Publicatieblad
van de Europese Unie

NL
L-serie

2026/1731

22.7.2026

UITVOERINGSVERORDENING (EU) 2026/1731 VAN DE COMMISSIE

van 15 juli 2026

tot wijziging van Uitvoeringsverordeningen (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 en (EU) 2024/2982 betreffende toepasselijke normen en specificaties

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG ([1]), en met name artikel 5 bis, lid 23,

Overwegende hetgeen volgt:

(1) Met het oog op het hoogste niveau van harmonisatie tussen de lidstaten voor de ontwikkeling van Europese portemonnees voor digitale identiteit, zijn de technische specificaties voor de portemonnees geschraagd op de werkzaamheden op basis van Aanbeveling (EU) 2021/946 van de Commissie ([2]), en met name de architectuur en het referentiekader. Aangezien de architectuur en het referentiekader sinds Uitvoeringsverordeningen (EU) 2024/2977 ([3]), (EU) 2024/2979 ([4]), (EU) 2024/2980 ([5]) en (EU) 2024/2982 ([6]) van de Commissie aanzienlijk zijn geëvolueerd, moet deze uitvoeringsverordeningen nu worden gewijzigd om die in overeenstemming te brengen met de nieuwe normen, specificaties en procedures.

Conform de doelstellingen van Verordening (EU) nr. 910/2014 is een aantal normen geselecteerd om aan deze specifieke vereisten te voldoen. Deze normen moeten vaste praktijken weerspiegelen en in de betrokken sectoren algemeen erkend worden. Het W3C-VCDM-formaat bijvoorbeeld wordt gebruikt als referentieformaat voor attesteringen, met name in de onderwijssector, en dus moeten de Europese portemonnees voor digitale identiteit dit formaat ook ondersteunen wanneer de nieuwe profielen in het W3C-VCDM-formaat beschikbaar zijn. Waar nodig moeten die normen worden aangepast of aangevuld om een hoog niveau van veiligheid en integriteit van Europese portemonnees voor digitale identiteit te waarborgen en de grensoverschrijdende interoperabiliteit en de doeltreffende werking van de interne markt te faciliteren.

(2) Voor elk gebruik van de portemonnee dat de weergave van het portret van de portemonneegebruiker vereist, moet de portemonnee de functionaliteit van selectieve openbaarmaking ondersteunen en moet de gebruiker volledige controle over de openbaarmaking hebben. Om de mogelijkheid om over de openbaarmaking te beslissen, te vrijwaren, en om het portret te beschermen tegen onbedoelde of ongeoorloofde verzoeken om openbaarmaking, moeten de Europese portemonnees voor digitale identiteit zo worden ontworpen dat zij waarschuwingsmechanismen bevatten en moeten alle transacties met betrekking tot het gebruik van het portret worden geregistreerd. Om ervoor te zorgen dat de portemonneegebruiker beseft dat hij biometrische gegevens gaat delen, moeten deze waarschuwingen aangeven dat het verzoek inhoudt dat biometrische gegevens zullen worden gedeeld, en moet de

([1]) PB L 257 van 28.8.2014, blz. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Aanbeveling (EU) 2021/946 van de Commissie van 3 juni 2021 betreffende een gemeenschappelijke EU-toolbox voor een gecoördineerde aanpak ten behoeve van een Europees kader voor digitale identiteit (PB L 210 van 14.6.2021, blz. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Uitvoeringsverordening (EU) 2024/2977 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de persoonsidentificatiegegevens en elektronische attesteringen van attributen, afgegeven voor de Europese portemonnee voor digitale identiteit (PB L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([4]) Uitvoeringsverordening (EU) 2024/2979 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de integriteit en de kernfunctionaliteiten van Europese portemonnees voor digitale identiteit (PB L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([5]) Uitvoeringsverordening (EU) 2024/2980 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de kennisgevingen aan de Commissie over het ecosysteem van de Europese portemonnee voor digitale identiteit, (PB L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

([6]) Uitvoeringsverordening (EU) 2024/2982 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de protocollen en interfaces die moeten worden ondersteund door het Europees kader voor digitale identiteit (PB L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

gebruiker specifiek worden gevraagd met de openbaarmaking in te stemmen. Wanneer een vertrouwende partij het portret verwerkt met het oog op de unieke identificatie van een natuurlijke persoon of ter bevestiging van de beweerde identiteit van die persoon, zijn de artikelen 6 en 9 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([7]) van toepassing, evenals alle andere vereisten van die verordening, waaronder het vereiste dat de verwerking van het portret door vertrouwende partijen beperkt moet blijven tot wat nodig is voor het beoogde gebruik. Dat beoogde gebruik moet samen met het verzoek om openbaarmaking in duidelijke en begrijpelijke taal aan de portemonneegebruiker worden meegedeeld. Gezien de gevoeligheid van biometrische gegevens, moet de portemonneegebruiker de openbaarmaking van het portret uitdrukkelijk en specifiek bevestigen. Toestemming door de portemonneegebruiker kan niet stilzwijgend of middels vooraf ingevulde vakjes als verleend worden beschouwd. De uitdrukkelijke bevestiging van de portemonneegebruiker moet een technische waarborg zijn en mag op zichzelf niet de rechtsgrond zijn waarop de verwerking wordt gebaseerd. Volgens artikel 9, lid 4, van Verordening (EU) 2016/679 kunnen de lidstaten bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid handhaven of invoeren.

(3) Om de lidstaten voldoende tijd te geven om hun nationale procedures aan te passen, kan het portret van de portemonneegebruiker pas vanaf 11 augustus 2028 deel uitmaken van de verplichte persoonsidentificatiegegevens voor de natuurlijke persoon. Wanneer deze afbeeldingen afkomstig zijn van bestaande identiteitsdocumenten, zoals identiteitskaarten of paspoorten, zijn de desbetreffende voorschriften van Verordeningen (EU) 2025/1208 ([8]) en (EG) nr. 2252/2004 ([9]) van de Raad van toepassing.

(4) Verordening (EU) nr. 910/2014 vereist dat portemonnees een EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit (EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit) kunnen weergeven als een verifieerbare, eenvoudige en herkenbare indicatie dat een portemonnee overeenkomstig de verordening is verstrekt. Het gebruik van een dergelijk betrouwbaarheidskeurmerk zal de doeltreffende werking van de interne markt ondersteunen, billijke concurrentie waarborgen en de belangen van de consument beschermen. Om een dergelijk betrouwbaarheidskeurmerk te kunnen gebruiken, moeten de visuele en technische kenmerken van het betrouwbaarheidskeurmerk worden vastgesteld.

(5) Overeenkomstig artikel 12 ter van Verordening (EU) nr. 910/2014 moeten poortwachters ervoor zorgen dat aanbieders van Europese portemonnees voor digitale identiteit en uitgevers van aangemelde elektronische identificatiemiddelen effectief interoperabel zijn en, ten behoeve van de interoperabiliteit, toegang hebben tot dezelfde besturingssystemen, hardware- of softwarefuncties. Dergelijke effectieve interoperabiliteit en toegang moeten kosteloos worden toegestaan, ongeacht of die hardware- of softwarefuncties deel uitmaken van het besturingssysteem, beschikbaar zijn voor of worden gebruikt door die poortwachter bij het verlenen van dergelijke diensten. Aangezien alle portemonnee-oplossingen een gemeenschappelijke set protocollen en interfaces moeten ondersteunen om de bruikbaarheid, de beveiliging en de interoperabiliteit tussen de lidstaten te waarborgen, moeten poortwachters het besturingssysteem of de hardware- of softwarefuncties zo uitrusten dat die de protocollen en interfaces van bijlage XII bij deze verordening kunnen uitvoeren. Bij onlinegegevensstromen tussen apparaten moeten poortwachters trouwens, zowel voor de controle van de fysieke nabijheid als voor de gegevensoverdracht tussen de twee apparaten, een lokaal communicatiekanaal op basis van Client To Authenticator Protocol (CTAP) specification version 2.3 ([10]) verkiezen boven CTAP-hybride tunneldiensten.

(6) Om de lidstaten, de aanbieders van registratiecertificaten voor op portemonnees vertrouwende partijen en de portemonneeaanbieders voldoende tijd te geven om portemonnee-eenheden registratiecertificaten voor op portemonnees vertrouwende partijen te kunnen laten authenticeren en valideren, mag dit vereiste pas van toepassing zijn met ingang van 11 augustus 2028.

(7) Verordening (EU) 2016/679 en, in voorkomend geval, Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([11]) zijn van toepassing op alle activiteiten betreffende de verwerking van persoonsgegevens uit hoofde van deze verordening.

([7]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Verordening (EU) 2025/1208 van de Raad van 12 juni 2025 betreffende de versterking van de beveiliging van identiteitskaarten van burgers van de Unie en van verblijfsdocumenten afgegeven aan burgers van de Unie en hun familieleden die hun recht van vrij verkeer uitoefenen (PB L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Verordening (EG) nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten (PB L 385 van 29.12.2004, blz. 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]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) De Europese Toezichthouder voor gegevensbescherming is overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([12]) geraadpleegd en heeft op 17 april 2026 advies uitgebracht ([13]).

(9) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 48 van Verordening (EU) nr. 910/2014 ingestelde comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Wijzigingen van Uitvoeringsverordening (EU) 2024/2977

Uitvoeringsverordening (EU) 2024/2977 wordt als volgt gewijzigd:

1) het volgende artikel 3 bis wordt ingevoegd:

"*Artikel 3 bis*

Portretrecht

1) Boven op de informatievoorschriften overeenkomstig Verordening (EU) 2016/679 zorgen portemonneeaanbieders ervoor dat de door hun aangeboden portemonnee-oplossingen portemonneegebruikers waarschuwen wanneer op portemonnees vertrouwende partijen om openbaarmaking van het portret verzoeken, waarbij zij aangeven dat het verzoek met het delen van biometrische gegevens gepaard gaat en vereist dat de selectieve openbaarmaking van het portret wordt bevestigd.

2) Voor de uitvoering van de selectieve openbaarmaking van het portret aan een op portemonnees vertrouwende partij zorgen de portemonneeaanbieders ervoor dat de portemonnee-oplossingen de portemonneegebruiker verplichten de weergave van het portret uitdrukkelijk en specifiek te bevestigen.

3) Het portret wordt niet bewaard door op portemonnees vertrouwende partijen, tenzij de verwerking ervan noodzakelijk is voor identificatie- en authenticatiedoeleinden overeenkomstig het Unierecht inzake gegevensbescherming of indien dat in het Unierecht of het nationale recht is bepaald, overeenkomstig het Unierecht inzake gegevensbescherming. Het portret wordt niet aan derde landen of internationale organisaties doorgegeven, tenzij dat overeenkomstig het Unierecht inzake gegevensbescherming is toegestaan.";

2) in artikel 4 wordt lid 1 vervangen door:

"1. Elektronische attesteringen van attributen die worden uitgegeven aan portemonnee-eenheden voldoen aan ten minste één van de normen in de lijst in bijlage II bij Uitvoeringsverordening (EU) 2024/2979.";

3) in artikel 5, lid 4, wordt punt b) vervangen door:

"b) wanneer de portemonnee-eenheidsattestering van de portemonnee-eenheid waaraan de persoonsidentificatiegegevens zijn afgegeven, is ingetrokken;";

4) de bijlage wordt vervangen door de tekst in bijlage I bij deze verordening.

([12]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([13]) Formeel advies van de Europese Toezichthouder voor gegevensbescherming over het ontwerp van uitvoeringsverordening inzake de toepasselijke normen en specificaties en tot rectificatie van Uitvoeringsverordening (EU) 2024/2980|Europese Toezichthouder voor gegevensbescherming.

Artikel 2

Wijzigingen van Uitvoeringsverordening (EU) 2024/2979

Uitvoeringsverordening (EU) 2024/2979 wordt als volgt gewijzigd:

1) in artikel 3 wordt lid 2 geschrapt;

2) in artikel 5, lid 1, wordt punt a) vervangen door:

"a) cryptografische bewerkingen van portemonnees met betrekking tot kritieke activa die zijn opgeslagen in een beveiligd cryptografisch middel voor portemonnees en die niet vereist zijn voor de authenticatie van de portemonneegebruiker, uitsluitend uitvoeren in gevallen waarin die toepassingen met succes portemonneegebruikers hebben geauthenticeerd;";

3) het volgende artikel 5 bis wordt ingevoegd:

"*Artikel 5 bis*

Cryptografische mechanismen

Portemonneeaanbieders gebruiken voor de toepassing van artikel 4, lid 2, alleen de in bijlage I bis bedoelde cryptografische mechanismen.";

4) artikel 6 wordt als volgt gewijzigd:

a) lid 1 wordt vervangen door:

"1. Portemonneeaanbieders geven portemonnee-eenheidsattesteringen af voor elke portemonnee-eenheid. Portemonneeaanbieders ondertekenen of verzegelen de attesteringen van de portemonnee-eenheid op zodanige wijze dat de handtekeningen of zegels kunnen worden gevalideerd door middel van een overeenkomstig bijlage II, deel 2, punt 1), h), van Uitvoeringsverordening (EU) 2024/2980 opgenomen certificaat.";

b) lid 2 wordt vervangen door:

"2. Portemonneeaanbieders waarborgen dat de in lid 1 bedoelde portemonnee-eenheidsattesteringen voldoen aan de technische specificaties van bijlage I ter.";

c) in lid 3 wordt punt b) vervangen door:

"b) verstrekken mechanismen voor de veilige identificatie en authenticatie van portemonneegebruikers die onafhankelijk zijn van portemonnee-eenheden;";

5) in artikel 9, lid 2, wordt punt b) vervangen door:

"b) de namen van de contactpersonen en de unieke identificatiecode van de overeenkomstige op portemonnes vertrouwende partij en de lidstaat waar die op portemonnees vertrouwende partij is gevestigd;";

6) in artikel 10 wordt lid 1 vervangen door:

"1. Portemonneeaanbieders waarborgen dat elektronische attesteringen van attributen die zijn uitgegeven in overeenstemming met de technische specificaties die gelden voor een gemeenschappelijk ingebed openbaarmakingsbeleid als bedoeld in bijlage III kunnen worden verwerkt door de portemonnee-eenheden die zij aanbieden.";

7) artikel 12 wordt als volgt gewijzigd:

a) in lid 2 wordt punt c) vervangen door:

"c) creëren van handtekeningen of zegels overeenkomstig ten minste het in bijlage IV bedoelde verplichte formaat voor handtekeningen of zegels;";

b) lid 3 wordt vervangen door:

"3. De toepassingen voor het aanmaken van handtekeningen kunnen in de portemonnee-instanties worden geïntegreerd of extern zijn.";

c) het volgende lid wordt toegevoegd:

"4. De door portemonnee-eenheden gebruikte toepassingen voor het aanmaken van handtekeningen ondersteunen ten minste de in bijlage IV bedoelde applicatieprogramma-interface.";

8) in artikel 14 wordt lid 1 geschrapt;

9) het volgende artikel 14 bis wordt ingevoegd:

"*Artikel 14 bis*

EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit

1) Portemonneeaanbieders waarborgen dat de portemonnee-eenheden het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit weergeven. Het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit heeft de in de bijlagen VI en VII vastgestelde vorm.

