Amtsblatt
der Europäischen Union

DE
Reihe L

2026/1731

22.7.2026

DURCHFÜHRUNGSVERORDNUNG (EU) 2026/1731 DER KOMMISSION

vom 15. Juli 2026

zur Änderung der Durchführungsverordnungen (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 und (EU) 2024/2982 in Bezug auf geltende Standards bzw. Normen und Spezifikationen

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG ([1]), insbesondere auf Artikel 5a Absatz 23,

in Erwägung nachstehender Gründe:

(1) Um ein Höchstmaß an Harmonisierung zwischen den Mitgliedstaaten bei der Entwicklung europäischer Brieftaschen für die digitale Identität zu gewährleisten, beruhen die technischen Spezifikationen für die Brieftaschen auf den Arbeiten, die auf Grundlage der Empfehlung (EU) 2021/946 der Kommission ([2]) durchgeführt wurden, insbesondere auf der Architektur und dem Referenzrahmen. Da sich die Architektur und der Referenzrahmen seit der Annahme der Durchführungsverordnungen (EU) 2024/2977 ([3]), (EU) 2024/2979 ([4]), (EU) 2024/2980 ([5]) und (EU) 2024/2982 ([6]) der Kommission erheblich weiterentwickelt haben, sollten diese Durchführungsverordnungen nun geändert werden, um sie an die neuen Standards bzw. Normen, Spezifikationen und Verfahren anzupassen.

Im Einklang mit den Zielen der Verordnung (EU) Nr. 910/2014 wurde eine Reihe von Standards bzw. Normen ausgewählt, um diese spezifischen Anforderungen zu erfüllen. Diese Standards bzw. Normen sollten bewährte Verfahren widerspiegeln und in den betreffenden Sektoren weithin anerkannt sein. Da beispielsweise das W3C-VCDM-Format als Referenzformat für Bescheinigungen insbesondere im Bildungssektor verwendet wird, sollten die europäischen Brieftaschen für die digitale Identität dieses Format auch unterstützen, wenn die neuen Profile im W3C-VCDM-Format verfügbar sind. Diese Standards bzw. Normen sollten erforderlichenfalls angepasst oder ergänzt werden, um die Sicherheit und Vertrauenswürdigkeit europäischer Brieftaschen für die digitale Identität zu gewährleisten und gleichzeitig die grenzübergreifende Interoperabilität und das wirksame Funktionieren des Binnenmarkts zu fördern.

(2) Bei jeder Nutzung der Brieftasche, die die Vorlage des Porträtbilds des Brieftaschennutzers erfordert, müssen die Brieftaschenlösungen die Funktion der selektiven Offenlegung unterstützen, und die Offenlegung muss vollständig vom Nutzer kontrolliert werden. Um die Fähigkeit zu bewahren, über die Offenlegung zu entscheiden, und das Porträtbild vor unbeabsichtigten oder unbefugten Offenlegungsverlangen zu schützen, sollte die Architektur der europäischen Brieftaschen für die digitale Identität so konzipiert sein, dass Warnmechanismen vorgesehen sind und dass alle Verwendungen des Porträtbilds protokolliert werden. Um sicherzustellen, dass sich der Brieftaschennutzer der Weitergabe biometrischer Daten bewusst ist, sollten die Warnhinweise deutlich machen, dass die Abfrage eine

([1]) ABl. L 257 vom 28.8.2014, S. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Empfehlung (EU) 2021/946 der Kommission vom 3. Juni 2021 für ein gemeinsames Instrumentarium der Union für ein koordiniertes Herangehen an einen Rahmen für die europäische digitale Identität (ABl. L 210 vom 14.6.2021, S. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Durchführungsverordnung (EU) 2024/2977 der Kommission vom 28. November 2024 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf an europäische Brieftaschen für die digitale Identität ausgestellte Personenidentifizierungsdaten und elektronische Attributsbescheinigungen (ABl. L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([4]) Durchführungsverordnung (EU) 2024/2979 der Kommission vom 28. November 2024 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Integrität und die Kernfunktionen europäischer Brieftaschen für die digitale Identität (ABl. L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([5]) Durchführungsverordnung (EU) 2024/2980 der Kommission vom 28. November 2024 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf Notifizierungen an die Kommission bezüglich des Ökosystems europäischer Brieftaschen für die digitale Identität (ABl. L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

([6]) Durchführungsverordnung (EU) 2024/2982 der Kommission vom 28. November 2024 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf vom europäischen Rahmen für die digitale Identität zu unterstützende Protokolle und Schnittstellen (ABl. L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

Weitergabe biometrischer Daten umfasst, und eindeutig die Bestätigung der Offenlegung durch den Nutzer verlangen. Verarbeitet ein vertrauender Beteiligter das Porträtbild zum Zwecke der eindeutigen Identifizierung einer natürlichen Person oder zur Bestätigung der von dieser Person angegebenen Identität, so gelten die Artikel 6 und 9 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([7]) sowie alle anderen Anforderungen der genannten Verordnung, einschließlich der Anforderung, dass die Verarbeitung des Porträtbilds durch vertrauende Beteiligte auf das für die beabsichtigte Verwendung notwendige Maß beschränkt sein sollte. Die beabsichtigte Verwendung sollte dem Brieftaschennutzer zusammen mit der dem Offenlegungsverlangen in klarer und verständlicher Sprache mitgeteilt werden. Um die Sensibilität biometrischer Daten gebührend zu berücksichtigen, sollte der Brieftaschennutzer die Offenlegung des Porträtbilds ausdrücklich und eindeutig bestätigen. Keine Antwort oder vorangekreuzte Kästchen sollten nicht als Bestätigung durch den Brieftaschennutzer gelten. Die ausdrückliche Bestätigung des Brieftaschennutzers sollte eine technische Schutzvorkehrung sein und an sich keine Rechtsgrundlage für die Verarbeitung darstellen. Gemäß Artikel 9 Absatz 4 der Verordnung (EU) 2016/679 können die Mitgliedstaaten zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

(3) Damit die Mitgliedstaaten ausreichend Zeit haben, ihre nationalen Verfahren anzupassen, darf das Porträtbild des Brieftaschennutzers erst ab dem 11. August 2028 Teil der obligatorischen Personenidentifizierungsdaten für die natürliche Person sein. Sollen diese Bilder aus bestehenden Ausweisdokumenten wie Personalausweisen oder Reisepässen entnommen werden, gelten die einschlägigen Anforderungen der Verordnungen (EU) 2025/1208 ([8]) bzw. (EG) Nr. 2252/2004 ([9]) des Rates.

(4) Nach der Verordnung (EU) Nr. 910/2014 müssen Brieftaschen ein Vertrauenssiegel der europäischen Brieftasche für die digitale Identität anzeigen können, um klar, einfach und erkennbar anzugeben, dass eine Brieftasche im Einklang mit der genannten Verordnung bereitgestellt wurde. Die Verwendung eines solchen Vertrauenssiegels wird das reibungslose Funktionieren des Binnenmarkts unterstützen, einen fairen Wettbewerb gewährleisten und die Verbraucherinteressen schützen. Um die Verwendung eines solchen Vertrauenssiegels zu ermöglichen, sollten die visuellen und technischen Merkmale des Vertrauenssiegels festgelegt werden.

(5) Nach Artikel 12b der Verordnung (EU) Nr. 910/2014 ermöglichen Torwächter den Anbietern europäischer Brieftaschen für die digitale Identität und den Ausstellern notifizierter elektronischer Identifizierungsmittel eine wirksame Interoperabilität mit und — für die Zwecke der Interoperabilität — den Zugang zu denselben Betriebssystem-, Hardware- oder Software-Funktionen. Eine solche wirksame Interoperabilität und ein solcher Zugang sind kostenlos und werden unabhängig davon bereitgestellt, ob diese Hardware- oder Software-Funktionen, die der Torwächter bei der Erbringung solcher Dienste zur Verfügung hat oder verwendet, Teil des Betriebssystems sind. Da alle Brieftaschenlösungen einen gemeinsamen Satz von Protokollen und Schnittstellen unterstützen sollten, um die Nutzbarkeit, Sicherheit und Interoperabilität in allen Mitgliedstaaten zu gewährleisten, sollten Torwächter die Betriebssystem-, Hardware- oder Software-Funktionen aktivieren, die für die Umsetzung der in Anhang XII dieser Verordnung festgelegten Protokolle und Schnittstellen erforderlich sind. In diesem Zusammenhang sollten Torwächter bei geräteübergreifenden Datenflüssen online sowohl für die Prüfung der räumlichen Nähe als auch für die Datenübertragung zwischen den beiden Geräten einen lokalen Kommunikationskanal, wie er durch die Spezifikation des Client-to-Authenticator-Protokolls (CTAP) Version 2.3 ([10]) ermöglicht wird, gegenüber der Nutzung von CTAP-Hybridtunneldiensten bevorzugen.

(6) Damit die Mitgliedstaaten, die Anbieter von Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte und die Brieftaschenanbieter ausreichend Zeit haben, Einzelbrieftaschen in die Lage zu versetzen, Registrierungszertifikate für auf Brieftaschen vertrauende Beteiligte zu authentifizieren und zu validieren, sollte diese Anforderung erst ab dem 11. August 2028 gelten.

(7) Die Verordnung (EU) 2016/679 und, sofern anwendbar, die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([11]) gelten für jede Verarbeitung personenbezogener Daten gemäß der vorliegenden Verordnung.

([7]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([8]) Verordnung (EU) 2025/1208 des Rates vom 12. Juni 2025 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben (ABl. L, 2025/1208, 20.6.2025, ELI: http://data.europa.eu/eli/reg/2025/1208/oj).

([9]) Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten (ABl. L 385 vom 29.12.2004, S. 1, ELI: http://data.europa.eu/eli/reg/2004/2252/oj).

([10]) Von der FIDO-Allianz vorgeschlagener Standard, Client-to-Authenticator-Protokoll (CTAP), 26. Februar 2026.

([11]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(8) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([12]) angehört und gab am 17. April 2026 seine Stellungnahme ab ([13]).

(9) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 48 der Verordnung (EU) Nr. 910/2014 eingesetzten Ausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Änderung der Durchführungsverordnung (EU) 2024/2977

Die Durchführungsverordnung (EU) 2024/2977 wird wie folgt geändert:

1. Folgender Artikel 3a wird eingefügt:

„*Artikel 3a*

Schutz des Porträtbilds

(1) Zusätzlich zu den Informationsanforderungen gemäß der Verordnung (EU) 2016/679 stellen die Brieftaschenanbieter sicher, dass die von ihnen bereitgestellten Brieftaschenlösungen den Brieftaschennutzern Warnhinweise geben, wenn auf Brieftaschen vertrauende Beteiligte die Offenlegung des Porträtbilds verlangen, und darauf hinweisen, dass die Abfrage eine Weitergabe biometrischer Daten umfasst, und dass dafür die Bestätigung der selektiven Offenlegung des Porträtbilds erforderlich ist.

(2) Für die Umsetzung der selektiven Offenlegung des Porträtbilds gegenüber einem auf Brieftaschen vertrauenden Beteiligten stellen die Brieftaschenanbieter sicher, dass die Brieftaschenlösungen verlangen, dass der Brieftaschennutzer die Vorlage des Porträtbilds ausdrücklich und eindeutig bestätigt.

(3) Das Porträtbild darf von auf Brieftaschen vertrauenden Beteiligten nicht gespeichert werden, es sei denn, dies ist für die Identifizierung und Authentifizierung im Einklang mit dem Datenschutzrecht der Union erforderlich oder im Unionsrecht oder im nationalen Recht im Einklang mit dem Datenschutzrecht der Union vorgesehen. Das Porträtbild darf nicht an Drittländer oder internationale Organisationen übermittelt werden, es sei denn, dies ist nach dem Datenschutzrecht der Union zulässig.“

2. Artikel 4 Absatz 1 erhält folgende Fassung:

„(1) Elektronische Attributsbescheinigungen, die an Einzelbrieftaschen ausgestellt werden, müssen zumindest einer der in Anhang II der Durchführungsverordnung (EU) 2024/2979 festgelegten Normen entsprechen.“

3. Artikel 5 Absatz 4 Buchstabe b erhält folgende Fassung:

„b) wenn die Einzelbrieftaschenbescheinigung der Einzelbrieftasche, an die die Personenidentifizierungsdaten ausgestellt wurden, widerrufen wurde;“.

4. Der Anhang erhält die Fassung des Anhangs I der vorliegenden Verordnung.

([12]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

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

Artikel 2

Änderung der Durchführungsverordnung (EU) 2024/2979

Die Durchführungsverordnung (EU) 2024/2979 wird wie folgt geändert:

1. Artikel 3 Absatz 2 wird gestrichen.

2. Artikel 5 Absatz 1 Buchstabe a erhält folgende Fassung:

„a) Kryptovorgänge in der Brieftasche in Bezug auf kritische Werte, die in einem sicheren Kryptomodul gespeichert und für die Authentifizierung der Brieftaschennutzer nicht erforderlich sind, nur dann durchführen, wenn diese Anwendungen die Brieftaschennutzer zuvor erfolgreich authentifiziert haben;".

