Europeiska unionens
officiella tidning

SV
L-serien

2026/1731

22.7.2026

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2026/1731

av den 15 juli 2026

om ändring av genomförandeförordningarna (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 och (EU) 2024/2982 vad gäller tillämpliga standarder och specifikationer

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG ([1]), särskilt artikel 5a.23 i den förordningen, och

av följande skäl:

(1) För att säkerställa största möjliga harmonisering mellan medlemsstaterna vid utvecklingen av europeiska digitala identitetsplånböcker bygger de tekniska specifikationerna för plånböckerna på det arbete som utförts på grundval av kommissionens rekommendation (EU) 2021/946 ([2]), i synnerhet på arkitekturen och referensramen. Eftersom arkitekturen och referensramen har utvecklats betydligt sedan kommissionens genomförandeförordningar (EU) 2024/2977 ([3]), (EU) 2024/2979 ([4]), (EU) 2024/2980 ([5]) och (EU) 2024/2982 ([6]) antogs bör dessa genomförandeförordningar nu ändras för att anpassa dem till nya standarder, specifikationer och förfaranden.

I enlighet med målen i förordning (EU) nr 910/2014 har ett antal standarder valts ut för att uppfylla dessa särskilda krav. Dessa standarder bör återspegla etablerad praxis och vara allmänt erkända inom de relevanta sektorerna. Eftersom W3C VCDM-formatet till exempel används som referensformat för intyg, särskilt inom utbildningssektorn, ska de europeiska digitala identitetsplånböckerna också stödja detta format när de nya profilerna för W3C VCDM-formatet finns tillgängliga. Vid behov bör dessa standarder anpassas eller kompletteras för att säkerställa säkerheten och tillförlitligheten hos europeiska digitala identitetsplånböcker samtidigt som gränsöverskridande interoperabilitet och den inre marknadens effektiva funktion underlättas.

(2) För all användning av plånboken som kräver att plånboksanvändarens porträtt visas måste plånbokslösningarna stödja funktionen för selektivt utlämnande och utlämnandet måste stå under användarens fulla kontroll. För att skydda användarens möjlighet att besluta om utlämnande och skydda porträttet mot oavsiktligt utlämnande eller otillåten begäran om utlämnande bör den arkitektoniska utformningen av de europeiska digitala identitetsplånböckerna omfatta varningsmekanismer och loggning av alla transaktioner som rör användningen av porträttet. För att säkerställa att plånboksanvändaren är medveten om att biometriska uppgifter delas bör varningarna ange att

([1]) EUT L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Kommissionens rekommendation (EU) 2021/946 av den 3 juni 2021 om en unionsgemensam verktygslåda för en samordnad strategi för en europeisk ram för digital identitet (EUT L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).
([3]) Kommissionens genomförandeförordning (EU) 2024/2977 av den 28 november 2024 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller personidentifieringsuppgifter och elektroniska attributsintyg som utfärdats för EU:s digitala identitetsplånböcker (EUT L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).
([4]) Kommissionens genomförandeförordning (EU) 2024/2979 av den 28 november 2024 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller integritet och centrala funktioner hos EU:s digitala identitetsplånböcker (EUT L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).
([5]) Kommissionens genomförandeförordning (EU) 2024/2980 av den 28 november 2024 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller anmälningar till kommissionen avseende ekosystemet för EU:s digitala identitetsplånböcker (EUT L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).
([6]) Kommissionens genomförandeförordning (EU) 2024/2982 av den 28 november 2024 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller protokoll och gränssnitt som ska stödjas av det europeiska ramverket för digital identitet (EUT L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

begäran inbegriper delning av biometriska uppgifter och särskilt kräva att användaren bekräftar utlämnandet. Om en förlitande part behandlar porträttet i syfte att unikt identifiera en fysisk person eller för att bekräfta den personens uppgivna identitet gäller artiklarna 6 och 9 i Europaparlamentets och rådets förordning (EU) 2016/679 ([7]) samt alla andra krav i den förordningen, inklusive att förlitande parters behandling av porträttet bör begränsas till vad som är nödvändigt för det avsedda ändamålet. Det avsedda ändamålet bör kommuniceras till plånboksanvändaren tillsammans med begäran om utlämnande på ett tydligt och begripligt språk. För att ta vederbörlig hänsyn till biometriska uppgifters känslighet bör plånboksanvändaren uttryckligen och specifikt bekräfta utlämnandet av porträttet. Tystnad eller förkryssade rutor bör inte anses utgöra en bekräftelse från plånboksanvändaren. Plånboksanvändarens uttryckliga bekräftelse bör vara en teknisk skyddsåtgärd och inte i sig utgöra en rättslig grund för behandling. Enligt artikel 9.4 i förordning (EU) 2016/679 får medlemsstaterna behålla eller införa ytterligare villkor, inklusive begränsningar, för behandling av genetiska uppgifter, biometriska uppgifter eller uppgifter om hälsa.

(3) För att ge medlemsstaterna tillräckligt med tid att anpassa sina nationella förfaranden får plånboksanvändarens porträtt ingå i de obligatoriska personidentifieringsuppgifterna för den fysiska personen först från och med 11 augusti 2028. Om dessa bilder hämtas från befintliga identitetshandlingar, såsom identitetskort eller pass, gäller de relevanta kraven i rådets förordningar (EU) 2025/1208 ([8]) respektive (EG) nr 2252/2004 ([9]).

(4) Förordning (EU) nr 910/2014 kräver att plånböcker ska kunna visa EU:s förtroendemärke för digitala identitetsplånböcker som en verifierbar, enkel och igenkännlig indikation på att en plånbok har tillhandahållits i enlighet med förordningen. Användningen av ett sådant förtroendemärke kommer att bidra till att den inre marknaden fungerar effektivt, garantera rättvis konkurrens och skydda konsumenternas intressen. För att möjliggöra användningen av ett sådant förtroendemärke ska förtroendemärkets visuella och tekniska egenskaper fastställas.

(5) Enligt artikel 12b i förordning (EU) nr 910/2014 ska grindvakter säkerställa att tillhandahållare av europeiska digitala identitetsplånböcker och utfärdare av anmälda medel för elektronisk identifiering får effektiv interoperabilitet med samt, för interoperabilitetens skull, tillgång till samma operativsystems-, maskinvaru- eller programvarufunktioner. Sådan effektiv interoperabilitet och sådan tillgång ska tillhandahållas kostnadsfritt och oavsett om dessa maskinvaru- eller programvarufunktioner utgör en del av operativsystemet, är tillgängliga för eller används av grindvakten när denne tillhandahåller sådana tjänster. Eftersom alla plånbokslösningar bör stödja en gemensam uppsättning protokoll och gränssnitt för att säkerställa användbarhet, säkerhet och interoperabilitet mellan medlemsstaterna bör grindvakter göra de funktioner i operativsystemet, maskinvaran eller programvaran som krävs för att genomföra de protokoll och gränssnitt som anges i bilaga XII till denna förordning tillgängliga. I detta sammanhang bör grindvakterna, i onlineflöden mellan enheter, både för den fysiska närhetskontrollen och för dataöverföringen mellan de två enheterna, föredra en lokal kommunikationskanal enligt CTAP-specifikationen (Client to Authenticator Protocol) version 2.3 ([10]) framför CTAP Hybrid-tunneltjänster.

(6) För att ge medlemsstaterna, leverantörerna av registreringsbevis för förlitande parter och plånboksleverantörerna tillräckligt med tid för att möjliggöra för plånboksenheterna att autentisera och validera registreringsbevis för förlitande parter bör detta krav endast gälla från och med [11 augusti 2028.

(7) Förordning (EU) 2016/679 och, i förekommande fall, Europaparlamentets och rådets direktiv 2002/58/EG ([11]) är tillämpliga på all behandling av personuppgifter i enlighet med denna förordning.

([7]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter, om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Rådets förordning (EU) 2025/1208 av den 12 juni 2025 om säkrare identitetskort för unionsmedborgare och uppehållshandlingar som utfärdas till unionsmedborgare och deras familjemedlemmar när de utövar rätten till fri rörlighet (Text av betydelse för EES) (EUT L 1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Rådets förordning (EG) nr 2252/2004 av den 13 december 2004 om standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna (EUT L 385, 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 februari 2026.

([11]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([12]) och avgav ett yttrande den 17 april 2026 ([13]).

(9) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som inrättats genom artikel 48 i förordning (EU) nr 910/2014.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Ändringar av genomförandeförordning (EU) 2024/2977

Genomförandeförordning (EU) 2024/2977 ska ändras på följande sätt:

(1) Följande artikel ska införas som artikel 3a:

”*Artikel 3a*

Skydd av porträttet

1. Utöver de informationskrav som följer av förordning (EU) 2016/679 ska plånbokstillhandahållare säkerställa att de plånbokslösningar som de tillhandahåller utfärdar varningar till plånboksanvändare när förlitande parter begär utlämnande av porträttet, med uppgift om att begäran innebär delning av biometriska uppgifter och kräver att det selektiva utlämnandet av porträttet bekräftas.

2. För selektivt utlämnande av porträttet till en förlitande part ska plånbokstillhandahållarna säkerställa att plånbokslösningarna kräver att plånboksanvändaren uttryckligen och särskilt bekräftar att porträttet visas.

3. Porträttet får inte lagras av förlitande parter såvida inte behandlingen är nödvändig för identifiering eller autentisering i enlighet med unionens dataskyddslagstiftning, eller såvida inte detta föreskrivs i unionsrätten eller nationell rätt i enlighet med unionens dataskyddslagstiftning. Porträttet får inte överföras till tredjeländer eller internationella organisationer, såvida inte detta är tillåtet enligt unionens dataskyddslagstiftning.”;

(2) I artikel 4 ska punkt 1 ersättas med följande:

”1. Elektroniska attributsintyg som utfärdas till plånboksenheter ska uppfylla minst en av standarderna i förteckningen i bilaga II till genomförandeförordning (EU) 2024/2979.”

(3) I artikel 5 ska punkt 4 b ersättas med följande:

”b) om plånboksenhetsintyget för den plånboksenhet för vilken personidentifieringsuppgifterna utfärdades har återkallats.”

(4) Bilagan ska ersättas med den text som anges i bilaga I till denna förordning.

([12]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) *EDPS Formal comments on the draft Implementing Regulation as regards applicable standards and specifications and correcting Implementing Regulation (EU) 2024/2980* | Europeiska datatillsynsmannen.

Artikel 2

Ändringar av genomförandeförordning (EU) 2024/2979

Genomförandeförordning (EU) 2024/2979 ska ändras på följande sätt:

(1) I artikel 3 ska punkt 2 utgå.

(2) I artikel 5.1 ska led a ersättas med följande:

”a) utföra kryptografiska plånboksoperationer som omfattar kritiska tillgångar som lagras i en krypteringshårdvara och inte krävs för autentisering av plånboksanvändaren endast i de fall då dessa applikationer har autentiserat plånboksanvändare,”

(3) Följande artikel 5a ska införas:

”*Artikel 5a*

Kryptografiska mekanismer

Plånbokstillhandahållare ska, för tillämpningen av artikel 4.2, endast använda de kryptografiska mekanismer som avses i bilaga Ia.”

(4) Artikel 6 ska ändras på följande sätt:

(a) Punkt 1 ska ersättas med följande:

”1. Plånbokstillhandahållare ska utfärda plånboksenhetsintyg för varje plånboksenhet. Plånbokstillhandahållare ska underteckna eller stämpla plånboksenhetsintygen på ett sådant sätt att underskrifterna eller stämplarna kan valideras med hjälp av ett certifikat som förtecknas i enlighet med avsnitt 2 punkt 1 h i bilaga II till genomförandeförordning (EU) 2024/2980.”

(b) Punkt 2 ska ersättas med följande:

”2. Plånbokstillhandahållare ska säkerställa att de plånboksenhetsintyg som avses i punkt 1 uppfyller de tekniska specifikationer som anges i bilaga Ib.”

(c) I punkt 3 ska led b ersättas med följande:

”(b) tillhandahålla plånboksanvändare säkra identifierings- och autentiseringsmekanismer som är oberoende av plånboksenheter,”

(5) I artikel 9.2 ska led b ersättas med följande:

”(b) namn, kontaktuppgifter och den unika identifieraren för motsvarande förlitande part samt den medlemsstat där den förlitande parten är etablerad,”

(6) I artikel 10 ska punkt 1 ersättas med följande:

”1. Plånbokstillhandahållare ska säkerställa att elektroniska attributsintyg som utfärdas i enlighet med de tekniska specifikationer som är tillämpliga på de gemensamma inbäddade utlämnandepolicyer som anges i bilaga III kan behandlas av de plånboksenheter som de tillhandahåller.”

(7) Artikel 12 ska ändras på följande sätt:

(a) I punkt 2 ska led c ersättas med följande:

”(c) Skapa underskrifter eller stämplar i enlighet med åtminstone det obligatoriska format för underskrift eller stämpel som avses i bilaga IV.”

(b) Punkt 3 ska ersättas med följande:

”3. Applikationer för skapande av underskrifter kan antingen vara integrerade i eller externa i förhållande till plånboksinstanserna.”

(c) Följande punkt ska införas:

”4. Applikationer för skapande av underskrifter som används av plånboksenheter ska åtminstone stödja det gränssnitt för tillämpningsprogram som avses i bilaga IV.”

(8) I artikel 14 ska punkt 1 utgå.

(9) Följande artikel 14a ska införas:

”*Artikel 14a*

EU:s förtroendemärke för digitala identitetsplånböcker

1. Plånbokstillhandahållare ska säkerställa att plånboksenheter visar EU:s förtroendemärke för digitala identitetsplånböcker. EU:s förtroendemärke för digitala identitetsplånböcker ska ha den utformning som anges i bilagorna VI och VII.