2) Portemonneeaanbieders waarborgen dat portemonnee-eenheden het voor portemonneegebruikers mogelijk maken toegang te krijgen tot informatie waarmee zij de certificeringsstatus van de portemonneeoplossing kunnen verifiëren. Daartoe waarborgen portemonneeaanbieders dat, na de registratie van een portemonnee-oplossing, de overeenkomstige portemonnee-eenheden de URL's bevatten die de Europese Commissie voor een dergelijke verificatie heeft verstrekt. Portemonneeaanbieders waarborgen dat hun portemonnee-eenheden toegang hebben tot de gegevens van het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit die voldoen aan de technische specificaties van bijlage VIII.

3) De referentiekleuren voor het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit zijn Pantone 661 en 116 of blauw (100 % cyaan + 67 % magenta + 0 % geel + 40 % zwart) en geel (0 % cyaan + 20 % magenta + 100 % geel + 0 % zwart), als gebruik wordt gemaakt van vierkleurendruk; wanneer RGB-kleuren worden gebruikt, is de referentie blauw (0 rood + 51 groen + 153 blauw) en geel (255 rood + 204 groen + 0 blauw).

4) Alleen wanneer het gebruik van kleur praktisch gezien niet haalbaar is, mag het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit in zwart-wit worden gebruikt, zoals bepaald in bijlage VII.

5) Wanneer het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit op een donkere achtergrond wordt gebruikt, mag het in negatief formaat worden gebruikt met dezelfde achtergrondkleur. Wanneer het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit in kleur wordt gebruikt op een gekleurde achtergrond waardoor het moeilijk te zien is, kan een begrenzende buitenlijn rond het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit worden gebruikt om het contrast met de achtergrondkleuren te verbeteren.

6) Het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit heeft een minimumgrootte van 64 × 85 pixels bij 150 dpi.

7) Portemonneeaanbieders waarborgen dat het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit zodanig wordt gebruikt dat duidelijk kan worden aangegeven op welke portemonnee-eenheid het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit betrekking heeft. Het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit kan worden gekoppeld aan grafische of tekstuele elementen die duidelijk aangeven voor welke portemonnee-eenheid het wordt gebruikt, op voorwaarde dat zij de herkenbaarheid ervan als EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit niet wijzigen, noch de associatie met de in artikel 5 quinquies van Verordening (EU) nr. 910/2014 bedoelde lijst van gecertificeerde Europese portemonnees voor digitale identiteit wijzigen.

8) Indien portemonneeaanbieders een portemonnee-eenheidsattestering hebben ingetrokken, waarborgen zij dat het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit niet langer door de overeenkomstige portemonnee-eenheid wordt weergegeven.";

10) bijlagen I bis en I ter worden ingevoegd overeenkomstig bijlagen II en III bij deze verordening;

11) bijlage II wordt vervangen door bijlage IV bij deze verordening;

12) bijlage III wordt vervangen door bijlage V bij deze verordening;

13) bijlage IV wordt gewijzigd overeenkomstig bijlage VI bij deze verordening;

14) bijlage V wordt geschrapt;

15) de tekst in bijlage VII bij deze verordening wordt toegevoegd als bijlage VI;

16) de tekst in bijlage VIII bij deze verordening wordt toegevoegd als bijlage VII;

17) de tekst in bijlage IX bij deze verordening wordt toegevoegd als bijlage VIII.

Artikel 3

Wijzigingen van Uitvoeringsverordening (EU) 2024/2980

Uitvoeringsverordening (EU) 2024/2980 wordt als volgt gewijzigd:

1) in artikel 5 wordt lid 2 vervangen door:

"2. In voorkomend geval zorgt de Commissie voor het opstellen, bijhouden en publiceren van een lijst met de door de lidstaten verstrekte informatie over portemonneeaanbieders, verstrekkers van persoonsidentificatiegegevens, aanbieders van toegangscertificaten voor vertrouwende partijen en aanbieders van registratiecertificaten voor vertrouwende partijen, als bedoeld in de delen 2, 3, 4 en 5 van bijlage II.";

2) bijlage II bij Uitvoeringsverordening (EU) 2024/2980 wordt gewijzigd overeenkomstig bijlage X bij deze verordening.

Artikel 4

Wijzigingen van Uitvoeringsverordening (EU) 2024/2982

Uitvoeringsverordening (EU) 2024/2982 wordt als volgt gewijzigd:

1) in artikel 1 wordt punt 2) vervangen door:

"2) de weergave van attributen van persoonsidentificatiegegevens en elektronische attesteringen van attributen aan op portemonnees vertrouwende partijen;";

2) artikel 3 wordt als volgt gewijzigd:

a) punt 1) wordt vervangen door:

"1) de toegangscertificaten voor op portemonnees vertrouwende partijen authenticeren en valideren in interacties met op portemonnees vertrouwende partijen; zonder de uitvoering van deze processen te delegeren aan een browser van het besturingssysteem of een andere intermediaire applicatie;";

b) punt 2) wordt geschrapt;

c) punt 3) wordt vervangen door:

"3) verzoeken authenticeren en valideren die zijn ingediend met behulp van toegangscertificaten voor op portemonnees vertrouwende partijen;";

d) punt 4) wordt vervangen door:

"4) registratiecertificaten van op portemonnees vertrouwende partijen authenticeren en valideren;";

e) punt 5) wordt vervangen door:

"5) aan portemonneegebruikers de informatie tonen die is opgenomen in de toegangscertificaten voor op portemonnees vertrouwende partijen;";

f) punt 8) wordt geschrapt;

g) punt 9) wordt vervangen door:

"9) geen gevraagde attributen weergeven aan op portemonnees vertrouwende partijen totdat aan de volgende vereisten is voldaan:

a) verificatie of het ingebed openbaarmakingsbeleid in de portemonnee-eenheid is verwerkt overeenkomstig artikel 10 van Uitvoeringsverordening (EU) 2024/2979;

b) controle of portemonneegebruikers de weergave geheel of gedeeltelijk hebben goedgekeurd;";

3) in artikel 4 wordt lid 1 vervangen door:

"1. Portemonneeaanbieders waarborgen dat portemonnee-oplossingen de in bijlage I vastgestelde protocollen en interfaces ondersteunen voor de uitgifte van persoonsidentificatiegegevens en elektronische attesteringen van attributen aan portemonnee-eenheden.";

4) artikel 5 wordt als volgt gewijzigd:

   a) de leden 1 en 2 worden vervangen door:

      "1. Portemonneeaanbieders waarborgen dat portemonnee-oplossingen protocollen en interfaces ondersteunen voor de weergave van attributen aan op portemonnees vertrouwende partijen, op afstand en in voorkomend geval dichtbij, overeenkomstig de in bijlage II vastgestelde technische specificaties.

      2. Portemonneeaanbieders waarborgen dat, op verzoek van gebruikers, portemonnee-eenheden reageren op met succes geauthenticeerde en gevalideerde verzoeken van de in artikel 3 bedoelde op portemonnees vertrouwende partijen, overeenkomstig de in bijlage II vastgestelde technische specificaties.";

   b) lid 5 wordt geschrapt;

5) artikel 8 wordt vervangen door:

   "*Artikel 8*

   Inwerkingtreding

   Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

   Artikel 3, lid 4, is van toepassing met ingang van 11 augustus 2028.

   Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.";

6) de bijlage wordt geschrapt;

7) de tekst in bijlage XI bij deze verordening wordt toegevoegd als bijlage I;

8) de tekst in bijlage XII bij deze verordening wordt toegevoegd als bijlage II.

Artikel 5

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 15 juli 2026.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE I

"BIJLAGE

Technische specificaties voor persoonsidentificatiegegevens als bedoeld in artikel 3, lid 3

1) Afdeling 1: Identificatiegegevens van natuurlijke personen

Tabel 1

Verplichte persoonsidentificatiegegevens voor natuurlijke personen voor selectieve openbaarmaking

Gegevensidentificatie	Definitie
`family_name`	Huidige achternaam (of achternamen) van de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben.
`given_name`	Huidige voornaam (of voornamen), met inbegrip van, indien van toepassing, middelste namen, van de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben.
`birth_date`	Dag, maand en jaar van geboorte van de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben.
`birth_place`	Het land in de vorm van een alpha-2-landcode zoals gespecificeerd in ISO 3166-1, of de staat, de provincie, het district of de regio, of de gemeente of plaats van geboorte van de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben.
`nationality`	Een of meer alpha-2-landcodes zoals gespecificeerd in ISO 3166-1, die de nationaliteit weergeven van de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben.
`portrait`	Tenzij bij expliciete opt-out van de gebruiker, in voorkomend geval, de gezichtsopname van de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben, die voldoet aan de kwaliteitseisen voor een full frontal image type conform ISO/IEC 39794-5, of — voor achterwaartse compatibiliteit — ISO/IEC 19794-5, punten 8.2, 8.3 en 8.4, verstrekt als gecodeerde beeldgegevens zonder de kopjes of blokken zoals gespecificeerd in punt 5 van ISO/IEC 19794-5, met uitzondering van de beeldgegevens zelf (een JPEG), die van toepassing zijn vanaf 11 augustus 2028.

— De lidstaten kunnen bepalen dat de gebruiker de mogelijkheid heeft om te weigeren het portret in de persoonsidentificatiegegevens op te nemen.

— De lidstaten zorgen ervoor dat de selectieve openbaarmaking van toepassing is op elke gegevensidentificatie, met inbegrip van het portret.

— Indien de geboortedatum van de natuurlijke persoon niet bekend is, kiezen de lidstaten passende waarden die voldoen aan de specificaties van deel 4.1 of deel 4.2 (naargelang het geval).

— Indien de nationaliteit van de natuurlijke persoon onbekend is, gebruiken de lidstaten de waarde "QU".

— Indien de natuurlijke persoon geen nationaliteit bezit, gebruiken de lidstaten de waarde "QS".

— Indien de gebruiker ervoor kiest het portret niet op te nemen (opt-out), laten de lidstaten de waarde leeg.

Tabel 2

Optionele persoonsidentificatiegegevens voor natuurlijke personen voor selectieve openbaarmaking

Gegevensidentificatie	Definitie
resident_address	Het volledige adres waar de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben, momenteel verblijft of bereikbaar is (straatnaam, huisnummer, stad enz.).
resident_country	Het land waar de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben, momenteel verblijft, als een alpha-2-landcode zoals gespecificeerd in ISO 3166-1.
resident_state	De staat, de provincie, het district of de regio waar de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben, momenteel verblijft.
resident_city	De gemeente of plaats waar de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben, momenteel verblijft.
resident_postal_code	De postcode van de huidige verblijfplaats van de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben.
resident_street	De naam van de straat waar de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben, momenteel verblijft, met inbegrip van huisnummer en eventuele toevoegingen.
personal_administrative_-number	Een aan de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben toegekende waarde die uniek is onder alle persoonlijke administratieve nummers die zijn uitgegeven door de verstrekker van persoonsidentificatiegegevens. Wanneer lidstaten ervoor kiezen dit attribuut op te nemen, beschrijven zij in hun stelsel voor elektronische identificatie op grond waarvan de persoonsidentificatiegegevens worden verstrekt, het beleid dat zij toepassen op de waarden van dit attribuut, met inbegrip van, in voorkomend geval, specifieke voorwaarden voor de verwerking van deze waarde.
family_name_birth	Achternaam (of achternamen) van de gebruiker op wie de persoonsidentificatiegegevens bij de geboorte betrekking hebben.
given_name_birth	Voornaam (of voornamen), met inbegrip van, indien van toepassing, middelste namen, van de gebruiker op wie de persoonsidentificatiegegevens bij de geboorte betrekking hebben.
sex	Deze waarde moet een van de volgende zijn: 0 = niet bekend; 1 = mannelijk; 2 = vrouwelijk; 3 = overig; 4 = interseksueel; 5 = divers; 6 = open; 9 = niet van toepassing. Voor de waarden 0, 1, 2 en 9 is ISO/IEC 5218 van toepassing.
email_address	E-mailadres van de gebruiker op wie de persoonsidentificatiegegevens betrekking hebben [overeenkomstig RFC 5322 [1]].

Gegevensidentificatie	Definitie
`mobile_phone_number`	Mobiel nummer van de gebruiker waarop de persoonsidentificatiegegevens betrekking hebben, dat begint met "+" als internationale code en de landcode, gevolgd door uitsluitend getallen

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

2) Afdeling 2: Identificatiegegevens van rechtspersonen

Tabel 3

Verplichte persoonsidentificatiegegevens voor rechtspersonen

Gegevensidentificatie
huidige wettelijke naam
unieke identificatiecode, door de lidstaat van verzending vastgesteld volgens de technische specificatie voor grensoverschrijdende identificatie, zodanig dat die zo lang mogelijk stabiel blijft

— Als een gegevensidentificatie niet bekend is voor de persoon of niet anderszins kan worden uitgegeven als onderdeel van de persoonsidentificatiegegevens, gebruiken de lidstaten in plaats daarvan een attribuutwaarde die passend is voor de situatie.

Tabel 4

Optionele persoonsidentificatiegegevens voor rechtspersonen

Gegevensidentificatie
huidig adres
btw-nummer
fiscaal registratienummer
Europese unieke identificatiecode in de zin van Richtlijn (EU) 2017/1132 van het Europees Parlement en de Raad ([1])
identificatiecode voor juridische entiteiten bedoeld in Uitvoeringsverordening (EU) 2022/1860 van de Commissie ([2])
registratie- en identificatienummer van marktdeelnemer (EORI-nr.) bedoeld in Uitvoeringsverordening (EU) nr. 1352/2013 van de Commissie ([3])
het accijnsnummer bedoeld in artikel 2, punt 12, van Verordening (EU) nr. 389/2012 van de Raad ([4])

([1]) Richtlijn (EU) 2017/1132 van het Europees Parlement en de Raad van 14 juni 2017 aangaande bepaalde aspecten van het vennootschapsrecht (PB L 169 van 30.6.2017, blz. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Uitvoeringsverordening (EU) 2022/1860 van de Commissie van 10 juni 2022 tot vaststelling van technische uitvoeringsnormen voor de toepassing van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad met betrekking tot de normen, formats, frequentie en methoden en regelingen voor rapportage (PB L 262 van 7.10.2022, blz. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Uitvoeringsverordening (EU) nr. 1352/2013 van de Commissie van 4 december 2013 tot vaststelling van de formulieren waarin is voorzien in Verordening (EU) nr. 608/2013 van het Europees Parlement en de Raad inzake de handhaving van intellectuele-eigendomsrechten door de douane (PB L 341 van 18.12.2013, blz. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Verordening (EU) nr. 389/2012 van de Raad van 2 mei 2012 betreffende administratieve samenwerking op het gebied van de accijnzen en houdende intrekking van Verordening (EG) nr. 2073/2004 (PB L 121 van 8.5.2012, blz. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

3) Afdeling 3: Metagegevens over persoonsidentificatiegegevens

Tabel 5

Metagegevens over de persoonsidentificatiegegevens

Gegevensidentificatie	Definitie	Vermelding
`issuing_authority`	Naam van de administratieve instantie die de persoonsidentificatiegegevens heeft uitgegeven, of de alpha-2-landcode als bedoeld in ISO 3166 van de desbetreffende lidstaat indien er geen afzonderlijke instantie is die bevoegd is om persoonsidentificatiegegevens uit te geven.	Verplicht
`issuing_country`	Alpha-2-landcode, zoals gespecificeerd in ISO 3166-1, van het land of gebied van de verstrekker van de persoonsidentificatiegegevens.	Verplicht
`expiry_date`	Datum (en indien mogelijk tijdstip) waarop de administratieve geldigheidsduur van de persoonsidentificatiegegevens verstrijkt.	Facultatief
`document_number`	Een nummer voor de persoonsidentificatiegegevens, toegekend door de verstrekker van persoonsidentificatiegegevens.	Facultatief
`issuing_jurisdiction`	Code voor de afdeling van de rechtsmacht in een land die de persoonsidentificatiegegevens heeft uitgegeven, zoals gespecificeerd in ISO 3166-2:2020, punt 8. Het eerste deel van de code moet gelijk zijn aan de waarde voor het land van uitgifte.	Facultatief
`issuance_date`	Datum (en indien mogelijk tijdstip) waarop de administratieve geldigheidsduur van de persoonsidentificatiegegevens is ingegaan.	Facultatief

4) Afdeling 4: Codering van attributen voor identificatiegegevens van natuurlijke personen

— De identificatiegegevens van natuurlijke personen worden uitgegeven overeenkomstig de normen van punt 5 (SD-JWT VC-formaat) en punt 6 (ISO/IEC mdoc-formaat) van bijlage II bij Uitvoeringsverordening (EU) 2024/2979, zoals van toepassing op elektronische attesteringen van attributen. De punten 5.2.2, 5.2.4, 5.2.5, EEA-6-1-03, 6.2.2, 6.2.3, 6.2.4 en 6.2.5 zijn niet van toepassing.