3. Folgender Artikel 5a wird eingefügt:

„*Artikel 5a*

Kryptografische Mechanismen

Die Brieftaschenanbieter verwenden für die Zwecke des Artikels 4 Absatz 2 nur die in Anhang Ia genannten kryptografischen Mechanismen."

4. Artikel 6 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Die Brieftaschenanbieter stellen Einzelbrieftaschenbescheinigungen für jede Einzelbrieftasche aus. Die Brieftaschenanbieter unterzeichnen oder besiegeln die Einzelbrieftaschenbescheinigungen so, dass die Signaturen oder Siegel durch ein Zertifikat gemäß Anhang II Abschnitt 2 Nummer 1 Buchstabe h der Durchführungsverordnung (EU) 2024/2980 validiert werden können."

b) Absatz 2 erhält folgende Fassung:

„(2) Die Brieftaschenanbieter stellen sicher, dass die in Absatz 1 genannten Einzelbrieftaschen den technischen Spezifikationen des Anhangs Ib entsprechen."

c) Absatz 3 Buchstabe b erhält folgende Fassung:

„b) stellen von Einzelbrieftaschen unabhängige sichere Identifizierungs- und Authentifizierungsmechanismen für die Brieftaschennutzer bereit;".

5. Artikel 9 Absatz 2 Buchstabe b erhält folgende Fassung:

„b) den Namen, Kontaktangaben und die eindeutige Kennung des betreffenden auf Brieftaschen vertrauenden Beteiligten und den Mitgliedstaat, in dem dieser auf Brieftaschen vertrauende Beteiligte niedergelassen ist;".

6. Artikel 10 Absatz 1 erhält folgende Fassung:

„(1) Die Brieftaschenanbieter stellen sicher, dass die von ihnen bereitgestellten Einzelbrieftaschen die im Einklang mit den technischen Spezifikationen für gemeinsame eingebettete Offenlegungsregelungen ausgestellten elektronischen Attributsbescheinigungen gemäß Anhang III verarbeiten können."

7. Artikel 12 wird wie folgt geändert:

a) Absatz 2 Buchstabe c erhält folgende Fassung:

„c) Erstellen von Signaturen oder Siegeln in mindestens dem in Anhang IV genannten obligatorischen Format für Signaturen und Siegel;".

b) Absatz 3 erhält folgende Fassung:

„(3) Signaturerstellungsanwendungen können entweder in Brieftascheninstanzen integriert oder extern eingerichtet sein."

c) Folgender Absatz wird eingefügt:

„(4) Die von Einzelbrieftaschen verwendeten Signaturerstellungseinheiten unterstützen zumindest die in Anhang IV genannte Anwendungsprogrammierschnittstelle."

8. Artikel 14 Absatz 1 wird gestrichen.

9. Folgender Artikel 14a wird eingefügt:

„*Artikel 14a*

Vertrauenssiegel der europäischen Brieftasche für die digitale Identität

(1) Die Brieftaschenanbieter stellen sicher, dass Einzelbrieftaschen das Vertrauenssiegel der europäischen Brieftasche für die digitale Identität anzeigen. Das Vertrauenssiegel der europäischen Brieftasche für die digitale Identität hat die in den Anhängen VI und VII festgelegte Form.

(2) Die Brieftaschenanbieter stellen sicher, dass Einzelbrieftaschen den Brieftaschennutzern den Zugang zu Informationen ermöglichen, anhand deren sie den Zertifizierungsstatus der Brieftaschenlösung überprüfen können. Zu diesem Zweck stellen die Brieftaschenanbieter sicher, dass die entsprechenden Einzelbrieftaschen nach der Registrierung einer Brieftaschenlösung die von der Europäischen Kommission für eine solche Überprüfung bereitgestellten URLs enthalten. Die Brieftaschenanbieter stellen sicher, dass ihre Einzelbrieftaschen Zugriff auf Daten des Vertrauenssiegels der europäischen Brieftasche haben, die den technischen Spezifikationen des Anhangs VIII entsprechen.

(3) Die Referenzfarben für das Vertrauenssiegel der europäischen Brieftasche für die digitale Identität sind Pantone Nr. 661 und Nr. 116 oder — bei 4-Farb-Druck — Blau (100 % Cyan + 67 % Magenta + 0 % Gelb + 40 % Schwarz) und Gelb (0 % Cyan + 20 % Magenta + 100 % Gelb + 0 % Schwarz); bei Verwendung von RGB-Farben sind die Referenzfarben Blau (0 Rot + 51 Grün + 153 Blau) und Gelb (255 Rot + 204 Grün + 0 Blau).

(4) Nur wenn eine Farbdarstellung nicht praktikabel ist, darf das Vertrauenssiegel der europäischen Brieftasche für die digitale Identität auch in Schwarz-Weiß gemäß Anhang VII verwendet werden.

(5) Wird das Vertrauenssiegel der europäischen Brieftasche für die digitale Identität auf einem dunklen Hintergrund dargestellt, so kann es in einem Negativformat derselben Hintergrundfarbe verwendet werden. Wird das farbige Vertrauenssiegel der europäischen Brieftasche für die digitale Identität auf einem farbigen Hintergrund dargestellt, sodass es schwer zu erkennen ist, kann eine das Vertrauenssiegel der europäischen Brieftasche für die digitale Identität abgrenzende Konturlinie verwendet werden, um den Kontrast zu den Hintergrundfarben zu verbessern.

(6) Die Mindestgröße des Vertrauenssiegels der europäischen Brieftasche für die digitale Identität beträgt 64 × 85 Pixel bei 150 dpi.

(7) Die Brieftaschenanbieter stellen sicher, dass das Vertrauenssiegel der europäischen Brieftasche für die digitale Identität in einer Weise verwendet wird, die eindeutig darstellt, auf welche Einzelbrieftasche sich das Vertrauenssiegel der europäischen Brieftasche für die digitale Identität bezieht. Das Vertrauenssiegel der europäischen Brieftasche für die digitale Identität kann mit grafischen Elementen oder Textelementen verknüpft werden, aus denen die Einzelbrieftasche, für die es verwendet wird, eindeutig hervorgeht, sofern dadurch weder seine Erkennbarkeit als Vertrauenssiegel der europäischen Brieftasche für die digitale Identität noch die Verbindung mit der Liste der zertifizierten Brieftaschen für die digitale Identität gemäß Artikel 5d der Verordnung (EU) Nr. 910/2014 geändert wird.

(8) Wenn Brieftaschenanbieter eine Einzelbrieftaschenbescheinigung widerrufen haben, stellen sie sicher, dass das Vertrauenssiegel der europäischen Brieftasche für die digitale Identität von der betreffenden Einzelbrieftasche nicht länger angezeigt wird.“

10. Die Anhänge Ia und Ib werden gemäß Anhang II und Anhang III der vorliegenden Verordnung angefügt.

11. Anhang II erhält die Fassung des Anhangs IV der vorliegenden Verordnung.

12. Anhang III erhält die Fassung des Anhangs V der vorliegenden Verordnung.

13. Anhang IV wird gemäß Anhang VI der vorliegenden Verordnung geändert.

14. Anhang V wird gestrichen.

15. Der Wortlaut in Anhang VII der vorliegenden Verordnung wird als Anhang VI eingefügt.

16. Der Wortlaut in Anhang VIII der vorliegenden Verordnung wird als Anhang VII eingefügt.

17. Der Wortlaut in Anhang IX der vorliegenden Verordnung wird als Anhang VIII eingefügt.

Artikel 3

Änderung der Durchführungsverordnung (EU) 2024/2980

Die Durchführungsverordnung (EU) 2024/2980 wird wie folgt geändert:

1. Artikel 5 Nummer 2 erhält folgende Fassung:

„(2) Die Kommission erstellt, führt und veröffentlicht gegebenenfalls eine Liste, in der die von den Mitgliedstaaten notifizierten Informationen über die in Anhang II Abschnitte 2, 3, 4 und 5 genannten Brieftaschenanbieter, Anbieter von Personenidentifizierungsdaten, Anbieter von Zugriffszertifikaten für auf Brieftaschen vertrauende Beteiligte und Anbieter von Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte zusammengeführt sind."

2. Anhang II der Durchführungsverordnung (EU) 2024/2980 wird gemäß Anhang X der vorliegenden Verordnung geändert.

Artikel 4

Änderung der Durchführungsverordnung (EU) 2024/2982

Die Durchführungsverordnung (EU) 2024/2982 wird wie folgt geändert:

1. Artikel 1 Nummer 2 erhält folgende Fassung:

„2. das Vorweisen von Attributen der Personenidentifizierungsdaten und von elektronischen Attributsbescheinigungen gegenüber auf Brieftaschen vertrauenden Beteiligten,".

2. Artikel 3 wird wie folgt geändert:

a) Nummer 1 erhält folgende Fassung:

„1. die Zugriffszertifikate für auf Brieftaschen vertrauende Beteiligte authentifizieren und validieren, wenn sie mit auf Brieftaschen vertrauenden Beteiligten interagieren, ohne dem Betriebssystem, Browser oder anderen zwischengeschalteten Anwendungen die Ausführung dieser Prozesse zu übertragen;".

b) Nummer 2 wird gestrichen.

c) Nummer 3 erhält folgende Fassung:

„3. Abfragen, die unter Verwendung von Zugriffszertifikaten für auf Brieftaschen vertrauende Beteiligte erfolgen, authentifizieren und validieren;".

d) Nummer 4 erhält folgende Fassung:

„4. das Registrierungszertifikat des auf Brieftaschen vertrauenden Beteiligten authentifizieren und validieren;".

e) Nummer 5 erhält folgende Fassung:

„5. den Brieftaschennutzern die Informationen anzeigen, die in den Zugriffszertifikaten für auf Brieftaschen vertrauende Beteiligte enthalten sind;".

f) Nummer 8 wird gestrichen.

g) Nummer 9 erhält folgende Fassung:

„9. keine abgefragten Attribute an auf Brieftaschen vertrauende Beteiligte übermitteln, solange nicht die folgenden Schritte abgeschlossen wurden:

a) Überprüfung, dass in der Einzelbrieftasche eingebettete Offenlegungsregelungen gemäß Artikel 10 der Durchführungsverordnung (EU) 2024/2979 verarbeitet wurden;

b) Überprüfung, dass die Brieftaschennutzer das Vorweisen der Daten teilweise oder vollständig genehmigt haben."

3. Artikel 4 Absatz 1 erhält folgende Fassung:

„(1) Brieftaschenanbieter stellen sicher, dass Brieftaschenlösungen Protokolle und Schnittstellen gemäß Anhang I für die Ausstellung von Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen an Einzelbrieftaschen unterstützen."

4. Artikel 5 wird wie folgt geändert:

   a) Die Absätze 1 und 2 erhalten folgende Fassung:

   „(1) Brieftaschenanbieter stellen sicher, dass Brieftaschenlösungen Protokolle und Schnittstellen für das Vorweisen von Attributen bei auf Brieftaschen vertrauenden Beteiligten aus der Ferne und gegebenenfalls aus der Nähe gemäß den im Anhang II festgelegten technischen Spezifikationen unterstützen.

   (2) Brieftaschenanbieter stellen sicher, dass Einzelbrieftaschen auf Veranlassung der Nutzer erfolgreich authentifizierte und validierte Abfragen der in Artikel 3 genannten auf Brieftaschen vertrauenden Beteiligten gemäß den im Anhang II festgelegten technischen Spezifikationen beantworten."

   b) Absatz 5 wird gestrichen.

5. Artikel 8 erhält folgende Fassung:

   „*Artikel 8*

   Inkrafttreten

   Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

   Artikel 3 Nummer 4 gilt ab dem 11. August 2028.

   Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat."