2. Plånbokstillhandahållare ska säkerställa att plånboksenheter ger plånboksanvändare tillgång till information som gör det möjligt för dem att kontrollera plånbokslösningens certifieringsstatus. För detta ändamål ska plånbokstillhandahållare säkerställa att de berörda plånboksenheterna, efter registreringen av en plånbokslösning, innehåller de URL:er som tillhandahålls av Europeiska kommissionen för sådan kontroll. Plånbokstillhandahållare ska säkerställa att deras plånboksenheter har tillgång till data för EU:s förtroendemärke för digitala identitetsplånböcker som uppfyller de tekniska specifikationer som anges i bilaga VIII.

3. Referensfärgerna för EU:s förtroendemärke för digitala identitetsplånböcker ska vara Pantone nr 661 och 116 eller blå (100 % cyan + 67 % magenta + 0 % gul + 40 % svart) och gul (0 % cyan + 20 % magenta + 100 % gul + 0 % svart) när fyrfärgstryck används. När RGB-färger används ska referensfärgerna vara blå (0 röd + 51 grön + 153 blå) och gul (255 röd + 204 grön + 0 blå).

4. Endast om det inte är praktiskt möjligt att använda färg får EU:s förtroendemärke för digitala identitetsplånböcker användas i svartvitt i enlighet med bilaga VII.

5. När EU:s förtroendemärke för digitala identitetsplånböcker används på en mörk bakgrund får det användas i negativt format med samma bakgrundsfärg. När EU:s förtroendemärke för digitala identitetsplånböcker används i färg på en färgad bakgrund så att det blir svårt att urskilja får en avgränsande yttre linje kring märket användas så att kontrasten mot bakgrundsfärgen blir bättre.

6. EU:s förtroendemärke för digitala identitetsplånböcker ska ha en minsta storlek på 64 × 85 pixlar vid 150 dpi.

7. Plånbokstillhandahållare ska säkerställa att EU:s förtroendemärke för digitala identitetsplånböcker används på ett sådant sätt att det tydligt framgår vilken plånboksenhet märket avser. EU:s förtroendemärke för digitala identitetsplånböcker får associeras med grafiska eller textuella element som tydligt anger den plånboksenhet som det används för, under förutsättning att dessa inte förändrar märkets igenkännbarhet som EU:s förtroendemärke för digitala identitetsplånböcker eller ändrar kopplingen till den förteckning över certifierade europeiska digitala identitetsplånböcker som avses i artikel 5d i förordning (EU) nr 910/2014.

8. Om plånbokstillhandahållare har återkallat ett plånboksenhetsintyg ska de säkerställa att EU:s förtroendemärke för digitala identitetsplånböcker inte längre visas av den motsvarande plånboksenheten.”

(10) Bilagorna Ia och Ib ska läggas till i enlighet med bilagorna II och III till denna förordning.

(11) Bilaga II ska ersättas med bilaga IV till denna förordning.

(12) Bilaga III ska ersättas med bilaga V till denna förordning.

(13) Bilaga IV ska ändras i enlighet med bilaga VI till denna förordning.

(14) Bilaga V ska utgå.

(15) Den text som anges i bilaga VII till denna förordning ska införas som bilaga VI.

(16) Texten i bilaga VIII till denna förordning ska införas som bilaga VII.

(17) Texten i bilaga IX till denna förordning ska införas som bilaga VIII.

Artikel 3

Ändringar av genomförandeförordning (EU) 2024/2980

Genomförandeförordning (EU) 2024/2980 ska ändras på följande sätt:

1. I artikel 5 ska punkt 2 ersättas med följande:

”2. Kommissionen ska i tillämpliga fall upprätta, underhålla och offentliggöra en förteckning över den information som medlemsstaterna har anmält om plånbokstillhandahållare, tillhandahållare av personidentifieringsuppgifter, tillhandahållare av förlitandepartcertifikat och tillhandahållare av förlitandepartregistreringscertifikat i enlighet med avsnitten 2, 3, 4 och 5 i bilaga II.”

2. Bilaga II till genomförandeförordning (EU) 2024/2980 ska ändras i enlighet med bilaga X till denna förordning.

Artikel 4

Ändringar av genomförandeförordning (EU) 2024/2982

Genomförandeförordning (EU) 2024/2982 ska ändras på följande sätt:

(1) I artikel 1 ska punkt 2 ersättas med följande:

”(2) presentation av attribut för personidentifieringsuppgifter och elektroniska attributsintyg för förlitande parter,”

(2) Artikel 3 ska ändras på följande sätt:

(a) Punkt 1 ska ersättas med följande:

”(1) autentiserar och validerar förlitandepartcertifikaten när de interagerar med förlitande parter utan att delegera utförandet av dessa processer till ett operativsystem, en webbläsare eller en annan mellanliggande applikation,”

(b) Punkt 2 ska utgå.

(c) Punkt 3 ska ersättas med följande:

”(3) autentiserar och validerar begäranden som gjorts med hjälp av förlitandepartcertifikat,”

(d) Punkt 4 ska ersättas med följande:

”(4) autentiserar och validerar förlitandepartregistreringscertifikatet,”

(e) Punkt 5 ska ersättas med följande:

”(5) för plånboksanvändare visar information som finns i förlitandepartcertifikaten,”

(f) Punkt 8 ska utgå.

(g) Punkt 9 ska ersättas med följande:

”(9) inte presenterar några begärda attribut för förlitande parter förrän följande steg har slutförts: det har

a) verifierats att inbyggda policyer för utlämnande har behandlats inom plånboksenheten i enlighet med artikel 10 i genomförandeförordning (EU) 2024/2979,

b) verifierats att plånboksanvändarna helt eller delvis har godkänt presentationen.”

(3) I artikel 4 ska punkt 1 ersättas med följande:

”1. Plånbokstillhandahållare ska säkerställa att plånbokslösningar stöder de protokoll och gränssnitt som anges i bilaga I för utfärdande av personidentifieringsuppgifter och elektroniska attributsintyg för plånboksenheter.”

(4) Artikel 5 ska ändras på följande sätt:

(a) Punkterna 1 och 2 ska ersättas med följande:

”1. Plånbokstillhandahållare ska säkerställa att plånbokslösningarna stöder protokoll och gränssnitt för att på distans och i förekommande fall i närheten presentera attribut för förlitande parter i enlighet med de tekniska specifikationer som anges i bilaga II.

2. Plånbokstillhandahållare ska säkerställa att plånboksenheterna på användarnas begäran svarar på autentiserade och validerade begäranden från förlitande parter som avses i artikel 3 i enlighet med de tekniska specifikationer som anges i bilaga II.”

(b) Punkt 5 ska utgå.

(5) Artikel 8 ska ersättas med följande:

”*Artikel 8*

Ikraftträdande

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

Artikel 3.4 ska tillämpas från och med 11 augusti 2028.

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

(6) Bilagan ska utgå.

(7) Den text som anges i bilaga XI till denna förordning ska läggas till som bilaga I.

(8) Den text som anges i bilaga XII till denna förordning ska läggas till som bilaga II.

Artikel 5

Ikraftträdande

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

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

Utfärdad i Bryssel den 15 juli 2026.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA I

”BILAGA

Tekniska specifikationer för de personidentifieringsuppgifter som avses i artikel 3.3

(1) Avsnitt 1: Personidentifieringsuppgifter för fysiska personer

Tabell 1

Obligatoriska personidentifieringsuppgifter för den fysiska personen för selektivt utlämnande

Uppgiftsidentifierare	Definition
`family_name`	Nuvarande efternamn på den användare som personidentifieringsuppgifterna avser.
`given_name`	Samtliga nuvarande förnamn på den användare som personidentifieringsuppgifterna avser.
`birth_date`	Dag, månad och år då den användare som personidentifieringsuppgifterna avser föddes.
`birth_place`	Det land uttryckt i form av en landskod med två bokstäver enligt ISO 3166–1, eller den stat, provins, distrikt, lokalområde, kommun, stad eller by där den användare som personidentifieringsuppgifterna avser föddes.
`nationality`	En eller flera landskoder med två bokstäver enligt ISO 3166-1, som representerar nationaliteten för den användare som personidentifieringsuppgifterna avser.
`portrait`	Utom i de fall då användaren, där så är tillämpligt, uttryckligen väljer att vägra, ska ansiktsbilden av den användare som personidentifieringsuppgifterna avser som uppfyller kvalitetskraven för en bildtyp med helt frontal bild enligt ISO/IEC 39794-5 eller, för bakåtkompatibilitet, ISO/IEC 19794-5, klausulerna 8.2, 8.3 och 8.4, lämnade som kodade bilddata utan de headers eller block som anges i klausul 5 i ISO/IEC 19794-5, med undantag för själva bilddatamängderna (en JPEG), tillämpas från och med 11 augusti 2028.

— Medlemsstaterna får föreskriva att användaren har valet att vägra att porträttet införs i personidentifieringsuppgifterna.

— Medlemsstaterna ska säkerställa att det selektiva utlämnandet gäller för varje uppgiftsidentifierare, inklusive porträttet.

— Om den fysiska personens födelsedatum inte är känt ska medlemsstaterna välja lämpliga värden som uppfyller de specifikationer som anges i avsnitt 4.1 eller 4.2 i denna bilaga, beroende på vad som är tillämpligt.

— Om den fysiska personens medborgarskap är okänt ska medlemsstaterna använda värdet ”QU”.

— Om den fysiska personen saknar medborgarskap ska medlemsstaterna använda värdet ”QS”.

— Om användaren väljer att vägra att porträttet införs, ska medlemsstaterna ange värdet tomt.

Tabell 2

Frivilliga personidentifieringsuppgifter för den fysiska personen för selektivt utlämnande

Uppgiftsidentifierare	Definition
`resident_address`	Fullständig adress till den plats där den användare som personidentifieringsuppgifterna avser för närvarande är bosatt eller kan kontaktas (gatunamn, husnummer, ort osv.).
`resident_country`	Det land där den användare som personidentifieringsuppgifterna avser för närvarande är bosatt, uttryckt i form av en landskod med två bokstäver enligt ISO 3166-1.
`resident_state`	Delstat, provins, distrikt eller lokalområde där den användare som personidentifieringsuppgifterna avser för närvarande är bosatt.
`resident_city`	Den kommun, stad eller by där den användare som personidentifieringsuppgifterna avser för närvarande är bosatt.
`resident_postal_code`	Postnummer till den plats där den användare som personidentifieringsuppgifterna avser för närvarande är bosatt.
`resident_street`	Namnet på den gata där den användare som personidentifieringsuppgifterna avser för närvarande är bosatt, inklusive husnummer och eventuella affix eller suffix till detta.
`personal_administrative_-number`	Ett värde som tilldelas den användare som personidentifieringsuppgifterna avser och som är unikt bland alla personnummer som utfärdas av tillhandahållaren av personidentifieringsuppgifter. Om medlemsstaterna väljer att inkludera detta attribut ska de i sina system för elektronisk identifiering, enligt vilka personidentifieringsuppgifterna utfärdas, beskriva den policy som de tillämpar på värdena för detta attribut, inbegripet, i tillämpliga fall, särskilda villkor för behandlingen av detta värde.
`family_name_birth`	Efternamn på den användare som personidentifieringsuppgifterna avser vid födseln.
`given_name_birth`	Samtliga förnamn på den användare som personidentifieringsuppgifterna avser vid födseln.
`sex`	Värdena ska vara ett av följande: 0 = okänt 1 = man 2 = kvinna 3 = annat 4 = intersexperson 5 = person med icke-normativa könsuttryck 6 = öppen 9 = ej tillämpligt För värdena 0, 1, 2 och 9 gäller ISO/IEC 5218.
`email_address`	E-postadress till den användare som personidentifieringsuppgifterna avser [i överensstämmelse med RFC 5322 ([1])].

Uppgiftsidentifierare	Definition
`mobile_phone_number`	Mobiltelefonnummer till den användare som personidentifieringsuppgifterna avser, med början med det internationella kodprefixet ”+” och landskoden, följt av siffror enbart.

([1]) P. Resnick (red.), *Internet Message Format*, RFC 5322, oktober 2008.

(2) Avsnitt 2: Personidentifieringsuppgifter för juridiska personer

Tabell 3

Obligatoriska personidentifieringsuppgifter för den juridiska personen

Uppgiftsidentifierare
nuvarande juridiskt namn
en unik identifieringskod som satts samman av den utsändande medlemsstaten i enlighet med de tekniska specifikationerna för gränsöverskridande identifiering och som är mest beständig i tid.

— Om en uppgiftsidentifierare inte är känd för personen eller på annat sätt inte kan utfärdas som en del av datasetet för personidentifiering ska medlemsstaterna i stället använda ett attributvärde som är lämpligt i situationen.

