmodtagere omhandlet i artikel 3, i overensstemmelse med de tekniske specifikationer, der er fastsat i bilag II.«

   b) Stk. 5 udgår.

5) Artikel 8 affattes således:

   »*Artikel 8*

   Ikrafttræden

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

   Artikel 3, stk. 4, finder anvendelse fra den 11. august 2028.

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

6) Bilaget udgår.

7) Teksten i bilag XI til nærværende forordning tilføjes som bilag I.

8) Teksten i bilag XII til nærværende forordning tilføjes som bilag II.

Artikel 5

Ikrafttræden

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 15. juli 2026.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG I

»BILAG

Tekniske specifikationer for personidentifikationsdata omhandlet i artikel 3, stk. 3

1) Afsnit 1: Sæt af personidentifikationsdata for fysiske personer

Tabel 1:

Obligatoriske personidentifikationsdata for fysiske personer til selektiv videregivelse

Dataidentifikator	Definition
`family_name`	Nuværende efternavn(e) på den bruger, som personidentifikationsdataene vedrører.
`given_name`	Nuværende fornavn(e), herunder eventuelle mellemnavne, på den bruger, som personidentifikationsdataene vedrører.
`birth_date`	Dag, måned og år, hvor den bruger, som personidentifikationsdataene vedrører, blev født.
`birth_place`	Det land, som en alfa-2-landekode som specificeret i ISO 3166-1, eller den stat, den provins, det distrikt eller det lokalområde eller den kommune eller by, hvor den bruger, som personidentifikationsdataene vedrører, blev født.
`nationality`	En eller flere alfa-2-landekoder som specificeret i ISO 3166-1, der repræsenterer nationaliteten af den bruger, som personidentifikationsdataene vedrører.
`portrait`	Ansigtsbillede af den bruger, som personidentifikationsdataene vedrører, undtagen, i det omfang det er relevant, når brugeren udtrykkeligt fravælger dette, i overensstemmelse med kvalitetskravene til et fuldt frontalbillede i ISO/IEC 39794-5 eller, med henblik på bagudkompatabilitet, ISO/IEC 19794-5, punkt 8.2, 8.3 og 8.4, og leveret som kodede billeddata uden overskrifter eller sløringer som specificeret i ISO/IEC 19794-5, punkt 5, bortset fra selve billeddataene (JPEG); finder anvendelse fra 11. august 2028.

— Medlemsstaterne kan fastsætte, at brugeren har mulighed for at afslå, at ID-billedet inkluderes i personidentifikationsdataene.

— Medlemsstaterne sikrer, at den selektive videregivelse gælder for hver enkelt dataidentifikator, herunder ID-billedet.

— Hvis den fysiske persons fødselsdato ikke er kendt, vælger medlemsstaterne passende værdier, som er i overensstemmelse med de specifikationer, der er anført i dette bilags afsnit 4.1 eller 4.2 (alt efter hvad der er relevant).

— Hvis den fysiske persons nationalitet er ukendt, anvender medlemsstaterne værdien »QU«.

— Hvis den fysiske person ikke har nogen nationalitet, anvender medlemsstaterne værdien »QS«.

— Hvis brugeren fravælger, at ID-billedet medtages, lader medlemsstaterne værdien stå tom.

Tabel 2:

Valgfrie personidentifikationsdata for fysiske personer til selektiv videregivelse

Dataidentifikator	Definition
resident_address	Den fulde adresse på det sted, hvor den bruger, som personidentifikationsdataene vedrører, i øjeblikket er bosiddende eller kan kontaktes (gadenavn, husnummer, by, osv.).
resident_country	Det land, hvor den bruger, som personidentifikationsdataene vedrører, i øjeblikket er bosiddende, som en alfa-2-landekode som specificeret i ISO 3166-1.
resident_state	Den stat, den provins, det distrikt eller det lokalområde, hvor den bruger, som personidentifikationsdataene vedrører, i øjeblikket er bosiddende.
resident_city	Den kommune eller by, hvor den bruger, som personidentifikationsdataene vedrører, i øjeblikket er bosiddende.
resident_postal_code	Postnummeret på det sted, hvor den bruger, som personidentifikationsdataene vedrører, i øjeblikket er bosiddende.
resident_street	Navnet på den gade, hvor den bruger, som personidentifikationsdataene vedrører, i øjeblikket er bosiddende, inklusive husnummeret og eventuelle præfikser eller suffikser.
personal_administrative_-number	En værdi, der tildeles den bruger, som personidentifikationsdataene vedrører, og som er unik blandt alle personlige administrative numre, der er udstedt af udbyderen af personidentifikationsdata. Hvis medlemsstaterne vælger at medtage denne attribut, skal de i deres elektroniske identifikationsordninger, som personidentifikationsdataene udstedes under, beskrive den politik, de anvender på værdierne for denne attribut, herunder særlige betingelser for behandling af denne værdi, hvor det er relevant.
family_name_birth	Efternavn(e) på den bruger, som personidentifikationsdataene vedrører, på fødselstidspunktet.
given_name_birth	Fornavn(e), herunder mellemnavn(e), på den bruger, som personidentifikationsdataene vedrører, på fødselstidspunktet.
sex	Værdierne skal være én af følgende: 0 = ikke kendt 1 = mand 2 = kvinde 3 = andet 4 = inter 5 = divers 6 = åben 9 = ikke relevant For værdierne 0, 1, 2 og 9 gælder ISO/IEC 5218.
email_address	E-mailadresse på den bruger, som personidentifikationsdataene vedrører [i overensstemmelse med RFC 5322 ([1])].

Dataidentifikator	Definition
`mobile_phone_number`	Mobiltelefonnummer på den bruger, som personidentifikationsdataene vedrører, begyndende med symbolet »+« som internationalt kodepræfiks og herefter landekoden efterfulgt af kun tal

([1]) P. Resnick, ed., »Internet Message Format,« RFC 5322, oktober 2008.

2) Afsnit 2: Sæt af personidentifikationsdata for juridiske personer

Tabel 3:

Obligatoriske personidentifikationsdata for juridiske personer

Dataidentifikator
Nuværende officielle navn
Et entydigt identifikationsnummer, som er tildelt af den afsendende medlemsstat i overensstemmelse med de tekniske specifikationer med henblik på grænseoverskridende identifikation, og som så vidt muligt består over tid.

— Hvis en dataidentifikator ikke er kendt for personen eller ikke på anden måde kan udstedes som en del af personidentifikationsdatasættet, anvender medlemsstaterne i stedet en attributværdi, der passer til situationen.

Tabel 4:

Valgfrie personidentifikationsdata for juridiske personer

Dataidentifikator
Nuværende adresse
Momsregistreringsnummer
Skatteregistreringsnummer
Europæisk unik identifikator omhandlet i Europa-Parlamentets og Rådets direktiv (EU) 2017/1132 ([1])
Identifikator for juridiske enheder (LEI) omhandlet i Kommissionens gennemførelsesforordning (EU) 2022/1860 ([2])
EORI-nummer (registrerings- og identifikationsnummer for økonomiske operatører) omhandlet i Kommissionens gennemførelsesforordning (EU) nr. 1352/2013 ([3])
Punktafgiftsnummeret omhandlet i artikel 2, nr. 12), i Rådets forordning (EU) nr. 389/2012 ([4])

([1]) Europa-Parlamentets og Rådets direktiv (EU) 2017/1132 af 14. juni 2017 om visse aspekter af selskabsret (EUT L 169 af 30.6.2017, s. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Kommissionens gennemførelsesforordning (EU) 2022/1860 af 10. juni 2022 om gennemførelsesbestemmelser tekniske standarder for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og af Rådet for så vidt angår standarder, formater, hyppighed og metoder og ordninger med henblik på rapportering (EUT L 262 af 7.10.2022, s. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Kommissionens gennemførelsesforordning (EU) nr. 1352/2013 af 4. december 2013 om oprettelse af formularer, der er omhandlet i Europa-Parlamentets og Rådets forordning (EU) nr. 608/2013 om toldmyndighedernes håndhævelse af intellektuelle ejendomsrettigheder (EUT L 341 af 18.12.2013, s. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Rådets forordning (EU) nr. 389/2012 af 2. maj 2012 om administrativt samarbejde på punktafgifter og ophævelse af forordning (EF) nr. 2073/2004 (EUT L 121 af 8.5.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3) Afsnit 3: Sæt af metadata om personidentifikationsdata

Tabel 5:

Metadata om personidentifikationsdata

Dataidentifikator	Definition	Anvendelse
`issuing_authority`	Navnet på den administrative myndighed, der har udstedt personidentifikationsdataene, eller alfa-2-landekoden som specificeret i ISO 3166 for den pågældende medlemsstat, hvis en særskilt myndighed ikke har ret til at udstede personidentifikationsdata.	Obligatorisk
`issuing_country`	Alfa-2-landekode som specificeret i ISO 3166-1 for det land eller område, hvor udbyderen af personidentifikationsdataene er etableret.	Obligatorisk
`expiry_date`	Dato (og klokkeslæt, hvis det er muligt), hvor den administrative gyldighedsperiode for personidentifikationsdataene udløber.	Valgfri
`document_number`	Et nummer, som udbyderen af personidentifikationsdata har tildelt de pågældende personidentifikationsdata.	Valgfri
`issuing_jurisdiction`	Landsdelskode for den jurisdiktion, der har udstedt personidentifikationsdataene som specificeret i ISO 3166-2:2020, punkt 8. Den første del af koden skal være den samme som værdien for det udstedende land.	Valgfri
`issuance_date`	Dato og, hvis det er muligt, klokkeslæt hvor den administrative gyldighedsperiode for personidentifikationsdataene startede.	Valgfri

4) Afsnit 4: Kodning af personidentifikationsdataattributter for fysiske personer

— Personidentifikationsdata for fysiske personer skal udstedes i overensstemmelse med de standarder, der er anført i bilag II til gennemførelsesforordning (EU) 2024/2979, punkt 5 (SD-JWT VC-format) og 6 (ISO/IEC-mdoc-format), alt efter hvad der er relevant for elektroniske attesteringer af attributter. Punkt 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3,6.2.4 og 6.2.5 finder ikke anvendelse.

— Kodningen af personidentifikationsdata for fysiske personer skal være i overensstemmelse med de tekniske specifikationer i dette bilags afsnit 4.1 og 4.2.

4.1 Kodning af personidentifikationsdata for fysiske personer i ISO/IEC-mdoc-format

— Attesteringstypen for personidentifikationsdata i ISO/IEC mdoc-format skal være »eu.europa.ec.eudi.pid.1«. Identifikatoren for navnemellemrummet for personidentifikationsdataattributterne i dette bilag skal være »eu.europa.ec.eudi.pid.1«.