6. Der Anhang wird gestrichen.

7. Der Wortlaut in Anhang XI der vorliegenden Verordnung wird als Anhang I angefügt.

8. Der Wortlaut in Anhang XII der vorliegenden Verordnung wird als Anhang II angefügt.

Artikel 5

Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 15. Juli 2026

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG I

„ANHANG

Technische Spezifikationen für Personenidentifizierungsdaten gemäß Artikel 3 Absatz 3

(1) Abschnitt 1 Identifizierungsdatensatz für natürliche Personen

Tabelle 1

Selektiv offenzulegende obligatorische Personenidentifizierungsdaten für natürliche Personen

Datenkennung	Definition
`family_name`	Derzeitige(r) Nachname(n) des Nutzers, auf den sich die Personenidentifizierungsdaten beziehen
`given_name`	Derzeitige(r) Vorname(n) des Nutzers, auf den sich die Personenidentifizierungsdaten beziehen, einschließlich weitere(r) Vorname(n)
`birth_date`	Geburtstag, -monat und -jahr des Nutzers, auf den sich die Personenidentifizierungsdaten beziehen
`birth_place`	Land als alpha-2-Ländercode gemäß ISO 3166-1 oder Staat, Provinz, Distrikt oder Gebiet, Gemeinde, Stadt, Kleinstadt oder Dorf, in der/dem der Nutzer, auf den sich die Personenidentifizierungsdaten bezieht, geboren wurde
`nationality`	Ein oder mehrere alpha-2-Ländercodes nach ISO 3166-1, die die Staatsangehörigkeit des Nutzers angeben, auf den sich die Personenidentifizierungsdaten beziehen
`portrait`	Das Gesichtsbild des Nutzers, auf den sich die Personenidentifizierungsdaten beziehen, das die Qualitätsanforderungen für eine vollständige Frontalaufnahme gemäß der Norm ISO/IEC 39794-5 oder – für die Zwecke der Abwärtskompatibilität – der Norm ISO/IEC 19794-5 Abschnitte 8.2, 8.3 und 8.4 erfüllt und das in Form verschlüsselter Bilddaten ohne Kopfzeilen oder Blöcke gemäß Abschnitt 5 der Norm ISO/IEC 19794-5 vorliegt, mit Ausnahme der Bilddaten selbst (JPEG) – gilt ab 11. August 2028, sofern der Nutzer die Verwendung des Bildes, soweit zutreffend, nicht ausdrücklich ablehnt.

— Die Mitgliedstaaten können vorsehen, dass der Nutzer die Möglichkeit hat, die Aufnahme des Porträtbilds in die Personenidentifizierungsdaten abzulehnen.

— Die Mitgliedstaaten stellen sicher, dass die selektive Offenlegung für jede Datenkennung, einschließlich des Porträtbilds, gilt.

— Ist das Geburtsdatum der natürlichen Person unbekannt, wählen die Mitgliedstaaten geeignete Werte, die den in den Abschnitten 4.1 bzw. 4.2 dieses Anhangs festgelegten Spezifikationen entsprechen.

— Ist die Staatsangehörigkeit der natürlichen Person unbekannt, verwenden die Mitgliedstaaten den Wert ‚QU'.

— Besitzt die natürliche Person keine Staatsangehörigkeit, verwenden die Mitgliedstaaten den Wert ‚QS'.

— Lehnt der Nutzer die Aufnahme des Porträtbilds ab, lassen die Mitgliedstaaten den Wert leer.

Tabelle 2

Selektiv offenzulegende fakultative Personenidentifizierungsdaten für natürliche Personen

Datenkennung	Definition
resident_address	Vollständige Anschrift des Ortes, in dem der Nutzer, auf den sich die Personenidentifizierungsdaten beziehen, derzeit seinen Wohnsitz hat oder erreichbar ist (Straße, Hausnummer, Stadt usw.)
resident_country	Derzeitiges Wohnsitzland des Nutzers, auf den sich die Personenidentifizierungsdaten beziehen, als Alpha-2-Ländercode nach ISO 3166-1
resident_state	Staat, Provinz, Distrikt oder Gebiet, in dem/der der Nutzer, auf den sich die Personenidentifizierungsdaten beziehen, derzeit seinen Wohnsitz hat
resident_city	Gemeinde, Stadt, Kleinstadt oder Dorf, in der/dem der Nutzer, auf den sich die Personenidentifizierungsdaten beziehen, derzeit seinen Wohnsitz hat
resident_postal_code	Postleitzahl des Orts, in dem der Nutzer, auf den sich die Personenidentifizierungsdaten beziehen, derzeit seinen Wohnsitz hat
resident_street	Name der Straße, in der der Nutzer, auf den sich die Personenidentifizierungsdaten beziehen, derzeit seinen Wohnsitz hat, einschließlich der Hausnummer und etwaiger Adresszusätze
personal_administrative_-number	Ein dem Nutzer, auf den sich die Personenidentifizierungsdaten beziehen, zugewiesener Wert, der unter allen vom Anbieter von Personenidentifizierungsdaten ausgestellten persönlichen Verwaltungsnummern eindeutig ist. Entscheiden sich die Mitgliedstaaten für die Aufnahme dieses Attributs, so beschreiben sie in ihren elektronischen Identifizierungssystemen, nach denen die Personenidentifizierungsdaten ausgestellt werden, die Grundsätze, die sie für die Werte dieses Attributs anwenden, gegebenenfalls einschließlich spezifischer Bedingungen für die Verarbeitung dieses Werts.
family_name_birth	Nachname(n) oder Familienname(n) des Personenidentifizierungsdatennutzers zum Zeitpunkt seiner Geburt
given_name_birth	Vorname(n), einschließlich weiterer Vornamen, des Nutzers, auf den sich die Personenidentifizierungsdaten beziehen, zum Zeitpunkt seiner Geburt
sex	Die Werte müssen einem der folgenden entsprechen: 0 = unbekannt, 1 = männlich, 2 = weiblich, 3 = sonstiges, 4 = inter, 5 = divers, 6 = offen, 9 = nicht zutreffend. Für die Werte 0, 1, 2 und 9 gilt ISO/IEC 5218.
email_address	E-Mail-Adresse des Nutzers, auf den sich die Personenidentifizierungsdaten beziehen [gemäß RFC 5322 ([1])]

Datenkennung	Definition
`mobile_phone_number`	Mobiltelefonnummer des Nutzers, auf den sich die Personenidentifizierungsdaten beziehen, beginnend mit dem Symbol ‚+' als internationalem Vorwahl-Präfix und dem Ländercode, ausschließlich gefolgt von Zahlen

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

(2) Abschnitt 2: Identifizierungsdatensatz für juristische Personen

Tabelle 3

Obligatorische Personenidentifizierungsdaten für juristische Personen

Datenkennung
Derzeitige amtliche Bezeichnung
Eine eindeutige Kennung, die vom übermittelnden Mitgliedstaat entsprechend den technischen Spezifikationen für die Zwecke der grenzüberschreitenden Identifizierung erstellt wurde und möglichst dauerhaft fortbesteht.

— Ist eine Datenkennung für die Person nicht bekannt oder kann es nicht auf andere Weise als Teil des Personenidentifizierungsdatensatzes ausgestellt werden, verwenden die Mitgliedstaaten stattdessen einen der Situation angemessenen Attributswert.

Tabelle 4

Fakultative Personenidentifizierungsdaten für juristische Personen

Datenkennung
Derzeitige Anschrift
Umsatzsteuer-Identifikationsnummer
Steuerregisternummer
Europäische einheitliche Kennung gemäß der Richtlinie (EU) 2017/1132 des Europäischen Parlaments und des Rates ([1])
Rechtsträgerkennung (LEI) gemäß der Durchführungsverordnung (EU) 2022/1860 der Kommission ([2])
Registrierungs- und Identifizierungsnummer für die Wirtschaftsbeteiligten (EORI-Nr.) gemäß der Durchführungsverordnung (EU) Nr. 1352/2013 der Kommission ([3])
Verbrauchsteuernummer gemäß Artikel 2 Nummer 12 der Verordnung (EU) Nr. 389/2012 des Rates ([4])

([1]) Richtlinie (EU) 2017/1132 des Europäischen Parlaments und des Rates vom 14. Juni 2017 über bestimmte Aspekte des Gesellschaftsrechts (ABl. L 169 vom 30.6.2017, S. 46, ELI: http://data.europa.eu/eli/dir/2017/1132/oj).

([2]) Durchführungsverordnung (EU) 2022/1860 der Kommission vom 10. Juni 2022 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates im Hinblick auf die Standards, Formate, Häufigkeit und Methoden und Modalitäten für die Meldung (ABl. L 262 vom 7.10.2022, S. 68, ELI: http://data.europa.eu/eli/reg_impl/2022/1860/oj).

([3]) Durchführungsverordnung (EU) Nr. 1352/2013 der Kommission vom 4. Dezember 2013 zur Festlegung der in der Verordnung (EU) Nr. 608/2013 des Europäischen Parlaments und des Rates zur Durchsetzung der Rechte geistigen Eigentums durch die Zollbehörden vorgesehenen Formblätter (ABl. L 341 vom 18.12.2013, S. 10, ELI: http://data.europa.eu/eli/reg_impl/2013/1352/oj).

([4]) Verordnung (EU) Nr. 389/2012 des Rates vom 2. Mai 2012 über die Zusammenarbeit der Verwaltungsbehörden auf dem Gebiet der Verbrauchsteuern und zur Aufhebung von Verordnung (EG) Nr. 2073/2004 (ABl. L 121 vom 8.5.2012, S. 1, ELI: http://data.europa.eu/eli/reg/2012/389/oj).

(3) Abschnitt 3: Metadatensatz für Personenidentifizierungsdaten

Tabelle 5

Metadaten für die Personenidentifizierungsdaten

Datenkennung	Definition	Vorhandensein
`issuing_authority`	Name der Verwaltungsbehörde, die die Personenidentifizierungsdaten ausgestellt hat, oder der alpha-2-Ländercode nach ISO 3166 des jeweiligen Mitgliedstaats, wenn es keine gesonderte Behörde gibt, die zur Ausstellung von Personenidentifizierungsdaten befugt ist	Obligatorisch
`issuing_country`	Alpha-2-Ländercode nach ISO 3166-1 des Landes oder Gebiets des Anbieters der Personenidentifizierungsdaten	Obligatorisch
`expiry_date`	Datum (und nach Möglichkeit Uhrzeit) des Ablaufs der verwaltungsmäßigen Gültigkeitsdauer der Personenidentifizierungsdaten	Fakultativ
`document_number`	Eine vom Anbieter der Personenidentifizierungsdaten zugeteilte Nummer für die Personenidentifizierungsdaten	Fakultativ
`issuing_jurisdiction`	Länderuntercode des Hoheitsgebiets, das die Personenidentifizierungsdaten ausgestellt hat, nach ISO 3166-2:2020, Abschnitt 8. Der erste Teil des Codes entspricht dem Wert für das ausstellende Land.	Fakultativ
`issuance_date`	Datum (und nach Möglichkeit Uhrzeit) des Beginns der verwaltungsmäßigen Gültigkeitsdauer der Personenidentifizierungsdaten	Fakultativ

(4) Abschnitt 4: Kodierung der Personenidentifizierungsdatenattribute natürlicher Personen

— Personenidentifizierungsdaten natürlicher Personen werden gemäß den für elektronische Attributsbescheinigungen geltenden Normen in Anhang II der Durchführungsverordnung (EU) 2024/2979, Abschnitte 5 (SD-JWT VC-Format) und 6 (ISO/IEC-mdoc-Format) ausgestellt. Die Abschnitte 5.2.2, 5.2.4, 5.2.5, EAA-6-1-03, 6.2.2, 6.2.3, 6.2.4 und 6.2.5 finden keine Anwendung.

— Die Kodierung der Personenidentifizierungsdaten natürlicher Personen muss den technischen Spezifikationen in den Abschnitten 4.1 und 4.2 dieses Anhangs entsprechen.

4.1 Kodierung der Personenidentifizierungsdaten natürlicher Personen im ISO/IEC-mdoc-Format

— Die Art der Bescheinigung für Personenidentifizierungsdaten im ISO/IEC-mdoc-Format lautet ‚eu.europa.ec.eudi.pid.1'. Die Kennung des Namensraums für die in diesem Anhang aufgeführten Personenidentifizierungsdatenattribute lautet ‚eu.europa.ec.eudi.pid.1'.

— Enthalten die Personenidentifizierungsdaten Daten, deren Datenkennungen nicht in diesem Anhang aufgeführt sind, so sind diese Daten innerhalb eines inländischen Namensraums für Personenidentifizierungsdaten zu definieren, der das allgemeine Format eu.europa.ec.eudi.pid.[Alpha-2-Ländercode nach ISO 3166-1 oder Regionscode nach ISO 3166-2] verwendet, fakultativ gefolgt von einem Punkt und einer Versionsnummer.

— Wird ein inländischer Namensraum verwendet, so wird dessen Systematik, einschließlich aller Datenkennungen, deren Definitionen, deren Vorhandensein und deren Kodierungsformaten, gemäß Artikel 8 der Durchführungsverordnung (EU) 2025/1569 der Kommission ([1]) veröffentlicht.

— Die Personenidentifizierungsdaten und deren Metadaten gemäß den Abschnitten 1 und 3 dieses Anhangs werden in Personenidentifizierungsdatenelemente im Sinne der Spezifikationen des ISO/IEC mdoc-Formats aufgenommen.

— Das deviceKey-Glied im deviceKeyInfo-Glied der Instanz des MobileSecurityObject-Typs enthält einen öffentlichen Schlüssel.

— Dieser öffentliche Schlüssel entspricht einem privaten Schlüssel, der im sicheren Kryptomodul für Brieftaschen (im Folgenden ‚WSCD') des Brieftaschennutzers gespeichert ist.

— Die geschützte Kopfzeile der digitalen CB-AdES-Signatur, mit der Personenidentifizierungsdaten im ISO/IEC-mdoc-Format signiert werden, enthält die x5u- und x5t-Kopfparameter, die beide in RFC 9360 ([2]) spezifiziert sind.