— De codering van identificatiegegevens van natuurlijke personen voldoet aan de technische specificaties in de punten 4.1 en 4.2 van deze bijlage.

4.1 Codering van identificatiegegevens van natuurlijke personen in ISO/IEC-mdoc-formaat

— Het soort attestering voor persoonsidentificatiegegevens in ISO/IEC-mdoc-formaat is “eu.europa.ec.eudi.pid.1”. De identificator van de naamruimte (“namespace”) voor de attributen voor persoonsidentificatiegegevens in deze bijlage is “eu.europa.ec.eudi.pid.1”.

— Wanneer de persoonsidentificatiegegevens gegevens bevatten waarvoor geen identificatiegegevens in deze bijlage zijn opgenomen, worden deze gegevens gedefinieerd in een nationale naamruimte voor persoonsidentificatiegegevens die gebruikmaakt van het algemene formaat eu.europa.ec.eudi.pid. [ISO 3166-1 alpha-2 landcode of de ISO 3166-2 regiocode], gevolgd door een optioneel punt en versienummer.

— Wanneer de nationale naamruimte wordt gebruikt, wordt de regeling ervan, met inbegrip van alle identificatiecodes, de definities, aanwezigheden en coderingsformaten ervan, bekendgemaakt overeenkomstig artikel 8 van Uitvoeringsverordening (EU) 2025/1569 van de Commissie ([1]).

— De persoonsidentificatiegegevens en de metagegevens daarvan, zoals vastgesteld in de punten 1 en 3 van deze bijlage, worden opgenomen in persoonsidentificatiegegevenselementen in de zin van de specificaties van het ISO/IEC mdoc-format.

— Het deviceKey-lid binnen het deviceKeyInfo-lid van de instantie van het type MobileSecurityObject bevat een openbare sleutel.

— Die openbare sleutel komt overeen met een privésleutel die is opgeslagen in het beveiligd cryptografisch middel voor portemonnees ("WSCD") van de portemonneegebruiker.

— De beschermde header van de CB-AdES-digitale handtekening ter ondertekening van persoonsidentificatiegegevens in ISO/IEC-mdoc-formaat bevat de headerparameters x5u en x5t, die beide zijn gespecificeerd in RFC 9360 ([2]).

— Het in de xt5-headerparameter gebruikte hash-algoritme is SHA-256.

— De vereisten voor het coderen van persoonsidentificatiegegevens in ISO/IEC-mdoc-formaat zijn opgenomen in tabel 6:

Tabel 6

Vereisten voor codering van persoonsidentificatiegegevens in ISO/IEC-mdoc-formaat

Gegevensidentificatie	Identificatiecode attribuut	Format van de codering
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]) Uitvoeringsverordening (EU) 2025/1569 van de Commissie van 29 juli 2025 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad inzake door of namens een voor een authentieke bron verantwoordelijke openbare instantie verstrekte gekwalificeerde elektronische attesteringen van attributen en elektronische attesteringen van attributen (PB 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/).

Gegevensidentificatie	Identificatiecode attribuut	Format van de codering
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate of 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 of full-date

— Voor de notatie van het coderingsformaat van de in tabel 6 gespecificeerde attributen wordt gebruikgemaakt van weergavetypen zoals gespecificeerd in RFC 8610 ([3]), met de volgende aanvullende vereisten:

a) een tstr wordt gecodeerd in UTF-8;

b) een tstr ondersteunt het volledige Unicode-bereik;

c) een tstr heeft een maximumlengte van 150 tekens;

d) een datum wordt gecodeerd zoals gespecificeerd in RFC 8943 ([4]);

e) een full-date (volledige datum) wordt geïnterpreteerd als #6.1004(tstr), met tag 1004 zoals gespecificeerd in RFC 8943;

f) een tdate-attribuut bevat een datumtijdreeks zoals gespecificeerd in RFC 3339 ([5]);

g) een full-date-attribuut bevat een full-date-string zoals gespecificeerd in RFC 3339, overeenkomstig RFC 8943;

h) tenzij anders aangegeven, geldt dat een weergave van een datum in attributen:

— geen gebruik maakt van fracties van seconden;

— geen gebruik maakt van lokale offset van UTC en dat de in RFC 3339 gespecificeerde tijdoffset "Z" moet zijn;

i) een geheel getal met hoofdwaarden 0 en 1 moet zo klein mogelijk zijn, zoals gespecificeerd in RFC 8949 ([6]), punt 4.2;

j) een place_of_birth (geboorteplaats) bevat ten minste een van de volgende sleutel-waarde-paren: "country", "region", of "locality" (land, regio of plaats);

k) de uitdrukking van de lengte in een bstr, tstr, array of map moet zo kort mogelijk zijn, zoals gespecificeerd in RFC 8949, punt 4.2;

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

l) het attribuut nationaliteit wordt gecodeerd als een array van alpha-2-landcodes zoals gespecificeerd in ISO 3166-1. Wanneer de in RFC 8610 gespecificeerde CDDL-notatie wordt gebruikt, is de codering van dit attribuut:

— nationalities = [+ CountryCode]

— CountryCode = tstr; alpha-2-landcode gespecificeerd in ISO 3166-1

— wanneer een portemonneegebruiker op wie de persoonsidentificatiegegevens betrekking hebben, meerdere nationaliteiten heeft en de verstrekker van persoonsidentificatiegegevens deze meerdere nationaliteiten attesteert, kan de verstrekker van persoonsidentificatiegegevens alle nationaliteiten in de persoonsidentificatiegegevens opnemen;

— het attribuut place_of_birth wordt gecodeerd als een type place_of_birth. Wanneer de in RFC 8610 gespecificeerde CDDL-notatie wordt gebruikt, is de codering van dit attribuut:

place_of_birth =

{

? “country”: tstr; een enkele alpha-2-landcode als gespecificeerd in ISO 3166-1

? “region”: tstr; de naam van een staat, provincie, district of lokale regio

? “locality”: tstr; de naam van een gemeente, stad of dorp

}

4.2 Vereisten voor codering van persoonsidentificatiegegevens in SD-JWT VC-formaat

— De persoonsidentificatiegegevens en de metagegevens daarvan zoals vastgesteld in dit deel, worden opgenomen in persoonsidentificatiegegevens als claims in de zin van de specificaties van het SD-JWT VC-formaat.

— Alle claims in de uitgegeven persoonsidentificatiegegevens, als bedoeld in het vorige streepje, moeten afzonderlijk selectief openbaar kunnen worden gemaakt, met uitzondering van claims die zijn gedefinieerd als niet-selectief openbaar te maken in SD-JWT VC-formaat.

— Tabel 7 specificeert de codering van namen van claims die publieke namen zijn.

— Tabel 8 specificeert de codering van namen van claims die specifiek zijn voor de persoonsidentificatiegegevens.

— Een JSON-string die wordt gebruikt in persoonsidentificatiegegevens die zijn gecodeerd in SD-JWT VC, wordt gecodeerd in UTF-8 en ondersteunt het volledige Unicode-bereik, tenzij uitdrukkelijk anders vermeld in onderstaande tabel 8 of de verwijzingen daarin.

— De JWT-claims nbf en exp zoals gedefinieerd in RFC 7519 ([7]) worden gebruikt om de technische geldigheidsperiode van persoonsidentificatiegegevens met SD-JWT VC formaat uit te drukken.

([7]) J. Jones, et al., “JSON Web Token (JWT)”, RFC 7519, mei 2015.

— Persoonsidentificatiegegevens bevatten de cnf-claim als gedefinieerd in RFC 7800 ([8]), die een openbare sleutel is, gegenereerd uit een privésleutel, opgeslagen in het WSCD van de portemonnee-eenheid van de portemonneegebruiker.

— De beschermde header van de digitale handtekening ter ondertekening van persoonsidentificatiegegevens in ISO/IEC-mdoc-formaat bevat de headerparameters x5u en x5t#S256, gespecificeerd in RFC 7515 ([9]).

Tabel 7

Vereisten voor codering van persoonsidentificatiegegevens in SD-JWT VC-formaat met gebruikmaking van publieke namen

Gegevensidentificatie	Identificatiecode attribuut	Format van de codering
`family_name`	`family_name`	string
`given_name`	`given_name`	string
`birth_date`	`birthdate`	string, ISO 8601-1, formaat JJJJ-MM-DD
`birth_place`	`place_of_birth`	JSON structure
`nationality`	`nationalities`	array van strings
`resident_address`	`address.formatted`	string
`resident_country`	`address.country`	string
`resident_state`	`address.region`	string
`resident_city`	`address.locality`	string
`resident_postal_code`	`address.postal_code`	string
`resident_street`	`address.street_address`	string
`family_name_birth`	`birth_family_name`	string
`given_name_birth`	`birth_given_name`	string
`email_address`	`email`	string
`mobile_phone_number`	`phone_number`	string
`portrait`	`picture`	string; gegevens-URL die een base64-gecodeerd portret in JPEG-formaat bevat

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

Tabel 8

Vereisten voor codering van persoonsidentificatiegegevens in SD-JWT VC-formaat met gebruikmaking van niet-publieke namen

Gegevensidentificatie	Identificatiecode attribuut	Format van de codering
expiry_date	date_of_expiry	string, ISO 8601-1, formaat JJJJ-MM-DD
issuance_date	date_of_issuance	string, ISO 8601-1, formaat JJJJ-MM-DD
personal_administrative_-number	personal_administrati-ve_number	string
sex	sex	getal
issuing_authority	issuing_authority	string
issuing_country	issuing_country	string
document_number	document_number	string
issuing_jurisdiction	issuing_jurisdiction	string

— Het basistype van persoonsidentificatiegegevens is “urn:eudi:pid:1”, dat is opgenomen in de vct-claim. Alle persoonsidentificatiegegevens gebruiken typen in de naamruimte “urn:eudi:pid:”.

— Wanneer persoonsidentificatiegegevens attributen omvatten die niet in deze bijlage zijn gespecificeerd, worden deze attributen gedefinieerd binnen een nationaal type.

— Wanneer het nationale type wordt gebruikt, wordt de regeling ervan, met inbegrip van alle identificatiecodes, de definities, aanwezigheid en coderingsformaten ervan, gedefinieerd in een stelsel dat is bekendgemaakt overeenkomstig artikel 8 van Uitvoeringsverordening (EU) 2025/1569.

5) Afdeling 5: Gegevens over de vertrouwensinfrastructuur

De lijst van verstrekkers van persoonsidentificatiegegevens die door de Commissie beschikbaar is gesteld overeenkomstig Uitvoeringsverordening (EU) 2024/2980 moet de authentificatie van persoonsidentificatiegegevens mogelijk maken.”

BIJLAGE II

"BIJLAGE I bis

Cryptografische mechanismen als bedoeld in artikel 5 bis

Europese Groep voor cyberbeveiligingscertificering, subgroep inzake cryptografie: "Agreed Cryptographic Mechanisms", gepubliceerd door het Agentschap van de Europese Unie voor cyberbeveiliging ("Enisa") [1]."

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

BIJLAGE III

"BIJLAGE I ter

Technische specificaties voor portemonnee-eenheidsattesteringen als bedoeld in artikel 6, lid 2 bis

1) Een portemonnee-eenheidsattestering bestaat uit een of meer portemonnee-instantie-attesteringen en een of meer sleutelattesteringen.

2) De portemonnee-instantie-attesteringen en de sleutelattesteringen voldoen aan de volgende vereisten:

a) Vereisten voor het formaat

— FR-WIA-1: Een portemonnee-instantie-attestering is een JSON Web Token (JWT) zoals gespecificeerd in RFC 7519 ([1]), ondertekend of verzegeld door de portemonneeaanbieder aan de hand van een Compact JAdES baseline B-handtekening.

— FR-WIA-1.1: Een portemonnee-instantie-attestering is een portemonnee-attestering zoals gespecificeerd in appendix E van OpenID for Verifiable Credential Issuance v1.0 ([2]) ("OID4VCI") en uitgebreid zoals gespecificeerd in C-CIA-1 en C-WIA-2 hieronder.

— FR-KA-1: Een sleutelattestering is een JWT zoals gespecificeerd in RFC 7519, ondertekend of verzegeld door de portemonneeaanbieder aan de hand van een Compact JAdES baseline B-handtekening.

— FR_KA_1.1: Een sleutelattestering is een sleutelattestering zoals gespecificeerd in appendix D van OID4VCI, uitgebreid zoals gespecificeerd in C_KA-1 en C_KA-2 hieronder.

b) Eisen voor veilig transport

— TR-WIA-1: Een portemonnee-eenheid gebruikt een portemonnee-instantie-attestering bij de uitgifte van persoonsidentificatiegegevens, gekwalificeerde of niet-gekwalificeerde elektronische attesteringen van attributen, of door of namens een voor een authentieke bron verantwoordelijke openbare instantie verstrekte elektronische attesteringen van attributen.

— TR-WIA-2: Een portemonneeaanbieder verifieert de integriteit van de portemonnee-instantie en ondertekent of verzegelt de portemonnee-instantie-attestering.

— TR-WIA-2.1: Wanneer een portemonneeaanbieder een portemonnee-instantie-attestering uitgeeft, bedraagt het verschil tussen het tijdstip waarop de portemonneeaanbieder de integriteit van de portemonnee-instantie heeft geverifieerd en het tijdstip dat hij in de "exp"-headerparameter van de uitgegeven portemonnee-instantie-attestering zal aangeven, minder dan 24 uur.

— TR-WIA-2.2: De portemonneeaanbieder waarborgt dat een portemonnee-eenheid de portemonnee-instantie-attesteringen bevat die nodig zijn voor de uitgifte van persoonsidentificatie-gegevens en elektronische attesteringen van attributen.