Tabell 4

Frivilliga personidentifieringsuppgifter för den juridiska personen

Uppgiftsidentifierare
nuvarande adress
momsregistreringsnummer
skatteregistreringsnummer
Europeisk unik identifieringskod som avses i Europaparlamentets och rådets direktiv (EU) 2017/1132 ([1])
den identifieringskod för juridiska personer som avses i kommissionens genomförandeförordning (EU) 2022/1860 ([2])
det registrerings- och identitetsnummer för ekonomiska aktörer som avses i kommissionens genomförandeförordning (EU) nr 1352/2013 ([3])
punktskattenummer som avses i artikel 2.12 i rådets förordning (EU) nr 389/2012 ([4])

([1]) Europaparlamentets och rådets direktiv (EU) 2017/1132 av den 14 juni 2017 om vissa aspekter av bolagsrätt (EUT L 169, 30.6.2017, s. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj

([2]) Kommissionens genomförandeförordning (EU) 2022/1860 av den 10 juni 2022 om fastställande av tekniska genomförandestandarder för tillämpningen av Europaparlamentets och rådets förordning (EU) nr 648/2012 vad gäller standarder, format, frekvens samt metoder och arrangemang för rapportering (EUT L 262, 7.10.2022, s. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Kommissionens genomförandeförordning (EU) nr 1352/2013 av den 4 december 2013 om fastställande av de formulär som avses i Europaparlamentets och rådets förordning (EU) nr 608/2013 om tullens säkerställande av skyddet för immateriella rättigheter (EUT L 341, 18.12.2013, s. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Rådets förordning (EU) nr 389/2012 av den 2 maj 2012 om administrativt samarbete i fråga om punktskatter och om upphävande av förordning (EG) nr 2073/2004 (EUT L 121, 8.5.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

(3) Avsnitt 3: Metadata om personidentifieringsuppgifter

Tabell 5

Metadata om personidentifieringsuppgifter

Uppgiftsidentifierare	Definition	Förekomst
`issuing_authority`	Namn på den administrativa myndighet som utfärdade personidentifieringsuppgifterna, eller landskoden med två bokstäver enligt ISO 3166 för den berörda medlemsstaten om det inte finns någon separat myndighet som har rätt att utfärda personidentifieringsuppgifter.	Obligatorisk
`issuing_country`	Landskod med två bokstäver enligt ISO 3166-1 för det land eller territorium som tillhandahållaren av personidentifieringsuppgifterna tillhör.	Obligatorisk
`expiry_date`	Datum (och om möjligt klockslag) då den administrativa giltighetsperioden för personidentifieringsuppgifterna löper ut.	Valfri
`document_number`	Ett nummer för personidentifieringsuppgifterna som tilldelats av tillhandahållaren av personidentifieringsuppgifter.	Valfri
`issuing_jurisdiction`	Landsdelskod för den jurisdiktion som utfärdade personidentifieringsuppgifterna, enligt klausul 8 i ISO 3166-2:2020. Den första delen av koden ska vara densamma som värdet för utfärdandelandet.	Valfri
`issuance_date`	Datum (och om möjligt klockslag) då den administrativa giltighetsperioden för personidentifieringsuppgifterna inleddes.	Valfri

(4) Avsnitt 4: Kodning av attribut för personidentifieringsuppgifter för fysisk person

— Personidentifieringsuppgifter för fysisk person ska utfärdas i enlighet med de standarder som anges i bilaga II till genomförandeförordning (EU) 2024/2979, avsnitten 5 (SD-JWT VC-format) och 6 (ISO/IEC-mdoc-format) i den mån de är tillämpliga på elektroniska intyg om attribut. Avsnitten 5.2.2, 5.2.4, 5.2.5, EAA-6.1-03, 6.2.2, 6.2.3,6.2.4 och 6.2.5 ska inte tillämpas.

— Kodningen av personidentifieringsuppgifter för fysisk person ska uppfylla de tekniska specifikationerna i avsnitten 4.1 och 4.2 i denna bilaga.

4.1 Kodning av personidentifieringsuppgifter för fysisk person i ISO/IEC-mdoc-format

— Intygstypen för personidentifieringsuppgifter i ISO/IEC mdoc-format ska vara ”eu.europa.ec.eudi.pid.1”. Identifieraren för namnrymden för attributen för personidentifieringsuppgifter som anges i denna bilaga ska vara ”eu.europa.ec.eudi.pid.1”.

— Om personidentifieringsuppgifterna innehåller data för vilka dataidentifierare inte anges i denna bilaga ska dessa data definieras inom en nationell namnrymd för personidentifieringsuppgifter som använder det allmänna formatet eu.europa.ec.eudi.pid.[ISO 3166-1 alpha-2-landskod eller ISO 3166-2-regionkod], följt av en valfri punkt och versionsnummer.

— Om den nationella namnrymden används ska dess schema, inklusive alla dataidentifierare samt deras definitioner, förekomst och kodningsformat, offentliggöras i enlighet med artikel 8 i kommissionens genomförandeförordning (EU) 2025/1569 ([1]).

— Personidentifieringsuppgifterna och deras metadata som anges i avsnitten 1 och 3 i denna bilaga ska ingå i dataelement för personidentifieringsuppgifter i den mening som avses i specifikationerna för ISO/IEC mdoc-format.

— Elementet deviceKey inom elementet deviceKeyInfo i instansen av typen MobileSecurityObject ska innehålla en publik nyckel.

— Den publika nyckeln ska motsvara en privat nyckel som lagras i krypteringshårdvaran (”WSCD”) hos plånboksanvändaren.

— Det skyddade headerfältet för den digitala CB-AdES-signatur som undertecknar personidentifieringsuppgifter i ISO/IEC-mdoc-format ska innehålla headerparametrarna x5u och x5t, vilka båda specificeras i RFC 9360 ([2]).

— Den hashningsalgoritm som används i headerparametern x5t ska vara SHA-256.

— Kraven för kodning av personidentifieringsuppgifter i ISO/IEC-mdoc-format anges i tabell 6:

Tabell 6

Krav för kodning av personidentifieringsuppgifter i ISO/IEC-mdoc-format

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

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

Uppgiftsidentifierare	Attributidentifierare	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

— Beteckningen på kodningsformatet för de attribut som anges i tabell 6 ska använda representationstyper enligt RFC 8610 ([3]), med följande ytterligare krav:

(a) En tstr ska kodas i UTF-8.

(b) En tstr ska stödja hela Unicode-intervallet.

(c) En tstr ska ha en maximal längd på 150 tecken.

(d) Ett datum ska kodas enligt RFC 8943 ([4]).

(e) Ett fullständigt datum ska tolkas som #6.1004(tstr), där tag 1004 är enligt RFC 8943.

(f) Ett tdate-attribut ska innehålla en date-time-sträng enligt RFC 3339 ([5]).

(g) Ett full-date-attribut ska innehålla en full-date-sträng enligt RFC 3339 i enlighet med RFC 8943.

(h) En återgivning av ett datum i attribut ska, om inget annat anges

— inte använda bråkdelar av sekunder,

— inte använda en lokal förskjutning från UTC och den tidsförskjutning som anges i RFC 3339 ska sättas till ”Z”.

(i) Ett heltal med huvudtyperna 0 och 1 ska vara så litet som möjligt enligt RFC 8949 ([6]), avsnitt 4.2.

(j) En place_of_birth ska innehålla minst ett av följande nyckelvärdespar: ”country”, ”region” eller ”locality”.

(k) Uttrycket för längden i en bstr, tstr, array eller karta ska vara så kort som möjligt enligt RFC 8949, avsnitt 4.2.

([3]) C. Vigano och 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 och J. Richter, *”Concise Binary Object Representation (CBOR) Tags for Date*, RFC 8943, november 2020.
([5]) G. Klyne och C. Newman, *”Date and Time on the Internet: Timestamps*, RFC 3339, juli 2002.
([6]) C. Bormann och P. Hoffman, *Concise Binary Object Representation (CBOR)*, RFC 8949, december 2020.

(l) Attributet nationality ska kodas som en array av alpha-2-landskoder enligt ISO 3166-1. Om CDDL-beteckning enligt RFC 8610 används ska kodningen av detta attribut vara följande:

— nationalities = [+ CountryCode].

— CountryCode = tstr . alpha-2-landskod enligt ISO 3166-1.

— Om en plånboksanvändare som personidentifieringsuppgifterna avser har flera nationaliteter och tillhandahållaren av personidentifieringsuppgifterna intygar dessa flera nationaliteter får tillhandahållaren inkludera samtliga nationaliteter i personidentifieringsuppgifterna.

— Attributet place_of_birth ska kodas som typen place_of_birth. Om CDDL-beteckning enligt RFC 8610 används ska kodningen av detta attribut vara

place_of_birth =

{

? 'country' : tstr ; En enskild landskod med två bokstäver enligt ISO 3166-1

? 'region': tstr ; Namnet på en stat, en provins, ett distrikt eller ett lokalområde

? 'locality': tstr ; Namnet på en kommun, stad eller by

}

4.2 Krav för kodning av personidentifieringsuppgifter i SD-JWT VC-format

— Personidentifieringsuppgifterna och deras metadata som anges i detta avsnitt ska ingå i en personidentifieringsuppgift som anspråk i den mening som avses i SD-JWT VC-formatspecifikationerna.

— Alla anspråk i de utfärdade personidentifieringsuppgifterna, som det hänvisas till i föregående strecksats, ska kunna lämnas ut selektivt individuellt, utom de anspråk som definieras som icke-selektivt utlämningsbara i SD-JWT VC-format.

— I tabell 7 anges kodningen av anspråksnamn som är offentliga namn.

— I tabell 8 anges kodningen av anspråksnamn som är specifika för personidentifieringsuppgifter.

— En JSON-sträng som används i personidentifieringsuppgifter kodade i SD-JWT VC ska kodas i UTF-8 och ska stödja hela Unicode-intervallet om inte annat uttryckligen anges i tabell 8 nedan eller hänvisningarna däri.

— JWT-anspråken nbf och exp enligt definitionen i RFC 7519 ([7]) ska användas för att uttrycka den tekniska giltighetsperioden för personidentifieringsuppgifter som överensstämmer med SD-JWT VC-formatet.

([7]) J. Jones m.fl., *JSON Web Token (JWT)*, RFC 7519, maj 2015.

— Personidentifieringsuppgifter ska innehålla cnf-anspråket enligt definitionen i RFC 7800 ([8]), som ska vara en publik nyckel som genereras från en privat nyckel som lagras i WSCD för plånboksanvändarens plånboksenhet.

— Det skyddade headerfältet för den digitala underskriften av personidentifieringsuppgifter i SD-JWT VC-format ska innehålla headerparametrarna x5u och x5t#S256, som anges i RFC 7515 ([9]).

Tabell 7

Krav för kodning av personidentifieringsuppgifter i SD-JWT VC-format med offentliga namn

Uppgiftsidentifierare	Attributidentifierare	Kodningsformat
`family_name`	`family_name`	sträng
`given_name`	`given_name`	sträng
`birth_date`	`birthdate`	sträng, ISO 8601-1, formatet ÅÅÅÅ-MM-DD
`birth_place`	`place_of_birth`	JSON-struktur
`nationality`	`nationalities`	array av strängar
`resident_address`	`address.formatted`	sträng
`resident_country`	`address.country`	sträng
`resident_state`	`address.region`	sträng
`resident_city`	`address.locality`	sträng
`resident_postal_code`	`address.postal_code`	sträng
`resident_street`	`address.street_address`	sträng
`family_name_birth`	`birth_family_name`	sträng
`given_name_birth`	`birth_given_name`	sträng
`email_address`	`email`	sträng
`mobile_phone_number`	`phone_number`	sträng
`portrait`	`picture`	sträng: data-URL som innehåller ett base64-kodat porträtt i JPEG-format

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

Tabell 8

Krav för kodning av personidentifieringsuppgifter i SD-JWT VC-format med privata namn

Uppgiftsidentifierare	Attributidentifierare	Kodningsformat
`expiry_date`	`date_of_expiry`	sträng, ISO 8601-1, formatet ÅÅÅÅ-MM-DD
`issuance_date`	`date_of_issuance`	sträng, ISO 8601-1, formatet ÅÅÅÅ-MM-DD
`personal_administrative_number`	`personal_administrative_number`	sträng
`sex`	`sex`	siffror
`issuing_authority`	`issuing_authority`	sträng
`issuing_country`	`issuing_country`	sträng
`document_number`	`document_number`	sträng
`issuing_jurisdiction`	`issuing_jurisdiction`	sträng

— Grundtypen för personidentifieringsuppgifter ska vara ”urn:eudi:pid:1”, inkluderad i vct-anspråket. Alla personidentifieringsuppgifter ska använda typer i namnrymden ”urn:eudi:pid:”.

— Om personidentifieringsuppgifter innehåller attribut som inte anges i denna bilaga ska dessa attribut definieras inom en nationell typ.

— När den nationella typen används ska dess schema, inklusive alla dataidentifierare samt deras definitioner, förekomst och kodningsformat, definieras i ett schema som offentliggörs i enlighet med artikel 8 i genomförandeförordning (EU) 2025/1569.

(5) Avsnitt 5: Uppgifter om infrastruktur för betrodda tjänster

Den förteckning över tillhandahållare av personidentifieringsuppgifter som kommissionen tillhandahåller i enlighet med genomförandeförordning (EU) 2024/2980 ska möjliggöra autentisering av personidentifieringsuppgifter.”

BILAGA II

”BILAGA Ia

Kryptografiska mekanismer som det hänvisas till i artikel 5a

Europeiska gruppen för cybersäkerhetscertifiering, undergruppen för kryptografi: *Agreed Cryptographic Mechanisms,* offentliggjord av Europeiska unionens cybersäkerhetsbyrå (Enisa) ([1]).”

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

BILAGA III

”BILAGA Ib

Tekniska specifikationer för plånboksenhetsintyg som avses i artikel 6.2a

(1) Ett plånboksenhetsintyg ska omfatta ett eller flera plånboksinstansintyg och ett eller flera nyckelintyg.

(2) Plånboksinstansintyget och nyckelintygen ska uppfylla följande krav:

(a) Formatkrav

— FR-WIA-1: Ett plånboksinstansintyg ska vara en JSON Web Token (JWT) enligt RFC 7519 ([1]), som har undertecknats eller stämplats av plånbokstillhandahållaren med en kompakt JAdES-baslinjesignatur av typ B.