— Der für den x5t-Kopfparameter verwendete Digest-Algorithmus ist SHA-256.

— Die Anforderungen an die Kodierung von Personenidentifizierungsdaten im ISO/IEC-mdoc-Format sind in Tabelle 6 festgelegt:

Tabelle 6

Anforderungen an die Kodierung von Personenidentifizierungsdaten im ISO/IEC-mdoc-Format

Datenkennung	Attributskennung	Kodierungsformat
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]) Durchführungsverordnung (EU) 2025/1569 der Kommission vom 29. Juli 2025 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf qualifizierte elektronische Attributsbescheinigungen und von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen bereitgestellte elektronische Attributsbescheinigungen (ABl. 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/).

Datenkennung	Attributskennung	Kodierungsformat
email_address	email_address	tstr
mobile_phone_number	mobile_phone_number	tstr
expiry_date	expiry_date	tdate oder 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 oder full-date

— Für die Angabe des Kodierungsformats der Attribute in Tabelle 6 sind die in RFC 8610 ([3]) festgelegten Darstellungsarten zu verwenden, wobei die folgenden zusätzlichen Anforderungen gelten:

a) Ein tstr wird in UTF-8 kodiert;

b) ein tstr unterstützt den gesamten Unicode-Bereich;

c) ein tstr darf höchstens 150 Zeichen lang sein;

d) ein Datum ist gemäß RFC 8943 ([4]) zu codieren;

e) ein full-date ist als #6.1004(tstr) zu verstehen, wobei tag 1004 gemäß RFC 8943 verwendet wird;

f) ein tdate-Attribut enthält eine Datum-Zeit-Zeichenkette gemäß RFC 3339 ([5]);

g) ein full-date-Attribut enthält eine full-date-Zeichenkette gemäß RFC 3339 in Übereinstimmung mit RFC 8943;

h) die Darstellung eines Datums in Attributen darf, sofern nichts anderes angegeben ist,

— keine Sekundenbruchteile enthalten,

— keine Ortszeitdifferenz in Bezug auf die UTC enthalten, und die in RFC 3339 spezifizierte Zeitverschiebung muss auf ‚Z' gesetzt sein;

i) eine ganze Zahl mit den Haupttypen 0 und 1 ist gemäß RFC 8949 ([6]) Abschnitt 4.2 so klein wie möglich;

j) ein place_of_birth enthält zumindest eines der folgenden Schlüsselwertpaare: ‚country', ‚region' oder ‚locality';

k) die Angabe der Länge in bstr, tstr, array oder map ist gemäß RFC 8949 Abschnitt 4.2 so kurz wie möglich;

([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 und C. Newman, Date and Time on the Internet: Timestamps, RFC 3339, Juli 2002.
([6]) C. Bormann und P. Hoffman, Concise Binary Object Representation (CBOR), RFC 8949, Dezember 2020.

l) das nationality-Attribut wird als eine Reihe von Alpha-2-Ländercodes gemäß ISO 3166-1 kodiert. Wird die CDDL-Notation gemäß RFC 8610 verwendet, ist dieses Attribut wie folgt zu codieren:

— nationalities = [+ CountryCode]

— CountryCode = tstr; Alpha-2-Ländercode nach ISO 3166-1

— Hat ein Brieftaschennutzer, auf den sich die Personenidentifizierungsdaten beziehen, mehrere Staatsangehörigkeiten und bescheinigt der Anbieter von Personenidentifizierungsdaten diese, so kann der Anbieter von Personenidentifizierungsdaten alle diese Staatsangehörigkeiten in die Personenidentifizierungsdaten aufnehmen.

— Das Attribut place_of_birth wird als Typ place_of_birth kodiert. Wird die CDDL-Notation gemäß RFC 8610 verwendet, ist dieses Attribut wie folgt zu codieren:

place_of_birth =

{

? 'country': tstr; ein einzelner Alpha-2-Ländercode nach ISO 3166-1

? 'region': tstr; der Name eines Staats, einer Provinz, eines Distrikts oder eines Gebiets

? 'locality': tstr; der Name einer Gemeinde, Stadt, Kleinstadt oder eines Dorfs

}

4.2 Anforderungen an die Kodierung von Personenidentifizierungsdaten im SD-JWT VC-Format

— Die Personenidentifizierungsdaten und deren Metadaten gemäß diesem Abschnitt werden in Personenidentifizierungsdaten als Aussagen im Sinne der Spezifikationen des SD-JWT VC-Formats aufgenommen.

— Alle Aussagen in den ausgestellten Personenidentifizierungsdaten, auf die unter dem vorstehenden Gedankenstrich Bezug genommen wird, müssen einzeln selektiv offengelegt werden können, mit Ausnahme der Aussagen, die im SD-JWT VC-Format als nicht selektiv offenlegbar definiert sind.

— Tabelle 7 enthält die Kodierung der Namen der Aussagen, bei denen es sich um öffentliche Bezeichnungen handelt.

— Tabelle 8 enthält die Kodierung der Namen der Aussagen, die mit den Personenidentifizierungsdaten verbunden sind.

— Eine JSON-Zeichenkette, die in mit SD-JWT VC kodierten Personenidentifizierungsdaten verwendet wird, wird in UTF-8 kodiert und unterstützt den gesamten Unicode-Bereich, sofern in Tabelle 8 oder den darin enthaltenen Verweisen nicht ausdrücklich etwas anderes angegeben ist.

— Die JWT-Aussagen nbf und exp gemäß RFC 7519 ([7]) sind zu verwenden, um die technische Gültigkeitsdauer von Personenidentifizierungsdaten auszudrücken, die dem SD-JWT VC-Format entsprechen.

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

— Personenidentifizierungsdaten enthalten die in RFC 7800 ([8]) definierte cnf-Aussage, bei der es sich um einen öffentlichen Schlüssel handelt, der aus einem privaten Schlüssel generiert wird, der im WSCD der Einzelbrieftasche des Brieftaschennutzers gespeichert ist.

— Die geschützte Kopfzeile der digitalen Signatur, mit der Personenidentifizierungsdaten im SD-JWT VC-Format signiert werden, enthält die x5u- und x5t#S256-Kopfparameter gemäß RFC 7515 ([9]).

Tabelle 7

Anforderungen an die Kodierung von Personenidentifizierungsdaten im SD-JWT VC-Format mit öffentlichen Bezeichnungen

Datenkennung	Attributskennung	Kodierungsformat
`family_name`	`family_name`	Zeichenkette
`given_name`	`given_name`	Zeichenkette
`birth_date`	`birthdate`	Zeichenkette, ISO 8601-1, Format JJJJ-MM-TT
`birth_place`	`place_of_birth`	JSON-Struktur
`nationality`	`nationalities`	Zeichenketten-Array
`resident_address`	`address.formatted`	Zeichenkette
`resident_country`	`address.country`	Zeichenkette
`resident_state`	`address.region`	Zeichenkette
`resident_city`	`address.locality`	Zeichenkette
`resident_postal_code`	`address.postal_code`	Zeichenkette
`resident_street`	`address.street_address`	Zeichenkette
`family_name_birth`	`birth_family_name`	Zeichenkette
`given_name_birth`	`birth_given_name`	Zeichenkette
`email_address`	`email`	Zeichenkette
`mobile_phone_number`	`phone_number`	Zeichenkette
`portrait`	`picture`	Zeichenkette; Daten-URL, die ein base64-kodiertes Porträtbild im JPEG-Format enthält

([8]) M. Jones, et al., Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs), RFC 7800, April 2016.
([9]) J. Jones, et al., JSON Web Signatur (JWS), RFC 7515, Mai 2015.

Tabelle 8

Anforderungen an die Kodierung von Personenidentifizierungsdaten im SD-JWT VC-Format mit privaten Namen

Datenkennung	Attributskennung	Kodierungsformat
`expiry_date`	`date_of_expiry`	Zeichenkette, ISO 8601-1, Format JJJJ-MM-TT
`issuance_date`	`date_of_issuance`	Zeichenkette, ISO 8601-1, Format JJJJ-MM-TT
`personal_administrative_-number`	`personal_administrati-ve_number`	Zeichenkette
`sex`	`sex`	Zahl
`issuing_authority`	`issuing_authority`	Zeichenkette
`issuing_country`	`issuing_country`	Zeichenkette
`document_number`	`document_number`	Zeichenkette
`issuing_jurisdiction`	`issuing_jurisdiction`	Zeichenkette

— Der Basistyp der Personenidentifizierungsdaten lautet ‚urn:eudi:pid:1' und ist in der vct-Aussage enthalten. Für alle Personenidentifizierungsdaten sind Typen im Namensraum ‚urn:eudi:pid:' zu verwenden.

— Enthalten Personenidentifizierungsdaten Attribute, die in diesem Anhang nicht aufgeführt sind, so werden diese Attribute innerhalb eines inländischen Typs definiert.

— Wird der inländische Typ verwendet, so wird dessen Systematik, einschließlich aller Datenkennungen, deren Definitionen, deren Vorhandensein und deren Kodierungsformaten, in einem System definiert, das gemäß Artikel 8 der Durchführungsverordnung (EU) 2025/1569 veröffentlicht wird.

(5) Abschnitt 5: Einzelheiten der Vertrauensinfrastruktur

Die Liste der Anbieter von Personenidentifizierungsdaten, die die Kommission gemäß der Durchführungsverordnung (EU) 2024/2980 bereitgestellt hat, ermöglicht die Authentifizierung der Personenidentifizierungsdaten."

ANHANG II

„ANHANG Ia

Kryptografische Mechanismen nach Artikel 5a

Europäische Gruppe für die Cybersicherheitszertifizierung, Untergruppe für Kryptografie: ‚Agreed Cryptographic Mechanisms' (Vereinbarte kryptografische Mechanismen), veröffentlicht von der Agentur der Europäischen Union für Cybersicherheit (ENISA) ([1])"

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

ANHANG III

„ANHANG Ib

Technische Spezifikationen für Einzelbrieftaschenbescheinigungen gemäß Artikel 6 Absatz 2a

(1) Eine Einzelbrieftaschenbescheinigung umfasst eine oder mehrere Brieftascheninstanzbescheinigungen und eine oder mehrere Schlüsselbescheinigungen.

(2) Die Brieftascheninstanzbescheinigung und die Schlüsselbescheinigungen müssen die folgenden Anforderungen erfüllen:

a) Formatanforderungen

— FR-WIA-1:l Eine Brieftascheninstanzbescheinigung muss ein JSON Web Token (JWT) gemäß RFC 7519 ([1]) sein, das vom Brieftaschenanbieter mit einer kompakten JAdES-B-Basissignatur unterzeichnet oder besiegelt wurde.

— FR-WIA-1.1: Eine Brieftascheninstanzbescheinigung ist eine Brieftaschenbescheinigung gemäß Anlage E von OpenID for Verifiable Credential Issuance v1.0 ([2]) (im Folgenden ‚OID4VCI') , die gemäß C-WIA-1 und C-WIA-2 verlängert wird.

— FR-KA-1: Eine Schlüsselbescheinigung ist ein JWT gemäß RFC 7519, das vom Brieftaschenanbieter mit einer kompakten JAdES-B-Basissignatur unterzeichnet oder besiegelt wurde.

— FR_KA_1.1: Eine Schlüsselbescheinigung ist eine Schlüsselbescheinigung gemäß Anlage D von OID4VCI, die gemäß C_KA-1 und C_KA-2 verlängert wird.

b) Anforderungen an den Transport

— TR-WIA-1: Eine Einzelbrieftasche verwendet bei der Ausstellung von Personenidentifizierungsdaten, qualifizierten oder nicht qualifizierten elektronischen Attributsbescheinigungen oder elektronischen Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, eine Brieftascheninstanzbescheinigung.

— TR-WIA-2: Ein Brieftaschenanbieter überprüft die Integrität der Brieftascheninstanz und unterzeichnet oder besiegelt die Brieftascheninstanzbescheinigung.

— TR-WIA-2.1: Wenn ein Brieftaschenanbieter eine Brieftascheninstanzbescheinigung ausstellt, muss die Differenz zwischen dem Zeitpunkt, zu dem der Brieftaschenanbieter die Integrität der Brieftascheninstanz überprüft hat, und dem Zeitpunkt, den er im Kopfparameter ‚exp' der ausgestellten Brieftascheninstanzbescheinigung angibt, weniger als 24 Stunden betragen.

— TR-WIA-2.2: Der Brieftaschenanbieter stellt sicher, dass eine Einzelbrieftasche nach Bedarf Brieftascheninstanzbescheinigungen enthält, die für die Ausstellung von Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen erforderlich sind.

— TR-WIA-3: Bei der Ausstellung übermittelt eine Einzelbrieftasche dem Autorisierungsserver eine Brieftascheninstanzbescheinigung in der Anfrage auf Push-Autorisierung und der Token-Anfrage gemäß OID4VCI.

— TR-WIA-3.1: Eine Einzelbrieftasche übermittelt die Brieftascheninstanzbescheinigung zusammen mit einem Besitznachweis (Proof of possession, PoP) gemäß Anlage E von OID4VCI.