— Hvis personidentifikationsdataene omfatter data, for hvilke der ikke er anført dataidentifikatorer i dette bilag, skal disse data defineres inden for et lande- eller regionsspecifikt navnemellemrum for personidentifikationsdata, der bruger det generelle format eu.europa.ec.eudi.pid.[alpha-2-landekode i ISO 3166-1 eller regionskoden i ISO 3166-2], efterfulgt af et valgfrit punkt- og versionsnummer.

— Når det lande- eller regionsspecifikke navnemellemrum anvendes, offentliggøres ordningen herfor, inklusive alle dataidentifikatorer og deres definitioner, anvendelse og kodningsformater, i overensstemmelse med artikel 8 i Kommissionens gennemførelsesforordning (EU) 2025/1569 ([1]).

— Personidentifikationsdataene og disses metadata, jf. dette bilags afsnit 1 og 3, skal indgå i personidentifikationsdataelementerne som omhandlet i specifikationerne for ISO/IEC mdoc-formatet.

— deviceKey-medlemmet i deviceKeyInfo-medlemmet i forekomsten af typen MobileSecurityObject skal indeholde en offentlig nøgle.

— Denne offentlige nøgle skal svare til en privat nøgle, der er lagret i tegnebogsbrugerens sikre kryptografiske tegnebogsanordning (»WSCD«).

— Den beskyttede header i den digitale CB-AdES-signatur, der bruges til at underskrive personidentifikationsdata i ISO/IEC-mdoc-format, skal indeholde headerparametrene x5u og x5t, begge specificeret i RFC 9360 ([2]).

— Den digest-algoritme, der anvendes i headerparameteren x5t, skal være SHA-256.

— Kravene til kodning af personidentifikationsdata i ISO/IEC-mdoc-format fremgår af tabel 6:

Tabel 6:

Krav til kodning af personidentifikationsdata i ISO/IEC-mdoc-format

Dataidentifikator	Attributidentifikator	Kodningsformat
family_name	family_name	tstr
given_name	given_name	tstr
birth_date	birth_date	full-date
birth_place	place_of_birth	place_of_birth
nationality	nationality	nationalities
resident_address	resident_address	tstr
resident_country	resident_country	tstr
resident_state	resident_state	tstr
resident_city	resident_city	tstr
resident_postal_code	resident_postal_code	tstr
resident_street	resident_street	tstr
personal_administrative_number	personal_administrative_number	tstr
portrait	portrait	bstr
family_name_birth	family_name_birth	tstr
given_name_birth	given_name_birth	tstr
sex	sex	uint

([1]) Kommissionens gennemførelsesforordning (EU) 2025/1569 af 29. juli 2025 om fastsættelse af regler for anvendelse 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).

([2]) J. Schaad, »CBOR Object Signing and Encryption (COSE): Header Parameters for Carrying and Referencing X.509 Certificates« (https://datatracker.ietf.org/doc/rfc9360/).

Dataidentifikator	Attributidentifikator	Kodningsformat
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate eller full-date
issuing_authority	issuing_authority	tstr
issuing_country	issuing_country	tstr
document_number	document_number	tstr
issuing_jurisdiction	issuing_jurisdiction	tstr
issuance_date	issuance_date	tdate eller full-date

— I notationen i kodningsformatet for de attributter, der er angivet i tabel 6, skal der anvendes repræsentationstyper som specificeret i RFC 8610 ([3]) med følgende yderligere krav:

a) en tstr skal kodes i UTF-8

b) en tstr skal understøtte det fulde unicode-register

c) en tstr må maksimalt være på 150 tegn

d) der skal kodes en dato som specificeret i RFC 8943 ([4])

e) en full-date skal fortolkes som #6.1004(tstr), hvor tag 1004 er som specificeret i RFC 8943

f) en tdate-attribut skal indeholde en date-time-streng som specificeret i RFC 3339 ([5])

g) en full-date-attribut skal indeholde en full-date-streng som specificeret i RFC 3339, i overensstemmelse med RFC 8943

h) en repræsentation af en dato i attributter må, medmindre andet er angivet:

— ikke benytte brøkdele af sekunder

— ikke benytte lokalforskydning i forhold til UTC, og den tidsforskydning, der er specificeret i RFC 3339, skal sættes til »Z«

i) et heltal med hovedtyperne 0 og 1 skal være så lille som muligt, som angivet i RFC 8949 ([6]), afsnit 4.2

j) en place_of_birth skal indeholde mindst et af følgende nøgleværdipar: »country«, »region« eller »locality«

k) angivelsen af længden i en bstr, tstr, et array eller et kort skal være så kort som muligt, som specificeret i RFC 8949, afsnit 4.2

([3]) C. Vigano and H. Birkholz, »Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures«, RFC 8610, juni 2019.
([4]) M. Jones, A. Nadalin and J. Richter, »Concise Binary Object Representation (CBOR) Tags for Date«, RFC 8943, november 2020.
([5]) G. Klyne and C. Newman, »Date and Time on the Internet: Timestamps,« RFC 3339, juli 2002.
([6]) C. Bormann and P. Hoffman, »Concise Binary Object Representation (CBOR),« RFC 8949, december 2020.

l) attributten nationality skal kodes som et array med alpha-2-landekoder som specificeret i ISO 3166-1. Hvis der anvendes CDDL-notation som specificeret i RFC 8610, skal kodningen af denne attribut være:

— nationalities = [+ CountryCode]

— CountryCode = tstr; alpha-2-landekode specificeret i ISO 3166-1

— hvis en tegnebogsbruger, som personidentifikationsdataene vedrører, har flere nationaliteter, og udbyderen af personidentifikationsdata attesterer disse flere nationaliteter, kan udbyderen af personidentifikationsdata medtage alle nationaliteterne i personidentifikationsdataene

— attributten place_of_birth skal kodes som en type place_of_birth. Hvis der anvendes CDDL-notation som specificeret i RFC 8610, skal kodningen af denne attribut være:

place_of_birth =

{

? »country«: tstr; en enkelt alpha-2-landekode som specificeret i ISO 3166-1

? »region«: tstr navnet på en stat, en provins, et distrikt eller et lokalområde

? »locality«: tstr; navnet på en kommune eller by

}

4.2 Krav til kodning af personidentifikationsdata i SD-JWT VC-format

— Personidentifikationsdataene og disses metadata som specificeret i dette afsnit skal indgå i personidentifikationsdata som claims (påstande) som omhandlet i ISO/IEC mdoc-formatet.

— Alle claims i de udstedte personidentifikationsdata, jf. foregående led, skal selektivt kunne videregives individuelt, bortset fra claims, der er defineret som ikkeselektivt videregivelige i SD-JWT VC-format.

— Kodningen af claim-navne, der er offentlige navne, fremgår af tabel 7.

— Kodningen af claim-navne, der er specifikke for personidentifikationsdata, fremgår af tabel 8.

— En JSON-streng, der bruges i personidentifikationsdata kodet i SD-JWT VC, skal kodes i UTF-8 og understøtte det fulde unicode-register, medmindre andet udtrykkeligt fremgår af tabel 8 nedenfor eller henvisningerne deri.

— JWT-claimene nbf og exp som defineret i RFC 7519 ([7]) skal bruges til at udtrykke den tekniske gyldighedsperiode for personidentifikationsdata, der er i overensstemmelse med SD-JWT VC-formatet.

([7]) J. Jones, et al., »JSON Web Token (JWT),« RFC 7519, maj 2015.

— Personidentifikationsdata skal indeholde claimet cnf som defineret i RFC 7800 ([8]), som skal være en offentlig nøgle, der er genereret fra en privat nøgle, der er lagret i tegnebogsbrugerens tegnebogsenheds WSCD.

— Den beskyttede header i den digitale signatur, der bruges til at underskrive personidentifikationsdata i SD-JWT VC-format, skal indeholde headerparametrene x5u og x5t#S256 , som er specificeret i RFC 7515 ([9]).

Tabel 7:

Krav til kodning af personidentifikationsdata i SD-JWT VC-format ved hjælp af offentlige navne

Dataidentifikator	Attributidentifikator	Kodningsformat
`family_name`	`family_name`	streng
`given_name`	`given_name`	streng
`birth_date`	`birthdate`	streng, ISO 8601-1, format YYYY-MM-DD
`birth_place`	`place_of_birth`	JSON-struktur
`nationality`	`nationalities`	streng-array
`resident_address`	`address.formatted`	streng
`resident_country`	`address.country`	streng
`resident_state`	`address.region`	streng
`resident_city`	`address.locality`	streng
`resident_postal_code`	`address.postal_code`	streng
`resident_street`	`address.street_address`	streng
`family_name_birth`	`birth_family_name`	streng
`given_name_birth`	`birth_given_name`	streng
`email_address`	`email`	streng
`mobile_phone_number`	`phone_number`	streng
`portrait`	`picture`	streng; data-URL, der indeholder et base64-kodet billede i JPEG-format

([8]) M. Jones, et al., »Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs),« RFC 7800, april 2016.
([9]) M. Jones, et al., »JSON Web Signature (JWS),« RFC 7515, maj 2015.

Tabel 8:

Krav til kodning af personidentifikationsdata i SD-JWT VC-format ved hjælp af private navne

Dataidentifikator	Attributidentifikator	Kodningsformat
`expiry_date`	`date_of_expiry`	streng, ISO 8601-1, format YYYY-MM-DD
`issuance_date`	`date_of_issuance`	streng, ISO 8601-1, format YYYY-MM-DD
`personal_administrative_number`	`personal_administrative_number`	streng
`sex`	`sex`	tal
`issuing_authority`	`issuing_authority`	streng
`issuing_country`	`issuing_country`	streng
`document_number`	`document_number`	streng
`issuing_jurisdiction`	`issuing_jurisdiction`	streng

— Basistypen af personidentifikationsdata skal være »urn:eudi:pid:1« og indeholdt i claimet vct. Alle personidentifikationsdata skal benytte typer i navnemellemrummet »urn:eudi:pid:«.

— Hvis personidentifikationsdata omfatter attributter, der ikke er specificeret i dette bilag, skal disse attributter defineres i en lande- eller regionsspecifik type.

— Når den lande- eller regionsspecifikke type anvendes, defineres ordningen herfor, inklusive alle dataidentifikatorer og deres definitioner, anvendelse og kodningsformater, i en ordning, der offentliggøres i overensstemmelse med artikel 8 i gennemførelsesforordning (EU) 2025/1569.

5) Afsnit 5: Nærmere oplysninger om tillidsinfrastruktur

Den liste over udbydere af personidentifikationsdata, som Kommissionen stiller til rådighed i overensstemmelse med gennemførelsesforordning (EU) 2024/2980, skal gøre det muligt at autentificere personidentifikationsdata.«

BILAG II

»*BILAG Ia*

Kryptografiske mekanismer, jf. artikel 5a

Den Europæiske Cybersikkerhedscertificeringsgruppe, undergruppen om kryptografi: »Agreed Cryptographic Mechanisms«, offentliggjort af Den Europæiske Unions Agentur for Cybersikkerhed (»ENISA«) ([1]).«

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_da.