— FR-WIA-1.1: Ett plånboksinstansintyg ska vara ett plånboksintyg enligt bilaga E i OpenID for Verifiable Credential Issuance v1.0 ([2]) (OID4VCI) och utökat enligt C-WIA-1 och C-WIA-2 nedan.

— FR-KA-1: Ett nyckelintyg ska vara en JWT enligt RFC 7519, undertecknat eller stämplat av plånbokstillhandahållaren med hjälp av en kompakt JAdES-baslinjeunderskrift av typ B.

— FR_KA_1.1: Ett nyckelintyg ska vara ett nyckelintyg enligt bilaga D i OID4VCI, utökat enligt C_KA-1 och C_KA-2 nedan.

(b) Transportkrav

— TR-WIA-1: En plånboksenhet ska använda ett plånboksinstansintyg vid utfärdande av personidentifieringsuppgifter, kvalificerade eller icke-kvalificerade elektroniska attributsintyg eller elektroniska attributsintyg som tillhandahålls av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa.

— TR-WIA-2: En plånbokstillhandahållare ska verifiera plånboksinstansens integritet och underteckna eller stämpla plånboksinstansintyget.

— TR-WIA-2.1: Om en plånbokstillhandahållare utfärdar ett plånboksinstansintyg ska skillnaden mellan klockslaget då plånbokstillhandahållaren verifierade plånboksinstansens integritet och det klockslag som anges i headerparametern ”exp” i det utfärdade plånboksinstansintyget vara mindre än 24 timmar.

— TR-WIA-2.2: Plånbokstillhandahållaren ska säkerställa att en plånboksenhet innehåller de plånboksinstansintyg som krävs för utfärdande av personidentifieringsuppgifter och elektroniska attributsintyg.

— TR-WIA-3: Vid utfärdande ska en plånboksenhet skicka ett plånboksinstansintyg till auktoriseringsservern i den pushade auktoriseringsbegäran och i tokenbegäran enligt OID4VCI.

— TR-WIA-3.1: En plånboksenhet ska skicka plånboksinstansintyget tillsammans med ett Proof-of-Possession (PoP) enligt bilaga E i OID4VCI.

— TR-WIA-3.2: En plånboksenhet ska skicka samma plånboksinstansintyg till endast en auktoriseringsserver.

([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: Om en plånbokstillhandahållare använder alternativet ”per-issuer reuse” enligt R_WIA_1 nedan får en plånboksenhet skicka ett plånboksinstansintyg till samma auktoriseringsserver flera gånger.

— TR-WIA-3.2.2: Om plånbokstillhandahållaren inte använder alternativet ”per-issuer reuse” ska en plånboksenhet använda ett plånboksinstansintyg i högst en utfärdandeprocess.

— TR-WIA-4: Om en auktoriseringsserver mottar ett plånboksinstansintyg ska den verifiera signaturen för plånboksinstansintyget genom att använda den publika nyckeln i signeringscertifikatet som ingår i parametern ”x5c” i JOSE-headern för plånboksinstansintyget.

— TR-WIA-4.1: Auktoriseringsservern ska även verifiera att detta signeringscertifikat kan verifieras med ett tillitsankare i förteckningen över plånbokstillhandahållare som avses i artikel 5 i genomförandeförordning (EU) 2024/2980, eventuellt med hjälp av mellanliggande certifikat som ingår i x5c-parametern.

— TR-WIA-4.2: Auktoriseringsservern ska verifiera att plånboksinstansintyget inte har upphört att gälla.

— TR-WIA-4.3: Auktoriseringsservern ska verifiera signaturen för PoP med den publika nyckel som finns i anspråket ”cnf”.

— TR_KA-1: En plånboksenhet ska använda ett nyckelintyg vid utfärdande av personidentifieringsuppgifter och vid utfärdande av enhetsbundna kvalificerade eller icke-kvalificerade elektroniska attributsintyg, eller elektroniska attributsintyg som tillhandahålls av ett offentligt organ som ansvarar för en autentisk källa eller för dess räkning.

— TR_KA-1.1: En plånboksenhet får inte använda ett nyckelintyg vid utfärdande av icke enhetsbundna kvalificerade eller icke-kvalificerade elektroniska attributsintyg, eller elektroniska attributsintyg som tillhandahålls av ett offentligt organ som ansvarar för en autentisk källa eller för dess räkning.

— TR_KA-2: En plånbokstillhandahållare ska tillhandahålla en plånboksenhet med olika nyckelintyg för WSCD i plånboksenheten och för vart och ett av dess nyckellager.

— TR_KA-2.1: Plånbokstillhandahållaren ska underteckna eller stämpla ett nyckelintyg efter att ha verifierat att de nycklar som intygas i nyckelintyget lagras i WSCD i plånboksenheten eller i det nyckellager som beskrivs i nyckelintyget.

— TR_KA-2.2: Ett nyckelintyg ska innehålla minst en intygad publik nyckel. Antalet nycklar i det nyckelintyg som skickas till en utfärdare av intygsuppgifter får inte överstiga den maximala partistorlek som anges av den utfärdaren i dess metadata för utfärdare av intygsuppgifter. Se ETSI TS 119 472-3 ([3]), parametern ”credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size”.

— TR_KA-2.3: En plånbokstillhandahållare ska inkludera en publik nyckel (som motsvarar en privat nyckel som är lagrad i plånboksenhetens WSCD eller nyckellager) i högst ett nyckelintyg.

— TR_KA-2.4: En plånboksenhet ska använda ett nyckelintyg under högst en process för utfärdande eller återutfärdande av intygsuppgifter.

— TR_KA-2.5: En plånbokstillhandahållare ska säkerställa att en plånboksenhet innehar nyckelintyg efter behov för utfärdande av personidentifieringsuppgifter och enhetsbundna elektroniska attributsintyg.

([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, mars 2026.

— TR_KA-3: Vid behov under utfärdandet ska en plånboksenhet inkludera ett nyckelintyg i fältet ”proofs” i en begäran om autentisering till utfärdaren av behörighetsuppgifter enligt OID4VCI, i ett bevis av antingen typen ”jwt” eller ”attestation”.

— TR_KA_3.1: Om en plånboksenhet inkluderar ett nyckelintyg i ett ”jwt”-element ska den underteckna eller stämpla nyckelintyget med den privata nyckel som motsvarar den publika nyckeln vid index 0 i ”attested_keys”-arrayen i ”key_attestation”-objektet.

— TR_KA-4: Om en utfärdare av behörighetsuppgifter utfärdar enhetsbundna behörighetsuppgifter ska utfärdaren i parametern ”proof_types_supported” i sina metadata för utfärdare av behörighetsuppgifter, enligt avsnitt 12.2.4 i OID4VCI, ange att den stöder både bevistypen ”jwt” och bevistypen ”attestation” för nyckelintyg som ska inkludera objektet ”key_attestations_required”.

— TR_KA-4.1: Om en utfärdare av behörighetsuppgifter utfärdar behörighetsuppgifter som inte är enhetsbundna ska utfärdaren utelämna parametrarna ”proof_types_supported” och ”cryptographic_binding_methods_supported” i metadata för utfärdare av behörighetsuppgifter.

— TR_KA-5: Om en utfärdare av behörighetsuppgifter tar emot ett nyckelintyg i bevistypen ”jwt” eller ”attestation”, ska utfärdaren verifiera nyckelintygets underskrift med hjälp av den publika nyckeln i det signeringscertifikat som ingår i parametern ”x5c” i JOSE-headern för nyckelintyget samt verifiera att detta signeringscertifikat kan verifieras med ett tillitsankare i den förteckning över plånbokstillhandahållare som avses i artikel 5 i genomförandeförordning (EU) 2024/2980, eventuellt med hjälp av mellanliggande certifikat som ingår i parametern ”x5c”.

— TR_KA-6: Om en utfärdare av behörighetsuppgifter tar emot ett nyckelintyg i bevistypen ”jwt”, ska utfärdaren verifiera underskriften för ”jwt”-elementet med hjälp av nyckeln vid index 0 i ”attested_keys”-arrayen i ”key_attestation”-objektet som ingår i ”jwt”-elementet.

— TR_KA-6.1: Utfärdaren av behörighetsuppgifter ska verifiera att fältet ”nonce” i ”jwt”-elementet innehåller ett giltigt c_nonce från utfärdarens nonce_endpoint enligt OID4VCI.

— TR_KA-7: Om en utfärdare av behörighetsuppgifter tar emot ett nyckelintyg i ett bevis av typen ”attestation” ska utfärdaren verifiera att ”key_attestation”-objektet innehåller ett giltigt c_nonce från utfärdarens nonce_endpoint.

— TR_KA-8: En tillhandahållare av personidentifieringsuppgifter ska säkerställa att personidentifieringsuppgifter är bundna till en publik nyckel som härrör från ett nyckelintyg som hänvisar till ett WSCD.

(c) Innehållskrav

— C_WIA-1: Ett plånboksinstansintyg ska innehålla följande:

— ”wallet_name”-anspråket enligt bilaga E till OID4VCI, där värdet ska vara identifieraren för den plånbokslösning som återfinns i förteckningen över plånbokstillhandahållare som avses i artikel 5 i genomförandeförordning (EU) 2024/2980.

— Ett ”wallet_version”-anspråk ([4]), som ska vara en sträng vars värde ska vara versionen av plånbokslösningen.

— Ett ”wallet_solution_certification_information”-anspråk, som ska vara ett JSON-objekt som innehåller information om det organ för bedömning av överensstämmelse som certifierade plånbokslösningen, certifieringsnumret i tillämpliga fall samt andra relevanta uppgifter om certifieringen.

([4]) Detta anspråk definieras i detta K/I-tal eftersom det inte ingår i OID4VCI-specifikationen.

— Ett ”client_status”-anspråk som innehåller två underfält:

— ”status”: En referens till en statuslista enligt bilaga E till OID4VCI som representerar återkallelsestatusen för plånboksinstansen. Se avsnitt (e) nedan för närmare uppgifter.

— ”exp”: Ett ”NumericDate” enligt RFC 7519, som anger det klockslag fram till vilket plånbokstillhandahållaren upprätthåller återkallelsestatusen i det statuslistindex som anges i ”status”.

— ”exp”-anspråket enligt bilaga E till OID4VCI.

— ANMÄRKNING: ”client_status.status”-anspråket i ett plånboksinstansintyg representerar återkallelsestatusen för plånboksinstansen och inte återkallelsestatusen för själva intyget. Enligt vad som beskrivs i R_WIA-1 nedan kan en plånbokstillhandahållare välja att begränsa varje plånboksinstansintyg till en specifik auktoriseringsserver baserat på att alla intyg som skickas till den servern innehåller samma indexvärde i posten ”client_status.status”.

— ANMÄRKNING: Värdet ”idx” i anspråket ”status” kan användas som en (parvis) unik identifierare för plånboksinstansen och plånboksenheten.

— C_WIA-2: Ett plånboksinstansintyg ska även innehålla anspråket ”wallet_link” enligt bilaga E till OID4VCI, och värdet av detta anspråk ska vara en URI där ytterligare information om plånbokslösningen kan erhållas.

— C_WIA-3: En auktoriseringsserver får inte tolka parametern ”exp” på översta nivån i ett plånboksinstansintyg som slutet på den period under vilken återkallelsestatusen för plånboksinstansen upprätthålls.

— ANMÄRKNING: Parametern ”exp” på översta nivån i ett plånboksinstansintyg anger när själva intyget upphör att gälla.

— C_KA-1: Ett nyckelintyg ska innehålla följande:

— Anspråken ”key_storage” och ”user_authentication” enligt bilaga D till OID4VCI.

— Attributen ”key_storage” och ”user_authentication” ska ha värdet ”iso_18045_high” när ett nyckelintyg hänvisar till ett WSCD,

— Anspråket ”certification” enligt bilaga D till OID4VCI, som innehåller en URL där information om den certifiering som uppnåtts av WSCD eller nyckellagret kan erhållas, exempelvis schema såsom Common Criteria eller GlobalPlatform, de utvärderade kraven såsom tillämplig skyddsprofil samt utvärderingsnivån.

— Det ska vara möjligt att utifrån denna information fastställa om nyckellagringen är ett WSCD.

— Ett ”key_storage_status”-anspråk som innehåller två underfält:

— ”status”: en referens till en statuslista enligt bilaga D.1 till OID4VCI. Värdet representerar antingen återkallelsestatusen för den typ av WSCD eller nyckellager som används för att lagra de intygade nycklarna eller – vid alternativet med index per-key-attestation – återkallelsestatusen för en enskild plånboksenhets WSCD eller nyckellager. Se R_KA_1 nedan för tillgängliga alternativ för indextilldelning.

— ”exp”: Ett ”NumericDate” enligt RFC 7519, som anger det klockslag fram till vilket plånbokstillhandahållaren upprätthåller återkallelsestatusen i det statuslistindex som anges i ”status”.

— ”exp”-anspråket enligt bilaga D till OID4VCI.

— ANMÄRKNING om värdet ”idx” i anspråket ”key_storage_status.status” i ett nyckelintyg: Om plånbokstillhandahållaren använder alternativet ”type-shared index” (se R_KA_1 nedan) delar alla nyckelintyg för samma typ av WSCD eller nyckellager samma statuslistindex. Därför är värdet ”idx” inte unikt per plånboksenhet. Om plånbokstillhandahållaren i stället använder alternativet ”per-key-attestation index” är värdet ”idx” unikt för plånboksenheten (eller parvis unikt per utfärdare av behörighetsuppgifter). I samtliga fall får dock inte en utfärdare av behörighetsuppgifter använda värdet ”idx” i ett nyckelintyg som identifierare för plånboksenheten utan ska i stället använda värdet ”idx” i ett plånboksinstansintyg.