— TR-WIA-3.2: Eine Einzelbrieftasche übermittelt dieselbe Brieftascheninstanzbescheinigung an nur einen Autorisierungsserver.

([1]) RFC 7519: JSON Web Token (JWT), Mai 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: Wenn ein Brieftaschenanbieter die Option ‚per-issuer reuse' gemäß R_WIA_1 nutzt, kann eine Einzelbrieftasche eine Brieftascheninstanzbescheinigung mehrmals an denselben Autorisierungsserver übermitteln.

— TR-WIA-3.2.2: Verwendet ein Brieftaschenanbieter die Option ‚per-issuer reuse' nicht, so darf eine Einzelbrieftasche eine Brieftascheninstanzbescheinigung in höchstens einem Ausstellungsverfahren verwenden.

— TR-WIA-4: Erhält ein Autorisierungsserver eine Brieftascheninstanzbescheinigung, so überprüft er die Signatur der Brieftascheninstanzbescheinigung unter Verwendung des öffentlichen Schlüssels im Signierzertifikat, der im x5c-Parameter der JOSE-Kopfzeile der Einzelbrieftaschenbescheinigung enthalten ist.

— TR-WIA-4.1: Der Autorisierungsserver überprüft auch, ob dieses Signierzertifikat mit einem Vertrauensanker auf der in Artikel 5 der Durchführungsverordnung (EU) 2024/2980 genannten Liste der Brieftaschenanbieter überprüft werden kann, möglicherweise mit Zwischenzertifikaten, die im x5c-Parameter enthalten sind.

— TR-WIA-4.2: Der Autorisierungsserver überprüft, ob die Brieftascheninstanzbescheinigung noch nicht abgelaufen ist.

— TR-WIA-4.3: Der Autorisierungsserver überprüft die Signatur des PoP mit dem öffentlichen Schlüssel, der in der cnf-Aussage enthalten ist.

— TR_KA-1: Eine Einzelbrieftasche verwendet bei der Ausstellung von Personenidentifizierungsdaten und bei der Ausstellung von gerätegebundenen qualifizierten oder nicht qualifizierten elektronischen Attributsbescheinigungen oder elektronischen Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, eine Schlüsselbescheinigung.

— TR_KA-1.1: Eine Einzelbrieftasche verwendet bei der Ausstellung von nicht gerätegebundenen qualifizierten oder nicht qualifizierten elektronischen Attributsbescheinigungen oder elektronischen Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, keine Schlüsselbescheinigung.

— TR_KA-2: Ein Brieftaschenanbieter stellt einer Einzelbrieftasche verschiedene Schlüsselbescheinigungen für das WSCD der Einzelbrieftasche und für jeden ihrer Schlüsselspeicher zur Verfügung.

— TR_KA-2.1: Der Brieftaschenanbieter unterzeichnet oder besiegelt eine Schlüsselbescheinigung, nachdem er sich vergewissert hat, dass die in der Schlüsselbescheinigung bescheinigten Schlüssel in dem in der Schlüsselbescheinigung beschriebenen WSCD der Einzelbrieftasche oder dem entsprechenden Schlüsselspeicher gespeichert sind.

— TR_KA-2.2: Die Schlüsselbescheinigung enthält zumindest einen bescheinigten öffentlichen Schlüssel. Die Anzahl der Schlüssel in der Schlüsselbescheinigung, die an den Nachweisaussteller übermittelt werden, sollte die von diesem Aussteller in seinen Nachweisausstellermetadaten angegebene maximale Batch-Größe nicht überschreiten; siehe ETSI TS 119 472-3 ([3]), Parameter ‚credential_configurations_supported. credential_metadata.credential_reuse_policy.options.batch_size'.

— TR_KA-2.3: Ein Brieftaschenanbieter nimmt einen öffentlichen Schlüssel (der einem privaten Schlüssel entspricht, der im WSCD oder im Schlüsselspeicher der Einzelbrieftasche gespeichert ist) in höchstens eine Schlüsselbescheinigung auf.

— TR_KA-2.4: Eine Einzelbrieftasche verwendet eine Schlüsselbescheinigung bei höchstens einem Verfahren zur Ausstellung oder erneuten Ausstellung von Nachweisen.

— TR_KA-2.5: Ein Brieftaschenanbieter stellt sicher, dass eine Einzelbrieftasche nach Bedarf über Schlüsselbescheinigungen verfügt, die für die Ausstellung von Personenidentifizierungsdaten und gerätegebundenen elektronischen Attributsbescheinigungen erforderlich sind.

([3]) ETSI, Elektronische Signaturen und Infrastrukturen (ESI) — JAdES digitale Signaturen — Teil 3; JAdES-Level und -Basissignaturprofile, ETSI TS 119 472-3, V1.1.1, März 2026.

— TR_KA-3: Wenn dies während der Ausstellung erforderlich ist, nimmt eine Einzelbrieftasche eine Schlüsselbescheinigung im Feld ‚proofs' einer Nachweisabfrage an den Nachweisaussteller gemäß OID4VCI in einen Nachweis des Typs ‚jwt' oder des Typs ‚attestation' auf.

— TR_KA_3.1: Enthält eine Einzelbrieftasche in einem ‚jwt'-Element eine Schlüsselbescheinigung, so unterzeichnet oder besiegelt sie die Schlüsselbescheinigung mit dem privaten Schlüssel, der dem öffentlichen Schlüssel in Index 0 des Arrays ‚attested_keys' im Objekt ‚key_attestation' entspricht.

— TR_KA-4: Wenn ein Nachweisaussteller gerätegebundene Nachweise ausgibt, gibt er im Parameter ‚proof_types_supported' in seinen Nachweisaustellermetadaten gemäß Abschnitt 12.2.4 von OID4VCI an, dass er sowohl den Nachweistyp ‚jwt' als auch den Nachweistyp ‚attestation' für Schlüsselbescheinigungen unterstützt, die das Objekt ‚key_attestation_required' enthalten.

— TR_KA-4.1: Wenn ein Nachweisaussteller nicht gerätegebundene Zertifikate ausstellt, verzichtet er auf die Parameter ‚proof_types_supported' und ‚cryptographic_binding_methods_supported' in den Nachweisausstellermetadaten.

— TR_KA-5: Erhält ein Nachweisaussteller eine Schlüsselbescheinigung in einem Nachweistyp ‚jwt' oder ‚attestation', so überprüft er die Signatur der Schlüsselbescheinigung unter Verwendung des öffentlichen Schlüssels im Signierzertifikat, das im x5c-Parameter der JOSE-Kopfzeile der Schlüsselbescheinigung enthalten ist, und ob dieses Signierzertifikat mit einem Vertrauensanker auf der in Artikel 5 der Durchführungsverordnung (EU) 2024/2980 genannten Liste der Brieftaschenanbieter überprüft werden kann, möglicherweise mit Zwischenzertifikaten, die im x5c-Parameter enthalten sind.

— TR_KA-6: Erhält ein Nachweisaussteller eine Schlüsselbescheinigung in einem Nachweistyp ‚jwt', so überprüft er die Signatur des ‚jwt'-Elements mit dem Schlüssel in Index 0 des Arrays ‚attested_keys' innerhalb des im ‚jwt'-Element enthaltenen Objekts ‚key_attestation'.

— TR_KA-6.1: Der Nachweisaussteller überprüft, ob das Feld ‚nonce' des ‚jwt'-Elements ein gültiges c_nonce von seinem nonce_endpoint gemäß OID4VCI enthält.

— TR_KA-7: Erhält ein Nachweisaussteller eine Schlüsselbescheinigung eines Nachweistyps ‚attestation', überprüft er, ob das Objekt ‚key_attestation' ein gültiges c_nonce von seinem nonce_endpoint enthält.

— TR_KA-8: Ein Anbieter von Personenidentifizierungsdaten stellt sicher, dass Personenidentifizierungsdaten an einen öffentlichen Schlüssel gebunden sind, der aus einer Schlüsselbescheinigung stammt, in der ein WSCD genannt wird.

c) Anforderungen an den Inhalt

— C_WIA-1: Eine Brieftascheninstanzbescheinigung enthält zumindest Folgendes:

— die Aussage ‚wallet_name' gemäß Anlage E von OID4VCI, wobei ihr Wert die Kennung der Brieftaschenlösung ist, die in der in Artikel 5 der Durchführungsverordnung (EU) 2024/2980 genannten Liste der Brieftaschenanbieter zu finden ist,

— eine Aussage ‚wallet_version' ([4]), bei der es sich um eine Zeichenkette handelt, deren Wert der Version der Brieftaschenlösung entspricht,

— eine Aussage ‚wallet_solution_certification_information', bei der es sich um ein JSON-Objekt handelt, das Informationen über die Konformitätsbewertungsstelle, die die Brieftaschenlösung zertifiziert hat, gegebenenfalls die Zertifizierungsnummer und andere relevante Einzelheiten in Bezug auf die Zertifizierung enthält,

([4]) Diese Aussage ist in dieser Durchführungsverordnung definiert, da sie nicht Teil der OID4VCI-Spezifikation ist.

— eine Aussage ‚client_status' mit zwei Unterfeldern:

— ‚status': Verweis auf die Statusliste gemäß Anlage E von OID4VCI, der den Widerrufsstatus der Brieftascheninstanz darstellt; Einzelheiten sind Abschnitt e zu entnehmen,

— ‚exp': ein NumericDate gemäß RFC 7519, das den Zeitraum festlegt, bis zu dem der Brieftaschenanbieter den Widerrufsstatus auf dem Statuslistenindex, auf den er in ‚status' verweist, aufrechterhalten wird;

— die Aussage ‚exp' gemäß Anlage E von OID4VCI.

— *ANMERKUNG:* Die Aussage ‚client_status.status' in einer Brieftascheninstanzbescheinigung steht für den Widerrufsstatus der Brieftascheninstanz, nicht den Widerrufsstatus der Bescheinigung selbst. Wie in R_WIA-1 beschrieben, kann ein Brieftaschenanbieter beschließen, jede Brieftascheninstanzbescheinigung auf einen bestimmten Autorisierungsserver auszurichten, da alle an diesen Server übermittelten Bescheinigungen im Eintrag ‚client_status.status' denselben Indexwert enthalten.

— *ANMERKUNG:* Der ‚idx'-Wert in der Aussage ‚status' kann als (paarweise) eindeutige Kennung der Brieftascheninstanz und der Einzelbrieftasche verwendet werden.

— C_WIA-2: Eine Brieftascheninstanzbescheinigung sollte auch die in Anlage E von OID4VCI genannte Aussage ‚wallet_link' enthalten, und der Wert dieser Aussage muss ein URI sein, bei dem weitere Informationen über die Brieftaschenlösung abgerufen werden können.

— C_WIA-3: Ein Autorisierungsserver darf den ‚exp'-Parameter auf der obersten Ebene einer Brieftascheninstanzbescheinigung nicht als Ende des Zeitraums der Aufrechterhaltung des Widerrufs der Brieftascheninstanz interpretieren.

— *ANMERKUNG:* Der ‚exp'-Parameter auf der obersten Ebene einer Brieftascheninstanzbescheinigung gibt an, wann die Bescheinigung selbst abläuft.

— C_KA-1: Eine Schlüsselbescheinigung enthält Folgendes:

— die Aussagen ‚key_storage' und ‚user_authentication' gemäß Anlage D von OID4VCI.

— Die Attribute ‚key_storage' und ‚user_authentication' haben den Wert ‚iso_18045_high', wenn in einer Schlüsselbescheinigung ein WSCD genannt wird;

— die Aussage ‚certification' gemäß Anlage D von OID4VCI, die eine URL enthält, über die Informationen über die von dem WSCD oder Schlüsselspeicher erlangte Zertifizierung, normalerweise das System wie Common Criteria oder GlobalPlatform, die bewerteten Anforderungen wie das geltende Schutzprofil und das Evaluierungsniveau abgerufen werden können.

— Anhand dieser Informationen muss feststellbar sein, ob es sich bei dem Schlüsselspeicher um ein WSCD handelt;

— eine Aussage ‚key_storage_status' mit zwei Unterfeldern:

— ‚status': Verweis auf die Statusliste gemäß Anlage D.1 von OID4VCI. Der Wert steht entweder für den Widerrufsstatus der Art des WSCD oder Schlüsselspeichers, der zur Speicherung der bescheinigten Schlüssel verwendet wird, oder – bei der Indexoption per-key-attestation – für den Widerrufsstatus des WSCD oder Schlüsselspeichers einer Einzelbrieftasche. Zu den verfügbaren Indexzuordnungsoptionen siehe R_KA_1;

— ‚exp': ein NumericDate gemäß RFC 7519, das den Zeitraum festlegt, bis zu dem der Brieftaschenanbieter den Widerrufsstatus auf dem Statuslistenindex, auf den er in ‚status' verweist, aufrechterhalten wird;

— die Aussage ‚exp' gemäß Anlage D von OID4VCI.