BILAG III

»BILAG Ib

Tekniske specifikationer for tegnebogsenhedsattesteringer, jf. artikel 6, stk. 2a

1) En tegnebogsenhedsattestering skal omfatte en eller flere tegnebogsforekomstattesteringer og en eller flere nøgleattesteringer.

2) Tegnebogsforekomstattesteringen og nøgleattesteringerne skal opfylde følgende krav:

a) Formelle krav

— FR-WIA-1: En tegnebogsforekomstattestering skal være en JSON Web Token (JWT) som specificeret i RFC 7519 ([1]), underskrevet eller forseglet af tegnebogsudbyderen ved hjælp af en kompakt JAdES-B-basissignatur.

— FR-WIA-1.1: En tegnebogsforekomstattestering skal være en tegnebogsattestering som specificeret i tillæg E til OpenID for Verifiable Credential Issuance v1.0 ([2]) (»OID4VCI«) og forlænget som angivet i C-WIA-1 og C-WIA-2 nedenfor.

— FR-KA-1: En nøgleattestering skal være en JWT som specificeret i RFC 7519, underskrevet eller forseglet af tegnebogsudbyderen ved hjælp af en kompakt JAdES-B-basissignatur.

— FR_KA_1.1: En nøgleattestering skal være en nøgleattestering som specificeret i tillæg D til OID4VCI og forlænget som angivet i C_KA-1 og C_KA-2 nedenfor.

b) Transportkrav

— TR-WIA-1: En tegnebogsenhed skal anvende en tegnebogsforekomstattestering under udstedelsen af personidentifikationsdata, kvalificerede eller ikkekvalificererede elektroniske attesteringer af attributter eller elektroniske attesteringer af attributter, der leveres af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde.

— TR-WIA-2: En tegnebogsudbyder skal verificere tegnebogsforekomstens integritet og underskrive eller forsegle tegnebogsforekomstattesteringen.

— TR-WIA-2.1: Når en tegnebogsudbyder udsteder en tegnebogsforekomstattestering, skal forskellen mellem det tidspunkt, hvor tegnebogsudbyderen verificerede integriteten af tegnebogsforekomsten, og det tidspunkt, som angives i headerparameteren »exp« for den udstedte tegnebogsforekomstattestering, være mindre end 24 timer.

— TR-WIA-2.2: Tegnebogsudbyderen sikrer, at en tegnebogsenhed indeholder tegnebogsforekomstattesteringer i det omfang, det er nødvendigt for udstedelse af personidentifikationsdata og elektroniske attesteringer af attributter.

— TR-WIA-3: Ved udstedelse skal en tegnebogsenhed sende en tegnebogsforekomstattestering til autorisationsserveren i PAR'en (Pushed Authorisation Request) og tokenanmodningen som specificeret i OID4VCI.

— TR-WIA-3.1: En tegnebogsenhed skal sende tegnebogsforekomstattesteringen sammen med et Proof-of-Possession (»PoP«) som specificeret i tillæg E til OID4VCI.

— TR-WIA-3.2: En tegnebogsenhed må kun sende den samme tegnebogsforekomstattestering til én autorisationsserver.

([1]) RFC 7519: JSON Web Token (JWT), maj 2015.
([2]) OpenID for Verifiable Credential Issuance v1.0, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

— TR-WIA-3.2.1: Hvis en tegnebogsudbyder bruger muligheden »per-issuer reuse« i henhold til R_WIA_1, må en tegnebogsenhed sende en tegnebogsforekomstattestering til den samme autorisationsserver flere gange.

— TR-WIA-3.2,2: Hvis en tegnebogsudbyder ikke bruger muligheden »per-issuer reuse«, må en tegnebogsenhed anvende en tegnebogsforekomstattestering i højst én udstedelsesproces.

— TR-WIA-4: Når en autorisationsserver modtager en tegnebogsforekomstattestering, skal den verificere tegnebogsforekomstattesteringens signatur med den offentlige nøgle i signeringscertifikatet, som er indeholdt i parameteren »x5c« i JOSE-headeren i tegnebogsforekomstattesteringen.

— TR-WIA-4.1: Autorisationsserveren skal også verificere, at dette signeringscertifikat kan verificeres med et tillidsanker på listen over tegnebogsudbydere, jf. artikel 5 i gennemførelsesforordning (EU) 2024/2980, eventuelt ved hjælp af midlertidige certifikater indeholdt i parameteren x5c.

— TR-WIA-4.2: Autorisationsserveren skal verificere, at tegnebogsforekomstattesteringen ikke er udløbet.

— TR-WIA-4.3: Autoriseringsserveren skal verificere signaturen i PoP'en med den offentlige nøgle i claimet »cnf«.

— TR_KA-1: En tegnebogsenhed skal anvende en nøgleattestering under udstedelsen af personidentifikationsdata og under udstedelsen af anordningsbundne kvalificerede eller ikkekvalificererede elektroniske attesteringer af attributter eller elektroniske attesteringer af attributter, der leveres af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde.

— TR_KA-1.1: En tegnebogsenhed må ikke anvende en nøgleattestering under udstedelsen af ikkeanordningsbundne kvalificerede eller ikkekvalificererede elektroniske attesteringer af attributter eller elektroniske attesteringer af attributter, der leveres af eller på vegne af en offentlig myndighed med ansvar for en autentisk kilde.

— TR_KA-2: En tegnebogsudbyder skal levere en tegnebogsenhed med forskellige nøgleattesteringer til tegnebogsenhedens WSCD og til hver at dens nøglelagre.

— TR_KA-2.1: Tegnebogsudbyderen skal underskrive eller forsegle en nøgleattestering, efter at tegnebogsudbyderen har verificeret, at de nøgler, der er attesteret i nøgleattesteringen, er lagret i tegnebogsenhedens WSCD eller nøglelager som beskrevet i nøgleattesteringen.

— TR_KA-2.2: En nøgleattestering skal indeholde mindst én attesteret offentlig nøgle. Antallet af nøgler i den nøgleattestering, der er sendt til en legitimationsudsteder, bør ikke overstige den maksimale batchstørrelse, som legitimationsudstederen har specificeret i sine legitimationsudstedermetadata; se ETSI TS 119 472-3 ([3]), parameteren »credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size«.

— TR_KA-2.3: En tegnebogsudbyder må medtage en offentlig nøgle (som svarer til en privat nøgle lagret i tegnebogsenhedens WSCD eller nøglelager) i højst én nøgleattestering.

— TR_KA-2.4: En tegnebogsenhed må anvende en nøgleattestering i højst én legitimationsudstedelses- eller -genudstedelsesproces.

— TR_KA-2.5: En tegnebogsudbyder skal sikre, at en tegnebogsenhed har nøgleattesteringer i det omfang, det er nødvendigt for udstedelse af personidentifikationsdata og anordningsbundne elektroniske attesteringer af attributter.

([3]) ETSI, »Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 3: JAdES levels and baseline profiles«, ETSI TS 119 472-3, V1.1.1, marts 2026.

— TR_KA-3: Hvis det er nødvendigt under udstedelsen, skal en tegnebogsenhed indeholde en nøgleattestering i feltet »proofs« i en legitimationsanmodning til legitimationsudstederen som specificeret i OID4VCI i et bevis af enten typen »jwt« eller typen »attestation«.

— TR_KA_3.1: Når en tegnebogsenhed indeholder en nøgleattestering i elementet »jwt«, skal den underskrive eller forsegle nøgleattesteringen ved hjælp af den private nøgle, der svarer til den offentlige nøgle i indeks 0 i arrayet »attested_keys« i objektet »key_attestation«.

— TR_KA-4: Når en legitimationsudsteder udsteder anordningsbunden legitimation, skal udstederen i parameteren »proof_types_supported« i sine legitimationsudstedermetadata som specificeret i afsnit 12.2.4 i OID4VCI angive, at den understøtter både »jwt« og bevistypen »attestation« for nøgleattesteringer, der skal indeholde objektet »key_attestations_required«.

— TR_KA-4.1: Når en legitimationsudsteder udsteder ikkeanordningsbunden legitimation, skal udstederen udelade parametrene »proof_types_supported« og »cryptographic_binding_methods_supported« i legitimationsudstedermetadataene.

— TR_KA-5: Når en legitimationsudsteder modtager en nøgleattestering i bevistypen »jwt« eller »attestation«, skal udstederen verificere nøgleattesteringens signatur med den offentlige nøgle i signeringscertifikatet, der er indeholdt i parameteren »x5c« i headeren JOSE i nøgleattesteringen, og om signeringscertifikatet kan verificeres med et tillidsanker på listen over tegnebogsudbydere, jf. artikel 5 i gennemførelsesforordning (EU) 2024/2980, eventuelt ved hjælp af midlertidige certifikater indeholdt i parameteren »x5c«.

— TR_KA-6: Når en legitimationsudsteder modtager en nøgleattestering i bevistypen »jwt«, skal udstederen verificere signatur i elementet »jwt« med den nøgle i indeks 0 i arrayet »attested_keys« i objektet »key_attestation«, som er indeholdt i elementet »jwt«.

— TR_KA-6.1: Legitimationsudstederen skal verificere, at feltet »nonce« i elementet »jwt« indeholder en gyldig c_nonce fra nonce_endpoint som specificeret i OID4VCI.

— TR_KA-7: Når en legitimationsudsteder modtager en nøgleattestering i bevistypen »attestation«, skal udstederen verificere, at objektet »key_attestation« indeholder en gyldig c_nonce fra nonce_endpoint.

— TR_KA-8: En udbyder af personidentifikationsdata skal sikre, at personidentifikationsdataene er bundet til en offentlig nøgle, der stammer fra en nøgleattestering, hvori en WSCD er nævnt.

c) Indholdskrav

— C_WIA-1: En tegnebogsforekomstattestering skal indeholde følgende:

— claimet »wallet_name« som specificeret i tillæg E til OID4VCI, hvor dets værdi er den identifikator for tegnebogsløsningen, der findes på listen over tegnebogsudbydere, jf. artikel 5 i gennemførelsesforordning (EU) 2024/2980.

— et »wallet_version«-claim ([4]), som er en streng, hvis værdi er versionen af tegnebogsløsningen.

— et »wallet_solution_certification_information«-claim, som er et JSON-objekt, der indeholder information om det overensstemmelsesvurderingsorgan, der har certificeret tegnebogsløsningen, certificeringsnummeret, hvis det er relevant, og andre relevante oplysninger med hensyn til certificering.

([4]) Dette claim er defineret i denne gennemførelsesforordning, da den ikke er en del af OID4VCI-specifikationen.

— et »client_status«-claim, som indeholder to underfelter:

— »status«: en henvisning til statuslisten som specificeret i tillæg E til OID4VCI, der repræsenterer tilbagekaldelsesstatus for tegnebogsforekomsten. Se afsnit (e) nedenfor for nærmere oplysninger

— »exp«: NumericDate som specificeret i RFC 7519, som angiver, indtil hvilket tidspunkt tegnebogsudbyderen opretholder tilbagekaldelsesstatus i det statuslisteindeks, der henvises til i »status«.