— C_KA-2: Om ett nyckelintyg skickas i ett bevis av typen ”attestation” ska det även innehålla ett giltigt ”c_nonce” enligt bilaga F.3 till OID4VCI.

— C_KA-3: En utfärdare av behörighetsuppgifter får inte tolka parametern ”exp” på översta nivån i ett nyckelintyg som slutet på perioden för upprätthållande av återkallelsestatusen för WSCD eller nyckellagret.

— ANMÄRKNING: Parametern ”exp” på översta nivån i ett nyckelintyg anger när själva nyckelintyget upphör att gälla.

(d) Livscykelkrav

— I denna bilaga specificeras följande parametrar för metadata för utfärdare av intygsuppgifter:

— ”preferred_client_status_period”: OPTIONAL. Ett heltal som anger den föredragna återstående perioden för upprätthållande av status för plånboksinstansintyget som ska presenteras av plånboksenheten vid utfärdande, i sekunder. Den återstående perioden för upprätthållande av status definieras som värdet av ”client_status.exp” i intyget minus klockslaget för mottagandet av intyget.

— ”preferred_key_storage_status_period”: OPTIONAL. Ett heltal som anger den föredragna återstående perioden för upprätthållande av status för nyckelintyget som ska presenteras av plånboksenheten vid utfärdande, i sekunder. Den återstående perioden för upprätthållande av status definieras som värdet ”key_storage_status.exp” i intyget minus klockslaget för mottagandet av intyget.

— LC_WIA-1: En auktoriseringsserver får kommunicera sina preferenser för den återstående perioden för upprätthållande av status i plånboksinstansintyg genom att inkludera metadataparametern ”preferred_client_status_period” i sin slutnod för metadata för utfärdare av behörighetsuppgifter enligt avsnitt 12.2.2 i OID4VCI.

— LC_WIA-1.1: Detta fält ska placeras på översta nivån i metadata för utfärdare av behörighetsuppgifter.

— LC_WIA_2: En auktoriseringsserver får inte tolka parametern ”exp” på översta nivån i ett plånboksinstansintyg som slutet på den period under vilken återkallelsestatusen för plånboksinstansen upprätthålls.

— LC_WIA_3: Om en plånbokstillhandahållare undertecknar eller stämplar ett plånboksinstansintyg ska plånbokstillhandahållaren upprätthålla återkallelsestatusen för den relevanta plånboksinstansen fram till dess att ”wallet_instance_status.exp” som anges i plånboksinstansintyget har löpt ut.

— LC_KA-1: Om ett nyckelintyg behövs får en utfärdare av behörighetsuppgifter kommunicera sina preferenser för den återstående perioden för upprätthållande av status i nyckelintyg genom att inkludera metadataparametern ”preferred_key_storage_status_period” som anges ovan i sin slutnod för metadata för utfärdare av behörighetsuppgifter enligt avsnitt 12.2.2 i OID4VCI.

— LC_KA-1.1: Detta fält ska placeras i objektet ”key_attestations_required” enligt avsnitt 12.2.4 i OID4VCI.

— LC_KA-2: En plånbokstillhandahållare ska fastställa den tekniska giltighetsperioden för de nyckelintyg som den utfärdar.

— LC_KA-3: Om en plånbokstillhandahållare undertecknar eller stämplar ett nyckelintyg ska plånbokstillhandahållaren upprätthålla återkallelsestatusen för det relevanta WSCD eller nyckellagret fram till dess att ”key_storage_status.exp” som anges i nyckelintyget har löpt ut.

— LC_GEN-1: En plånbokstillhandahållare ska säkerställa att en plånboksenhet alltid kan presentera plånboksenhetsintyg och nyckelintyg vars ”client_status.exp” respektive ”key_storage_status.exp” ligger minst 31 dagar fram i tiden vid tidpunkten för presentation till en auktoriseringsserver eller en utfärdare av behörighetsuppgifter.

— *ANMÄRKNING*: Detta säkerställer att tillhandahållare av personidentifieringsuppgifter kan förlita sig på en återkallelsekedja utan att tvingas utfärda kortlivade personidentifieringsuppgifter.

— LC_GEN-2: En plånbokstillhandahållare ska säkerställa att en plånboksenhet hämtar metadata för utfärdare av intygsuppgifter under utfärdandet.

  — LC_GEN_2.1: Om fältet ”preferred_key_storage_status_period” ingår i dessa metadata ska plånboksenheten skicka ett nyckelintyg där (”key_storage_status.exp” - aktuellt klockslag) - ”preferred_key_storage_status_duration” är så litet som möjligt men inte negativt. Om ett sådant nyckelintyg inte är tillgängligt för plånboksenheten ska plånboksenheten inhämta ett nytt nyckelintyg från plånbokstillhandahållaren som uppfyller att ”key_storage_status.exp” - aktuellt klockslag ≥ ”preferred_key_storage_status_period”.

  — LC_GEN_2.2: Om fältet ”preferred_client_status_period” ingår i dessa metadata ska plånboksenheten skicka ett plånboksinstansintyg där (”client_status.exp” - aktuellt klockslag) - ”preferred_client_status_period” är så litet som möjligt men inte negativt. Om ett sådant plånboksinstansintyg inte är tillgängligt för plånboksenheten ska plånboksenheten begära ett nytt plånboksinstansintyg från plånbokstillhandahållaren som uppfyller att ”client_status.exp” - aktuellt klockslag ≥ ”preferred_client_status_period”.

— LC_GEN-3: Den tekniska giltighetsperioden för personidentifieringsuppgifter ska löpa ut före både ”client_status.exp” i plånboksinstansintyget och ”key_storage_status.exp” i det nyckelintyg som skickas till tillhandahållaren av personidentifieringsuppgifter i utfärdandeprocessen.

— LC_GEN-4: En tillhandahållare av personidentifieringsuppgifter med en teknisk giltighetsperiod som överstiger 24 timmar ska kontrollera återkallelsestatusen för både plånboksinstansintyget och nyckelintyget som mottogs vid utfärdandet minst en gång var 24:e timme under den tekniska giltighetsperioden för personidentifieringsuppgifterna. Om någon av dessa har återkallats ska tillhandahållaren återkalla personidentifieringsuppgifterna.

(e) Återkallelsekrav

— R_GEN-1: En plånbokstillhandahållare ska använda Token Status Lists (enligt IETF Token Status List) som återkallelsemekanism för både nyckelintyg och plånboksinstansintyg enligt bilagorna D respektive E till OID4VCI.

— ANMÄRKNING: För att förbättra skalbarheten hos sina statuslistor kan en plånbokstillhandahållare använda följande optimeringar:

  — dela upp statuslistan i flera delar, om plånbokstillhandahållarna har ett stort antal användare och utfärdade intyg, använda olika uppdelningsstrategier, t.ex. baserade på fast storlek eller tidsperiod, välja uppdelningsstrategi efter eget gottfinnande med hänsyn till t.ex. nedladdningsstorlek och användarnas integritet,

  — använda flera statuslistor,

  — komprimera en statuslista för att minska dess storlek.

— R_WIA-1: En plånbokstillhandahållare får tilldela samma värde till anspråket ”idx” i anspråket ”client_status.status” i alla plånboksinstansintyg som en viss plånboksenhet presenterar för samma auktoriseringsserver. Detta kallas alternativet ”per-issuer reuse”. Om detta alternativ används:

  — R_WIA-1.1: Plånboksenheten ska upprätthålla status för vilket indexvärde den har använt för varje auktoriseringsserver som den tidigare har interagerat med, och ska begära ett plånboksinstansintyg som innehåller samma indexvärde när den interagerar med samma auktoriseringsserver igen.

  — R_WIA-1.2: Om en plånbokstillhandahållare tar emot en begäran om ett plånboksinstansintyg som innehåller ett specifikt indexvärde ska den verifiera att den begärande plånboksenheten tidigare har tilldelats detta indexvärde innan den utfärdar ett nytt plånboksinstansintyg med detta indexvärde.

  — R_WIA-1.3: Plånboksenheten får inte återanvända samma indexvärde vid interaktioner med olika auktoriseringsservrar.

— ANMÄRKNING: Om alternativet ”per-issuer reuse” används kommer plånbokstillhandahållaren att kunna fastställa hur många auktoriseringsservrar en plånboksenhet har varit i kontakt med och hur ofta den interagerar med var och en av dem.

— R_WIA-2: I sin integritetspolicy ska en plånbokstillhandahållare dokumentera om plånbokstillhandahållaren använder alternativet ”per-issuer reuse” för återkallelse av plånboksinstanser.

— R_WIA-3: Om en plånbokstillhandahållare inte använder alternativet ”per-issuer reuse” ska plånbokstillhandahållaren tilldela ett nytt, olänkbart indexvärde till varje plånboksinstansintyg som den utfärdar.

— R_WIA-4: Om en plånboksenhet måste återkallas ska en plånbokstillhandahållare återkalla indexvärdena i anspråket ”client_status.status” i alla plånboksinstansintyg som är kopplade till den plånboksenheten.

— R_WIA-5: En plånbokstillhandahållare ska beakta omfattningen av dess utplacering och den underliggande arkitekturen när den fastställer storleken på sina statuslistor för plånboksinstansintyg, och säkerställa att dessa är tillräckligt stora för att förhindra korrelation och skydda användarnas integritet. Som minimum ska en statuslista, där så är möjligt, omfatta minst 10 000 intyg.

— R_KA_1: En plånbokstillhandahållare ska välja ett av följande alternativ för indextilldelning i anspråket ”key_storage_status.status” i ett nyckelintyg:

  — Alternativ 1, benämnt ”type-shared index”, där alla nyckelintyg som intygar nycklar som lagras i samma typ av WSCD eller nyckellager innehåller samma indexvärde i ”key_storage_status.status”.

  — Alternativ 2, benämnt ”per-key-attestion index”, där ett nyckelintyg som intygar nycklar som lagras i ett enskilt WSCD eller nyckellager innehåller ett (parvist) unikt indexvärde i ”key_storage_status.status”.

— ANMÄRKNING: Om en plånbokstillhandahållare använder alternativ 1 leder en enda återkallelseåtgärd till att alla nyckelintyg av den berörda typen ogiltigförklaras i samtliga plånboksenheter. Eftersom alla nyckelintyg för samma typ av WSCD eller nyckellager delar ett och samma statuslistindex återspeglar dessutom antalet poster i en statuslista för nyckelintyg antalet typer av WSCD eller nyckellager som stöds av plånbokstillhandahållaren – inte antalet distribuerade plånboksenheter. De integritetsöverväganden som ligger till grund för minimistorleken på statuslistor för plånboksinstanser är därför inte tillämpliga på statuslistor för nyckelintyg enligt alternativ 1, förutsatt att det finns ett tillräckligt stort antal plånboksenheter som använder samma typ av WSCD eller nyckellager.

— ANMÄRKNING: Om en plånbokstillhandahållare använder alternativ 2 representerar varje index återkallelsestatusen för det specifika WSCD eller nyckellager som intygas i det aktuella nyckelintyget.

— ANMÄRKNING: Om en plånbokstillhandahållare använder alternativ 2 kan ett specifikt WSCD eller nyckellager även återkallas på begäran av användaren.

— R_KA-2: Om en plånbokstillhandahållare använder alternativ 2 får plånbokstillhandahållaren använda alternativet ”per-issuer reuse” som beskrivs i R_WIA-1. Om plånbokstillhandahållaren använder detta alternativ ska kraven R_WIA-1–R_WIA-3 gälla i tillämpliga delar.

— R_KA-3: Om en plånbokstillhandahållare använder alternativ 2 ska den beakta omfattningen av dess utplacering och den underliggande arkitekturen när den fastställer storleken på sina statuslistor för nyckelintyg, och säkerställa att dessa är tillräckligt stora för att förhindra korrelation och skydda användarnas integritet. Som minimum ska en statuslista, där så är möjligt, omfatta minst 10 000 nyckelintyg.

— R_KA-4: Om en plånbokstillhandahållare använder alternativ 1 (type-shared index) ska plånbokstillhandahållaren återkalla en post i ”key_storage_status.status” endast om typen av WSCD eller nyckellager har en säkerhetssårbarhet.

(f) Krav avseende signaturalgoritmer

— SA-1: För undertecknande av plånboksinstansintyg, nyckelintyg, tillhörande bevis på innehav av privat nyckel samt Token Status List ska en av följande algoritmer användas:

— ES256 (ECDSA med SHA-256 och P-256)

— ES384 (ECDSA med SHA-384 och P-384)

— ES512 (ECDSA med SHA-512 och P-521)

— SA-2: En plånbokstillhandahållare ska välja vilken av de algoritmer som anges i SA-1 som ska användas.

— SA-3: En auktoriseringsserver eller en utfärdare av behörighetsuppgifter (enligt OID4VCI) ska stödja samtliga algoritmer som anges i SA-1.”

BILAGA IV

”BILAGA II

Förteckning över standarder som avses i artikel 8

De tekniska specifikationer som anges i avsnitten 2–6 i ETSI TS 119 472-1 V1.2.1 (2026-02) ska tillämpas. De ska läsas tillsammans med följande anpassningar:

(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: När ett statuselement används för personidentifieringsuppgifter, kvalificerade elektroniska attributsintyg eller elektroniska attributsintyg som tillhandahålls av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa ska det endast ange om intyget är återkallat eller inte återkallat och får inte stödja några andra statusvärden, såsom tillfälligt upphävande.