— *ANMERKUNG* zum ‚idx'-Wert in der Aussage ‚key_storage_status.status' in einer Schlüsselbescheinigung: Wendet der Brieftaschenanbieter die Option ‚type-shared index' an (siehe R_KA_1), haben alle Schlüsselbescheinigungen für dieselbe Art eines WSCD oder eines Schlüsselspeichers denselben Statuslistenindex. Daher ist der ‚idx'-Wert pro Einzelbrieftasche nicht eindeutig. Wendet der Brieftaschenanbieter hingegen die Indexoption ‚per-key-attestation' an, ist der ‚idx'-Wert für die Einzelbrieftasche eindeutig (oder für jeden Nachweisaussteller paarweise eindeutig). In allen Fällen darf ein Nachweisaussteller den ‚idx'-Wert in einer Schlüsselbescheinigung jedoch nicht als Einzelbrieftaschenkennung verwenden, sondern muss stattdessen den ‚idx'-Wert in einer Brieftascheninstanzbescheinigung verwenden.

— C_KA-2: Wird eine Schlüsselbescheinigung als Nachweistyp ‚attestation' übermittelt, muss sie auch ein gültiges c_nonce gemäß Anlage F.3 von OID4VCI enthalten.

— C_KA-3: Ein Nachweisaussteller darf den ‚exp'-Parameter auf der obersten Ebene einer Schlüsselbescheinigung nicht als Ende des Zeitraums der Aufrechterhaltung des Widerrufs des WSCD oder des Schlüsselspeichers interpretieren.

— *ANMERKUNG:* Der ‚exp'-Parameter auf der obersten Ebene einer Schlüsselbescheinigung gibt an, wann die Schlüsselbescheinigung selbst abläuft.

d) Anforderungen an den Lebenszyklus

— In diesem Anhang werden die folgenden Parameter der Nachweisausstellermetadaten festgelegt:

— ‚preferred_client_status_period': OPTIONAL. eine ganze Zahl zur Angabe des bevorzugten Restzeitraums der Statusaufrechterhaltung der Brieftascheninstanzbescheinigung, die von der Einzelbrieftasche bei der Ausstellung vorzulegen ist, in Sekunden. Der Restzeitraum der Statusaufrechterhaltung ist definiert als der Wert von ‚client_status.exp' in der Bescheinigung abzüglich des Zeitpunkts des Eingangs der Bescheinigung.

— ‚preferred_key_storage_status_period': OPTIONAL. eine ganze Zahl zur Angabe des bevorzugten Restzeitraums der Statusaufrechterhaltung der Schlüsselbescheinigung, die von der Einzelbrieftasche bei der Ausstellung vorzulegen ist, in Sekunden. Der Restzeitraum der Statusaufrechterhaltung ist definiert als der Wert von ‚key_storage_status.exp' in der Bescheinigung abzüglich des Zeitpunkts des Eingangs der Bescheinigung.

— LC_WIA-1: Ein Autorisierungsserver kann seinen bevorzugten Restzeitraum der Statusaufrechterhaltung in Brieftascheninstanzbescheinigungen mitteilen, indem er den Metadatenparameter ‚preferred_client_status_period' in seinen Nachweisaustellermetadaten-Endpunkt gemäß Abschnitt 12.2.2 von OID4VCI aufnimmt.

— LC_WIA-1.1: Dieses Feld wird auf der obersten Ebene der Nachweisausstellermetadaten platziert.

— LC_WIA_2: Ein Autorisierungsserver darf den ‚exp'-Parameter auf der obersten Ebene einer Brieftascheninstanzbescheinigung nicht als Ende des Zeitraums der Aufrechterhaltung des Widerrufs der Brieftascheninstanz interpretieren.

— LC_WIA_3: Wenn ein Brieftaschenanbieter eine Brieftascheninstanzbescheinigung unterzeichnet oder besiegelt, erhält er den Widerrufsstatus der betreffenden Brieftascheninstanz so lange aufrecht, bis der in dieser Brieftascheninstanzbescheinigung angegebene ‚wallet_instance_status.exp' abgelaufen ist.

— LC_KA-1: Wird eine Schlüsselbescheinigung benötigt, kann ein Nachweisaussteller seinen bevorzugten Restzeitraum der Statusaufrechterhaltung in Schlüsselbescheinigungen mitteilen, indem er den Metadatenparameter ‚preferred_key_storage_status_period' in seinen Nachweisaustellermetadaten-Endpunkt gemäß Abschnitt 12.2.2 von OID4VCI aufnimmt.

— LC_KA-1.1: Dieses Feld ist in das Objekt ‚key_attestations_required' gemäß Abschnitt 12.2.4 von OID4VCI zu platzieren.

— LC_KA-2: Ein Brieftaschenanbieter wählt die technische Gültigkeitsdauer der Schlüsselbescheinigungen, die er ausstellt.

— LC_KA-3: Wenn ein Brieftaschenanbieter eine Schlüsselbescheinigung unterzeichnet oder besiegelt, erhält er den Widerrufsstatus des betreffenden WSCD oder des Schlüsselspeichers so lange aufrecht, bis der in dieser Schlüsselbescheinigung angegebene ‚key_storage_status.exp' abgelaufen ist.

— LC_GEN-1: Ein Brieftaschenanbieter stellt sicher, dass eine Einzelbrieftasche stets Einzelbrieftaschenbescheinigungen und Schlüsselbescheinigungen vorlegen kann, deren ‚client_status.exp' bzw. ‚key_storage_status.exp' zum Zeitpunkt der Vorlage bei einem Autorisierungsserver oder Nachweisaussteller mindestens 31 Tage in der Zukunft liegt.

— *ANMERKUNG:* Dadurch wird sichergestellt, dass die Anbieter von Personenidentifizierungsdaten auf Widerrufsketten vertrauen können, ohne kurzlebige Personenidentifizierungsdaten ausstellen zu müssen.

— LC_GEN-2: Ein Brieftaschenanbieter stellt sicher, dass eine Einzelbrieftasche bei der Ausstellung die Nachweisausstellermetadaten abfragt.

  — LC_GEN_2.1: Wenn diese Metadaten ein Feld ‚preferred_key_storage_status_period' enthalten, übermittelt die Einzelbrieftasche eine Schlüsselbescheinigung mit einer möglichst kurzen, aber nicht negativen (‚key_storage_status.exp' – aktuelle Zeit) – ‚preferred_key_storage_status_period'. Steht der Einzelbrieftasche keine solche Schlüsselbescheinigung zur Verfügung, so erlangt sie vom Brieftaschenanbieter eine neue Schlüsselbescheinigung, die die Bedingung ‚key_storage_status.exp' – aktuelle Zeit ≥ ‚preferred_key_storage_status_period' erfüllt.

  — LC_GEN_2.2: Wenn diese Metadaten ein Feld ‚preferred_client_status_period' enthalten, übermittelt die Einzelbrieftasche eine Brieftascheninstanzbescheinigung mit einer möglichst kurzen, aber nicht negativen (‚client_status.exp' – aktuelle Zeit) – ‚preferred_client_status_period'. Steht der Einzelbrieftasche keine solche Brieftascheninstanzbescheinigung zur Verfügung, so erlangt sie vom Brieftaschenanbieter eine neue Brieftascheninstanzbescheinigung, die die Bedingung ‚client_status.exp' – aktuelle Zeit ≥ ‚preferred_client_status_period' erfüllt.

— LC_GEN-3: Die technische Gültigkeitsdauer von Personenidentifizierungsdaten endet sowohl vor dem ‚client_status.exp' der Brieftascheninstanzbescheinigung als auch vor dem ‚key_storage_status.exp' der Schlüsselbescheinigung, die im Ausstellungsverfahren an den Anbieter von Personenidentifizierungsdaten übermittelt wird.

— LC_GEN-4: Ein Anbieter von Personenidentifizierungsdaten mit einer technischen Gültigkeitsdauer von mehr als 24 Stunden überprüft während der technischen Gültigkeitsdauer der Personenidentifizierungsdaten mindestens einmal alle 24 Stunden den Widerrufsstatus sowohl der Brieftascheninstanzbescheinigung als auch der Schlüsselbescheinigung, die er bei der Ausstellung erhalten hat. Wird eine der beiden widerrufen, so widerruft der Anbieter die Personenidentifizierungsdaten.

e) Widerrufsanforderungen

— R_GEN-1: Ein Brieftaschenanbieter verwendet Token-Statuslisten (gemäß IETF-Token-Statusliste) als Widerrufsmechanismus sowohl für Schlüsselbescheinigungen als auch für Brieftascheninstanzbescheinigungen gemäß Anlage D bzw. E von OID4VCI.

— *ANMERKUNG:* Um die Skalierbarkeit seiner Statuslisten zu verbessern, kann ein Brieftaschenanbieter die folgenden Optimierungen verwenden:

  — Aufteilung der Statusliste in mehrere Blöcke, sofern die Brieftaschenanbieter eine beträchtliche Zahl von Nutzern und ausgestellten Bescheinigungen haben. Es gibt viele Blockbildungsstrategien (*chunking strategies*), z. B. auf der Grundlage einer festen Größe oder eines bestimmten Zeitraums. Die Blockbildungsstrategie liegt im Ermessen des Brieftaschenanbieters. Überlegungen können sich auf die Größe einer Statusliste für das Herunterladen und die Privatsphäre des Nutzers beziehen.

  — Führen mehrerer Statuslisten.

  — Komprimierung einer Statusliste zur Verringerung ihre Größe.

— R_WIA-1: Ein Brieftaschenanbieter kann in allen Brieftascheninstanzbescheinigungen, die eine bestimmte Einzelbrieftasche demselben Autorisierungsserver übermittelt, der ‚idx'-Aussage in der Aussage ‚client_status.status' denselben Wert zuweisen. Dies wird als Option ‚per-issuer reuse' bezeichnet. Wenn diese Option Gebrauch verwendet wird:

  — R_WIA-1.1: Die Einzelbrieftasche behält für jeden Autorisierungsserver, mit dem sie zuvor interagiert hat, den verwendeten Indexwert bei und fordert bei einer erneuten Interaktion mit demselben Autorisierungsserver eine Brieftascheninstanzbescheinigung mit demselben Indexwert an.

  — R_WIA-1.2: Wenn bei einem Brieftaschenanbieter eine Einzelbrieftaschenbescheinigung mit einem bestimmten Indexwert angefordert wird, überprüft dieser, ob die anfordernde Einzelbrieftasche diesen Indexwert zuvor erhalten hat, bevor er eine neue Einzelbrieftaschenbescheinigung mit diesem Indexwert ausstellt.

  — R_WIA-1.3: Die Einzelbrieftasche darf nicht denselben Indexwert für Interaktionen mit verschiedenen Autorisierungsservern wiederverwenden.

— *ANMERKUNG:* Wird die Option ‚per-issuer reuse' verwendet, kann der Brieftaschenanbieter feststellen, mit wie vielen Autorisierungsservern eine Einzelbrieftasche interagiert hat und wie oft sie mit den einzelnen Servern interagiert.

— R_WIA-2: Ein Brieftaschenanbieter dokumentiert in seiner Datenschutzerklärung, ob er die Option ‚per-issuer reuse' für den Widerruf einer Brieftascheninstanz verwendet.

— R_WIA-3: Verwendet ein Brieftaschenanbieter die Option ‚per-issuer reuse' nicht, weist er jeder von ihm ausgestellten Brieftascheninstanzbescheinigung einen neuen, nicht verknüpfbaren Indexwert zu.

— R_WIA-4: Muss eine Einzelbrieftasche widerrufen werden, so widerruft der Brieftaschenanbieter die Indexwerte in der Aussage ‚client_status.status' in allen mit dieser Einzelbrieftasche verbundenen Brieftascheninstanzbescheinigungen.

— R_WIA-5: Ein Brieftaschenanbieter berücksichtigt bei der Festlegung der Größe seiner Statuslisten für Brieftascheninstanzbescheinigungen den Nutzungsumfang und die zugrunde liegende Architektur und stellt sicher, dass diese groß genug sind, um Korrelationen zu verhindern und die Privatsphäre der Nutzer zu schützen. Eine Statusliste bezieht sich nach Möglichkeit auf mindestens 10 000 Bescheinigungen.

— R_KA_1: Ein Brieftaschenanbieter wählt in einer Schlüsselbescheinigung eine der folgenden Indexzuweisungsoptionen für die Aussage ‚key_storage_status.status':

  — Option 1: der sogenannte ‚type-shared index', bei dem alle Schlüsselbescheinigungen, die in derselben Art von WSCD oder Schlüsselspeicher gespeicherte Schlüssel bescheinigen, denselben Indexwert in ‚key_storage_status.status' enthalten.

  — Option 2: der sogenannte ‚per-key-attestation index', bei dem eine Schlüsselbescheinigung, die in einem einzelnen WSCD oder Schlüsselspeicher gespeicherte Schlüssel bescheinigt, einen (paarweise) eindeutigen Indexwert in ‚key_storage_status.status' enthält.