— TR-WIA-3: Tijdens de uitgifte stuurt een portemonnee-eenheid een portemonnee-instantie-attestering naar een autorisatieserver in het vooraf ingediende autorisatieverzoek en het tokenverzoek, zoals gespecificeerd in OID4CI.

— TR-WIA-3.1: Een portemonnee-eenheid stuurt de portemonnee-instantie-attestering samen met bewijs van bezit ("PoP"), zoals gespecificeerd in appendix E van OID4VCI.

— TR-WIA-3.2: Een portemonnee-eenheid stuurt eenzelfde portemonnee-instantie-attestering naar slechts één autorisatieserver.

([1]) RFC 7519: JSON Web Token (JWT), mei 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: Wanneer een portemonneeaanbieder de “per-issuer reuse”-optie zoals hierna gespecificeerd in R_WIA_1 gebruikt, kan een portemonnee-eenheid een portemonnee-instantie-attestering meerdere keren naar dezelfde autorisatieserver sturen.

— TR-WIA-3.2.2: Wanneer een portemonneeaanbieder de “per-issuer reuse”-optie niet gebruikt, gebruikt een portemonnee-eenheid een portemonnee-instantie-attestering in ten hoogste één uitgifteproces.

— TR-WIA-4: Wanneer een autorisatieserver een portemonnee-instantie-attestering ontvangt, controleert die de handtekening van de portemonnee-instantie-attestering die gebruikmaakt van de openbare sleutel van het handtekeningcertificaat in de x5c-parameter in de JOSE-header van de portemonnee-instantie-attestering.

— TR-WIA-4.1: De autorisatieserver verifieert ook dat het handtekeningcertificaat kan worden geverifieerd met een vertrouwensanker op de lijst in verband met portemonneeaanbieders als genoemd in artikel 5 van Uitvoeringsverordening (EU) 2024/2980, mogelijk met gebruikmaking van in de x5c parameter inbegrepen tussencertificaten.

— TR-WIA-4.2: De autorisatieserver verifieert dat de portemonnee-instantie-attestering niet is vervallen.

— TR-WIA-4.3: De autorisatieserver verifieert de handtekening van de PoP in de openbare sleutel die aanwezig is in de “cnf”-claim.

— TR_KA-1: Een portemonnee-eenheid gebruikt een sleutelattestering bij de uitgifte van persoonsidentificatiegegevens en bij de uitgifte van apparaatgebonden gekwalificeerde of niet-gekwalificeerde elektronische attesteringen van attributen of door of namens een voor een authentieke bron verantwoordelijke openbare instantie verstrekte elektronische attesteringen van attributen.

— TR_KA-1.1: Een portemonnee-eenheid gebruikt geen sleutelattestering bij de uitgifte van niet-apparaatgebonden gekwalificeerde of niet-gekwalificeerde elektronische attesteringen van attributen of door of namens een voor een authentieke bron verantwoordelijke openbare instantie verstrekte elektronische attesteringen van attributen.

— TR_KA-2: Een portemonneeaanbieder verstrekt een portemonnee-eenheid verschillende sleutelattesteringen voor het WSCD van de portemonnee-eenheid en voor elk van de keystores daarvan.

— TR_KA-2.1: De portemonneeaanbieder tekent of verzegelt een sleutelattestering, na verificatie door de portemonneeaanbieder dat de in de sleutelattestering geattesteerde sleutels zijn opgeslagen in het WSCD van de in de sleutelattestering omschreven portemonnee-eenheid of keystore.

— TR_KA-2.2: Een sleutelattestering bevat ten minste één geattesteerde openbare sleutel. Het aantal sleutels in de sleutelattestering dat naar een referentieverstrekker wordt verzonden, mag niet hoger liggen dan de maximale batchgrootte die door de referentieverstrekker is gespecificeerd in de metadata van de referentieverstrekker; zie ETSI TS 119 472-3 ([3]), parameter “credential_configurations_supported.” credential_metadata.credential_reuse_policy.options.batch_size.

— TR_KA-2.3: Een portemonneeaanbieder neemt een openbare sleutel (die overeenstemt met een privésleutel opgeslagen in het WSCD of de keystore van de portemonnee-eenheid) op in ten minste één sleutelattestering.

— TR_KA-2.4: Een portemonnee-eenheid gebruikt een sleutelattestering tijdens ten hoogste één uitgifte- of heruitgifteproces.

— TR_KA-2.5: Een portemonneeaanbieder waarborgt dat een portemonnee-eenheid in het bezit is van sleutelattesteringen die nodig zijn voor de uitgifte van persoonsidentificatiegegevens en apparaatgebonden elektronische attesteringen van attributen.

([3]) ETSI, “Elektronische handtekeningen en infrastructuren (ESI); JAdES digitale handtekeningen; deel 3: JAdES-niveaus en basisprofielen, “ETSI TS 119 472-3, V1.1.1, maart 2026.

— TR_KA-3: Wanneer dit tijdens de uitgifte nodig is, bevat een portemonnee-eenheid een sleutelattestering in het veld “proofs” van een referentieverzoek aan de referentieverstrekker, zoals gespecificeerd in OID4VCI, in een proof van ofwel het type “jwt” ofwel het type “attestation”.

— TR_KA_3.1: Wanneer een portemonnee-eenheid een sleutelattestering in een “jwt”-element omvat, ondertekent of verzegelt zij de sleutelattestering met gebruikmaking van de privésleutel die overeenstemt met de openbare sleutel bij index 0 van de “attested_keys”-array binnen het “key_attestation”-object.

— TR_KA-4: Wanneer een referentieverstrekker apparaatgebonden referenties uitgeeft, geeft hij in de “proof_types_supported”-parameter in de metadata van de referentieverstrekker, zoals gespecificeerd in punt 12.2.4 van OID4VCI, aan dat het zowel het “jwt”- als het “attestation”-bewijstype ondersteunt voor sleutelattesteringen die het “key_attestations_required”object bevatten.

— TR_KA-4.1: Wanneer een referentieverstrekker niet-apparaatgebonden referenties uitgeeft, laat hij de “proof_types_supported” en de “cryptographic_binding_methods_supported” parameters weg uit de metadata van de referentieverstrekker.

— TR_KA-5: Wanneer een referentieverstrekker een sleutelattestering ontvangt in een “jwt”- of een “attestation”-bewijstype, verifieert hij de handtekening van de sleutelattestering op basis van de openbare sleutel in het handtekeningcertificaat in de “x5c”-parameter in de JOSE-header van de sleutelattestering en of dit handtekeningcertificaat met een vertrouwensanker op de lijst voor in verband met portemonneeaanbieders als genoemd in artikel 5 van Uitvoeringsverordening (EU) 2024/2980 staat, mogelijk met gebruikmaking van in de “x5c”-parameter inbegrepen tussencertificaten.

— TR_KA-6: Wanneer een referentieverstrekker een sleutelattestering ontvangt in een “jwt”-bewijstype, gaat hij de handtekening na van het “jwt”-element in de sleutel bij index 0 van de “attested_keys”-array in het “key_attestation”-object dat vervat is in het “jwt”-element.

— TR_KA-6.1: De referentieverstrekker verifieert dat het “nonce”-veld van het “jwt”-element een geldig c_nonce van hun nonce_endpoint bevat, zoals gespecificeerd in OID4VCI.

— TR_KA-7: Wanneer een referentieverstrekker een sleutelattestering ontvangt in een “attestation”-bewijstype, verifieert hij of het “key_attestation”-object een geldig c_nonce van hun nonce_endpoint bevat.

— TR_KA-8: Een verstrekker van persoonsidentificatiegegevens waarborgt dat de persoonsidentificatiegegevens gebonden zijn aan een openbare sleutel die voortkomt uit een sleutelattestering waarin een WSCD wordt vermeld.

c) Inhoudelijke vereisten

— C_WIA-1: Een portemonnee-instantie-attestering bevat:

— de “wallet_name”-claim zoals gespecificeerd in appendix E van OID4VCI, waarbij de waarde de identificatiecode van de portemonnee-oplossing is die kan worden gevonden op de lijst van portemonneeaanbieders als genoemd in artikel 5 van Uitvoeringsverordening (EU) 2024/2980;

— een “wallet_version”-claim ([4]), die een string is waarvan de waarde de versie van de portemonnee-oplossing is;

— een “wallet_solution_certification_information”-claim, die een JSON-object is dat informatie bevat over de instantie voor conformiteitsbeoordeling die de portemonnee-oplossing heeft gecertificeerd, het certificeringsnummer, naargelang het geval, en andere relevante details met betrekking tot certificering;

([4]) Deze claim wordt in dit CIR gedefinieerd omdat hij geen deel uitmaakt van de OID4VCI-specificatie.

— een “client_status”-claim, met twee subvelden:

— “status”: een referentie van de statuslijst zoals gespecificeerd in appendix E van OID4VCI die staat voor de intrekkingsstatus van de portemonnee-instantie. Zie punt e) hieronder voor nadere bijzonderheden;

— “exp”: een “NumericDate”, zoals gespecificeerd in RFC 7519, waarin het tijdstip wordt gedefinieerd tot wanneer de portemonneeaanbieder de intrekkingsstatus zal behouden op de statuslijstindex bedoeld in “status”;

— de “exp”-claim zoals gespecificeerd in appendix E van OID4VCI.

— *OPMERKING*: De “client_status.status”-claim in een portemonnee-instantie-attestering staat voor de intrekkingsstatus van de portemonnee-instantie, niet voor de intrekkingsstatus van de attestering zelf. Zoals hieronder beschreven in R_WIA-1 kan een portemonneeaanbieder besluiten elke portemonnee-instantie-attestering te beperken tot een specifieke autorisatieserver op basis van de het feit dat alle attesteringen die naar die server worden gestuurd, dezelfde indexwaarde hebben in de vermelding “client_status.status”.

— *OPMERKING*: De “idx”-waarde in de “status”-claim kan worden gebruikt als een (paarsgewijze) unieke identificatiecode van de portemonnee-instantie en van de portemonnee-eenheid.

— C_WIA-2: Een portemonnee-instantie-attestering moet ook de “wallet_link”-claim zoals gespecificeerd in appendix E van OID4VCI bevatten en de waarde van deze claim is een URI waar nadere informatie over de portemonnee-oplossing beschikbaar is.

— C_WIA-3: Een autorisatieserver interpreteert de “exp”-parameter in het hoogste niveau van een portemonnee-instantie-attestering niet als het einde van de intrekkingsonderhoudsperiode van de portemonnee-instantie.

— *OPMERKING*: De “exp”-parameter in het hoogste niveau van de portemonnee-instantie-attestering geeft aan wanneer de attestering zelf verstrijkt.

— C_KA-1: Een sleutelattestering bevat:

— de claims “key_storage” en “user_authentication” zoals gespecificeerd in appendix D van OID4VCI:

— de attributen “key_storage” en “user_authentication” hebben de waarde “iso_18045_high” wanneer een sleutelattestering een WSCD vermeldt;

— de “certification”-claim zoals gespecificeerd in appendix D van OID4VCI, die een URL bevat waar de informatie kan worden verkregen over de door de WSCD of keystore bereikte certificatie, indicatief de regeling zoals Common Criteria of GlobalPlatform, de geëvalueerde vereisten zoals het toepasselijke Protection Profile, en het evaluatieniveau.

— Uit deze informatie moet kunnen worden opgemaakt of de sleutelopslag een WSCD is;

— een “key_storage_status”-claim, met twee subvelden:

— “status”: een referentie van de statuslijst zoals gespecificeerd in appendix D.1 van OID4VCI. De waarde staat ofwel voor de intrekkingsstatus van het WSCD of keystoretype dat wordt gebruikt om de geattesteerde sleutels op te slaan, of — bij de indexoptie per-key-attestation — de intrekkingsstatus van een WSCD of keystore van een individuele portemonnee-eenheid. Zie R_KA_1 hieronder voor de beschikbare indextoewijzingsopties;

— “exp”: een “NumericDate”, zoals gespecificeerd in RFC 7519, waarin het tijdstip wordt gedefinieerd tot wanneer de portemonneeaanbieder de intrekkingsstatus zal behouden op de statuslijstindex bedoeld in “status”;

— de “exp”-claim zoals gespecificeerd in appendix D van OID4VCI.

— *OPMERKING* over de “idx”-waarde in de “key_storage_status.status”-claim in een sleutelattestering: Wanneer de portemonneeaanbieder de “type-shared index”-optie (zie R_KA_1 hieronder) gebruikt, hebben alle sleutelattesteringen voor hetzelfde type WSCD of keystore dezelfde statuslijstindex. De “idx”-waarde is daarom niet uniek per portemonnee-eenheid. Anderzijds, wanneer de portemonneeaanbieder de “per-key-attestation index”-optie gebruikt, is de “idx” value uniek voor de portemonnee-eenheid (of paarsgewijs uniek per referentieverstrekker). In alle gevallen gebruikt een referentieverstrekker echter geen “idx”-waarde in een sleutelattestering als een identificatiecode voor een portemonnee-eenheid, maar in plaats daarvan de “idx”-waarde in een portemonnee-instantie-attestering.

— C_KA-2: Wanneer een sleutelattestering wordt verzonden in een “attestation”-bewijstype, bevat die ook een geldig “c_nonce” zoals gespecificeerd in appendix F.3 van OID4VCI.

— C_KA-3: Een referentieverstrekker interpreteert de “exp”-parameter in het hoogste niveau van een sleutelattestering niet als het einde van de intrekkingsonderhoudsperiode van het WSCD of keystore.

— *OPMERKING*: De “exp”-parameter in het hoogste niveau van een sleutelattestering geeft aan wanneer de sleutelattestering zelf verstrijkt.

d) Levenscyclusvereisten

— Deze bijlage specificeert de volgende metadata parameters van de metadata van de referentieverstrekker:

  — “preferred_client_status_period”: OPTIONAL. Een geheel getal dat de geprefereerde resterende statusonderhoudsperiode van de portemonnee-instantie-attestering specificeert die de portemonnee-eenheid tijdens de uitgifte moet tonen, in seconden. De resterende statusonderhoudsperiode wordt gedefinieerd als de waarde van “client_status.exp” in de attestering min het tijdstip van ontvangst van de attestering;

  — “preferred_key_storage_status_period”: OPTIONAL. Een geheel getal dat de geprefereerde resterende statusonderhoudsperiode van de sleutelattestering specificeert die de portemonnee-eenheid tijdens de uitgifte moet tonen, in seconden. De resterende statusonderhoudsperiode wordt gedefinieerd als de waarde “key_storage_status.exp” in de attestering min het tijdstip van ontvangst van de attestering.

— LC_WIA-1: Een autorisatieserver mag zijn voorkeuren voor de resterende statusonderhoudsperiode bij portemonnee-instantie-attesteringen meedelen door de “preferred_client_status_period”-metadataparameter op te nemen in de endpoint van de metadata van de referentieverstrekker zoals gespecificeerd in deel 12.2.2 van OID4VCI.

  — LC_WIA-1.1: Dit veld wordt op het hoogste niveau van de metadata van de referentieverstrekker geplaatst.

— LC_WIA_2: Een autorisatieserver interpreteert de “exp”-parameter in het hoogste niveau van een portemonnee-instantie-attestering niet als het einde van de intrekkingsonderhoudsperiode van de portemonnee-instantie.