— EAA-4.2.11.1-06.1: Om ett intyg återkallas ska det vara permanent återkallat.

(3) 4.2.13 EAA short-lived

— EAA-4.2.13-03: Om elektroniska attributsintyg med kort giltighetstid (en giltighetsperiod på högst 24 timmar) utfärdas krävs ingen återkallelse.

(4) 4.6.3 Krav för EU EAA utfärdat av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa (PuB-EAA)

— PuB-EAA-4.6.2-03: void.

— Pub-EAA-4.6.2-04: void.

— PuB-EAA-4.6.3-03: PuB-EAA:s digitala signatur ska innehålla det kvalificerade certifikat som stöder PuB-EAA:s digitala signatur.

— PuB-EAA-4.6.3-04: Det kvalificerade certifikat som stöder PuB-EAA:s digitala signatur ska uppfylla kraven i klausul 8 i ETSI TS 119 412-6 v1.1.1 och ska innehålla QcType qcStatement enligt definitionen i ETSI EN 319 412-5 v2.5.1, med värdet id-etsi-qct-eidaspsbeaa definierat enligt följande:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } -- certifikat som avses i artikel 45f.1 b och som stöder det offentliga organets kvalificerade elektroniska signatur eller kvalificerade elektroniska stämpel enligt artikel 3.46 i förordning (EU) nr 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: Statuselementet kan innehålla status_list-elementet i enlighet med avsnitt 6.2 i 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: När ett elektroniskt attributsintyg som överensstämmer med ISO/IEC mdoc använder mekanismen med intygsstatuslista enligt EAA-6.2.10.1-02.2 eller mekanismen med intygsåterkallelselista enligt EAA-6.2.10.1-02.3 ska det elektroniska attributsintygets Mobile Security Object (MSO) innehålla statusstrukturen enligt EAA-6.2.10.1-17, som innehåller återkallelseinformation för MSO.

— EAA-6.2.10.1-01.1: Vid implementering av mekanismen med identifierarlista ska statuselementet innehålla elementet identifier_list enligt EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: Vid implementering av mekanismen med statuslista ska statuselementet innehålla elementet status_list enligt EAA-6.2.10.1-13.

— *ANMÄRKNING:*

  — Statusstrukturen innehåller en hänvisning till en återkallelselista för MSO.

  — Återkallelselistan för MSO är en COSE_Sign1-struktur som anger om ett visst MSO har återkallats eller inte.

  — Statusstrukturen innehåller all information som krävs för att den förlitande parten ska kunna fastställa om återkallelselistan för MSO är autentisk.

— EAA-6.2.10.1-02: Tillhandahållaren av personidentifieringsuppgifter, tillhandahållaren av kvalificerade elektroniska attributsintyg eller tillhandahållaren av elektroniska attributsintyg som tillhandahålls av eller på uppdrag av ett offentligt organ med ansvar för en autentisk källa ska använda en av följande metoder för återkallelse av personidentifieringsuppgifter, kvalificerade elektroniska attributsintyg eller elektroniska attributsintyg som tillhandahålls av eller på uppdrag av ett offentligt organ med ansvar för en autentisk källa:

— EAA-6.2.10.1-02.1: Om de utfärdar elektroniska attributsintyg med kort giltighetstid som har en giltighetsperiod på högst 24 timmar ska återkallelse inte krävas.

— EAA-6.2.10.1-02.2: Använd en mekanism med intygsstatuslista för att koda återkallelseinformationen som en statuslista.

— EAA-6.2.10.1-02.2.1: Mekanismen med statuslista återkallar ett MSO baserat på om biten i den av utfärdaren definierade bitpositionen i MSO har värdet sant i statuslistan.

— EAA-6.2.10.1-02.2.2: Mekanismen med statuslista specificeras i specifikationen för Token Status List (draft-ietf-oauth-status-list-20).

— EAA-6.2.10.1-02.3: Använd en mekanism med intygsåterkallelselista för att koda återkallelseinformationen som en identifierarlista.

— EAA-6.2.10.1-02.3.1: Mekanismen med identifierarlista återkallar ett MSO baserat på om den av utfärdaren definierade identifieraren i MSO finns i identifierarlistan.

— 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 och EAA-6.2.10.1-11 specificerar mekanismen med identifierarlista baserat på kraven i specifikationen för Token Status List, inklusive det som är gemensamt för mekanismerna med statuslista och identifierarlista.

— EAA-6.2.10.1-03: När statuselementet används för personidentifieringsuppgifter, kvalificerade elektroniska attributsintyg eller elektroniska attributsintyg som tillhandahålls av eller på uppdrag av ett offentligt organ med ansvar för en autentisk källa ska uteslutande statusen ”revoked” användas.

— EAA-6.2.10.1-03.1: För en statuslista innebär detta att endast värdena ”valid” och ”invalid”, enligt specifikationen för Token Status List, ska användas.

— EAA-6.2.10.1-03.2: För identifierarlistan ska endast återkallade MSO, till skillnad från tillfälligt upphävda MSO, föras upp på identifierarlistan.

— EAA-6.2.10.1-04: Om ett MSO återkallas ska MSO återkallas permanent.

— EAA-6.2.10.1-05: Verifiering av återkallelselistan för MSO är frivillig för den förlitande parten och ska i tillämpliga fall uppfylla verifieringskraven i specifikationen för Token Status List och statusstrukturspecifikationen i EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: Om en förlitande part behöver kunna verifiera återkallelsestatusen för personidentifieringsuppgifter eller elektroniska attributsintyg ska den stödja både mekanismen med intygsstatuslista och mekanismen med intygsåterkallelselista enligt EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: identifier_list och status_list i MSO får innehålla certifikatelementet.

— EAA-6.2.10.1-06.1: Om certifikatelementet förekommer ska det innehålla ett certifikat som innehåller den publika nyckel som undertecknade eller stämplade det överordnade certifikatet i x5chain-elementet i strukturen för återkallelselistan för MSO.

— EAA-6.2.10.1-06.1.1: Instansen av förlitande part ska använda det certifikatet som tillitsankare för verifieringen av x5chain-elementet i strukturen för återkallelselistan för MSO.

— EAA-6.2.10.1-06.2: Om certifikatelementet inte förekommer ska det överordnade certifikatet i x5chain-elementet i strukturen för återkallelselistan för MSO undertecknas eller stämplas med det certifikat som används för att underteckna certifikatet i x5chain-elementet i MSO.

— EAA-6.2.10.1-06.2.1: Instansen av förlitande part ska använda det certifikatet som tillitsankare för verifieringen av x5chain-elementet i strukturen för återkallelselistan för MSO.

— EAA-6.2.10.1-07: En återkallelselista för MSO ska implementeras i enlighet med specifikationen för Token Status List som en status list-token i CWT-format.

— EAA-6.2.10.1-08: För återkallelselistan för MSO för mekanismen med identifierarlista och statuslista gäller följande krav:

  — anspråket exp ska finnas.

  — anspråket ttl får finnas.

  — anspråket aggregation_uri i anspråket IdentifierList eller StatusList får finnas, och tillhandahållaren av personidentifieringsuppgifter, tillhandahållaren av kvalificerade elektroniska attributsintyg eller tillhanda-

hållaren av elektroniska attributsintyg som tillhandahålls av eller på uppdrag av ett offentligt organ med ansvar för en autentisk källa får använda anspråket aggregation_uri för att ange stöd för aggregeringsmekanismen enligt specifikationen för Token Status List.

— CWT ska vara ett COSE_Sign1-objekt som använder någon av följande signaturalgoritmer för att beräkna underskriften:

(a) ”ES256” (ECDSA med kurvan NIST P-256 och SHA-256),

(b) ”ES384” (ECDSA med kurvan NIST P-384 och SHA-384),

(c) ”ES512” (ECDSA med kurvan NIST P-521 och SHA-512),

(d) ”ESB256” (ECDSA med kurvan brainpoolP256r1 och SHA-256),

(e) ”ESB384” (ECDSA med kurvan brainpoolP384r1 och SHA-384),

(f) ”ESB512” (ECDSA med kurvan brainpoolP512r1 och SHA-512),

— CWT ska innehålla x5chain i det skyddade headerfältet, som innehåller certifikatet eller certifikatkedjan för verifiering av underskriften för återkallelselistan för MSO.

— Den utökade nyckelanvändningen för objektidentifieraren som anges i specifikationen för Token Status List får användas för signeringscertifikatet för statuslistan och identifierarlistan, och instanser av förlitande part får stödja den utökade nyckelanvändningen av objektidentifierare som anges i specifikationen för Token Status List. För objektidentifieraren ska tillhandahållaren av kvalificerade elektroniska attributsintyg eller tillhandahållaren av elektroniska attributsintyg som tillhandahålls av eller på uppdrag av ett offentligt organ inte göra fältet för utökad nyckelanvändning kritiskt när OID för utökad nyckelanvändning enligt specifikationen för Token Status List används.

— EAA-6.2.10.1-09: Med avvikelse från kraven i specifikationen för Token Status List gäller följande krav för mekanismen med identifierarlista:

— värdet för anspråket type ska vara ”application/identifierlist+cwt”,

— anspråket StatusList får inte finnas i CWT-anspråksuppsättningen,

— strukturen IdentifierList som definieras i EAA-6.2.10.1-11 ska finnas som ett anspråk i CWT-anspråksuppsättningen med nyckeln 65530.

— EAA-6.2.10.1-10: Strukturen IdentifierList ska vara en CBOR-struktur med följande 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: Om identifieraren finns i IdentifierList är den MSO som innehåller identifieraren i statuselementet återkallad.

— EAA-6.2.10.1-10.2: Anspråket Aggregation_uri specificeras i avsnitt 9.2 i specifikationen för Token Status List.

— EAA-6.2.10.1-10.3: Innehållstypen för identifierarlistan ska vara ”application/identifierlist+cwt” enligt kraven i avsnitt 8.2 i specifikationen för Token Status List.