— claimet »exp« som specificeret i tillæg E til OID4VCI.

— BEMÆRK: Claimet »client_status.status« i en tegnebogsforekomstattestering repræsenterer tilbagekaldelsesstatus for tegnebogsforekomsten og ikke tilbagekaldelsesstatus for selve attesteringen. Som beskrevet i R_WIA-1 nedenfor kan en tegnebogsudbyder beslutte at målrette hver tegnebogsforekomstattestering en specifik autorisationsserver, fordi alle attesteringer, der sendes til den pågældende server, indeholder den samme indeksværdi i indtastningen »client_status.status«.

— BEMÆRK: Værdien »idx« i claimet »status« kan bruges som en (parvis) entydig identifikator for tegnebogsforekomsten og tegnebogsenheden.

— C_WIA-2: En tegnebogsforekomstattestering bør også indeholde claimet »wallet_link« som specificeret i tillæg E til OID4VCI, og værdien af dette claim skal være en URI, hvor yderligere oplysninger om tegnebogsløsningen findes.

— C_WIA-3: En autorisationsserver må ikke fortolke parameteren »exp« på det øverste niveau af en tegnebogsforekomstattestering som afslutningen af perioden for opretholdelse af tilbagekaldelsen af tegnebogsforekomsten.

— BEMÆRK: Parameteren »exp« på det øverste niveau af en tegnebogsforekomstattestering angiver, hvornår selve attesteringen udløber.

— C_KA-1: En nøgleattestering skal indeholde:

— claimene »key_storage« og »user_authentication« som specificeret i tillæg D til OID4VCI.

— attributterne »key_storage« og »user_authentication« skal have værdien »iso_18045_high« , når der nævnes en WSCD i en nøgleattestering.

— claimet »certification« som specificeret i tillæg D til OID4VCI, som indeholder en URL, hvor der findes oplysninger om den certificering, der er opnået gennem WSCD'en eller nøglelageret, typisk en ordning såsom Common Criteria eller GlobalPlatform, de vurderede krav, som f.eks. den gældende beskyttelsesprofil, og vurderingsniveauet.

— Det skal være muligt ud fra disse oplysninger at bestemme, om nøglelageret er en WSCD.

— et »key_storage_status«-claim, som indeholder to underfelter:

— »status«: en henvisning til statuslisten som specificeret i tillæg D.1 til OID4VCI. Værdien repræsenterer enten tilbagekaldelsesstatus for den type WSCD eller nøglelager, der er anvendt til at lagre de attesterede nøgler, eller – ved indeksmuligheden per-key-attestation – tilbagekaldelsesstatus for en individuel tegnebogsenheds WSCD eller nøglelager. Se R_KA_1 nedenfor for de tilgængelige indekstildelingsmuligheder

— »exp«: NumericDate som specificeret i RFC 7519, som angiver, indtil hvilket tidspunkt tegnebogsudbyderen opretholder tilbagekaldelsesstatus i det statuslisteindeks, der henvises til i »status«.

— claimet »exp« som specificeret i tillæg D til OID4VCI.

— BEMÆRKNING til værdien »idx« i claimet »key_storage_status.status« i en nøgleattestering: Når tegnebogsudbyderen anvender muligheden »type-shared index« (se R_KA_1 nedenfor), deler alle nøgleattesteringer for samme type WSCD eller nøglelager det samme statuslisteindeks. Derfor er »idx«-værdien ikke entydig for hver tegnebogsenhed. Når tegnebogsudbyderen derimod anvender muligheden »per-key-attestation index«, er »idx«-værdien entydig for tegnebogsenheden (eller parvis entydig for hver legitimationsudsteder). I alle tilfælde må en legitimationsudsteder dog ikke bruge »idx«-værdien i en nøgleattestering som en tegnebogsenhedsidentifikator, men skal i stedet bruge »idx«-værdien i en tegnebogsforekomstattestering.

— C_KA-2: Når en nøgleattestering sendes i bevistypen »attestation«, skal den også indeholde en gyldig c_nonce som specificeret i tillæg F.3 til OID4VCI.

— C_KA-3: En legitimationsudsteder må ikke fortolke parameteren »exp« på det øverste niveau af en nøgleattestering som afslutningen af perioden for opretholdelse af tilbagekaldelsen af WSCD'en eller nøglelageret.

— BEMÆRK: Parameteren »exp« på det øverste niveau af en nøgleattestering angiver, hvornår selve nøgleattesteringen udløber.

d) Livscykluskrav

— I dette bilag specificeres følgende parametre for legitimationsudstedermetadata:

— »preferred_client_status_period«: VALGFRI. Et heltal, der angiver den foretrukne resterende periode for opretholdelse af status for den tegnebogsforekomstattestering, som tegnebogsenheden skal vise under udstedelsen, i sekunder. Den resterende periode for opretholdelse af status defineres som værdien af »client_status.exp« i attesteringen minus tidspunktet for modtagelse af attesteringen.

— »preferred_key_storage_status_period«: VALGFRI. Et heltal, der angiver den foretrukne resterende periode for opretholdelse af status for den nøgleattestering, som tegnebogsenheden skal vise under udstedelsen, i sekunder. Den resterende periode for opretholdelse af status defineres som værdien »key_storage_status.exp« i attesteringen minus tidspunktet for modtagelse af attesteringen.

— LC_WIA-1: En autorisationsserver kan kommunikere sine præferencer for den resterende periode for opretholdelse af status i tegnebogsforekomstattesteringer ved at medtage metadataparameteren »preferred_client_status_period« i slutpunktet for legitimationsudstedermetadata som specificeret i afsnit 12.2.2 i OID4VCI.

— LC_WIA-1.1: Dette felt skal placeres i det øverste niveau af legitimationsudstedermetadatene.

— LC_WIA_2: En autorisationsserver må ikke fortolke parameteren »exp« på det øverste niveau af en tegnebogsforekomstattestering som afslutningen af perioden for opretholdelse af tilbagekaldelsen af tegnebogsforekomsten.

— LC_WIA_3: Når en tegnebogsudbyder underskriver eller forsegler en tegnebogsforekomstattestering, skal tilbagekaldelsesstatus for den pågældende tegnebogsforekomst opretholdes, indtil »wallet_instance_-status.exp« som angivet i tegnebogsforekomstattesteringen er udløbet.

— LC_KA-1: Når en nøgleattestering er nødvendig, kan en legitimationsudsteder kommunikere sine præferencer for den resterende periode for opretholdelse af status i nøgleattesteringer ved at medtage den ovenfor angivne metadataparameter »preferred_key_storage_status_period« i slutpunktet for legitimationsudstedermetadata som specificeret i afsnit 12.2.2 i OID4VCI.

— LC_KA-1.1: Dette felt skal placeres i objektet »key_attestations_required« som specificeret i afsnit 12.2.4 i OID4VCI.

— LC_KA-2: En tegnebogsudbyder skal vælge den tekniske gyldighedsperiode for de nøgleattesteringer, denne udsteder.

— LC_KA-3: Når en tegnebogsudbyder underskriver eller forsegler en nøgleattestering, skal tilbagekaldelsesstatus for den pågældende WSCD eller det pågældende nøglelager opretholdes, indtil »key_storage_status.exp« som angivet i nøgleattesteringen er udløbet.

— LC_GEN-1: En tegnebogsudbyder skal sikre, at en tegnebogsenhed altid kan vise tegnebogsenhedsattesteringer og nøgleattesteringer, hvis henholdsvis »client_status.exp« og »key_storage_status.exp« ligger mindst 31 dage ude i fremtiden på tidspunktet for fremvisningen for en autorisationsserver eller en legitimationsudsteder.

— *BEMÆRK*: Dette garanterer, at udbydere af personidentifikationsdata kan benytte tilbagekaldelseskæder uden at være tvunget til at udstede kortlivede personidentifikationsdata.

— LC_GEN-2: En tegnebogsudbyder skal sikre, at en tegnebogsenhed henter legitimationsudstederdataene under udstedelsen.

  — LC_GEN_2.1: Hvis disse metadata indeholder et »preferred_key_storage_status_period«-felt, skal tegnebogsenheden sende en nøgleattestering, hvor værdien (»key_storage_status.exp« – aktuelt tidspunkt) – »preferred_key_storage_status_period« er så lille som muligt uden at være negativ. Hvis en sådan nøgleattestering ikke er tilgængelig for tegnebogsenheden, skal den indhente en ny nøgleattestering fra tegnebogsudbyderen, som opfylder »key_storage_status.exp« – aktuelt tidspunkt ≥ »preferred_key_storage_status_period«.

  — LC_GEN_2.2: Hvis disse metadata indeholder et »preferred_client_status_period«-felt, skal tegnebogsenheden sende en tegnebogsforekomstattestering, hvor værdien (»client_status.exp« – aktuelt tidspunkt) – »preferred_client_status_period« er så lille som muligt uden at være negativ. Hvis en sådan tegnebogsforekomstattestering ikke er tilgængelig for tegnebogsenheden, skal den anmode om en ny tegnebogsforekomstattestering fra tegnebogsudbyderen, som opfylder »client_status.exp« – aktuelt tidspunkt ≥ »preferred_client_status_period«.

— LC_GEN-3: Den tekniske gyldighedsperiode for personidentifikationsdata skal ende før både »client_status.exp« i tegnebogsforekomstattesteringen og »key_storage_status.exp« i nøgleattesteringen, som sendes til udbyderen af personidentifikationsdata i udstedelsesprocessen.

— LC_GEN-4: En udbyder af personidentifikationsdata med en teknisk gyldighedsperiode på mere end 24 timer skal kontrollere tilbagekaldelsesstatus for både den tegnebogsforekomstattestering og den nøgleattestering, der modtages under udstedelsen, mindst hver 24. time i løbet af den tekniske gyldighedsperiode for personidentifikationsdataene. Hvis en af disse tilbagekaldes, skal udbyderen tilbagekalde personidentifikationsdataene.

e) Tilbagekaldelseskrav

— R_GEN-1: En tegnebogsudbyder skal anvende tokenstatuslister (specificeret i IETF Token Status List) som tilbagekaldelsesmekanisme for både nøgleattesteringer og tegnebogsforekomstattesteringer og nøgleattesteringer som specificeret i henholdsvis tillæg D og E til OID4VCI.

— BEMÆRK: For at forbedre skalerbarheden af statuslisterne kan en tegnebogsudbyder gøre brug af følgende optimeringer:

  — Opdele statuslisten i flere stykker, hvis tegnebogsudbyderne har et betydeligt antal brugere og udstedte attesteringer. Der findes mange chunking-strategier, f.eks. ud fra en fast størrelse eller efter tidsperiode. Strategien for opdeling i stykker er op til tegnebogsudbyderen. Der kan blandt andet tages hensyn til en statuslistes størrelse med henblik på download og brugerens privatliv.