— LC_WIA_3: Wanneer een portemonneeaanbieder een portemonnee-instantie-attestering ondertekent of verzegelt, behoudt die de intrekkingsstatus van de relevante portemonnee-instantie totdat de in die portemonnee-instantie-attestering aangegeven “wallet_instance_status.exp” verstreken is.

— LC_KA-1: Wanneer een sleutelattestering nodig is, kan een referentieverstrekker zijn voorkeuren voor de resterende statusonderhoudsperiode in sleutelattesteringen meedelen door opname van de “preferred_-key_storage_status_period” metadataparameter zoals hierboven aangegeven in het endpoint van de metadata van de referentieverstrekker zoals gespecificeerd in deel 12.2.2 van OID4VCI.

  — LC_KA-1.1: Dit veld wordt geplaatst binnen het “key_attestations_required”-object zoals gespecificeerd in deel 12.2.4 van OID4VCI.

— LC_KA-2: Een portemonneeaanbieder bepaalt de technische geldigheidsduur van de sleutelattesteringen die hij uitgeeft.

— LC_KA-3: Wanneer een portemonneeaanbieder een sleutelattestering ondertekent of verzegelt, behoudt die de intrekkingsstatus van de relevante WSCD of keystore totdat de in die attestering aangegeven "key_storage_status.exp" verstreken is.

— LC_GEN-1: Een portemonneeaanbieder waarborgt dat een portemonnee-eenheid steeds portemonnee-eenheidsattesteringen en sleutelattesteringen kan voorleggen met een geldigheidsduur van de "client_status.exp" respectievelijk de "key_storage_status.exp"van ten minste 31 dagen na het moment van voorlegging aan een autorisatieserver of een referentieverstrekker.

— *OPMERKING*: Dit waarborgt dat verstrekkers van persoonsidentificatiegegevens kunnen vertrouwen op een intrekkingsketen zonder gedwongen te zijn persoonsidentificatiegegevens met een korte levensduur af te geven.

— LC_GEN-2: Een portemonneeaanbieder waarborgt dat een portemonnee-eenheid tijdens de uitgifte metadata van de referentieverstrekker ophaalt.

  — LC_GEN_2.1: Wanneer deze metadata een veld "preferred_key_storage_status_period" bevatten, stuurt de portemonnee-eenheid een sleutelattestering met ("key_storage_status.exp" — huidige tijd) — "preferred_key_storage_status_period" die zo klein mogelijk maar niet negatief is. Wanneer de portemonnee-eenheid niet over een dergelijke sleutelattestering beschikt, verkrijgt zij van de portemonneeaanbieder een nieuwe sleutelattestering die voldoet aan "key_storage_status.exp" — huidige tijd ≥ "preferred_key_storage_status_period".

  — LC_GEN_2.2: Wanneer deze metadata een veld "preferred_client_status_period" bevatten, stuurt de portemonnee-eenheid een portemonnee-instantie-attestering met ("client_status.exp" — huidige tijd) — "preferred_client_status_period" die zo klein mogelijk maar niet negatief is. Wanneer de portemonnee-eenheid niet over een dergelijke portemonnee-instantie-attestering beschikt, verzoekt zij de portemonneeaanbieder om een nieuwe portemonnee-instantie-attestering die voldoet aan "client_status.exp" — current time ≥ "preferred_client_status_period".

— LC_GEN-3: De technische geldigheidsduur van de persoonsidentificatiegegevens verloopt vóór zowel de "client_status.exp" van de portemonnee-instantie-attestering als de "key_storage_status.exp" van de sleutelattestering die tijdens het uitgifteproces naar de verstrekkers van persoonsidentificatiegegevens wordt gestuurd.

— LC_GEN-4: Een verstrekker van persoonsidentificatiegegevens met een technische geldigheidsduur van meer dan 24 uur controleert ten minste om de 24 uur, tijdens de technische geldigheidsduur van de persoonsidentificatiegegevens, de intrekkingsstatus van zowel de portemonnee-instantie-attestering als de sleutelattestering die tijdens de uitgifte is ontvangen. Indien een van beide is ingetrokken, trekt de aanbieder de persoonsidentificatiegegevens in.

e) Vereisten voor intrekking

— R_GEN-1: Een portemonneeaanbieder gebruikt Token Status Lists (zoals gespecificeerd in IETF Token Status List) als intrekkingsmechanisme voor zowel sleutelattesteringen als portemonnee-instantie-attesteringen, zoals gespecificeerd in respectievelijk appendices D en E van OID4VCI.

— *OPMERKING*: Om de schaalbaarheid van zijn statuslijsten (Status Lists) te verbeteren, kan een portemonneeaanbieder de volgende optimalisaties gebruiken:

  — de statuslijst opsplitsen in meerdere blokken (chunks), wanneer de portemonneeaanbieders een aanzienlijk aantal gebruikers hebben en attesteringen hebben uitgegeven. Er bestaan veel blokverdelingsstrategieën (chunking strategies), bijvoorbeeld op basis van een vaste omvang of per periode. De chunking strategy wordt overgelaten aan de portemonneeaanbieder. Overwegingen kunnen betrekking hebben op de omvang van een statuslijst voor downloaden en de privacy van de gebruiker;

  — meerdere statuslijsten hebben;

  — een statuslijst comprimeren om de omvang te verkleinen.

— R_WIA-1: Een portemonneeaanbieder kan dezelfde waarde toewijzen aan de “idx”-claim in de “client_status.status”-claim in alle portemonnee-instantie-attesteringen die een bepaalde portemonnee-eenheid aan eenzelfde server aanbiedt. Dit wordt de “per-issuer reuse”-optie genoemd. Indien voor deze optie wordt gekozen:

  — R_WIA-1.1: De portemonnee-eenheid houdt bij welke indexwaarde zij heeft gebruikt voor elke autorisatieserver waarmee zij eerder heeft gecommuniceerd, en verzoekt om een portemonnee-instantie-attestering met dezelfde indexwaarde wanneer zij opnieuw met dezelfde autorisatieserver communiceert.

  — R_WIA-1.2: Wanneer een portemonneeaanbieder een verzoek ontvangt voor een portemonnee-instantie-attestering met een specifieke indexwaarde, verifieert hij of de verzoekende portemonnee-eenheid die indexwaarde eerder heeft ontvangen, alvorens een nieuwe portemonnee-instantie-attestering met die indexwaarde af te geven.

  — R_WIA-1.3: De portemonnee-eenheid gebruikt eenzelfde indexwaarde niet opnieuw voor interacties met andere autorisatieservers.

— *OPMERKING*: Wanneer gebruik wordt gemaakt van de “per-issuer reuse”-optie, is de portemonneeaanbieder in staat te bepalen met hoeveel autorisatieservers een portemonnee-eenheid heeft gecommuniceerd en hoe vaak zij met iedere server communiceert.

— R_WIA-2: In zijn privacybeleid geeft de portemonneeaanbieder aan of hij de “per-issuer reuse”-optie gebruikt voor intrekking van een portemonnee-instantie.

— R_WIA-3: Wanneer een portemonneeaanbieder de “per-issuer reuse”-optie niet gebruikt, kent de portemonneeaanbieder een nieuwe, niet-koppelbare indexwaarde toe aan elke portemonnee-instantie-attestering die hij uitgeeft.

— R_WIA-4: Wanneer een portemonnee-eenheid moet worden ingetrokken, trekt een portemonneeaanbieder de indexwaarden in de “client_status.status”-claim in voor alle portemonnee-instantie-attesteringen die bij die portemonnee-eenheid horen.

— R_WIA-5: Een portemonneeaanbieder houdt bij het bepalen van de omvang van de statuslijsten van zijn portemonnee-instantie-attestering rekening met de schaal van zijn implementatie en de onderliggende architectuur, en waarborgt dat die groot genoeg zijn om correlatie te voorkomen en de privacy van gebruikers te beschermen. Een statuslijst heeft, indien mogelijk, ten minste betrekking op 10 000 attesteringen.

— R_KA_1: Een portemonneeaanbieder kiest een van de volgende indextoewijzingsopties voor de “key_storage_status.status”-claim in een sleutelattestering:

  — optie 1, de “type-shared index”, waarin alle sleutelattesteringen die sleutels attesteren die zijn opgeslagen en eenzelfde type WSCD of keystore dezelfde indexwaarde hebben in “key_storage_status.status”;

  — optie 2, de “per-key-attestion index”, waarin een sleutelattestering die sleutels attesteren die zijn opgeslagen in een individuele WSCD of keystore een (paarsgewijs) unieke indexwaarde hebben in “key_storage_status.status”.

— *OPMERKING*: Wanneer een portemonneeaanbieder optie 1 gebruikt, worden alle belangrijke attesteringen van het betrokken type in alle portemonnee-eenheden ongeldig gemaakt door één enkele intrekkingsactie. Omdat alle sleutelattesteringen voor eenzelfde type WSCD of keystore één enkele statuslijstindex delen, weerspiegelt het aantal vermeldingen in de sleutelattesteringstatuslijst het aantal types WSCD of keystore dat de portemonneeaanbieder ondersteunt, en niet het aantal geïmplementeerde portemonnee-eenheden. De privacy-overwegingen die ten grondslag liggen aan de minimale omvang van de statuslijst voor portemonnee-instantie-statuslijsten zijn daarom niet van toepassing op de sleutelattesteringslijsten van optie 1, mits er genoeg portemonnee-eenheden zijn die gebruikmaken van hetzelfde type WSCD of keystore.

— *OPMERKING*: Wanneer een portemonneeaanbieder optie 2 gebruikt, staat elke index voor de intrekkingsstatus van de specifieke WSCD of keystore die in die sleutelattestering is geattesteerd.

— *OPMERKING*: Wanneer een portemonneeaanbieder optie 2 gebruikt, kan een specifieke WSCD of keystore ook worden ingetrokken op verzoek van de gebruiker.

— R_KA-2: Wanneer een portemonneeaanbieder optie 2 gebruikt, mag de portemonneeaanbieder optioneel gebruikmaken van de “per-issuer reuse”-optie zoals beschreven in R_WIA-1. Als de portemonneeaanbieder deze optie gebruikt, zijn de vereisten R_WIA-1-R_WIA-3 mutatis mutandis van toepassing.

— R_KA-3: Wanneer een portemonneeaanbieder optie 2 gebruikt, houdt de portemonneeaanbieder bij het bepalen van de omvang van zijn sleutelattesterings-statuslijsten rekening met de schaal van zijn implementatie en de onderliggende architectuur, en waarborgt dat die groot genoeg zijn om correlatie te voorkomen en de privacy van gebruikers te beschermen. Een statuslijst heeft, indien mogelijk, ten minste betrekking op 10 000 sleutelattesteringen.

— R_KA-4: Wanneer een portemonneeaanbieder optie 1 (type-shared index) gebruikt, trekt de portemonneeaanbieder de “key_storage_status.status”-vermelding enkel in als het type WSCD of keystore een beveiligingslek vertoont.

f) Vereisten met betrekking tot handtekeningalgoritmen

— SA-1: Voor de ondertekening van portemonnee-instantie-attesteringen, sleutelattesteringen, gerelateerde bewijzen van bezit en token status lists wordt een van de volgende algoritmen gebruikt:

— ES256 (ECDSA met SHA-256 en P-256)

— ES384 (ECDSA met SHA-384 en P-384)

— ES512 (ECDSA met SHA-512 en P-521)

— SA-2: Een portemonneeaanbieder kiest welke van de in SA-1 vermelde algoritmen hij zal gebruiken.

— SA-3: Een autorisatieserver of een referentieverstrekker (zoals gespecificeerd in OID4VCI) ondersteunt alle in SA-1 genoemde algoritmen.”

BIJLAGE IV

"BIJLAGE II

Lijst van normen als bedoeld in artikel 8

De technische specificaties zoals bepaald in de punten 2 tot en met 6 van ETSI TS 119 472-1 V1.2.1 (2026-02) zijn van toepassing. Zij worden gelezen met de volgende aanpassingen:

1) 2.1 Normative references

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06): "Elektronische handtekeningen en infrastructuren (ESI); Certificaatprofielen; deel 1: Overzicht en gemeenschappelijke gegevensstructuren"

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09): "Elektronische handtekeningen en vertrouwensinfrastructuren (ESI); Certificaatprofielen; deel 6: Certificaatprofielvereisten voor verstrekkers van PID, portemonnee, EAA, QEAA en PSBEAA"

— [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: Wanneer een statuselement wordt gebruikt voor persoonsidentificatiegegevens, gekwalificeerde elektronische attesteringen van attributen of door of namens een voor een authentieke bron verantwoordelijke openbare instantie verstrekte elektronische attesteringen van attributen, geeft het alleen aan of de attestering al dan niet is ingetrokken en ondersteunt het geen andere statuswaarden, bijvoorbeeld schorsing.

— EAA-4.2.11.1-06.1: Wanneer een attestering wordt ingetrokken, wordt zij permanent ingetrokken.

3) 4.2.13 Kortlevende EAA

— EAA-4.2.13-03: Wanneer kortlevende elektronische attesteringen van attributen met een geldigheidsduur van ten hoogste 24 uur worden uitgegeven, is intrekking niet vereist.

4) 4.6.3 Vereisten voor EU-EAA, afgegeven door of namens een voor een authentieke bron verantwoordelijke openbare instantie (PuB-EAA)

— PuB-EAA-4.6.2-03: ongeldig

— Pub-EAA-4.6.2-04: ongeldig

— PuB-EAA-4.6.3-03: De digitale handtekening PuB-EAA moet het gekwalificeerde certificaat ter ondersteuning van de digitale handtekening PuB-EAA bevatten.

— PuB-EAA-4.6.3-04: Het gekwalificeerde certificaat ter ondersteuning van de digitale handtekening PuB-EAA voldoet aan de vereisten van punt 8 van ETSI TS 119 412-6 v1.1.1 en bevat de QcType qcStatement als gedefinieerd in ETSI EN 319 412-5 v2.5.1, met de waarde id-etsi-qct-eidaspsbeaa als volgt gedefinieerd:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } -- Certificaat als bedoeld in artikel 45 septies, lid 1, punt b), tot ondersteuning van de gekwalificeerde elektronische handtekening of de gekwalificeerde elektronische zegel van de in artikel 3, punt 46, van Verordening (EU) nr. 910/2014 bedoelde openbare instantie.

5) 5.2.10.1 General requirements

— EAA-5.2.10.1-04: ongeldig

— EAA-5.2.10.1-05: ongeldig

— EAA-5.2.10.1-06: Het statuslid kan het status_list-lid bevatten zoals gespecificeerd in punt 6.2 van IETF draft-ietf-oauth-status-list-20 [25].

— EAA-5.2.10.1-07: ongeldig

— EAA-5.2.10.1-08: ongeldig

— EAA-5.2.10.1-09: ongeldig

— EAA-5.2.10.1-10: ongeldig

— EAA-5.2.10.1-11: ongeldig

— EAA-5.2.10.1-12: ongeldig

6) 6.2.10.1 General requirements

— EAA-6.2.10.1-01: Wanneer een elektronische attestering van attributen volgens ISO/IEC mdoc gebruikmaakt van het attesteringsstatuslijstmechanisme als bepaald in EAA-6.2.10.1-02.2 of met het attesteringsintrekkingslijstmechanisme in EAA-6.2.10.1-02.3, bevat het Mobile Security Object ("MSO") de statusstructuur zoals gespecificeerd in EAA-6.2.10.1-17, waarin MSO-intrekkingsinformatie vervat zit.