— *ANMERKUNG:* Verwendet ein Brieftaschenanbieter die Option 1, werden alle Schlüsselbescheinigungen der betroffenen Art für alle Einzelbrieftaschen in einem einzigen Widerrufsvorgang für ungültig erklärt. Da alle Schlüsselbescheinigungen für dieselbe Art von WSCD oder Schlüsselspeicher einen einzigen Statuslistenindex haben, spiegelt die Zahl der Einträge in einer Statusliste der Schlüsselbescheinigungen die Zahl der vom Brieftaschenanbieter unterstützten Arten von WSCD oder Schlüsselspeichern und nicht die Zahl der genutzten Einzelbrieftaschen wider. Die Datenschutzerwägungen, die die Mindestgröße der Statuslisten für Brieftascheninstanzen begründen, gelten daher nicht für Statuslisten der Schlüsselbescheinigungen im Rahmen von Option 1, sofern es genügend Einzelbrieftaschen gibt, die dieselbe Art von WSCD oder Schlüsselspeicher verwenden.

— *ANMERKUNG:* Verwendet ein Brieftaschenanbieter die Option 2, steht jeder Index für den Widerrufsstatus des bestimmten WSCD oder des bestimmten Schlüsselspeichers, der in dieser Schlüsselbescheinigung bescheinigt wird.

— *ANMERKUNG:* Verwendet ein Brieftaschenanbieter die Option 2, kann ein bestimmtes WSCD oder ein bestimmter Schlüsselspeicher auch auf Veranlassung des Nutzers widerrufen werden.

— R_KA-2: Verwendet ein Brieftaschenanbieter die Option 2, kann der Brieftaschenanbieter optional die in R_WIA-1 beschriebene Option ‚per-issuer reuse' verwenden. Verwendet der Brieftaschenanbieter diese Option, gelten die Anforderungen R_WIA-1 bis R_WIA-3 entsprechend.

— R_KA-3: Verwendet ein Brieftaschenanbieter die Option 2, berücksichtigt er bei der Festlegung der Größe seiner Statuslisten für Schlüsselbescheinigungen den Nutzungsumfang und die zugrunde liegende Architektur und stellt sicher, dass diese groß genug sind, um Korrelationen zu verhindern und die Privatsphäre der Nutzer zu schützen. Eine Statusliste bezieht sich nach Möglichkeit auf mindestens 10 000 Schlüsselbescheinigungen.

— R_KA-4: Verwendet ein Brieftaschenanbieter die Option 1 (type-shared index), widerruft der Brieftaschenanbieter einen ‚key_storage_status.status'-Eintrag nur dann, wenn die Art des WSCD oder des Schlüsselspeichers eine Sicherheitsschwachstelle aufweist.

f) Anforderungen an Signaturalgorithmen

— SA-1: Für die Unterzeichnung von Brieftascheninstanzbescheinigungen, Schlüsselbescheinigungen, damit verbundenen Besitznachweisen und Token-Statuslisten wird einer der folgenden Algorithmen verwendet:

  — ES256 (ECDSA mit SHA-256 und P-256)

  — ES384 (ECDSA mit SHA-384 und P-384)

  — ES512 (ECDSA mit SHA-512 und P-521)

— SA-2: Ein Brieftaschenanbieter bestimmt, welchen der in SA-1 genannten Algorithmen er verwenden wird.

— SA-3: Ein Autorisierungsserver oder ein Nachweisaussteller (gemäß OID4VCI) unterstützt alle in SA-1 genannten Algorithmen."

ANHANG IV

„ANHANG II

Normenverzeichnis gemäß Artikel 8

Es gelten die technischen Spezifikationen in den Abschnitten 2 bis 6 der Norm ETSI TS 119 472-1 V1.2.1 (2026-02). Sie gelten mit den folgenden Anpassungen:

(1) 2.1 Normative references (Normative Verweise)

— [16] ETSI EN 319 412-1 V1.6.1 (2025-06) – Elektronische Signaturen und Infrastrukturen (ESI) – Zertifikatsprofile – Teil 1: Übersicht und gemeinsame Datenstrukturen.

— [17] ETSI TS 119 412-6 V1.1.1 (2025-09) – Elektronische Signaturen und Vertrauensinfrastrukturen (ESI); Zertifikatsprofile; Teil 6: Zertifikatsprofilanforderungen für PID-, Brieftaschen-, EAA-, QEAA- und PSBEAA-Anbieter.

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

(2) 4.2.11.1 General requirements (Allgemeine Anforderungen)

— EAA-4.2.11.1-06: Wird ein Status-Element für Personenidentifizierungsdaten, qualifizierte elektronische Attributsbescheinigungen oder elektronische Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, verwendet, so gibt dieses lediglich an, ob die Bescheinigung widerrufen wurde oder nicht, und es dürfen keine anderen Statuswerte, etwa zur Aussetzung, unterstützt werden.

— EAA-4.2.11.1-06.1: Wird eine Bescheinigung widerrufen, so ist dies endgültig.

(3) 4.2.13 EAA short-lived (EAA kurzlebig)

— EAA-4.2.13-03: Werden kurzlebige elektronische Attributsbescheinigungen mit einer Gültigkeitsdauer von höchstens 24 Stunden ausgestellt, so ist kein Widerruf erforderlich.

(4) 4.6.3 Requirements for EU EAA issued by or on behalf of a public body responsible for an authentic source (PuB-EAA) (Anforderungen an EU-EEA, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden)

— PuB-EAA-4.6.2-03: ungültig.

— PuB-EAA-4.6.2-04: ungültig.

— PuB-EAA-4.6.3-03: Die digitale PuB-EAA-Signatur sollte das qualifizierte Zertifikat zur Unterstützung der digitalen PuB-EAA-Signatur enthalten.

— PuB-EAA-4.6.3-04: Das qualifizierte Zertifikat zur Unterstützung der digitalen PuB-EAA-Signatur muss die Anforderungen von Abschnitt 8 der Norm ETSI TS 119 412-6 v1.1.1 erfüllen und das QcType qcStatement gemäß der Norm ETSI EN 319 412-5 v2.5.1 enthalten, wobei der Wert id-etsi-qct-eidaspsbeaa wie folgt definiert ist:

id-etsi-qct-eidaspsbeaa OBJECT IDENTIFIER ::= { id-etsi-eidas2-qct-extensions 3 } – Zertifikat gemäß Artikel 45f Absatz 1 Buchstabe b zur Unterstützung der qualifizierten elektronischen Signatur oder des qualifizierten elektronischen Siegels der öffentlichen Stelle gemäß Artikel 3 Nummer 46 der Verordnung (EU) Nr. 910/2014.

(5) 5.2.10.1 General requirements (Allgemeine Anforderungen)

— EAA-5.2.10.1-04: ungültig.

— EAA-5.2.10.1-05: ungültig.

— EAA-5.2.10.1-06: Das status-Glied kann das status_list-Glied gemäß Abschnitt 6.2 des IETF-draft-ietf-oauth-status-list-20 [25] enthalten.

— EAA-5.2.10.1-07: ungültig.

— EAA-5.2.10.1-08: ungültig.

— EAA-5.2.10.1-09: ungültig.

— EAA-5.2.10.1-10: ungültig.

— EAA-5.2.10.1-11: ungültig.

— EAA-5.2.10.1-12: ungültig.

(6) 6.2.10.1 General requirements (Allgemeine Anforderungen)

— EAA-6.2.10.1-01: Verwendet eine elektronische Attributsbescheinigung gemäß ISO/IEC mdoc den Bescheinigungsstatuslistenmechanismus gemäß EAA-6.2.10.1-02.2 oder den Bescheinigungswiderrufslistenmechanismus gemäß EAA-6.2.10.1-02.3, so muss ihr mobiles Sicherheitsobjekt (MSO) die Statusstruktur gemäß EAA-6.2.10.1-17 enthalten, die Informationen über den Widerruf der MSO enthält.

— EAA-6.2.10.1-01.1: Bei der Umsetzung des Kennungslistenmechanismus muss das Statuselement das identifier_list-Element gemäß EAA-6.2.10.1-11 enthalten.

— EAA-6.2.10.1-01.2: Bei der Umsetzung des Statuslistenmechanismus muss das Statuselement das status_list-Element gemäß EAA-6.2.10.1-13 enthalten.

— *ANMERKUNG:*

  — Die Statusstruktur enthält einen Verweis auf eine MSO-Widerrufsliste.

  — Die MSO-Widerrufsliste ist eine COSE_Sign1-Struktur, die anzeigt, ob ein bestimmtes MSO widerrufen wurde oder nicht.

  — Die Statusstruktur enthält alle Informationen, die der auf Brieftaschen vertrauende Beteiligte benötigt, um festzustellen, ob die MSO-Widerrufsliste authentisch ist.

— EAA-6.2.10.1-02: Der Anbieter von Personenidentifizierungsdaten, der Anbieter qualifizierter elektronischer Attributsbescheinigungen oder der Anbieter elektronischer Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, verwendet eine der folgenden Methoden für den Widerruf von Personenidentifizierungsdaten, qualifizierten elektronischen Attributsbescheinigungen oder elektronischen Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden:

— EAA-6.2.10.1-02.1: Stellen sie kurzlebige elektronische Attributsbescheinigungen mit einer Gültigkeitsdauer von höchstens 24 Stunden aus, ist kein Widerruf erforderlich.

— EAA-6.2.10.1-02.2: Verwendung eines Bescheinigungsstatuslistenmechanismus, um die Widerrufsinformationen als Statusliste zu codieren.

— EAA-6.2.10.1-02.2.1: Der Statuslistenmechanismus widerruft ein MSO, je nachdem, ob das Bit der vom Aussteller definierten Bitposition in der Statusliste auf ‚wahr' gesetzt ist.

— EAA-6.2.10.1-02.2.2: Der Statuslistenmechanismus ist in der Spezifikation der Token-Statusliste (draft-ietf-oauth-status-list-20) festgelegt.

— EAA-6.2.10.1-02.3: Verwendung eines Widerrufslistenmechanismus für die Bescheinigung, um die Widerrufsinformationen als Kennungsliste zu codieren.

— EAA-6.2.10.1-02.3.1: Der Kennungslistenmechanismus widerruft ein MSO, je nachdem, ob die vom Aussteller definierte Kennung im MSO auf der Kennungsliste vorliegt.

— 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 und EAA-6.2.10.1-11 legen den Kennungslistenmechanismus auf der Grundlage der Anforderungen der Spezifikation der Token-Statusliste fest, einschließlich der Gemeinsamkeit zwischen dem Statuslisten- und dem Kennungslistenmechanismus.

— EAA-6.2.10.1-03: Wird ein Status-Element für Personenidentifizierungsdaten, qualifizierte elektronische Attributsbescheinigungen oder elektronische Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, verwendet, so wird lediglich der Status ‚widerrufen' verwendet.

— EAA-6.2.10.1-03.1: Für eine Statusliste bedeutet dies, dass lediglich die Werte ‚valid' und ‚invalid' gemäß der Spezifikation der Token-Statusliste verwendet werden dürfen.

— EAA-6.2.10.1-03.2: Für die Kennungsliste: Es werden nur widerrufene MSO in die Kennungsliste aufgenommen, und keine vorübergehend ausgesetzten MSO.

— EAA-6.2.10.1-04: Wird ein MSO widerrufen, so ist dies endgültig.

— EAA-6.2.10.1-05: Die Überprüfung der MSO-Widerrufsliste ist für den auf Brieftaschen vertrauenden Beteiligten fakultativ, und die Überprüfung entspricht gegebenenfalls den in der Spezifikation der Token-Statusliste festgelegten Überprüfungsanforderungen und der in EAA-6.2.10.1-01 festgelegten Spezifikation der Statusstruktur.

— EAA-6.2.10.1-05.1: Muss ein auf Brieftaschen vertrauender Beteiligter in der Lage sein, den Widerrufsstatus von Personenidentifizierungsdaten oder elektronischen Attributsbescheinigungen zu überprüfen, so unterstützt er sowohl den Bescheinigungsstatuslistenmechanismus als auch den Bescheinigungswiderrufslistenmechanismus gemäß EAA-6.2.10.1-02.

— EAA-6.2.10.1-06: identifier_list und status_list im MSO können das Zertifikatselement enthalten.

— EAA-6.2.10.1-06.1: Liegt das Zertifikatselement vor, so muss es ein Zertifikat mit dem öffentlichen Schlüssel enthalten, mit dem das Zertifikat der obersten Ebene im x5chain-Element in der Struktur der MSO-Widerrufsliste unterzeichnet oder besiegelt wurde.

— EAA-6.2.10.1-06.1.1: Die Instanz des auf Brieftaschen vertrauenden Beteiligten verwendet dieses Zertifikat als Vertrauensanker zur Überprüfung des x5chain-Elements in der Struktur der MSO-Widerrufsliste.

— EAA-6.2.10.1-06.2: Liegt das Zertifikatselement nicht vor, so muss das Zertifikat der obersten Ebene im x5chain-Element in der Struktur der MSO-Widerrufsliste von dem Zertifikat unterzeichnet oder besiegelt werden, das zur Unterzeichnung des Zertifikats im x5chain-Element des MSO verwendet wird.