  — Benytte flere statuslister.

  — Komprimere en statusliste for at reducere dens størrelse.

— R_WIA-1: En tegnebogsudbyder kan tildele samme værdi til claimet »idx« i claimet »client_status.status« i alle tegnebogsforekomstattesteringer, som en given tegnebogsenhed fremviser for den samme autorisationsserver. Dette kaldes for »per-issuer reuse«-muligheden. Hvis denne mulighed anvendes, gælder følgende:

  — R_WIA-1.1: Tegnebogsenheden skal huske, hvilken indeksværdi den har anvendt for hver autorisationsserver, den tidligere har interageret med, og skal anmode om en tegnebogsforekomstattestering med den samme indeksværdi, når den interagerer med den samme autorisationsserver igen.

  — R_WIA-1.2: Når en tegnebogsudbyder modtager en anmodning om en tegnebogsforekomstattestering med en specifik indeksværdi, skal udbyderen kontrollere, om den anmodende tegnebogsenhed tidligere har modtaget denne indeksværdi, inden der udstedes en ny tegnebogsforekomstattestering med denne indeksværdi.

  — R_WIA-1.3: Tegnebogsenheden må ikke genbruge den samme indeksværdi i interaktioner med forskellige autorisationsservere.

— BEMÆRK: Hvis muligheden »per-issuer reuse« anvendes, vil tegnebogsudbyderen kunne fastslå, hvor mange autorisationsservere en tegnebogsenhed har interageret med, og hvor ofte den interagerer med hver enkelt.

— R_WIA-2: En tegnebogsudbyder skal i sin databeskyttelseserklæring dokumentere, om udbyderen bruger muligheden »per-issuer reuse« til tilbagekaldelse af tegnebogsforekomster.

— R_WIA-3: Hvis en tegnebogsudbyder ikke bruger muligheden »per-issuer reuse«, skal udbyderen tildele en ny, ikkelinkbar indeksværdi til hver tegnebogsforekomstattestering, som denne udsteder.

— R_WIA-4: Når en tegnebogsenhed skal tilbagekaldes, skal tegnebogsudbyderen tilbagekalde indeksværdierne i claimet »client_status.status« i alle tegnebogsforekomstattesteringer knyttet til den pågældende tegnebogsenhed.

— R_WIA-5: Når en tegnebogsudbyder fastsætter størrelsen på sine statuslister for tegnebogsforekomstattesteringer, skal udbyderen tage hensyn til anvendelsesomfanget og den underliggende arkitektur og sikre, at de er tilstrækkeligt store til at forhindre korrelation og beskytte brugernes privatliv. Når det er muligt, skal en statusliste som minimum omfatte 10 000 attesteringer.

— R_KA_1: En tegnebogsudbyder skal vælge én af følgende indekstildelingsmuligheder for claimet »key_storage_status.status« i en nøgleattestering:

  — Mulighed 1, kaldet »type-shared index«, hvor alle nøgleattesteringer, der attesterer nøgler lagret i samme type WSCD eller nøglelager, har den samme indeksværdi i »key_storage_status.status«.

  — Mulighed 2, kaldet »per-key-attestion index«, hvor en nøgleattestering, der attesterer nøgler lagret i en individuel WSCD eller et individuelt nøglelager, har en (parvis) entydig indeksværdi i »key_storage_status.status«.

— BEMÆRK: Hvis en tegnebogsudbyder bruger mulighed 1, vil en enkelt tilbagekaldelseshandling ugyldiggøre alle nøgleattesteringer af den berørte type på tværs af alle tegnebogsenheder. Fordi alle nøgleattesteringer for den samme type WSCD eller nøglelager deler et fælles statuslisteindeks, afspejler antallet af indtastninger på en statusliste for nøgleattesteringer desuden antallet af WSCD- eller nøglelagertyper, der understøttes af tegnebogsudbyderen, og ikke antallet af tegnebogsenheder i brug. De databeskyttelseshensyn, der ligger til grund for minimumsstørrelsen for statuslister for tegnebogsforekomster finder derfor ikke anvendelse på statuslister for nøgleattesteringer som omhandlet i mulighed 1, hvis tilstrækkeligt mange tegnebogsenheder anvender den samme type WSCD eller nøglelager.

— BEMÆRK: Hvis en tegnebogsudbyder bruger mulighed 2, repræsenterer hvert indeks tilbagekaldelsesstatus for den specifikke WSCD eller det specifikke nøglelager, der er attesteret i den pågældende nøgleattestering.

— BEMÆRK: Hvis en tegnebogsudbyder bruger mulighed 2, kan en specifik WSCD eller et specifikt nøglelager også tilbagekaldes på brugerens anmodning.

— R_KA-2: Hvis en tegnebogsudbyder bruger mulighed 2, kan udbyderen frit vælge at bruge muligheden »per-issuer reuse« som beskrevet i R_WIA-1. Hvis tegnebogsudbyderen bruger denne mulighed, finder kravene R_WIA-1 - R_WIA-3 tilsvarende anvendelse.

— R_KA-3: Hvis en tegnebogsudbyder bruger mulighed 2, skal udbyderen ved fastlæggelsen af størrelsen på sine statuslister for nøgleattesteringer tage hensyn til anvendelsesomfanget og den underliggende arkitektur og sikre, at listerne er tilstrækkeligt store til at forhindre korrelation og beskytte brugernes privatliv. Når det er muligt, skal en statusliste som minimum omfatte 10 000 nøgleattesteringer.

— R_KA-4: Hvis en tegnebogsudbyder bruger mulighed 1 (type-shared index), må udbyderen kun tilbagekalde en »key_storage_status.status«-indtastning, hvis typen af WSCD eller nøglelager har en sikkerhedssvaghed.

f) Krav vedrørende signaturalgoritmer

— SA-1: Ved underskrivelse af tegnebogsforekomstattesteringer, nøgleattesteringer, tilhørende proof-of-possessions og tokenstatuslister skal én af følgende algoritmer anvendes:

— ES256 (ECDSA med SHA-256 og P-256)

— ES384 (ECDSA med SHA-384 og P-384)

— ES512 (ECDSA med SHA-512 og P-521)

— SA-2: En tegnebogsudbyder skal vælge, hvilken af de i SA-1 nævnte algoritmer udbyderen vil anvende.

— SA-3: En autorisationsserver eller legitimationsudsteder (som specificeret i OID4VCI) skal understøtte alle de i SA-1 nævnte algoritmer.«

BILAG IV

»*BILAG II*

Liste over standarder, jf. artikel 8

De tekniske specifikationer i punkt 2-6 i ETSI TS 119 472-1 V1.2.1 (2026-02) finder anvendelse. De læses med følgende tilpasninger:

1) 2.1 Normative references

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): »Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures«.

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): »Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles; Part 6: Certificate profile requirements for PID, Wallet, EAA, QEAA, and PSBEAA providers«.

— [25] IETF Token Status List (TSL), draft-ietf-oauth-status-list-20: »Token Status List«, 20 April 2026.

2) 4.2.11.1 General requirements

— EAA-4.2.11.1-06: When a status element is used for person identification data, qualified electronic attestations of attributes, or electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source, it shall only indicate whether the attestation is revoked or not revoked and shall not support any other status values, such as suspension.

— EAA-4.2.11.1-06.1: Where an attestation is revoked, it shall be permanently revoked.

3) 4.2.13 EAA short-lived

— EAA-4.2.13-03: Where short-lived electronic attestations of attributes with a validity period of 24 hours or less are issued, revocation shall not be required.

4) 4.6.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA)

— PuB-EAA-4.6.2-03: void.

— Pub-EAA-4.6.2-04: void.

— PuB-EAA-4.6.3-03: The PuB-EAA digital signature should contain the qualified certificate supporting the PuB-EAA digital signature.

— PuB-EAA-4.6.3-04: The qualified certificate supporting the PuB-EAA digital signature shall meet the requirements of clause 8 of ETSI TS 119 412-6 v1.1.1 and shall contain the QcType qcStatement as defined in ETSI EN 319 412-5 v2.5.1, with the value id-etsi-qct-eidaspsbeaa defined as follows:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } -- Certificate referred to in Art.45f(1)(b) supporting the qualified electronic signature or qualified electronic seal of the public sector body referred to in Article 3, point (46) of Regulation (EU) No 910/2014.

5) 5.2.10.1 General requirements

— EAA-5.2.10.1-04: void.

— EAA-5.2.10.1-05: void.

— EAA-5.2.10.1-06: The status member may contain the status_list member as specified in clause 6.2 of IETF draft-ietf-oauth-status-list-20 [25].

— EAA-5.2.10.1-07: void.

— EAA-5.2.10.1-08: void.

— EAA-5.2.10.1-09: void.

— EAA-5.2.10.1-10: void.

— EAA-5.2.10.1-11: void.

— EAA-5.2.10.1-12: void.

6) 6.2.10.1 General requirements

— EAA-6.2.10.1-01: When an electronic attestation of attributes compliant with ISO/IEC mdoc uses the attestation status list mechanism as set out in EAA-6.2.10.1-02.2 or the attestation revocation list mechanism as set out in EAA-6.2.10.1-02.3, its Mobile Security Object (MSO) shall contain the status structure, as specified in EAA-6.2.10.1-17, which contains MSO revocation information.

— EAA-6.2.10.1-01.1: When implementing the identifier list mechanism, the status element shall contain the identifier_list element as set out in EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: When implementing the status list mechanism, the status element shall contain the status_list element as set out in EAA-6.2.10.1-13.

— *NOTE*:

  — The status structure contains a reference to an MSO revocation list.

  — The MSO revocation list is a COSE_Sign1 structure that indicates whether a particular MSO is revoked or not.

  — The status structure contains all the information necessary for the wallet-relying party to determine whether the MSO revocation list is authentic.

— EAA-6.2.10.1-02: The provider of person identification data, the provider of qualified electronic attestations of attributes or the provider of electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source shall use one of the following methods for revocation of person identification data, qualified electronic attestations of attributes or electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source:

— EAA-6.2.10.1-02.1: Where they issue short-lived electronic attestations of attributes having a validity period of equal to or less than 24 hours, then revocation shall not be required.

— EAA-6.2.10.1-02.2: Use an attestation status list mechanism to encode the revocation information as a status list.

— EAA-6.2.10.1-02.2.1: The status list mechanism revokes an MSO based on whether the bit of the issuer-defined bit position in the MSO is set to true in the status list.

— EAA-6.2.10.1-02.2.2: The status list mechanism is specified in the token status list (draft-ietf-oauth-status-list-20) specification.

— EAA-6.2.10.1-02.3: Use an attestation revocation list mechanism to encode the revocation information as an identifier list.

— EAA-6.2.10.1-02.3.1: The identifier list mechanism revokes an MSO based on whether the issuer-defined identifier in the MSO is present on the identifier list.