— EAA-6.2.10.1-01.1: Wanneer het identificatielijstmechanisme wordt uitgevoerd, bevat het statuselement het identifier_list element als bepaald in EAA-6.2.10.1-11.

— EAA-6.2.10.1-01.2: Wanneer het statuslijstmechanisme wordt uitgevoerd, bevat het statuselement het status_list element als bepaald in EAA-6.2.10.1-13.

— *OPMERKING*:

  — De statusstructuur bevat een verwijzing naar een MSO-intrekkingslijst.

  — De MSO-intrekkingslijst is een COSE_Sign1-structuur die aangeeft of een bepaald MSO al dan niet is ingetrokken.

  — De statusstructuur bevat alle informatie die de op portemonnees vertrouwende partij nodig heeft om te bepalen of de MSO-intrekkingslijst authentiek is.

— EAA-6.2.10.1-02: De verstrekker van persoonsidentificatiegegevens, de verstrekker van gekwalificeerde elektronische attesteringen van attributen of de verstrekker van door of namens een voor een authentieke bron verantwoordelijke openbare instantie verstrekte elektronische attesteringen van attributen, gebruikt een van de volgende methoden voor de intrekking van persoonsidentificatiegegevens, gekwalificeerde elektronische attesteringen van attributen of elektronische attesteringen van attributen die worden verstrekt door of namens een voor een authentieke bron verantwoordelijke openbare instantie:

— EAA-6.2.10.1-02.1: Wanneer zij kortlevende elektronische attesteringen van attributen met een geldigheidsduur van ten hoogste 24 uur uitgeven, is intrekking niet vereist.

— EAA-6.2.10.1-02.2: Gebruik een attesteringsstatuslijstmechanisme om de intrekkingsinformatie als een statuslijst te gebruiken.

— EAA-6.2.10.1-02.2.1: De intrekking van een MSO door het statuslijstmechanisme hangt af van het feit of het bit in de door de uitgever gedefinieerde bit-positie in het MSO als "waar" in de statuslijst staat.

— EAA-6.2.10.1-02.2.2: Het statuslijstmechanisme wordt gespecificeerd in de token status list (draft-ietf-oauth-status-list-20)-specificatie.

— EAA-6.2.10.1-02.3: Gebruik een attesteringsintrekkingslijstmechanisme om de intrekkingsinformatie als een identificatiecodelijst te gebruiken.

— EAA-6.2.10.1-02.3.1: De intrekking van een MSO door het identificatiecodelijstmechanisme hangt af van het feit of de door de uitgever gedefinieerde identificatiecode in het MSO aanwezig is op de identificatiecodelijst.

— 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 en EAA-6.2.10.1-11 specificeren het identificatiecodelijstmechanisme, op basis van de vereisten uit de token status list-specificatie met inbegrip van de gemeenschappelijkheid tussen de statuslijst en het identificatiecodelijstmechanisme.

— EAA-6.2.10.1-03: Wanneer een statuselement wordt gebruikt voor persoonsidentificatiegegevens, gekwalificeerde elektronische attesteringen van attributen of door of namens een voor een authentieke bron verantwoordelijke openbare instantie verstrekte elektronische attesteringen van attributen, wordt uitsluitend de status "ingetrokken" (revoked) gebruikt.

— EAA-6.2.10.1-03.1: Voor een statuslijst betekent dit dat alleen de waarden "valid" en "invalid", zoals gespecificeerd in de token status list-specificatie worden gebruikt.

— EAA-6.2.10.1-03.2: Voor de identificatiecodelijst worden enkel ingetrokken MSO's, in tegenstelling tot tijdelijk opgeschorte MSO's, op de identificatiecodelijst geplaatst.

— EAA-6.2.10.1-04: Wanneer een MSO wordt ingetrokken, wordt het MSO permanent ingetrokken.

— EAA-6.2.10.1-05: Verificatie van de MSO-intrekkingslijst is facultatief voor de op portemonnees vertrouwende partij en voldoet, in voorkomend geval, aan de verificatievereisten gespecificeerd in de token status list-specificatie en de status structure-specificatie van de vereisten van EAA-6.2.10.1-01.

— EAA-6.2.10.1-05.1: Wanneer een op portemonnees vertrouwende partij de intrekkingsstatus van persoonsidentificatiegegevens of elektronische attesteringen van attributen moet kunnen verifiëren, wordt zowel het attestatiestatuslijstmechanisme als het attestatie-intrekkingslijstmechanisme als bepaald in EAA-6.2.10.1-02 ondersteund.

— EAA-6.2.10.1-06: De identifier_list en status_list in het MSO mogen het certificaatonderdeel bevatten.

— EAA-6.2.10.1-06.1: Wanneer het certificaatonderdeel aanwezig is, bevat het een certificaat met daarin de openbare sleutel die het basiscertificaat in het x5chain-element in de MSO-intrekkingslijststructuur heeft ondertekend.

— EAA-6.2.10.1-06.1.1: De op portemonnees vertrouwende partij gebruikt dat certificaat als vertrouwensanker voor de verificatie van het x5chain-element in de MSO-intrekkingslijststructuur.

— EAA-6.2.10.1-06.2: Wanneer het certificaatonderdeel niet aanwezig is, wordt het basiscertificaat in het x5chain-element in de MSO-intrekkingslijststructuur ondertekend of verzegeld door het certificaat dat wordt gebruikt om het certificaat in het x5chain-element van het MSO te ondertekenen.

— EAA-6.2.10.1-06.2.1: De op portemonnees vertrouwende partij gebruikt dat certificaat als vertrouwensanker voor de verificatie van het x5chain-element in de MSO-intrekkingslijststructuur.

— EAA-6.2.10.1-07: Een MSO-intrekkingslijst wordt uitgevoerd in overeenstemming met de token status list-specificatie als statuslijsttoken in CWT-formaat.

— EAA-6.2.10.1-08: Voor de MSO-intrekkingslijst voor het identificatiecodelijst- en statuslijstmechanisme, gelden de volgende vereisten:

  — de exp-claim moet aanwezig zijn;

  — de ttl-claim mag aanwezig zijn;

  — de aggregation_uri-claim in de IdentifierList or StatusList-claim mag aanwezig zijn en de verstrekker van persoonsidentificatiegegevens, de verstrekker van gekwalificeerde elektronische attesteringen van attributen of de verstrekker van door of namens een voor een authentieke bron verantwoordelijke

openbare instantie verstrekte elektronische attesteringen van attributen, mag gebruikmaken van de aggregation_uri-claim om steun aan te geven voor het aggregatiemechanisme zoals gespecificeerd in de token status list-specificatie;

— de CWT is een COSE_Sign1-object dat een van de volgende handtekeningalgoritmen gebruikt voor de berekening van de handtekening:

a) "ES256" (ECDSA met curve NIST P-256 en SHA-256);

b) "ES384" (ECDSA met curve NIST P-384 en SHA-384);

c) "ES512" (ECDSA met curve NIST P-521 en SHA-512);

d) "ESB256" (ECDSA met curve brainpoolP256r1 en SHA-256);

e) "ESB384" (ECDSA met curve brainpoolP384r1 en SHA-384);

f) "ESB512" (ECDSA met curve brainpoolP512r1 en SHA-512);

— de CWT bevat de x5chain in de beschermde header die het certificaat of de keten van certificaten bevat om de handtekening van de MSO-intrekkingslijst te verifiëren;

— het uitgebreide sleutelgebruik van de in de token status list-specificatie gespecificeerde objectidentificatiecode kan worden gebruikt voor de statuslijst en voor het handtekeningcertificaat van de identificatiecodelijst, en de op portemonnees vertrouwende partijen kunnen ondersteuning bieden voor het uitgebreide sleutelgebruik van in de token status list-specificatie gespecificeerde objectidentificatiecodes; en voor de objectidentificatiecode mag de verstrekker van gekwalificeerde elektronische attesteringen van attributen of de verstrekker van elektronische attesteringen van attributen die worden verstrekt door of namens een voor een authentieke bron verantwoordelijke openbare instantie, het uitgebreide sleutelgebruikveld niet van kritiek belang maken bij het gebruik van de in de token status list-specificatie gespecificeerde objectidentificatiecode van het uitgebreide sleutelgebruik.

— EAA-6.2.10.1-09: In afwijking van de vereisten voor de token status list-specificatie, gelden voor het identificatiecodelijstmechanisme de volgende vereisten:

— de waarde van de type-claim is "application/identifierlist+cwt";

— de StatusList-claim mag niet aanwezig zijn in de CWT-claimsset;

— de IdentifierList-structuur zoals gedefinieerd in EAA-6.2.10.1-11 is aanwezig als een claim in de CWT-claimsset met gebruikmaking van de sleutel 65530.

— EAA-6.2.10.1-10: De structuur van de IdentifierList is een CBOR-structuur met de volgende 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: Wanneer de identificatiecode in de IdentifierList aanwezig is, wordt het MSO dat de identificatiecode in het statuselement bevat, ingetrokken.

— EAA-6.2.10.1-10.2: De Aggregation_uri-claim wordt gespecificeerd in punt 9.2 van de token status list-specificatie.

— EAA-6.2.10.1-10.3: Het content-type van de identificatiecodelijst is “application/identifierlist+cwt” zoals bepaald in deel 8.2 van de token status list-specificatie.