— EAA-6.2.10.1-11: Följande krav gäller för elementet identifier_list i MSO (se EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: Elementet identifier_list är en CBOR-struktur med följande CDDL:

```
IdentifierListInfo = {

        'id': Identifier ,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2,10.1-11,2: REV-11.2: För att förhindra att identifieraren används som korrelation mellan presentationer ska den vara unik per MSO.

— EAA-6.2,10.1-12: Följande krav gäller för statuslistan:

  — EAA-6.2.10.1-12.1: Elementet bits i strukturen StatusList ska sättas till 1.

— EAA-6.2.10.1-13: Följande krav gäller för elementet status_list i MSO (se EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: Elementet status_list ska följa kraven för strukturen StatusListInfo enligt specifikationen för Token Status List, och det valfria elementet certificate som definieras i EAA-6.2.10.1-06 ska läggas till.

  — EAA-6.2.10.1-13.2: För att förhindra att statusindexet används som korrelation mellan presentationer ska kombinationen av statusindex och URI vara unik per MSO.

— EAA-6.2.10.1-14: Plånbokstillhandahållaren ska använda den andra (EAA-6.2.10.1-02.2) eller den tredje (EAA-6.2.10.1-02.3) av de metoder som anges i EAA-6.2.10.1-02 för återkallelse av ett plånboksinstansintyg (WIA) och för återkallelse av ett nyckelintyg (KA).

— EAA-6.2.10.1-15: Plånbokstillhandahållaren ska implementera de mekanismer för återkallelse av intyg som anges i EAA-6.2.10.1-02 i sin plånbokslösning.

— EAA-6.2.10.1-16: Tillhandahållaren av personidentifieringsuppgifter och tillhandahållaren av elektroniska attributsintyg ska stödja både mekanismen med intygsstatuslista och mekanismen med intygsåterkallelselista som anges i EAA-6.2.10.1-02 för verifiering av återkallelsestatusen för ett plånboksinstansintyg (WIA) och för ett nyckelintyg (KA).

— EAA-6.2.10.1-17: Statusstrukturen i MSO ska vara en CBOR-struktur med följande CDDL:

Status = {

? 'identifier_list' : IdentifierListInfo,

? 'status_list' : StatusListInfo,

* tstr => RFU

}”

BILAGA V

”BILAGA III

Tekniska specifikationer som avses i artikel 10

— Tekniska specifikationer:

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

BILAGA VI

Bilaga IV till genomförandeförorning (EU) 2024/2979 ska ändras på följande sätt:

(1) Punkt 1 ska ersättas med följande:

”1. Format för obligatorisk underskrift eller stämpel:

a) PAdES (PDF Advanced Electronic Signature) enligt ETSI EN 319 142-1 V1.2.1 (2024-01). Elektroniska underskrifter och infrastrukturer (Electronic Signatures and Infrastructures, ESI). PAdES digital signatures; Del 1: Building blocks and PAdES baseline signatures.”,

(2) Punkt 3 ska ersättas med följande:

”3. Gränssnitt för tillämpningsprogram:
ETSI TS 119 432 v1.3.1 (2026-03) avsnitten 6.4.3, A.6, A.7 och A.8.”.

BILAGA VII

”BILAGA VI

EU:s förtroendemärke för digitala identitetsplånböcker i färg



”

BILAGA VIII

”BILAGA VII

EU:s förtroendemärke för digitala identitetsplånböcker i svartvitt



”

BILAGA IX

”BILAGA VIII

Data för EU:s förtroendemärke för digitala identitetsplånböcker

Uppgifter	Beskrivning	Kodning	Status
TrustMarkResourceURL	URL till grafiken för EU:s förtroendemärke för digitala identitetsplånböcker och resurser med användarinformation i plånbokens användargränssnitt.	URL	Obligatorisk
ListOfCertifiedWalletsURL	URL till den offentliga listan över certifierade plånbokslösningar i EU enligt kommissionens genomförandeförordning (EU) 2025/849 ([1]).	URL	Obligatorisk
ListOfCertifiedWalletsQRCode	QR-kod som innehåller informationen i ListOfCertifiedWalletsURL.	ISO-8859-1 Byte mode QR code	Valfri
WalletSolutionInfoPageURL	URL till informationssidan för den certifierade plånbokslösningen i listan över certifierade plånbokslösningar, baserad på ListOfCertifiedWalletsURL med tillägget”?” och identifieraren WalletSolutionID för plånbokslösningen.	URL	Obligatorisk
WalletSolutionInfoPageQRCode	QR-kod som innehåller informationen i WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	Valfri
WalletVerifierToolURL*	URL som pekar på endpointen */.well-known/openid-credential-issuer* i verifieringsverktyget för plånboken, vilken används för hämtning av metadata för intygstillhandahållaren	URL	valfritt

([1]) Kommissionens genomförandeförordning (EU) 2025/849 av den 6 maj 2025 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller inlämning av information till kommissionen och till samarbetsgruppen för förteckningen över certifierade europeiska digitala identitetsplånböcker (EUT L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).”

BILAGA X

Bilaga II till genomförandeförordning (EU) 2024/2980 ska ändras på följande sätt:

(1) Bilaga II, avsnitt 1, punkt 1 i ska ersättas med följande:

”i) Ett eller flera intyg som uppfyller standarden ETSI EN 319 412-2 V2.4.1 (2025-06) eller standarden ETSI EN 319 412-3 V1.3.1 (2023-09) och som kan användas för att kontrollera registerförvaltarens underskrift eller stämpel på registeruppgifterna och för vilka de certifierade identitetsuppgifterna innehåller registerförvaltarens namn och, i tillämpliga fall, registerförvaltarens registreringsnummer, i enlighet med led c respektive d.”

(2) Bilaga II, avsnitt 2, punkt 1 h ska ersättas med följande:

”h) Ett eller flera intyg som uppfyller standarden ETSI EN 319 412-2 V2.4.1 (2025-06) eller standarden ETSI EN 319 412-3 V1.3.1 (2023-09) och som kan användas för att autentisera och validera de plånboksenhetsintyg som plånbokstillhandahållaren har utfärdat och för vilka de certifierade identitetsuppgifterna omfattar plånbokstillhandahållarens namn och, i tillämpliga fall, registreringsnummer enligt vad som anges i led a respektive b.”

(3) Bilaga II, avsnitt 3, punkt 1 h ska ersättas med följande:

”h) Ett eller flera intyg som uppfyller standarden ETSI EN 319 412-2 V2.4.1 (2025-06) eller standarden ETSI EN 319 412-3 V1.3.1 (2023-09) och som kan användas för att kontrollera den underskrift eller stämpel som tillhandahållaren av personidentifieringsuppgifter har skapat på de personidentifieringsuppgifter som tillhandahållaren tillhandahåller och för vilka de certifierade identitetsuppgifterna innehåller namn på och, i tillämpliga fall, registreringsnummer för tillhandahållaren av personidentifieringsuppgifter enligt vad som anges i led a respektive b.”

(4) Bilaga II, avsnitt 4, punkt 1 g ska ersättas med följande:

‘(g) Ett eller flera certifikat som uppfyller standarden ETSI EN 319 412-2 V2.4.1 (2025-06) eller standarden ETSI EN 319 412-3 V1.3.1 (2023-09) och som kan användas för att kontrollera den underskrift eller stämpel som tillhandahållaren av åtkomstcertifikat för förlitande parter har skapat på de åtkomstcertifikat som tillhandahållaren tillhandahåller förlitande parter och som, i tillämpliga fall, innehåller den information som krävs för att särskilja åtkomstcertifikat för förlitande parter från andra certifikat.”

(5) Avsnitt 5 i bilaga II ska läggas till enligt följande:

”5. Anmälningar av information om tillhandahållare av förlitandepartregistreringscertifikat

1. Medlemsstaterna ska till kommissionen lämna följande information om tillhandahållare av förlitandepartregistreringscertifikat:

a) Namnet på tillhandahållaren av förlitandepartregistreringscertifikat.

b) I tillämpliga fall ett registreringsnummer för tillhandahållaren av förlitandepartregistreringscertifikat.

c) Den medlemsstat där tillhandahållaren av förlitandepartregistreringscertifikat är etablerad.

d) E-postadress och telefonnummer på vilka tillhandahållaren av förlitandepartregistreringscertifikat kan kontaktas i frågor om de registreringscertifikat som tillhandahållaren tillhandahåller förlitande parter.

e) I tillämpliga fall URL till webbsidan för tillhandahållaren av förlitandepartregistreringscertifikat som innehåller ytterligare information om tillhandahållaren och de registreringscertifikat som tillhandahållaren tillhandahåller förlitande parter.

f) URL till webbsidan med de policyer samt villkor och bestämmelser som gäller för tillhandahållandet och användningen av de registreringscertifikat som tillhandahållaren tillhandahåller förlitande parter.

g) Ett eller flera certifikat som uppfyller standarden ETSI EN 319 412-2 V2.4.1 (2025-06) eller standarden ETSI EN 319 412-3 V1.3.1 (2023-09) och som kan användas för att kontrollera den underskrift eller stämpel som tillhandahållaren av förlitandepartregistreringscertifikat skapat på det förlitandepartregistreringscertifikat som den tillhandahåller förlitande parter, och som i tillämpliga fall innehåller den information som krävs för att särskilja förlitandepartregistreringscertifikat från andra certifikat.”

2. Den information som avses i led 1 ska tillhandahållas per tillhandahållare av förlitandepartregistreringscertifikat.

BILAGA XI

”BILAGA I

Protokoll och gränssnitt som avses i artikel 4

Den tekniska specifikationen ETSI TS 119 472-3 V1.1.1 (2026-03) ska tillämpas med följande anpassningar:

(1) 4.1 General requirements

— GEN-REQ-4.1-05: void

— ANMÄRKNING: void

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

— ISS-MDATA-REG_CERT-4.2.3-04: Ett av elementen i arrayparametern issuer_info ska innehålla PID/EAA-tillhandahållarens registreringscertifikat.

— 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: Om elementet id har värdet ”arf_annex_ii” och den array som mappats till etiketten ”details” innehåller värdet ”once_only” eller värdet ”per-relying-party” ska det JSON-objekt som innehåller arrayen mappad till etiketten ”details” även innehålla ett JSON-tal mappat till etiketten ”reissue_trigger_unused”.

(4) Bilaga A ska inte tillämpas.”

BILAGA XII

"BILAGA II

Tekniska specifikationer som avses i artikel 5

Den tekniska specifikationen i bilaga C till ISO/IEC 18013-7:2025 ska tillämpas.

De tekniska specifikationerna i avsnitten 4.1, 4.2, 5 och 6 i ETSI TS 119 472-2 V1.2.1 (2026-03) ska tillämpas med följande anpassningar, inklusive införande av ett nytt avsnitt 4.3:

(1) 1 Scope

— I detta dokument specificeras två profiler av protokoll som gör det möjligt för förlitande parter (nedan kallade RP) att begära EAAP eller personidentifieringsuppgifter (*PID*) till EUDI-plånboken, och för EUDI-plånboken att skicka de begärda EAAP/PID till RP. Varje profil stöder två överföringsmekanismer, nämligen API-förmedlad och icke API-förmedlad enligt nedan:

(a) En profil bygger på:

— ISO/IEC 18013-5 [10] endast för icke API-förmedlad överföringsmekanism och

— bilaga C till ISO/IEC 18013-7 [16] för API-förmedlad överföringsmekanism.

Denna profil benämns ISO/IEC-mdoc-profilen och definieras i avsnitt 5 i detta dokument.

(b) En profil bygger på:

OpenID4VC-HAIP [11] för både API-förmedlade och icke API-förmedlade överföringsmekanismer enligt följande:

— Avsnitten 5, 5.1, 5.3, 7 och 8 i [11] för överföring via omdirigeringar eller icke API-förmedlad överföringsmekanism.

— Avsnitten 5, 5.2, 5.3, 7 och 8 i [11] för API-förmedlad överföringsmekanism.

Denna profil benämns OpenID4VC-HAIP-profilen och definieras i avsnitt 6 i detta dokument.

(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: ogiltig.

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

— EAAP-ISO/IEC-mdoc-01: ogiltig.

— Note2: ogiltig.

— EAAP-ISO/IEC-mdoc-02: ogiltig.

(5) 4.3 EAAP implementation with mediating API

— EAAP-API-GEN-01: EUDI-plånboken ska stödja ett förmedlande API som stöder både de protokoll som definieras i punkt 5.2 i [11] och i bilaga C till [16].

— ANMÄRKNING: Om den enhet på vilken den europeiska e-identitetsplånboken är installerad inte stöder båda protokollen, kan detta krav inte uppfyllas och leder till bristande överensstämmelse på grund av att underliggande operativsystem och webbläsare inte har de nödvändiga interoperabilitetsegenskaperna.

— EAAP-API-GEN-02: EUDI-plånboken ska stödja ett förmedlande API åtminstone för PID och EAA-typer som är registrerade i katalogen över scheman enligt definitionen i genomförandeförordning (EU) 2025/1569, och åtminstone för alla format som definieras i bilaga II till genomförandeförordning (EU) 2024/2979.

— ANMÄRKNING 1: Om det underliggande operativsystemet, webbläsaren, förmedlande API eller något annat tekniskt skikt utanför EUDI-plånbokens kontroll inskränker, filtrerar, förväljer eller på annat sätt begränsar formaten för autentiseringsuppgifter och PID- och EAA-typerna som är registrerade i katalogen över scheman kan detta krav inte uppfyllas. Om en sådan inskränkning hindrar EUDI-plånboken från att stödja en registrerad typ av autentiseringsuppgifter eller ett registrerat format beror den resulterande felaktigheten på att dessa underliggande operativsystem, webbläsare, förmedlande API eller andra relevanta tekniska skikt inte tillhandahåller de nödvändiga interoperabilitetsfunktionerna.

(6) 4.4 Wallet-relying party validation and overasking checks

— WRP-VALIDATION-01: EUDI-plånboken ska validera det förlitandepartregistreringscertifikat som tagits emot i begäran innan den presenterar ett begärt PID eller ett elektroniskt attributsintyg för plånboksanvändaren för godkännande.

— WRP-VALIDATION-02: Om valideringen av förlitandepartregistreringscertifikatet misslyckas, inbegripet om certifikatet har upphört att gälla, återkallats, inte utfärdats av en giltig betrodd tillhandahållare av förlitandepartregistreringscertifikat, har ett ogiltigt format eller inte kan verifieras kryptografiskt, ska EUDI-plånboken varna plånboksanvändaren om att den förlitande parten inte kunde valideras och inte presentera begäran som framgångsrikt validerad. Plånboksanvändaren ska uttryckligen godkänna den förlitande partens begäran. Tystnad eller förkryssade rutor ska inte räcka för uttryckligt godkännande.

— WRP-VALIDATION-03: Plånbokstillhandahållaren ska, på grundval av sin riskanalys och säkerhetspolicy, avgöra om och under vilka förhållanden specifika misslyckade valideringskontroller får kringgås av plånboksanvändaren.

— WRP-OVERASKING-01: EUDI-plånboken ska jämföra de intyg och attribut som den förlitande parten begär med de registrerade intygen och attributen i förlitandepartregistreringscertifikatet.

— WRP-OVERASKING-02: Om den förlitande parten begär PID eller elektroniska intyg för attribut eller anspråk som inte omfattas av förlitandepartregistreringscertifikatet ska EUDI-plånboken tydligt varna plånboksanvändaren innan något utlämnande görs. Varningen ska ange att den förlitande parten begär mer information än vad den har registrerat. Plånboksanvändaren ska uttryckligen godkänna den förlitande partens begäran. Tystnad eller förkryssade rutor ska inte räcka för uttryckligt godkännande.

— WRP-OVERASKING-03: Plånbokstillhandahållaren ska, på grundval av sin riskanalys, säkerhetspolitik och tillämpliga rätt, fastställa om plånboksanvändaren får fortsätta trots en sådan varning, om endast den undergrupp av begärda uppgifter som omfattas av registreringsbeviset får lämnas ut eller om begäran ska avslås.

(7) 5.1 Introduction

— Avsnitt 5 och dess underavsnitt definierar en profil för ett protokoll som gör det möjligt för en RP att begära EAAP eller PID till EUDI-plånboken, och för EUDI-plånboken att skicka begärda EAAP/PID till RP med hjälp av antingen en icke API-förmedlad överföringsmekanism som bygger på ISO/IEC 18013-5 [] eller en API-förmedlad överföringsmekanism som bygger på bilaga C till ISO/IEC 18013-7 [16] för överföring av de datastrukturer som definieras i ISO/IEC 18013-5 [] i lämpligt inkapslad form.

— Resten av avsnitt 5 är organiserat enligt följande:

  — Avsnitt 5.2 definierar krav på stöd för profilen och överföringsmekanismerna hos RP och EUDI-plånboken.

  — Avsnitt 5.3 specificerar krav som är specifika för den icke API-förmedlade överföringsmekanismen.

  — Avsnitt 5.4 och dess underavsnitt specificerar krav som är specifika för den API-förmedlade överföringsmekanismen.

(8) 5.2 Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: Plånboksenheter, PID-tillhandahållare, intygstillhandahållare, plånbokstillhandahållare och förlitande parter får inte stödja serverhämtning enligt ISO/IEC 18013-5 [10] för begäran och presentation av PID eller intygsattribut.

— ISO/IEC 18013-SUPPORT-02: EUDI-plånboken ska uppfylla de krav som definieras i avsnitten 5.3 och 5.4 i detta dokument.

— ISO/IEC 18013-SUPPORT-04: En förlitande part ska implementera den profil som definieras i avsnitt 5.4 i detta dokument.

(9) 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: Enhetsbegäranden som skickas till EUDI-plånböcker ska innehålla nyckelvärdesparet ”requestInfo” som anges i avsnitt 8.3.2.1.2.1 i [10]. Värdet av detta par ska vara av typen RequestInfo.

— ISO/IEC 18013-5-REQ-05: Typen RequestInfo ska vara enligt CDDL-definitionen nedan.