— EAA-6.2.10.1-02.3.2: EAA-6.2.10.1-06, EAA-6.2.10.1-08, EAA-6.2.10.1-09, EAA-6.2.10.1-10 and EAA-6.2.10.1-11 specify the identifier list mechanism, based on the requirements from the token status list specification including the commonality between the status list and identifier list mechanism.

— EAA-6.2.10.1-03: When a status element is used for person identification data, qualified electronic attestations of attributes or electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source, the status 'revoked' shall be exclusively used.

— EAA-6.2.10.1-03.1: For a status list this implies that only values 'valid' and 'invalid', as specified in the token status list specification shall be used.

— EAA-6.2.10.1-03.2: For the identifier list, only revoked MSOs, as opposed to temporarily suspended MSOs, shall be put in the identifier list.

— EAA-6.2.10.1-04: Where an MSO is revoked, the MSO shall be permanently revoked.

— EAA-6.2.10.1-05: Verification of the MSO revocation list is optional for the wallet-relying party and where applicable, verification shall comply with the verification requirements specified in the token status list specification and the status structure specification set out in in EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: Where a wallet-relying party needs to be able to verify the revocation status of person identification data or electronic attestations of attributes, it shall support both the attestation status list mechanism and the attestation revocation list mechanism set out in EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: The identifier_list and status_list in the MSO may contain the certificate element.

— EAA-6.2.10.1-06.1: Where the certificate element is present, it shall contain a certificate containing the public key that signed or sealed the top-level certificate in the x5chain element in the MSO revocation list structure.

— EAA-6.2.10.1-06.1.1: The wallet-relying party instance shall use that certificate as a trust anchor for the verification of the x5chain element in the MSO revocation list structure.

— EAA-6.2.10.1-06.2: Where the certificate element is not present, the top-level certificate in the x5chain element in the MSO revocation list structure shall be signed or sealed by the certificate used to sign the certificate in the x5chain element of the MSO.

— EAA-6.2.10.1-06.2.1: The wallet-relying party instance shall use that certificate as a trust anchor for the verification of the x5chain element in the MSO revocation list structure.

— EAA-6.2.10.1-07: An MSO revocation list shall be implemented in accordance with the token status list specification as a status list token in CWT format.

— EAA-6.2.10.1-08: For the MSO revocation list for the identifier list and status list mechanism, the following requirements apply:

  — the exp claim shall be present.

  — the ttl claim may be present.

  — the aggregation_uri claim in the IdentifierList or StatusList claim may be present and the provider of person identification data, the provider of qualified electronic attestations of attributes, or the provider

of electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source may use the aggregation_uri claim to indicate support for the aggregation mechanism as specified in the token status list specification.

— the CWT shall be a COSE_Sign1 object using one of the following signature algorithms for calculating the signature:

a) 'ES256' (ECDSA with curve NIST P-256 and SHA-256);

b) 'ES384' (ECDSA with curve NIST P-384 and SHA-384);

c) 'ES512' (ECDSA with curve NIST P-521 and SHA-512);

d) 'ESB256' (ECDSA with curve brainpoolP256r1 and SHA-256);

e) 'ESB384' (ECDSA with curve brainpoolP384r1 and SHA-384);

f) 'ESB512' (ECDSA with curve brainpoolP512r1 and SHA-512);

— the CWT shall contain the x5chain in the protected header that contains the certificate or chain of certificates to verify the signature of the MSO revocation list.

— the extended key usage of the object identifier specified in the token status list specification may be used for the status list and the identifier list signing certificate and the wallet-relying party instances may support the extended key usage of object identifiers specified in the token status list specification and for the object identifier, the provider of qualified electronic attestations of attributes, or the provider of electronic attestations of attributes provided by or on behalf of a public sector body are not to make the extended key usage field critical when using the extended key usage OID specified in the token status list specification.

— EAA-6.2.10.1-09: In deviation to the requirements of the token status list specification, for the identifier list mechanism the following requirements apply:

— the value of the type claim shall be 'application/identifierlist+cwt';

— the StatusList claim shall not be present in the CWT claims set;

— the IdentifierList structure defined in EAA-6.2.10.1-11 shall be present as a claim in the CWT claims set using the key 65530.

— EAA-6.2.10.1-10: The IdentifierList structure shall be a CBOR structure with the following CDDL:

```
IdentifierList = {

    'identifiers': { * Identifier => IdentifierInfo },

    ? 'aggregation_uri': Aggregation_uri

    * tstr => RFU

}

IdentifierInfo = { tstr/int => RFU }

Identifier = bstr

Aggregation_uri = tstr
```

— EAA-6.2.10.1-10.1: Where the identifier in the IdentifierList is present the MSO that contains the identifier in the status element is revoked.

— EAA-6.2.10.1-10.2: The Aggregation_uri claim is specified in section 9.2 of the token status list specification.

— EAA-6.2.10.1-10.3: The identifier list content-type shall be 'application/identifierlist+cwt' set out in the requirements specified in section 8.2 of token status list specification.