— EAA-6.2.10.1-11: De volgende vereisten gelden voor het identifier_list-element in het MSO (zie EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: Het identifier_list-element is een CBOR-structuur met de volgende CDDL:

```
IdentifierListInfo = {

        “id” : Identifier,

        “uri” : URI,

        ? “certificate”: Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: Om ervoor te zorgen dat de identificatiecode niet kan worden gebruikt als een correlatie tussen opvragingen, is die uniek per MSO.

— EAA-6.2.10.1-12: De volgende vereisten gelden voor de statuslijst:

  — EAA-6.2.10.1-12.1: Het bits-element in de StatusList-structuur is 1.

— EAA-6.2.10.1-13: De volgende vereisten gelden voor het status_list-element in het MSO (zie EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: Het status_list-element volgt de vereisten voor de StatusListInfo-structuur zoals gespecificeerd in de token status list-specificatie, en het facultatieve certificaatonderdeel zoals gedefinieerd in EAA-6.2.10.1-06 wordt toegevoegd.

  — EAA-6.2.10.1-13.2: Om ervoor te zorgen dat de statusindex geen correlatie tussen opvragingen kan vormen, is de combinatie van statusindex en URI uniek per MSO.

— EAA-6.2.10.1-14: De portemonneeaanbieder gebruikt de tweede (EAA-6.2.10.1-02.2) of derde (EAA-6.2.10.1-02.3) methode zoals gespecificeerd in EAA-6.2.10.1-02 voor de intrekking van een portemonnee-instantie-attestering en voor de intrekking van een sleutelattestering.

— EAA-6.2.10.1-15: De portemonneeaanbieder gebruikt de mechanismen voor de intrekking van attesteringen zoals gespecificeerd in EAA-6.2.10.1-02 in de portemonnee-oplossing.

— EAA-6.2.10.1-16: De verstrekker van persoonsidentificatiegegevens en de verstrekker van elektronische attesteringen van attributen ondersteunen zowel het attesteringsstatuslijstmechanisme als het attesteringsintrekkingslijstmechanisme zoals gespecificeerd in EAA-6.2.10.1-02 voor de verificatie van de intrekkingsstatus van een portemonnee-instantie-attestering en van een sleutelattestering.

— EAA-6.2.10.1-17: De statusstructuur in het MSO is een CBOR-structuur met de volgende CDDL:

Status = {

? “identifier_list”: IdentifierListInfo,

? “status_list”: StatusListInfo,

* tstr => RFU

}”

BIJLAGE V

"BIJLAGE III

De in artikel 10 bedoelde technische specificaties

— Technische specificaties:

  — Punt 4.2.5 van ETSI TS 119 472-3 V1.1.1 (2026-03)."

"BIJLAGE VI

Bijlage IV bij Uitvoeringsverordening (EU) 2024/2979 wordt als volgt gewijzigd:

1) punt 1 wordt vervangen door:

"1. Verplicht formaat voor handtekeningen of zegels:

a) PAdES (PDF Advanced Electronic Signature) zoals gespecificeerd in ETSI EN 319 142-1 V1.2.1 (2024-01); Elektronische handtekeningen en infrastructuren (ESI); PAdES digitale handtekeningen; deel 1: Building blocks and PAdES baseline signatures.";

2) punt 3 wordt vervangen door:

"3. Applicatieprogramma-interface:
ETSI TS 119 432 v1.3.1 (2026-03) punten 6.4.3, A.6, A.7 en A.8."."

BIJLAGE VII

"BIJLAGE VI

EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit in kleur

"

BIJLAGE VIII

"BIJLAGE VII

EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit in zwart-wit

"

BIJLAGE IX

"BIJLAGE VIII

Gegevens van het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit

Gegevens	Beschrijving	Codering	Status
TrustMarkResourceURL	URL van de graphics van het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit en gebruikersinfo in de portemonneegebruiker-interface.	URL	Verplicht
ListOfCertifiedWalletsURL	URL van de openbare lijst van gecertificeerde portemonnee-oplossingen in de EU zoals vastgesteld in Uitvoeringsverordening (EU) 2025/849 van de Commissie ([1]).	URL	Verplicht
ListOfCertifiedWalletsQRCode	QR-code met de informatie van de ListOfCertifiedWalletsURL	ISO-8859-1 Byte mode QR code	Facultatief
WalletSolutionInfoPageURL	URL naar de informatiepagina van de gecertificeerde portemonnee-oplossing op de pagina van de lijst van gecertificeerde portemonnee-oplossingen van de ListOfCertifiedWalletsURL URL, aangevuld met"?" en de WalletSolutionID-identificatiecode van de portemonnee-oplossing.	URL	Verplicht
WalletSolutionInfoPageQRCode	QR-code met de informatie van de WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	Facultatief
WalletVerifierToolURL*	URL die leidt naar het endpoint van het instrument voor portemonnee-verificatie */.well-known/openid-credential-issuer* dat wordt gebruikt voor de opvraging van metadata van verstrekkers van attesteringen.	URL	Facultatief

([1]) Uitvoeringsverordening (EU) 2025/849 van de Commissie van 6 mei 2025 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad inzake de indiening van informatie bij de Commissie en de samenwerkingsgroep betreffende de lijst van gecertificeerde Europese portemonnees voor digitale identiteit (PB L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj)."

BIJLAGE X

Bijlage II bij Uitvoeringsverordening (EU) 2024/2980 wordt als volgt gewijzigd:

1) in bijlage II, deel 1, wordt punt 1), i), vervangen door:

"i) een of meer certificaten die aan norm ETSI EN 319 412-2 V2.4.1 (2025-06) of norm ETSI EN 319 412-3 V1.3.1 (2023-09) voldoen en die kunnen worden gebruikt voor het verifiëren van handtekeningen of zegels die door de registerhouder op de registergegevens zijn aangebracht en waarvoor de gecertificeerde identiteitsgegevens de naam van de registerhouder en, in voorkomend geval, het registratienummer van de registerhouder bevatten, zoals vermeld in respectievelijk de punten c) en d).";

2) in bijlage II, deel 2, wordt punt 1), h), vervangen door:

"h) een of meer certificaten die aan norm ETSI EN 319 412-2 V2.4.1 (2025-06) of norm ETSI EN 319 412-3 V1.3.1 (2023-09) voldoen en die kunnen worden gebruikt om de door de portemonneeaanbieder uitgegeven portemonnee-eenheidsattesteringen te verifiëren en waarvoor de gecertificeerde identiteitsgegevens de naam en, in voorkomend geval, het registratienummer van de portemonneeaanbieder bevatten, zoals vermeld in respectievelijk de punten a) en b);";

3) in bijlage II, deel 3, wordt punt 1), h), vervangen door:

"h) een of meer certificaten die aan norm ETSI EN 319 412-2 V2.4.1 (2025-06) of norm ETSI EN 319 412-3 V1.3.1 (2023-09) voldoen en die kunnen worden gebruikt voor het verifiëren van handtekeningen of zegels die door de verstrekker van persoonsidentificatiegegevens zijn aangebracht op de persoonsidentificatiegegevens die hij uitgeeft, en waarvoor de gecertificeerde identiteitsgegevens de naam en, in voorkomend geval, het registratienummer van de verstrekker van persoonsidentificatiegegevens bevatten, zoals vermeld in respectievelijk de punten a) en b).";

4) in bijlage II, deel 4, wordt punt 1), g), vervangen door:

"g) een of meer certificaten die aan norm ETSI EN 319 412-2 V2.4.1 (2025-06) of norm ETSI EN 319 412-3 V1.3.1 (2023-09) voldoen en die kunnen worden gebruikt voor het verifiëren van handtekeningen of zegels die door de verstrekker van toegangscertificaten voor op portemonnees vertrouwende partijen zijn aangebracht op het toegangscertificaat dat hij aan op portemonnees vertrouwende partijen verstrekt, met, in voorkomend geval, de informatie die nodig is om toegangscertificaten voor op portemonnees vertrouwende partijen te onderscheiden van andere certificaten.";

5) aan bijlage II wordt het volgende deel 5 toegevoegd:

"5. Kennisgevingen van informatie over aanbieders van registratiecertificaten voor op portemonnees vertrouwende partijen

1) De lidstaten verstrekken aan de Commissie de volgende informatie over aanbieders van registratiecertificaten voor op portemonnees vertrouwende partijen:

a) de naam van de aanbieder van registratiecertificaten voor op portemonnees vertrouwende partijen;

b) in voorkomend geval, een registratienummer van de aanbieder van registratiecertificaten voor op portemonnees vertrouwende partijen;

c) de lidstaat waar de aanbieder van registratiecertificaten voor op portemonnees vertrouwende partijen is gevestigd;

d) het e-mailadres en het telefoonnummer van de aanbieder van registratiecertificaten voor op portemonnees vertrouwende partijen, voor aangelegenheden in verband met de registratiecertificaten die hij aan op portemonnees vertrouwende partijen verstrekt;

e) in voorkomend geval, de URL van de webpagina van de aanbieder van registratiecertificaten voor op portemonnees vertrouwende partijen die aanvullende informatie bevat over de aanbieder en de door hem aan op portemonnees vertrouwende partijen verstrekte registratiecertificaten;

f) de URL van de webpagina met de beleidsdocumenten en algemene voorwaarden die van toepassing zijn op de levering en het gebruik van de door hem aan op portemonnees vertrouwende partijen verstrekte registratiecertificaten;

g) een of meer certificaten die aan norm ETSI EN 319 412-2 V2.4.1 (2025-06) of norm ETSI EN 319 412-3 V1.3.1 (2023-09) voldoen en die kunnen worden gebruikt voor het verifiëren van handtekeningen of zegels die door de verstrekker van registratiecertificaten voor op portemonnees vertrouwende partijen zijn aangebracht op het registratiecertificaat dat hij aan op portemonnees vertrouwende partijen verstrekt, met, in voorkomend geval, de informatie die nodig is om registratiecertificaten voor op portemonnees vertrouwende partijen te onderscheiden van andere certificaten.

2) De in punt 1) bedoelde informatie moet per aanbieder van registratiecertificaten voor op portemonnees vertrouwende partijen worden verstrekt.”.

BIJLAGE XI

"BIJLAGE I

Protocollen en interfaces als bedoeld in artikel 4

De technische specificatie ETSI TS 119 472-3 V1.1.1 (2026-03) geldt met de volgende aanpassingen:

1) 4.1 General requirements

— GEN-REQ-4.1-05: ongeldig

— OPMERKING: ongeldig

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

— ISS-MDATA-REG_CERT-4.2.3-04: Een van de elementen in de issuer_info array-parameter bevat het registratiecertificaat van de PID/EAA-Provider.

— ISS-MDATA-REG_CERT-4.2.3-07: ongeldig

— ISS-MDATA-REG_CERT-4.2.3-08: ongeldig

— ISS-MDATA-REG_CERT-4.2.3-09: ongeldig

— ISS-MDATA-REG_CERT-4.2.3-10: ongeldig

— ISS-MDATA-REG_CERT-4.2.3-11: ongeldig

— ISS-MDATA-REG_CERT-4.2.3-12: ongeldig

— ISS-MDATA-REG_CERT-4.2.3-13: ongeldig

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

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Wanneer het id-lid de waarde "arf_annex_ii" heeft en de array die gemapped is met het label "details" de waarde "once_only" of de waarde "per-relying-party" bevat, bevat het JSON-object dat deze met het label "details" gemapte array bevat, eveneens een JSON-nummer dat gemapt is met het label "reissue_trigger_unused".

4) Bijlage A is niet van toepassing."

BIJLAGE XII

"BIJLAGE II

De in artikel 5 bedoelde technische specificaties

De technische specificaties in bijlage C bij ISO/IEC 18013-7:2025 zijn van toepassing.

De technische specificaties in de punten 4.1, 4.2, 5, 6 en 6 van ETSI TS 119 472-2 V1.2.1 (2026-03) gelden met de volgende aanpassingen, waaronder de toevoeging van een nieuw punt 4.3:

1) 1 Scope

— Dit document specificeert twee profielen van protocollen aan de hand waarvan vertrouwende partijen (hierna RP genoemd) om EAAPs of persoonsidentificatiegegevens (hierna PID genoemd) kunnen verzoeken bij de Europese portemonnee voor digitale identiteit, en de Europese portemonnee voor digitale identiteit de gevraagde EAAPs/PIDs aan de RP kan sturen. Elk profiel ondersteunt twee transmissiemechanismen, namelijk API-mediated en niet-API-mediated, als volgt:

a) Een profiel is gebaseerd op:

— ISO/IEC 18013-5 [10] alleen voor het niet-API mediated transmissiemechanisme, en

— Bijlage C bij ISO/IEC 18013-7 [16] voor het API-mediated transmissiemechanisme.

Dit is het zogenoemde ISO/IEC-mdoc-profiel en wordt gedefinieerd in punt 5) van dit document.

b) Een profiel is gebaseerd op:

OpenID4VC-HAIP [11] voor zowel API-mediated als niet-API-mediated transmissiemechanismen, als volgt:

— de punten 5, 5.1, 5.3, 7 en 8 van [11] voor transmissie via redirects of een niet-API-mediated transmissiemechanisme, en

— de punten 5, 5.2, 5.3, 7 en 8 van [11] voor een API-mediated transmissiemechanisme.

Dit profiel heet OpenID4VC-HAIP-profiel en wordt gedefinieerd in punt 6 van dit document.

2) 2.1 Normative references

— [15] ISO 639: "Language code"

— [16] ISO/IEC 18013-7:2025 "Persoonsidentificatie — ISO — conform rijbewijs — Deel 7: Aanvullende functies voor mobiel rijbewijs (mDL)"

3) 4.1 EAAP implementation based on SD-JWT VC

— EAAP-SD-JWT VC-04: ongeldig

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

— EAAP-ISO/IEC-mdoc-01: ongeldig

— Note2: ongeldig

— EAAP-ISO/IEC-mdoc-02: ongeldig

5) 4.3 EAAP implementation with mediating API

— EAAP-API-GEN-01: De Europese portemonnee voor digitale identiteit ondersteunt een mediating API die beide protocollen als gedefinieerd in punt 5.2 van [11] en in bijlage C bij [16] ondersteunt.

— *OPMERKING*: Wanneer het apparaat waarop de Europese portemonnee voor digitale identiteit is geïnstalleerd geen van beide protocollen ondersteunt, kan niet aan deze eis worden voldaan en wordt een non-conformiteit geactiveerd als gevolg van onderliggende besturingssystemen en browsers die niet de nodige interoperabiliteitskenmerken implementeren.

— EAAP-API-GEN-02: De Europese portemonnee voor digitale identiteit ondersteunt een mediating API, ten minste voor PID's en EAA-typen die zijn geregistreerd in de catalogus van regelingen zoals gedefinieerd in Uitvoeringsverordening (EU) 2025/1569, en ten minste voor alle in bijlage II bij Uitvoeringsverordening (EU) 2024/2979 gedefinieerde formats.

— *OPMERKING 1*: Wanneer het onderliggende besturingssysteem, de browser, de mediating API's of een andere technische laag buiten de controle van de Europese portemonnee voor digitale identiteit, de credential formats en de in de catalogus van regelingen geregistreerde PID- en EAA-types beperkt, filtert, vooraf selecteert of anderszins beperkt, kan niet aan dit vereiste worden voldaan. Indien een dergelijke beperking verhindert dat de Europese portemonnee voor digitale identiteit een geregistreerd credential type of format ondersteunt, is de daaruit voortvloeiende non-conformiteit toe te schrijven aan het feit dat die onderliggende besturingssystemen, browsers, mediating API's of een andere relevante technische laag niet in staat zijn de nodige interoperabiliteitskenmerken te bieden.

6) 4.4 Validering van de op portemonnees vertrouwende partij en controles op overmatige vraag

— WRP-VALIDATION-01: De Europese portemonnee voor digitale identiteit valideert het in het verzoek ontvangen registratiecertificaat van een op portemonnees vertrouwende partij alvorens een gevraagde PID of elektronische attestering van attributen ter goedkeuring aan de portemonneegebruiker voor te leggen.

— WRP-VALIDATION-02: Indien de validering van het registratiecertificaat van een op portemonnees vertrouwende partij mislukt, onder meer wanneer het certificaat is verstreken, is ingetrokken, niet is afgegeven door een geldige betrouwbare aanbieder van registratiecertificaten van een op portemonnees vertrouwende partij, verkeerd is vormgegeven of niet cryptografisch kan worden geverifieerd, waarschuwt de Europese portemonnee voor digitale identiteit de portemonneegebruiker dat de op portemonnees vertrouwende partij niet kon worden gevalideerd en geeft hij het verzoek als niet succesvol gevalideerd weer. De portemonneegebruiker moet het verzoek van de vertrouwende partij uitdrukkelijk bevestigen. Stilzwijgen of vooraf aangevinkte vakjes volstaan niet als uitdrukkelijke toestemming.

— WRP-VALIDATION-03: De portemonneeaanbieder bepaalt op basis van zijn risicoanalyse en beveiligingsbeleid of en onder welke voorwaarden specifieke mislukte valideringscontroles door de portemonneegebruiker kunnen worden omzeild.

— WRP-OVERASKING-01: De Europese portemonnee voor digitale identiteit vergelijkt de door de op portemonnees vertrouwende partij gevraagde attesteringen en attributen met de geregistreerde attesteringen en attributen in het registratiecertificaat van de op portemonnees vertrouwende partij.