```
RequestInfo = {

    'euWrprc': bstr ; innehåller ett registreringscertifikat (se kraven nedan)

}
```

— ISO/IEC 18013-5-REQ-06: Det nämnda requestInfo-elementet ska innehålla ett element med etiketten ”euWrprc”

— ISO/IEC 18013-5-REQ-07: Värdet av ”euWrprc” ska vara ett CBOR-kodat registreringscertifikat.

— ISO/IEC 18013-5-REQ-08: ogiltig.

— ANMÄRKNING 3: ogiltig.

— ISO/IEC 18013-5-REQ-09: void.

— ISO/IEC 18013-5-REQ-10: ogiltig.

— ISO/IEC 18013-5-REQ-11: void.

(10) 5.3.3 ISO/IEC-mdoc EAAP Response profile

— I detta avsnitt definieras krav för meddelandetypen DeviceResponse, som är gemensamma för de två typerna av överföringsmekanismer (API-förmedlad och icke API-förmedlad).

— ANMÄRKNING 1: När en icke API-förmedlad mekanism som bygger på ISO/IEC 18013-5 [10] används är ett EAAP-svar exakt en instans av DeviceResponse enligt profilen i detta avsnitt. När en API-förmedlad mekanism som bygger på bilaga C till ISO/IEC 18013-7 [16] används inkapslas instansen av DeviceRequest enligt specifikationerna i bilaga C i [16].

— ISO/IEC 18013-5-RESP-02: Tillhandahållaren av personidentifieringsuppgifter och elektroniska attributsintyg får inte inkludera några dataelement i KeyAuthorizations-mappningen i Mobile Security Object för de personidentifieringsuppgifter och elektroniska attributsintyg som tillhandahållaren utfärdar, med undantag för dataelement som tillhandahålls av den förlitande parten i transaktionsuppgifterna i den mdoc-begäran som ska undertecknas eller stämplas av plånboksenheten med den privata nyckeln för personidentifieringsuppgifterna eller de elektroniska attributsintygen.

— ANMÄRKNING 2: Som en följd av detta kan plånboksenheter inte presentera några enhetsundertecknade dataelement för förlitande parter, med undantag för undertecknande av data som den förlitande parten har tillhandahållit, till exempel i användningsfall för säker användarautentisering.

— ANMÄRKNING 3: ISO/IEC 18013-5:2021 specificerar inte hur förlitande parter kan inkludera transaktionsuppgifter i en mdoc-begäran. Inkludering av transaktionsuppgifter i en mdoc-begäran ska ske genom tillägg av tekniska specifikationer.

— ISO/IEC 18013-5-RESP-03: Tillhandahållare av personidentifieringsuppgifter får inte tillåta att den privata nyckeln för personidentifieringsuppgifterna undertecknar dataelement som tillhandahålls av den förlitande parten i transaktionsuppgifterna i mdoc-begäran.

(11) 5,4 Requirements for API mediated mechanism

5.4.1 ISO/IEC 18013-7-related requirements

I detta avsnitt definieras krav för API-förmedlad överföringsmekanism som är relaterade till de krav som definieras i bilaga C till [16].

— ISO/IEC 18013-7-API-01: Profilen som stöder API-förmedlade presentationer ska uppfylla kraven i bilaga C till ISO/IEC 18013-7 [16] enligt ytterligare profilering i avsnitten 5.3 och 5.4 i detta dokument.

— ISO/IEC 18013-7-API-02: Alla obligatoriska krav som definieras i bilaga C till [16] ska tillämpas enligt ytterligare profilering i avsnitten 5.3 och 5.4 i detta dokument.

— ISO/IEC 18013-7-API-03: Alla valfria krav som definieras i bilaga C till [16] ska förbli valfria om inte annat anges i detta dokument.

(12) 5.4.2 Additional requirements

— I detta avsnitt specificeras ytterligare krav för API-förmedlad överföringsmekanism.

— ISO/IEC 18013-ADD-API-01: EUDI-plånboken ska som standard lämna ut förekomsten av alla lagrade typer av elektroniska attributsintyg till den förmedlande API som fungerar i enlighet med bilaga C till [16], men den får inte lämna ut attributen och deras värden i dessa elektroniska attributsintyg.

— *ANMÄRKNING 1*: Begränsningen av attributvärden gäller även om ett sådant utlämnande skulle förbättra de tjänster som operativsystemet tillhandahåller för EUDI-plånboken, t.ex. val av intyg inom ramen för den förmedlande API.

— Det finns överväganden relaterade till operativsystem och webbläsare som faller utanför implementerarnas kontroll, vilka kan beaktas enligt vad som anges i anmärkningarna 2–4 nedan:

— *ANMÄRKNING 2*: En presentationsbegäran från en förlitande part som stöder bilaga C till [16] kan behandlas av webbläsaren och/eller operativsystemet för att söka efter tillgängliga elektroniska attributsintyg för att förebygga bedrägerier riktade mot användaren eller för felsökningsändamål.

— *ANMÄRKNING 3*: En presentationsbegäran från en förlitande part som stöder bilaga C till [16] förväntas behandlas av webbläsaren och/eller operativsystemet i säkerhetssyfte för användaren.

— *ANMÄRKNING 4*: En presentationsbegäran från en förlitande part som stöder bilaga C till [16] förväntas inte behandlas av webbläsaren och/eller operativsystemet för marknadsanalysändamål (inbegripet som sekundärt ändamål) eller för webbläsarens och/eller operativsystemets interna ändamål.

— ISO/IEC 18013-ADD-API-02: Om en EUDI-plånbok, på användarens begäran, raderar ett PID eller ett elektroniskt attributsintyg som tidigare lämnades ut till det förmedlande API som fungerar i enlighet med bilaga C till [16] ska EUDI-plånboken lämna uppgift till det förmedlande API om att den inte längre lagrar detta PID eller detta elektroniskt attributsintyg.

— ISO/IEC 18013-ADD-API-03: Om användaren avinstallerar sin EUDI-plånbok ska EUDI-plånboken lämna uppgift till det förmedlande API, som fungerar i enlighet med bilaga C till [16], om att den inte längre lagrar några tidigare utlämnade PID eller elektroniska attributsintyg.

— ISO/IEC 18013-ADD-API-04: EUDI-plånboken ska tillhandahålla en global användarinställning för att inaktivera utlämnande av lagrade elektroniska attributsintyg via ett förmedlande API som fungerar enligt vad som anges i ISO/IEC 18013-ADD-API-01. När denna inställning är inaktiverad får EUDI-plånboken inte annonsera eller besvara API-förmedlade begäranden om presentation eller utfärdande.

— ISO/IEC 18013-ADD-API-05: EUDI-plånböckerna ska i flöden mellan enheter, med hjälp av det förmedlande API, kontrollera att den interagerande enheten befinner sig i fysisk närhet till EUDI-plånboken med hjälp av en säker, direkt och användarförmedlad lokal kommunikationskanal, t.ex. trådlös kommunikationsteknik för korta avstånd, för att kunna utföra den fysiska närhetskontrollen.

— *ANMÄRKNING*: CTAP 2.3 gör det möjligt att använda BLE för att utföra den fysiska närhetskontrollen, och när protokollet har implementerats av båda enheterna blir det även möjligt att överföra data mellan enheterna via teknik för överföring över korta avstånd. Underliggande operativsystem, webbläsare, förmedlande API eller något annat tekniskt skikt utanför EUDI-plånbokens kontroll ska prioritera att både den fysiska närhetskontrollen och dataöverföringen mellan de två enheterna sker via en lokal kommunikationskanal som möjliggörs av CTAP 2.3 framför användning av tjänster för CTAP Hybrid-tunnel.

(13) 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: EUDI-plånboken ska uppfylla kraven i avsnitt 6.5 i denna bilaga.

— OIDFVP-HAIP-SUPPORT-03: EUDI-plånboken får inte stödja den omdirigeringsbaserade mekanism som anges i avsnitt 6.4 för presentationsflöden mellan enheter.

— ANMÄRKNING 3: Användning av denna mekanism kan ge upphov till sårbarheter som kan utnyttjas genom attacker, till exempel sessionsfixeringsangrepp. Ansvaret för att motverka sådana attacker ligger hos förlitande parter. Implementering av denna mekanism får inte medföra bristande efterlevnad.

— OIDFVP-HAIP-SUPPORT-05: En förlitande part ska uppfylla kraven som anges i avsnitt 6.5 i denna bilaga.

— ANMÄRKNING 5: ogiltig.

(14) 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: Alla obligatoriska krav som anges i avsnitten 5, 5.3, 7 och 8 i HAIP [11] ska vara tillämpliga.

— ANMÄRKNING 1: ”HAIP [11] avsnitt 5” avser endast de krav som anges direkt under rubriken för avsnitt 5. Detta omfattar inte avsnitten 5.1, 5.2 och 5.3.

— OIDFVP-HAIP-GEN-03: Om denna bilaga ändrar ett krav i OpenID4VC-HAIP [11] ska det ändrade krav som anges i denna bilaga ha företräde.

— *ANMÄRKNING 2*: Detta möjliggör till exempel att ett valfritt krav i OpenID4VC-HAIP [11] görs obligatoriskt eller att obligatoriska krav utökas.

— OIDFVP-HAIP-GEN-04: När formatet för det begärda intyget överensstämmer med [10] ska förlitande parter och EUDI-plånböcker uppfylla kraven i profilen ”ISO mdocs” i [11] avsnitt 6.

— *ANMÄRKNING 3*: Obs: Profilen ”ISO mdocs” i HAIP innebär att förlitande parter och EUDI-plånböcker måste uppfylla de tillämpliga kraven i [7] bilaga B.2.

— OIDFVP-HAIP-GEN-05: När formatet för det begärda intyget överensstämmer med [2] ska förlitande parter och EUDI-plånböcker uppfylla kraven i profilen ”IETF SD-JWT VCs” i [11] avsnitt 6.

— *ANMÄRKNING 4*: Obs: Profilen ”IETF SD-JWT VCs” innebär att förlitande parter och EUDI-plånböcker måste uppfylla kraven i [7] bilaga B.3 samt kraven i [11] avsnitt 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

— *Anmärkning 2*: void

— OIDFVP-HAIP-COMMON-REQ-RO-13: Ett av elementen i parametern verifier_info ska inkludera registreringscertifikatet.

— OIDFVP-HAIP-COMMON-REQ-RO-23: Det slutcertifikat som anges i OpenID4VP avsnitt 5.9.3 för användning med x509_hash Client Identifier Prefix ska vara ett RP-åtkomstcertifikat såsom anges i ETSI TS 119 475 [14].

(17) 6.3.3 Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: ogiltig.

(18) 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: ogiltig.

— *ANMÄRKNING*: ogiltig.

(19) 6.5.2 Additional requirements

— OIDFVP-HAIP-ADD-API-01: EUDI-plånboken ska som standard lämna ut information om förekomsten av alla lagrade typer av elektroniska attributsintyg till det förmedlande API som fungerar i enlighet med avsnitt 5.2 i [11], men den ska inte lämna ut attributen och deras värden i dessa elektroniska attributsintyg.

— OIDFVP-HAIP-ADD-API-04: Om EUDI-plånboken stöder ett förmedlande API som fungerar enligt vad som anges i OIDFVP-HAIP-ADD-API-01 ska den tillhandahålla en global användarinställning för att inaktivera utlämnandet av lagrade EAAs via det förmedlande API:et. När denna inställning är satt till inaktiverat utlämnande ska EUDI-plånboken därefter göra det möjligt för användaren att välja enskilda intyg som ska lämnas ut till det förmedlande API.

— OIDFVP-HAIP-ADD-API-05: EUDI-plånböckerna ska i flöden mellan enheter, med hjälp av det förmedlande API, kontrollera att den interagerande enheten befinner sig i fysisk närhet till EUDI-plånboken med hjälp av en säker, direkt och användarförmedlad lokal kommunikationskanal, t.ex. trådlös kommunikationsteknik för korta avstånd, för att kunna utföra den fysiska närhetskontrollen.

— *ANMÄRKNING 5*: CTAP 2.3 gör det möjligt att använda BLE för att utföra den fysiska närhetskontrollen, och när protokollet har implementerats av båda enheterna blir det även möjligt att överföra data mellan enheterna via teknik för överföring över korta avstånd. Underliggande operativsystem, webbläsare, förmedlande API eller något annat tekniskt skikt utanför EUDI-plånbokens kontroll ska prioritera att både den fysiska närhetskontrollen och dataöverföringen mellan de två enheterna sker via en lokal kommunikationskanal som möjliggörs av CTAP 2.3 framför användning av tjänster för CTAP Hybrid-tunnel.

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

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Alla krav som anges i detta dokument och som är tillämpliga på strukturerna Device Request och Device Response enligt ISO/IEC 18013-5 gäller även när EUDI-plånboken tar emot en begäran om ISO/IEC mdoc-presentation via en API-överförd mekanism som anges i avsnitt C.1 i [16].”