— EAA-6.2.10.1-11: The following requirements apply to the identifier_list element in the MSO (see EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: The identifier_list element is a CBOR structure with the following CDDL:

```
IdentifierListInfo = {

        'id': Identifier ,

        »uri«: URI,

        ? »certificate«: Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: To prevent the identifier from being used as a correlation across presentations, it shall be unique per MSO.

— EAA-6.2.10.1-12: The following requirements apply to the status list:

  — EAA-6.2.10.1-12.1: The bits element in the StatusList structure shall be set to 1.

— EAA-6.2.10.1-13: The following requirements apply to the status_list element in the MSO (see EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: The status_list element shall follow the requirements for the StatusListInfo structure as specified in the token status list specification and the optional certificate element defined in EAA-6.2.10.1-06 shall be added.

  — EAA-6.2.10.1-13.2: To prevent the status index from being a correlation across presentations, the combination of status index and URI shall be unique per MSO.

— EAA-6.2.10.1-14: The wallet provider shall use the second (EAA-6.2.10.1-02.2) or the third (EAA-6.2.10.1-02.3) of the methods specified in EAA-6.2.10.1-02 for the revocation of a wallet instance attestation (WIA) and for the revocation of a key attestation (KA).

— EAA-6.2.10.1-15: The wallet provider shall implement the attestation revocation mechanisms specified in EAA-6.2.10.1-02 in their wallet solution.

— EAA-6.2.10.1-16: The provider of person identification data and the provider of electronic attestations of attributes shall support both the attestation status list mechanism and the attestation revocation list mechanism specified in EAA-6.2.10.1-02 for verifying the revocation status of a wallet instance attestation (WIA) and of a key attestation (KA).

— EAA-6.2.10.1-17: The status structure in the MSO shall be a CBOR structure with the following CDDL:

Status = {

? »identifier_list« : IdentifierListInfo,

? »status_list« : StatusListInfo,

* tstr => RFU

}«

BILAG V

»*BILAG III*

Tekniske specifikationer, jf. artikel 10

— Tekniske specifikationer:

  — Punkt 4.2.5 i ETSI TS 119 472-3 V1.1.1 (2026-03).«

BILAG VI

I bilag IV til gennemførelsesforordning (EU) 2024/2979 foretages følgende ændringer:

1) Punkt 1 affattes således:

»1. Obligatorisk signatur- eller seglformat:

a) PAdES (PDF Advanced Electronic Signature) som specificeret i ETSI EN 319 142-1 V1.2.1 (2024-01), Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures.«

2) Punkt 3 affattes således:

»3. API-grænseflade:
ETSI TS 119 432 v1.3.1 (2026-03), punkt 6.4.3, A.6, A.7 og A.8.«

BILAG VII

»*BILAG VI*

EU-tillidsmærket for europæiske digitale identitetstegnebøger i farve



«

BILAG VIII

»*BILAG VII*

EU-tillidsmærket for europæiske digitale identitetstegnebøger i sort-hvid



«

BILAG IX

»BILAG VIII

Data i EU-tillidsmærket for europæiske digitale identitetstegnebøger

Data	Beskrivelse	Kodning	Status
TrustMarkResourceURL	URL for EU-tillidsmærket for europæiske digitale identitetstegnebøger og brugeroplysningsressourcer i tegnebogens brugergrænseflade.	URL	Obligatorisk
ListOfCertifiedWalletsURL	URL for den offentlige liste over certificerede tegnebogsløsninger i EU, jf. Kommissionens gennemførelsesforordning (EU) 2025/849 ([1]).	URL	Obligatorisk
ListOfCertifiedWalletsQRCode	QR Code med oplysningerne om ListOfCertifiedWalletsURL	ISO-8859-1 Byte mode QR code	Valgfri
WalletSolutionInfoPageURL	URL for oplysningssiden om den certificerede tegnebogsløsning på listen over certificerede tegnebogsløsninger fra ListOfCertifiedWalletsURL URL tilføjet '?' og identifikatoren WalletSolutionID for tegnebogsløsningen.	URL	Obligatorisk
WalletSolutionInfoPageQRCode	QR-kode med oplysningerne om WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	Valgfri
WalletVerifierToolURL*	URL til slutpunktet for tegnebogsverificeringsværktøjet */.well-known/openid-credential-issuer*, som bruges til at hente attesteringsudbydermetadataene.	URL	Valgfri

([1]) Kommissionens gennemførelsesforordning (EU) 2025/849 af 6. maj 2025 om fastsættelse af regler for anvendelse af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår indsendelse af oplysninger til Kommissionen og samarbejdsgruppen med henblik på listen over certificerede Europæisk format: Digitale ID-tegnebøger (EUT L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj)«.

BILAG X

I bilag II til gennemførelsesforordning (EU) 2024/2980 foretages følgende ændringer:

1) Bilag II, afsnit 1, punkt 1, litra i), affattes således:

»i) et eller flere certifikater, der er i overensstemmelse med standard ETSI EN 319 412-2 V2.4.1 (2025-06) eller standard ETSI EN 319 412-3 V1.3.1 (2023-09) og kan anvendes til at verificere den underskrift eller det segl, som registratoren har oprettet for registerdataene, og for hvilke de certificerede identitetsdata omfatter registratorens navn og, hvis det er relevant, registratorens registreringsnummer, som omhandlet i henholdsvis litra c) og d)«

2) Bilag II, afsnit 2, punkt 1, litra h), affattes således:

»h) et eller flere certifikater, der er i overensstemmelse med standard ETSI EN 319 412-2 V2.4.1 (2025-06) eller standard ETSI EN 319 412-3 V1.3.1 (2023-09) og kan anvendes til at autentificere og validere tegnebogsenhedsattesteringer, som tegnebogsudbyderen har udstedt, og for hvilke de certificerede identitetsdata omfatter tegnebogsudbyderens navn og, hvis det er relevant, registreringsnummer, som omhandlet i henholdsvis litra a) og b)«.

3) Bilag II, afsnit 3, punkt 1, litra h), affattes således:

»h) et eller flere certifikater, der er i overensstemmelse med standard ETSI EN 319 412-2 V2.4.1 (2025-06) eller standard ETSI EN 319 412-3 V1.3.1 (2023-09) og kan anvendes til at verificere den underskrift eller det segl, som udbyderen af personidentifikationsdata har oprettet for de personidentifikationsdata, som denne leverer, og for hvilke de certificerede identitetsdata omfatter navnet på og, hvis det er relevant, registreringsnummeret på udbyderen af personidentifikationsdata, som omhandlet i henholdsvis litra a) og b).«

4) Bilag II, afsnit 4, punkt 1, litra g), affattes således:

»g) et eller flere certifikater, der er i overensstemmelse med standard ETSI EN 319 412-2 V2.4.1 (2025-06) eller standard ETSI EN 319 412-3 V1.3.1 (2023-09) og kan bruges til at verificere den signatur eller det segl, der er oprettet af udbyderen af adgangscertifikater for tegnebogsmodtagere, på det adgangscertifikat, denne giver til tegnebogsmodtagere, med, hvor det er relevant, de oplysninger, der kræves for at skelne adgangscertifikater for tegnebogsmodtagere fra andre certifikater.«

5) I bilag II tilføjes som afsnit 5:

»5. Anmeldelse af oplysninger om udbydere af registreringscertifikater for tegnebogsmodtagere

1. Medlemsstaterne indgiver følgende oplysninger til Kommissionen om udbydere af registreringscertifikater for tegnebogsmodtagere:

a) navnet på udbyderen af registreringscertifikater for tegnebogsmodtagere

b) hvis det er relevant, registreringsnummeret for udbyderen af registreringscertifikater for tegnebogsmodtagere

c) den medlemsstat, hvor udbyderen af registreringscertifikater for tegnebogsmodtagere er etableret

d) kontakt-e-mail og telefonnummer for udbyderen af registreringscertifikater for tegnebogsmodtagere, for så vidt angår spørgsmål vedrørende de registreringscertifikater, som vedkommende udsteder til tegnebogsmodtagere

e) hvis det er relevant, URL'en på websiden for udbyderen af registreringscertifikater for tegnebogsmodtagere, som indeholder yderligere oplysninger om udbyderen og de registreringscertifikater, som denne leverer til tegnebogsmodtagere

f) URL'en på den webside, der indeholder politikker, vilkår og betingelser, der gælder for udlevering og brug af de registreringscertifikater, vedkommende leverer til tegnebogsmodtagere

g) et eller flere certifikater, der er i overensstemmelse med standard ETSI EN 319 412-2 V2.4.1 (2025-06) eller standard ETSI EN 319 412-3 V1.3.1 (2023-09) og kan bruges til at verificere den signatur eller det segl, der er oprettet af udbyderen af registreringscertifikater for tegnebogsmodtagere, på det registreringscertifikat, denne giver til tegnebogsmodtagere, med, hvor det er relevant, de oplysninger, der kræves for at skelne registreringscertifikater for tegnebogsmodtagere fra andre certifikater.

2. De oplysninger, der henvises til i punkt 1, skal opgives for hver udbyder af registreringscertifikater for tegnebogsmodtagere.«

BILAG XI

»BILAG I

Protokoller og grænseflader, jf. artikel 4

Den tekniske specifikation ETSI TS 119 472-3 V1.1.1 (2026-03) finder anvendelse med følgende tilpasninger:

1) 4.1 General requirements

— GEN-REQ-4.1-05: Void

— NOTE: Void

2) 4.2.3 Provision of registration certificates of PID/EAA Provider to EUDI Wallet

— ISS-MDATA-REG_CERT-4.2.3-04: One of the elements in the issuer_info array parameter shall contain the PID/EAA Provider's registration certificate.

— ISS-MDATA-REG_CERT-4.2.3-07: void

— ISS-MDATA-REG_CERT-4.2.3-08: void

— ISS-MDATA-REG_CERT-4.2.3-09: void

— ISS-MDATA-REG_CERT-4.2.3-10: void

— ISS-MDATA-REG_CERT-4.2.3-11: void

— ISS-MDATA-REG_CERT-4.2.3-12: void

— ISS-MDATA-REG_CERT-4.2.3-13: void

3) 4.2.4.2 ARF pre-defined PID/EAA reuse policy

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Where the id member has the value 'arf_annex_ii' and the array mapped to the label 'details' contains the value 'once_only' or the value 'per-relying-party', then the JSON Object that contains this array mapped to the label 'details' shall also contain a JSON number mapped to the label 'reissue_trigger_unused'.

4) Annex A shall not apply.«

BILAG XII

»BILAG II

Tekniske specifikationer, jf. artikel 5

De tekniske specifikationer i bilag C til ISO/IEC 18013-7:2025 finder anvendelse.

De tekniske specifikationer i punkt 4.1, 4.2, 5 og 6 i ETSI TS 119 472-2 V1.2.1 (2026-03) finder anvendelse med følgende tilpasninger, herunder indsættelsen af et nyt punkt 4.3:

1) 1 Scope

— The present document specifies two profiles of protocols for allowing Relying Parties (RP hereinafter) to request EAAPs or Personal Identification Data (PID hereinafter) to the EUDI Wallet, and the EUDI Wallet to send the requested EAAPs/PIDs to the RP. Each of the profiles supports two transmission mechanisms, namely: API-mediated and non-API mediated, as shown below:

a) A profile is built on:

— ISO/IEC 18013-5 [10] for non-API mediated transmission mechanism only, and

— Annex C of ISO/IEC 18013-7 [16] for API-mediated transmission mechanism.

This profile is named ISO/IEC-mdoc profile and it is defined in clause 5 of the present document.

b) A profile is built on:

OpenID4VC-HAIP [11] for both API-mediated and non-API mediated transmission mechanisms, as follows:

— Sections 5, 5.1, 5.3, 7, and 8 of [11] for transmission via Redirects or non-API mediated transmission mechanism, and

— Sections 5, 5.2, 5.3, 7, and 8 of [11] for API-mediated transmission mechanism.

This profile is named OpenID4VC-HAIP profile and it is defined in clause 6 of the present document.

2) 2.1 Normative references

— [15] ISO 639: 'Language code'.

— [16] ISO/IEC 18013-7:2025 'Personal identification – ISO – compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions'.

3) 4.1 EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: void.

4) 4.2 EAAP implementation based on ISO/IEC-mdoc

— EAAP-ISO/IEC-mdoc-01: void.

— *Note 2*: void.

— EAAP-ISO/IEC-mdoc-02: void.

5) 4.3 EAAP implementation with mediating API

— EAAP-API-GEN-01: The EUDI Wallet shall support a mediating API that supports both protocols defined in clause 5.2 of [11] and in Annex C of [16].

— *NOTE*: Where the device on which the EUDI Wallet is installed does not support both protocols, this requirement cannot be met and triggers a non-conformity due to underlying operating systems and browsers not implementing the necessary interoperability features.

— EAAP-API-GEN-02: The EUDI Wallet shall support a mediating API at least for PIDs and EAA types registered in the catalogue of schemes as defined in Implementing Regulation (EU) 2025/1569, and at least for all the formats defined in Annex II to Implementing Regulation (EU) 2024/2979.

— *NOTE 1*: Where the underlying operating system, browser, mediating APIs, or any other technical layer outside the control of the EUDI Wallet restricts, filters, preselects, or otherwise constrains the credential formats, and the PID and EAA types registered in the catalogue of schemes, this requirement cannot be met. Where such a restriction prevents the EUDI Wallet from supporting a registered credential type or format, the resulting non-conformity is attributable to the failure of those underlying operating systems, browsers, mediating API, or other relevant technical layer to provide the necessary interoperability features.

6) 4.4 Wallet-relying party validation and overasking checks

— WRP-VALIDATION-01: The EUDI Wallet shall validate the wallet-relying party registration certificate received in the request before presenting any requested PID or electronic attestation of attributes to the wallet user for approval.

— WRP-VALIDATION-02: Where the validation of the wallet-relying party registration certificate fails, including where the certificate is expired, revoked, not issued by a valid trusted provider of wallet-relying party registration certificates, malformed, or cannot be cryptographically verified, the EUDI Wallet shall warn the wallet user that the wallet-relying party could not be validated and shall not present the request as successfully validated. The wallet user shall explicitly approve the request of the relying party. Silence or pre-ticked boxes shall not suffice for explicit approval.

— WRP-VALIDATION-03: The wallet provider shall determine, based on its risk analysis and security policy, whether and under which conditions specific failed validation checks may be bypassed by the wallet user.

— WRP-OVERASKING-01: The EUDI Wallet shall compare the attestations and attributes requested by the wallet-relying party with the registered attestations and attributes in the wallet-relying party registration certificate.

— WRP-OVERASKING-02: Where the wallet-relying party requests PID or electronic attestations of attributes or claims that are not covered by the wallet-relying party registration certificate, the EUDI Wallet shall clearly warn the wallet user before any disclosure. The warning shall identify that the wallet-relying party is requesting more information than it has registered. The wallet user shall explicitly approve the request of the relying party. Silence or pre-ticked boxes shall not suffice for explicit approval.

— WRP-OVERASKING-03: The wallet provider shall determine, based on its risk analysis, security policy and applicable law, whether the wallet user may continue despite such warning, whether only the subset of requested data covered by the registration certificate may be disclosed, or whether the request shall be rejected.

7) 5.1 Introduction

— Clause 5 and its subclauses define a profile for a protocol allowing a RP to request EAAPs or PIDs to the EUDI Wallet, and the EUDI Wallet to send the requested EAAPs/PIDs to the RP using either a non-API mediated transmission mechanism, built on ISO/IEC 18013-5 [10] or an API-mediated transmission mechanism built on Annex C of ISO/IEC 18013-7 [16] for transferring the data structures defined in ISO/IEC 18013-5 [10] suitably encapsulated.

— The rest of clause 5 is organised as follows:

  — Clause 5.2 defines requirements on support of the profile and transmission mechanisms by RPs and EUDI Wallet;

  — Clause 5.3 specifies requirements that are specific for the non-API mediated transmission mechanism;

  — Clause 5.4 and its subclauses specify requirements that are specific for the API-mediated transmission mechanism.

8) 5.2 Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: Wallet Units, PID Providers, Attestation Providers, Wallet Providers, and Relying Parties shall not support server retrieval as specified in ISO/IEC 18013-5 [10] for requesting and presenting PID or attestation attributes.

— ISO/IEC 18013-SUPPORT-02: The EUDI Wallet shall meet the requirements defined in clauses 5.3 and 5.4 of the present document.

— ISO/IEC 18013-SUPPORT-04: A Relying Party should implement the profile defined in clause 5.4 of the present document.

9) 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: Device requests sent to EUDI Wallets shall contain the 'requestInfo' key-value pair specified in clause 8.3.2.1.2.1 of [10]. The value of this pair shall be of type RequestInfo.

— ISO/IEC 18013-5-REQ-05: The RequestInfo type shall be as the CDDL definition shows below.