— WRP-OVERASKING-02: Indien de op portemonnees vertrouwende partij PID of elektronische attesteringen van attributen of claims aanvraagt die niet onder het registratiecertificaat van de op portemonnees vertrouwende partij vallen, waarschuwt de Europese portemonnee voor digitale identiteit de portemonneegebruiker duidelijk vóór elke openbaarmaking. In de waarschuwing wordt aangegeven dat de op portemonnees vertrouwende partij om meer informatie verzoekt dan zij heeft geregistreerd. De portemonneegebruiker moet het verzoek van de vertrouwende partij uitdrukkelijk bevestigen. Stilzwijgen of vooraf aangevinkte vakjes volstaan niet als uitdrukkelijke toestemming.

— WRP-OVERASKING-03: De portemonneeaanbieder bepaalt op basis van zijn risicoanalyse, beveiligingsbeleid en het toepasselijke recht of de portemonneegebruiker ondanks een dergelijke waarschuwing mag doorgaan, of alleen de subset van gevraagde gegevens waarop het registratiecertificaat betrekking heeft, openbaar mag worden gemaakt, dan wel of het verzoek moet worden afgewezen.

7) 5.1 Introduction

— Punt 5 en subpunten definiëren een profiel voor een protocol waarmee een RP de Europese portemonnee voor digitale identiteit kan verzoeken om EAAP's or PID's, en waarmee de Europese portemonnee voor digitale identiteit de gevraagde EAAP's/PID's naar de RP kan sturen met ofwel een niet-API mediated transmissiemechanisme, gebouwd op basis van ISO/IEC 18013-5 [10], ofwel een API-mediated transmissiemechanisme gebouwd op basis van bijlage C bij ISO/IEC 18013-7 [16] voor de overdracht van gegevensstructuren als gedefinieerd in ISO/IEC 18013-5 [10], passend ingekapseld.

— De rest van punt 5 is als volgt opgesteld:

— in punt 5.2 worden vereisten vastgesteld inzake de ondersteuning van het profiel en de transmissiemechanismen door RP's en de Europese portemonnee voor digitale identiteit;

— in punt 5.3 worden vereisten gespecificeerd die specifiek zijn voor het niet-API-mediated transmissiemechanisme;

— in punt 5.4 en subpunten worden vereisten gespecificeerd die specifiek zijn voor het API-mediated transmissiemechanisme.

8) 5.2 Requirements on EUDI Wallet and RP support

— ISO/IEC 18013-SUPPORT-01: Portemonnee-eenheden, PID-verstrekkers, attesteringsverstrekkers, portemonneeaanbieders en vertrouwende partijen ondersteunen geen serveropvraging zoals gespecificeerd in ISO/IEC 18013-5 [10] voor het verzoeken om en aanbieden van PID of attributen van attesteringen.

— ISO/IEC 18013-SUPPORT-02: De Europese portemonnee voor digitale identiteit voldoet aan de vereisten die zijn bepaald in de punten 5.3 en 5.4 van dit document.

— ISO/IEC 18013-SUPPORT-04: Een vertrouwende partij voert het profiel uit dat is bepaald in punt 5.4 van dit document.

9) 5.3.2 ISO/IEC-mdoc EAAP Request contents

— ISO/IEC 18013-5-REQ-04: Apparaatverzoeken die naar Europese portemonnees voor digitale identiteit worden gestuurd, bevatten het "requestInfo" sleutel-waardepaar zoals gespecificeerd in punt 8.3.2.1.2.1 van [10]. De waarde van dit paar is van het type RequestInfo.

— ISO/IEC 18013-5-REQ-05: Het RequestInfo-type is zoals de CDDL-definitie hieronder toont:

RequestInfo = {

"euWrprc": bstr, contains a registration certificate (see requirements below)

}

— ISO/IEC 18013-5-REQ-06: Het genoemde requestInfo-lid moet een lid met het label "euWrprc" bevatten.

— ISO/IEC 18013-5-REQ-07: De waarde van het "euWrprc" is een CBOR-gecodeerd registratiecertificaat.

— ISO/IEC 18013-5-REQ-08: ongeldig

— OPMERKING 3: ongeldig

— ISO/IEC 18013-5-REQ-09: ongeldig

— ISO/IEC 18013-5-REQ-10: ongeldig

— ISO/IEC 18013-5-REQ-11: ongeldig

10) 5.3.3 ISO/IEC-mdoc EAAP Response profile

— Dit punt bevat de vereisten voor het DeviceResponse-boodschaptype dat gemeenschappelijk is voor de beide types transmissiemechanismen (API-mediated en niet-API mediated).

— *OPMERKING 1*: Wanneer een op basis van ISO/IEC 18013-5 [10] gebouwd niet-API mediated mechanisme wordt gebruikt, is een EAAP Response exact een instantie van een DeviceResponse zoals opgenomen in dit punt. Wanneer een op basis van bijlage C bij ISO/IEC 18013-7 [16] gebouwd API-mediated mechanisme wordt gebruikt, wordt de instantie van een DeviceRequest ingekapseld zoals gespecificeerd in bijlage C bij [16].

— ISO/IEC 18013-5-RESP-02: De verstrekker van persoonsidentificatiegegevens en elektronische attesteringen van attributen neemt geen gegevenselementen op in de map KeyAuthorizations van het mobile security object (MSO) van de persoonsidentificatiegegevens en elektronische attesteringen van attributen die hij uitgeeft, met uitzondering van gegevenselementen die zijn verstrekt door de op portemonnees vertrouwende partij in de transactiegegevens in het mdoc-verzoek dat moet worden ondertekend of verzegeld door de portemonnee-eenheid met de privésleutel van de persoonsidentificatiegegevens of elektronische attesteringen van attributen.

— *OPMERKING 2*: Als gevolg daarvan kunnen portemonnee-eenheden geen door een apparaat ondertekende gegevenselementen aan op portemonnees vertrouwende partijen tonen, behalve ondertekengegevens die de op portemonnees vertrouwende partij heeft verstrekt, bijvoorbeeld in gebruiksgevallen voor beveiligde gebruikersauthenticatie.

— *OPMERKING 3*: ISO/IEC 18013-5:2021 specificeert niet hoe op portemonnees vertrouwende partijen transactiegegevens kunnen opnemen in een mdoc-verzoek. Bij het opnemen van transactiegegevens in een mdoc-verzoek worden technische specificaties toegevoegd.

— ISO/IEC 18013-5-RESP-03: Verstrekkers van persoonsidentificatiegegevens staan niet toe dat de privésleutel van de persoonsidentificatiegegevens elementen ondertekent die zijn verstrekt door op portemonnees vertrouwende partijen in de transactiegegevens van het mdoc-verzoek.

11) 5.4 Requirements for API mediated mechanism

5.4.1 ISO/IEC 18013-7-related requirements

In dit punt worden vereisten vastgesteld voor het API-mediated transmissiemechanisme met betrekking tot de vereisten die zijn gedefinieerd in bijlage C bij [16].

— ISO/IEC 18013-7-API-01: Het profiel dat API-mediated aanbiedingen ondersteunt, voldoet aan de vereisten in bijlage C bij ISO/IEC 18013-7 [16] zoals verder bepaald in deel 5.3 en deel 5.4 van dit document.

— ISO/IEC 18013-7-API-02: Alle verplichte vereisten vastgesteld in bijlage C bij [16] gelden zoals uiteengezet in punt 5.3 en punt 5.4 van dit document.

— ISO/IEC 18013-7-API-03: Alle facultatieve vereisten vastgesteld in bijlage C bij [16] blijven facultatief tenzij anders aangegeven in dit document.

12) 5.4.2 Additional requirements

— In deze bepaling worden aanvullende vereisten gespecificeerd voor API-mediated transmissiemechanismen.

— ISO/IEC 18013-ADD-API-01: De Europese portemonnee voor digitale identiteit maakt de aanwezigheid van alle opgeslagen typen elektronische attesteringen van attributen standaard bekend aan de mediating API die werkt overeenkomstig bijlage C bij [16], maar maakt de attributen en hun waarden in deze elektronische attesteringen van attributen niet openbaar.

— *OPMERKING 1*: De beperking in verband met de waarde van attributen is ook van toepassing als een dergelijke openbaarmaking de door het besturingssysteem aan de Europese portemonnee voor digitale identiteit verleende diensten zou verbeteren, bijvoorbeeld de selectie van attesteringen in het kader van de mediating API.

— Er zijn overwegingen met betrekking tot besturingssystemen en browsers die buiten de controle van toepassers vallen, waarmee rekening kan worden gehouden zoals aangegeven in de volgende opmerkingen 2, 3 en 4:

— *OPMERKING 2*: Een aanbiedingsverzoek van een vertrouwende partij ter ondersteuning van bijlage C bij [16] kan door de browser en/of het besturingssysteem worden verwerkt voor het zoeken naar beschikbare EAA's, voor het voorkomen van fraude ten aanzien van de gebruiker of voor het oplossen van problemen.

— *OPMERKING 3*: Een aanbiedingsverzoek van een vertrouwende partij ter ondersteuning van bijlage C bij [16] wordt naar verwachting door de browser en/of het besturingssysteem verwerkt voor beveiligingsdoeleinden.

— *OPMERKING 4*: Een aanbiedingsverzoek van een vertrouwende partij ter ondersteuning van bijlage C bij [16] zal naar verwachting niet door de browser en/of het besturingssysteem worden verwerkt voor marktanalysedoeleinden (ook niet als secundair doel) of voor de interne doeleinden van de browser en/of het besturingssysteem.

— ISO/IEC 18013-ADD-API-02: Wanneer een Europese portemonnee voor digitale identiteit op verzoek van de gebruiker PID of EAA verwijdert die voordien waren bekendgemaakt aan de mediating API die in overeenstemming met bijlage C bij [16] werkt, licht de Europese portemonnee voor digitale identiteit de mediating API in over het feit dat hij deze PID of EAA niet langer opslaat.

— ISO/IEC 18013-ADD-API-03: Wanneer een gebruiker zijn Europese portemonnee voor digitale identiteit verwijdert, licht de Europese portemonnee voor digitale identiteit de mediating API die in overeenstemming met bijlage C bij [16] werkt, in over het feit dat hij de eerder bekendgemaakte PID of EAA niet langer opslaat.

— ISO/IEC 18013-ADD-API-04: De Europese portemonnee voor digitale identiteit verstrekt een algemene gebruikersinstelling voor het uitschakelen van de bekendmaking van opgeslagen EAA's via een mediating API die werkt zoals gespecificeerd in ISO/IEC 18013-ADD-API-01. Wanneer deze instelling is uitgeschakeld, maakt de Europese portemonnee voor digitale identiteit niets bekend over of reageert hij niet op API-mediated aanbiedings- of uitgifteverzoeken.

— ISO/IEC 18013-ADD-API-05: In stromen tussen apparaten met behulp van de mediating API gaan Europese portemonnees voor digitale identiteit met behulp van een beveiligd, direct en door de gebruiker gemedieerd lokaal communicatiekanaal, zoals draadloze communicatietechnologie voor de korte afstand ter controle van fysieke nabijheid, na of het reagerende apparaat zich in de onmiddellijke fysieke nabijheid van de Europese portemonnee voor digitale identiteit bevindt.

— *OPMERKING*: CTAP 2.3 maakt het mogelijk BLE te gebruiken om de fysieke nabijheid te controleren en om, wanneer deze controle door beide apparaten wordt uitgevoerd, de gegevens tussen de apparaten over te dragen via korteafstandstransmissietechnologieën. Het uitvoeren van zowel de fysieke nabijheidscontrole als de gegevensoverdracht tussen de twee apparaten met behulp van een lokaal communicatiekanaal op basis van CTAP 2.3, moet door onderliggende besturingssystemen, browsers, mediating API's of een andere technische laag buiten de controle van de EUDI-portemonnee, worden verkozen boven het gebruik van CTAP-hybride tunneldiensten.

13) 6.2 Requirements on EUDI Wallet and RP support

— OIDFVP-HAIP-SUPPORT-02: De Europese portemonnee voor digitale identiteit moet voldoen aan de vereisten van punt 6.5 van deze bijlage.

— OIDFVP-HAIP-SUPPORT-03: De Europese portemonnee voor digitale identiteit zou het in punt 6.4 gespecificeerde omleidingsmechanisme niet mogen ondersteunen voor aanbiedingsstromen tussen apparaten.

— *OPMERKING 3*: Het gebruik van dit mechanisme is kwetsbaar voor aanvallen, zoals session fixation. Het is aan de vertrouwende partijen om dergelijke aanvallen te beperken. De uitvoering van dit mechanisme mag niet leiden tot niet-naleving.

— OIDFVP-HAIP-SUPPORT-05: Een vertrouwende partij moet voldoen aan de vereisten van punt 6.5 van deze bijlage.

— *OPMERKING 5*: ongeldig

14) 6.3.1. General requirements

— OIDFVP-HAIP-GEN-01: Alle verplichte vereisten van de punten 5, 5.3, 7, en 8 van HAIP [11] zijn van toepassing.

— *OPMERKING 1*: "HAIP [11] punt 5" verwijst enkel naar de vereisten onder de titel van punt 5. Hier zijn de punten 5.1, 5.2 en 5.3 geen deel van.

— OIDFVP-HAIP-GEN-03: Als de huidige bijlage een vereiste in OpenID4VC-HAIP [11] wijzigt, heeft het gewijzigde vereiste als bepaald in deze bijlage, voorrang.

— *OPMERKING 2*: Zo kan bijvoorbeeld een facultatief vereiste uit OpenID4VC-HAIP [11] worden omgezet in een verplicht vereiste, of kunnen verplichte vereisten worden uitgebreid.

— OIDFVP-HAIP-GEN-04: Wanneer het formaat van de gevraagde attestering voldoet aan [10], moeten vertrouwende partijen en Europese portemonnees voor digitale identiteit voldoen aan het "ISO mdocs"-profiel in [11] deel 6.

— *OPMERKING 3*: Voor alle duidelijkheid: het "ISO mdocs-profiel" in HAIP houdt in dat vertrouwende partijen en Europese portemonnees voor digitale identiteit moeten voldoen aan de toepasselijke vereisten in [7] bijlage B.2.

— OIDFVP-HAIP-GEN-05: Wanneer het formaat van de gevraagde attestering voldoet aan [2], moeten vertrouwende partijen en Europese portemonnees voor digitale identiteit voldoen aan het "IETF SD-JWT VCs"-profiel in [11] deel 6.

— *OPMERKING 4*: Voor alle duidelijkheid: het "IETF SD-JWT VCs profile" impliceert dat vertrouwende partijen en Europese portemonnees voor digitale identiteit moeten voldoen aan de vereisten van [7] bijlage B.3 en aan de vereisten van [11] punt 6.1.

15) 6.3.2.1 General requirements

— OIDFVP-HAIP-COMMON-REQ-01: ongeldig

16) 6.3.2.2 Requirements for the Request Object

— OIDFVP-HAIP-COMMON-REQ-RO-02: ongeldig

— OIDFVP-HAIP-COMMON-REQ-RO-03: ongeldig

— OIDFVP-HAIP-COMMON-REQ-RO-04: ongeldig

— OIDFVP-HAIP-COMMON-REQ-RO-05: ongeldig

— OIDFVP-HAIP-COMMON-REQ-RO-06: ongeldig

— OIDFVP-HAIP-COMMON-REQ-RO-07: ongeldig

— OIDFVP-HAIP-COMMON-REQ-RO-08: ongeldig

— OIDFVP-HAIP-COMMON-REQ-RO-09: ongeldig

— OIDFVP-HAIP-COMMON-REQ-RO-10: ongeldig

— OIDFVP-HAIP-COMMON-REQ-RO-11: ongeldig

— OIDFVP-HAIP-COMMON-REQ-RO-12: ongeldig

— *OPMERKING 2*: ongeldig

— OIDFVP-HAIP-COMMON-REQ-RO-13: Een van de elementen van de parameter verifier_info omvat het registratiecertificaat.

— OIDFVP-HAIP-COMMON-REQ-RO-23: Het in OpenID4VP deel 5.9.3 genoemde eindcertificaat voor gebruik met de x509_hash Client Identifier Prefix is een RP-toegangscertificaat zoals gespecificeerd in ETSI TS 119 475 [14].

17) 6.3.3 Authorization Response (EAAP response) profile

— OIDFVP-HAIP-COMMON-RESP-01: ongeldig

18) 6.4.1 General requirements

— OIDFVP-HAIP-REDIRECTS-04: ongeldig

— *OPMERKING*: ongeldig

19) 6.5.2 Additional requirements

— OIDFVP-HAIP-ADD-API-01: De Europese portemonnee voor digitale identiteit maakt de aanwezigheid van alle opgeslagen EAA-typen standaard bekend aan de mediating API die werkt overeenkomstig punt 5.2 van [11], maar maakt de attributen en hun waarden in deze EAA's niet openbaar.

— OIDFVP-HAIP-ADD-API-04: Wanneer de Europese portemonnee voor digitale identiteit een mediating API ondersteunt die werkt zoals gespecificeerd in OIDFVP-HAIP-ADD-API-01, verstrekt hij een algemene gebruikersinstelling voor het uitschakelen van de bekendmaking van opgeslagen EAA's via een mediating API. Wanneer "blokkering van de openbaarmaking" is ingesteld, moet de Europese portemonnee voor digitale identiteit de gebruiker vervolgens in staat stellen individuele attesteringen te selecteren die aan de mediating API moeten worden bekendgemaakt.

— OIDFVP-HAIP-ADD-API-05: In stromen tussen apparaten gaan Europese portemonnees voor digitale identiteit, met behulp van de mediating API, na dat het interagerende apparaat zich in de onmiddellijke fysieke nabijheid van de Europese portemonnee voor digitale identiteit bevindt met behulp van een beveiligd, direct en door de gebruiker gemedieerd lokaal communicatiekanaal, zoals draadloze communicatietechnologie voor de korte afstand, om de fysieke nabijheid te controleren.

— *OPMERKING 5*: CTAP 2.3 maakt het mogelijk BLE te gebruiken om de fysieke nabijheid te controleren en om, wanneer deze controle door beide apparaten wordt uitgevoerd, de gegevens tussen de apparaten over te dragen via korteafstandstransmissietechnologieën. Het uitvoeren van zowel de fysieke nabijheidscontrole als de gegevensoverdracht tussen de twee apparaten met behulp van een lokaal communicatiekanaal op basis van CTAP 2.3, moet door onderliggende besturingssystemen, browsers, mediating API's of een andere technische laag buiten de controle van de EUDI-portemonnee, worden verkozen boven het gebruik van CTAP-hybride tunneldiensten.

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

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Alle in dit document gespecificeerde vereisten die gelden voor Device Request en Device Response-structuren zoals gespecificeerd in ISO/IEC 18013-5, gelden ook wanneer de Europese portemonnee voor digitale identiteit een verzoek voor een ISO/IEC mdoc-presentatie ontvangt via een API-transmitted mechanisme zoals gespecificeerd in deel C.1 van [16]."