```
RequestInfo = {

    'euWrprc': bstr ; contains a registration certificate (see requirements below)

}
```

— ISO/IEC 18013-5-REQ-06: The mentioned requestInfo member shall contain a member with label 'euWrprc'

— ISO/IEC 18013-5-REQ-07: The value of the 'euWrprc' shall be a CBOR-encoded registration certificate.

— ISO/IEC 18013-5-REQ-08: void.

— *NOTE 3*: void.

— ISO/IEC 18013-5-REQ-09: void.

— ISO/IEC 18013-5-REQ-10: void.

— ISO/IEC 18013-5-REQ-11: void.

10) 5.3.3 ISO/IEC-mdoc EAAP Response profile

— The present clause defines requirements for the DeviceResponse message type, common to the two types of transmission mechanisms (API-mediated and non-API mediated).

— *NOTE 1*: Where a non-API mediated mechanism built on ISO/IEC 18013-5 [10] is used, an EAAP Response is exactly an instance of DeviceResponse as profiled in the present clause, Where an API-mediated mechanism built on Annex C of ISO/IEC 18013-7 [16] is used, the instance of DeviceRequest is encapsulated as specified in Annex C of [16].

— ISO/IEC 18013-5-RESP-02: The provider of person identification data and electronic attestations of attributes shall not include any data elements in the KeyAuthorizations map in the Mobile Security Object of the person identification data and electronic attestations of attributes they issue, except for data elements that are provided by the wallet-relying party in the transactional data in the mdoc request to be signed or sealed by the wallet unit using the private key of the person identification data or electronic attestations of attributes.

— *NOTE 2*: As a result, wallet units cannot present any device-signed data elements to wallet-relying parties, except to signing data that the wallet-relying party provided, for example in use cases for secure user authentication.

— *NOTE 3*: ISO/IEC 18013-5:2021 does not specify how wallet-relying parties can include transactional data in an mdoc request. The inclusion of transactional data in an mdoc request shall take place with the addition of technical specifications.

— ISO/IEC 18013-5-RESP-03: Providers of person identification data shall not allow the private key of the person identification data to sign data elements that are provided by the wallet-relying party in the transactional data in the mdoc request.

11) 5.4 Requirements for API mediated mechanism

5.4.1 ISO/IEC 18013-7-related requirements

The present clause defines requirements for API-mediated transmission mechanism related to the requirements defined in Annex C of [16].

— ISO/IEC 18013-7-API-01: The profile supporting API-mediated presentations shall comply with the requirements in Annex C of ISO/IEC 18013-7 [16] as further profiled in clauses 5.3 and 5.4 of the present document.

— ISO/IEC 18013-7-API-02: All the mandatory requirements defined in Annex C of [16] shall apply as further profiled in clauses 5.3 and 5.4 of the present document.

— ISO/IEC 18013-7-API-03: All the optional requirements defined in Annex C of [16] shall remain optional unless stated otherwise in the present document.

12) 5.4.2 Additional requirements

— The present clause specifies additional requirements for API-mediated transmission mechanism.

— ISO/IEC 18013-ADD-API-01: The EUDI Wallet shall by default disclose the presence of all stored electronic attestations of attributes' type to the mediating API that works in accordance with Annex C of [16], but it shall not disclose the attributes and their values in these electronic attestations of attributes.

— *NOTE 1*: The attribute value restriction applies even if such disclosure would enhance the services provided by the Operating System to the EUDI Wallet, for example, attestation selection in the context of the mediating API.

— There are the considerations related to operating systems and browsers which fall out of the control of implementers, which can be taken into account as indicated in the following notes 2 to 4:

— *NOTE 2*: A presentation request from a Relying Party supporting Annex C of [16] can be processed by the browser and/or the Operating System for searching available EAAs, for preventing fraud targeting the User, or for troubleshooting purposes.

— *NOTE 3*: A presentation request from a Relying Party supporting Annex C of [16] is expected to be processed by the browser and/or the Operating System for User security purposes.

— NOTE 4: A presentation request from a Relying Party supporting Annex C of [16] is expected not to be processed by the browser and/or the Operating System for market analysis purposes (including as a secondary purpose) or for the browser's and/or the Operating System's internal purposes.

— ISO/IEC 18013-ADD-API-02: Where an EUDI Wallet deletes on the User's request a PID or EAA previously disclosed to the mediating API that works in accordance with Annex C of [16], the EUDI Wallet shall disclose the fact that it no longer stores this PID or EAA to the mediating API.

— ISO/IEC 18013-ADD-API-03: If the User uninstalls their EUDI Wallet, the EUDI Wallet shall disclose the fact that it no longer stores any previously disclosed PID(s) or EAA(s) to the mediating API that works in accordance with Annex C of [16].

— ISO/IEC 18013-ADD-API-04: The EUDI Wallet shall provide a global user setting to disable the disclosure of stored EAAs via a mediating API that works as is specified in ISO/IEC 18013-ADD-API-01. When this setting is disabled, the EUDI Wallet shall not advertise or respond to the API-mediated presentation or issuance requests.

— ISO/IEC 18013-ADD-API-05: EUDI Wallets shall verify in cross-device flows, using the mediating API, that the interacting device is in close physical proximity to the EUDI Wallet using a secure, direct, and user-mediated local communication channel, such as a short-range wireless communication technology to perform the physical proximity check.

— *NOTE*: CTAP 2.3 enables to use BLE to perform the close physical proximity check and when implemented by both devices, also enables to transport the data between the devices via short-range transmission technologies. Performing both the physical proximity check and data transfer between the two devices using a local communication channel as enabled by CTAP 2.3, should be preferred by underlying operating systems, browsers, mediating APIs, or any other technical layer outside the control of the EUDI Wallet over the use of CTAP Hybrid tunnel services.

13) 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: The EUDI Wallet shall meet the requirements specified in clause 6.5 of the present Annex.

— OIDFVP-HAIP-SUPPORT-03: The EUDI Wallet should not support the redirects-based mechanism specified in clause 6.4 for cross-device presentation flows.

— *NOTE 3*: Using this mechanism is vulnerable to attacks, such as session fixation. Mitigating such attacks is up to relying parties. Implementing this mechanism should not trigger non-compliance.

— OIDFVP-HAIP-SUPPORT-05: A Relying Party shall meet the requirements specified in clauses 6.5 of the present Annex.

— *NOTE 5*: void.

14) 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: All the mandatory requirements specified in clauses 5, 5.3, 7, and 8 of HAIP [11] shall apply.

— *NOTE 1*: 'HAIP [11] Section 5' refers only to the requirements directly under the Section 5 heading. This does not include sections 5.1, 5.2, and 5.3.

— OIDFVP-HAIP-GEN-03: If the present Annex modifies a requirement in OpenID4VC-HAIP [11], the modified requirement specified by the present Annex shall prevail.

— *NOTE 2*: This would allow, for instance, to convert in mandatory an optional requirement from OpenID4VC-HAIP [11] or to extend mandatory requirements.

— OIDFVP-HAIP-GEN-04: When the format of the requested attestation complies with [10] Relying Parties and EUDI Wallets shall comply with the 'ISO mdocs' profile in [11] Section 6.

— *NOTE 3*: For clarity: the 'ISO mdocs profile' in HAIP implies that Relying Parties and EUDI Wallets must comply with the applicable requirements in [7] Annex B.2.

— OIDFVP-HAIP-GEN-05: When the format of the requested attestation complies with [2], Relying Parties and EUDI Wallets shall comply with the 'IETF SD-JWT VCs' profile in [11] Section 6.

— *NOTE 4*: For clarity: the 'IETF SD-JWT VCs profile' implies that Relying Parties and EUDI Wallets must comply with the requirements in [7] Annex B.3, as well as with the requirements in [11] Section 6.1.

15) 6.3.2.1 General requirements

— OIDFVP-HAIP-COMMON-REQ-01: void.

16) 6.3.2.2 Requirements for the Request Object

— OIDFVP-HAIP-COMMON-REQ-RO-02: void

— OIDFVP-HAIP-COMMON-REQ-RO-03: void

— OIDFVP-HAIP-COMMON-REQ-RO-04: void

— OIDFVP-HAIP-COMMON-REQ-RO-05: void

— OIDFVP-HAIP-COMMON-REQ-RO-06: void.

— OIDFVP-HAIP-COMMON-REQ-RO-07: void

— OIDFVP-HAIP-COMMON-REQ-RO-08: void

— OIDFVP-HAIP-COMMON-REQ-RO-09: void

— OIDFVP-HAIP-COMMON-REQ-RO-10: void

— OIDFVP-HAIP-COMMON-REQ-RO-11: void

— OIDFVP-HAIP-COMMON-REQ-RO-12: void

— *Note 2*: void

— OIDFVP-HAIP-COMMON-REQ-RO-13: One of the elements of the verifier_info parameter shall include the registration certificate.

— OIDFVP-HAIP-COMMON-REQ-RO-23: The leaf certificate mentioned in OpenID4VP section 5.9.3 for use with the x509_hash Client Identifier Prefix shall be a RP access certificate as specified in ETSI TS 119 475 [14].

17) 6.3.3 Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: void.

18) 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: void.

— *NOTE*: void.

19) 6.5.2 Additional requirements

— OIDFVP-HAIP-ADD-API-01: The EUDI Wallet shall by default disclose the presence of all stored EAA types to the mediating API that works in accordance with clause 5.2 of [11], but it shall not disclose the attributes and their values in these EAAs.

— OIDFVP-HAIP-ADD-API-04: If the EUDI Wallet supports a mediating API that works as is specified in OIDFVP-HAIP-ADD-API-01, it shall provide a global user setting to disable the disclosure of stored EAAs via the mediating API. When this setting is set to disabled disclosure, the EUDI Wallet should subsequently enable the User to select individual attestations to be disclosed to the mediating API.

— OIDFVP-HAIP-ADD-API-05: EUDI Wallets shall verify, in cross-device flows, using the mediating API, that the interacting device is in close physical proximity to the EUDI Wallet using a secure, direct, and user-mediated local communication channel, such as a short-range wireless communication technology to perform the physical proximity check.

— *NOTE 5*: CTAP 2.3, enables to use BLE to perform the close physical proximity check and when implemented by both devices, also enables to transport the data between the devices via short-range transmission technologies. Performing both the physical proximity check and data transfer between the two devices using a local communication channel as enabled by CTAP 2.3, should be preferred by underlying operating systems, browsers, mediating APIs, or any other technical layer outside the control of the EUDI Wallet over the use of CTAP Hybrid tunnel services.

20) 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: All requirements specified in this document applicable to Device Request and Device Response structures specified in ISO/IEC 18013-5 also apply when the EUDI Wallet receives a request for ISO/IEC mdoc presentation through an API-transmitted mechanism specified in clause C.1 of [16].«