— EAA-6.2.10.1-06.2.1: Die Instanz des auf Brieftaschen vertrauenden Beteiligten verwendet dieses Zertifikat als Vertrauensanker zur Überprüfung des x5chain-Elements in der Struktur der MSO-Widerrufsliste.

— EAA-6.2.10.1-07: Eine MSO-Widerrufsliste wird nach der Spezifikation der Token-Statusliste als Token-Statusliste im CWT-Format implementiert.

— EAA-6.2.10.1-08: Für die MSO-Widerrufsliste: Für den Kennungslisten- und Statuslistenmechanismus gelten die folgenden Anforderungen:

  — Die exp-Aussage muss vorliegen.

  — Die ttl-Aussage muss vorliegen.

  — Die aggregation_uri-Aussage in der IdentifierList- oder StatusList-Aussage kann vorliegen, und der Anbieter von Personenidentifizierungsdaten, der Anbieter qualifizierter elektronischer Attributsbescheinigungen oder der Anbieter elektronischer Attributsbescheinigungen, die von einer für eine authentische

Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, kann die aggregation_uri-Aussage verwenden, um anzugeben, dass der Aggregationsmechanismus gemäß der Spezifikation der Token-Statusliste unterstützt wird.

— CWT ist ein COSE_Sign1-Objekt, das einen der folgenden Signaturalgorithmen zur Berechnung der Signatur verwendet:

a) ‚ES256' (ECDSA mit Kurve NIST P-256 und SHA-256),

b) ‚ES384' (ECDSA mit Kurve NIST P-384 und SHA-384),

c) ‚ES512' (ECDSA mit Kurve NIST P-521 und SHA-512),

d) ‚ESB256' (ECDSA mit Kurve brainpoolP256r1 und SHA-256).

e) ‚ESB384' (ECDSA mit Kurve brainpoolP384r1 und SHA-384).

f) ‚ESB512' (ECDSA mit Kurve brainpoolP512r1 und SHA-512).

— CWT enthält x5chain in der geschützten Kopfzeile, die das Zertifikat oder die Zertifikatkette zur Überprüfung der Signatur der MSO-Widerrufsliste enthält.

— Die erweiterte Schlüsselnutzung der in der Spezifikation der Token-Statusliste angegebenen Objektkennung kann für das Statuslisten- und das Kennungslistensignierzertifikat verwendet werden, und die Instanzen der auf Brieftaschen vertrauenden Beteiligten können die erweiterte Schlüsselnutzung der in der Spezifikation der Token-Statusliste angegebenen Objektkennungen unterstützen; für die Objektkennung darf der Anbieter qualifizierter elektronischer Attributsbescheinigungen oder der Anbieter elektronischer Attributsbescheinigungen, die von einer öffentlichen Stelle oder in deren Namen ausgestellt werden, das Feld für die erweiterte Schlüsselnutzung bei der Verwendung der in der Spezifikation der Token-Statusliste angegebenen erweiterten Schlüsselnutzungs-OID nicht als kritisch festlegen.

— EAA-6.2.10.1-09: Abweichend von den Anforderungen der Spezifikation der Token-Statusliste gelten für den Kennungslistenmechanismus die folgenden Anforderungen:

— Der Wert der Typaussage lautet ‚application/identifierlist+cwt';

— die Statusliste-Aussage liegt in den CWT-Aussagen nicht vor;

— die in EAA-6.2.10.1-11 definierte IdentifierList-Struktur liegt als Aussage in den CWT-Aussagen unter Verwendung des Schlüssels 65530 vor.

— EAA-6.2.10.1-10: Die IdentifierList-Struktur ist eine CBOR-Struktur mit folgender 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: Liegt die Kennung in der IdentifierList vor, wird das MSO, das die Kennung im Statuselement enthält, widerrufen.

— EAA-6.2.10.1-10.2: Die aggregation_uri-Aussage ist in Abschnitt 9.2 der Spezifikation der Token-Statusliste angegeben.

— EAA-6.2.10.1-10.3: Der Inhaltstyp der Kennungsliste ist ‚application/identifierlist+cwt' gemäß den Anforderungen in Abschnitt 8.2 der Spezifikation der Token-Statusliste.

— EAA-6.2.10.1-11: Die folgenden Anforderungen gelten für das identifier_list-Element im MSO (siehe EAA-6.2.10.1-17).

— EAA-6.2.10.1-11.1: Das identifier_list-Element ist eine CBOR-Struktur mit folgender CDDL:

```
IdentifierListInfo = {

        'id': Identifier,

        'uri': URI,

        ? 'certificate': Certificate

        * tstr => RFU

}

URI = tstr

Certificate = bstr
```

— EAA-6.2.10.1-11.2: REV-11.2: Um zu verhindern, dass die Kennung zur Korrelation mehrerer Vorlagen verwendet wird, muss sie für jedes MSO eindeutig sein.

— EAA-6.2.10.1-12: Die folgenden Anforderungen gelten für die Statusliste:

  — EAA-6.2.10.1-12.1: Das Bits-Element in der StatusList-Struktur wird auf 1 gesetzt.

— EAA-6.2.10.1-13: Die folgenden Anforderungen gelten für das status_list-Element im MSO (siehe EAA-6.2.10.1-17):

  — EAA-6.2.10.1-13.1: Das status_list-Element muss den Anforderungen an die StatusListInfo-Struktur gemäß der Spezifikation der Token-Statusliste entsprechen, und das in EAA-6.2.10.1-06 definierte fakultative Zertifikatselement ist hinzuzufügen.

  — EAA-6.2.10.1-13.2: Um zu verhindern, dass der Statusindex zur Korrelation mehrerer Vorlagen verwendet wird, muss die Kombination aus Statusindex und URI für jedes MSO eindeutig sein.

— EAA-6.2.10.1-14: Der Brieftaschenanbieter verwendet die zweite (EAA-6.2.10.1-02.2) oder dritte (EAA-6.2.10.1-02.3) der in EAA-6.2.10.1-02 festgelegten Methoden für den Widerruf einer Brieftascheninstanzbescheinigung (WIA) und für den Widerruf einer Schlüsselbescheinigung (KA).

— EAA-6.2.10.1-15: Der Brieftaschenanbieter setzt die in EAA-6.2.10.1-02 festgelegten Bescheinigungswiderrufsmechanismen in seiner Brieftaschenlösung um.

— EAA-6.2.10.1-16: Der Anbieter von Personenidentifizierungsdaten und der Anbieter elektronischer Attributsbescheinigungen unterstützen sowohl den Bescheinigungsstatuslistenmechanismus als auch den Bescheinigungswiderrufslistenmechanismus gemäß EAA-6.2.10.1-02, um den Widerrufsstatus einer Brieftascheninstanzbescheinigung (WIA) und einer Schlüsselbescheinigung (KA) zu überprüfen.

— EAA-6.2.10.1-17: Die Statusstruktur im MSO ist eine CBOR-Struktur mit folgender CDDL:

Status = {

? 'identifier_list': IdentifierListInfo,

? 'status_list': StatusListInfo,

* tstr => RFU

}“

ANHANG V

„ANHANG III

Technische Spezifikationen gemäß Artikel 10

— Technische Spezifikationen:

  — Abschnitt 4.2.5 der Norm ETSI TS 119 472-3 V1.1.1 (2026-03).“

ANHANG VI

Anhang IV der Durchführungsverordnung (EU) 2024/2979 wird wie folgt geändert:

(1) Nummer 1 erhält folgende Fassung:

„1. Vorgeschriebenes Format für Signaturen und Siegel:

a) PAdES (PDF Advanced Electronic Signature) gemäß ETSI EN 319 142-1 V1.2.1 (2024-01) – Elektronische Signaturen und Infrastrukturen (ESI) – PAdES digitale Signaturen – Teil 1: Bausteine und PAdES-Basissignaturen."

(2) Nummer 3 erhält folgende Fassung:

„3. Anwendungsprogrammierschnittstelle:
ETSI TS 119 432 v1.3.1 (2026-03) Abschnitte 6.4.3, A.6, A.7 und A.8."

ANHANG VII

„ANHANG VI

Vertrauenssiegel der europäischen Brieftasche für die digitale Identität in Farbe



“

ANHANG VIII

„ANHANG VII

Vertrauenssiegel der europäischen Brieftasche für die digitale Identität in Schwarz-Weiß



“

ANHANG IX

„ANHANG VIII

Daten des Vertrauenssiegels der europäischen Brieftasche für die digitale Identität

Daten	Beschreibung	Kodierung	Status
TrustMarkResourceURL	URL des Vertrauenssiegels der europäischen Brieftasche für die digitale Identität und von Ressourcen zur Information der Nutzer in der Brieftaschennutzerschnittstelle.	URL	Obligatorisch
ListOfCertifiedWalletsURL	URL der öffentlichen Liste zertifizierter Brieftaschenlösungen in der EU gemäß der Durchführungsverordnung (EU) 2025/849 der Kommission ([1]).	URL	Obligatorisch
ListOfCertifiedWalletsQRCode	QR-Code mit den Informationen von ListOfCertifiedWalletsURL	ISO-8859-1 Byte mode QR code	Fakultativ
WalletSolutionInfoPageURL	URL der Informationsseite über die zertifizierte Brieftaschenlösung in der Liste der Seite der zertifizierten Brieftaschenlösungen von der ListOfCertifiedWalletsURL-URL, mit angehängtem ‚?' und der WalletSolutionID-Kennung der Brieftaschenlösung.	URL	Obligatorisch
WalletSolutionInfoPageQRCode	QR-Code mit den Informationen von WalletSolutionInfoPageURL	ISO-8859-1 Byte mode QR code	Fakultativ
WalletVerifierToolURL*	URL zum Endpunkt des Brieftaschenüberprüfungswerkzeugs */.well-known/openid-credential-issuer*, der für den Abruf der Metadaten des Bescheinigungsanbieters verwendet wird.	URL	Fakultativ

([1]) Durchführungsverordnung (EU) 2025/849 der Kommission vom 6. Mai 2025 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Übermittlung von Informationen an die Kommission und die Kooperationsgruppe für die Liste der zertifizierten europäischen Brieftaschen für die digitale Identität (ABl. L, 2025/849, 7.5.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/849/oj).“

ANHANG X

Anhang II der Durchführungsverordnung (EU) 2024/2980 wird wie folgt geändert:

(1) Anhang II Abschnitt 1 Nummer 1 Buchstabe i erhält folgende Fassung:

„i) ein oder mehrere Zertifikate, die mit der Norm ETSI EN 319 412-2 V2.4.1 (2025-06) oder der Norm ETSI EN 319 412-3 V1.3.1 (2023-09) im Einklang stehen und zur Überprüfung der Signaturen oder Siegel verwendet werden können, die von der Registrierstelle für die Registerdaten erstellt wurden und deren zertifizierte Identitätsdaten den Namen der Registrierstelle und gegebenenfalls die Registriernummer der Registrierstelle gemäß Buchstabe c bzw. Buchstabe d enthalten."

(2) Anhang II Abschnitt 2 Nummer 1 Buchstabe h erhält folgende Fassung:

„h) ein oder mehrere Zertifikate, die mit der Norm ETSI EN 319 412-2 V2.4.1 (2025-06) oder der Norm ETSI EN 319 412-3 V1.3.1 (2023-09) im Einklang stehen, zur Authentifizierung und Validierung der vom Brieftaschenanbieter ausgestellten Einzelbrieftaschenbescheinigungen verwendet werden können und deren zertifizierte Identitätsdaten den Namen und gegebenenfalls die Registriernummer des Brieftaschenanbieters gemäß Buchstabe a bzw. Buchstabe b enthalten;".

(3) Anhang II Abschnitt 3 Nummer 1 Buchstabe h erhält folgende Fassung:

„h) ein oder mehrere Zertifikate, die mit der Norm ETSI EN 319 412-2 V2.4.1 (2025-06) oder der Norm ETSI EN 319 412-3 V1.3.1 (2023-09) im Einklang stehen und zur Überprüfung der Signaturen oder Siegel verwendet werden können, die vom Anbieter von Personenidentifizierungsdaten für die von ihm bereitgestellten Personenidentifizierungsdaten erstellt wurden und deren zertifizierte Identitätsdaten den Namen und gegebenenfalls die Registriernummer des Anbieters von Personenidentifizierungsdaten gemäß Buchstabe a bzw. Buchstabe b enthalten."

(4) Anhang II Abschnitt 4 Nummer 1 Buchstabe g erhält folgende Fassung:

„g) ein oder mehrere Zertifikate, die mit der Norm ETSI EN 319 412-2 V2.4.1 (2025-06) oder der Norm ETSI EN 319 412-3 V1.3.1 (2023-09) im Einklang stehen und zur Überprüfung der Signaturen oder Siegel verwendet werden können, die vom Anbieter von Zugriffszertifikaten für auf Brieftaschen vertrauende Beteiligte für die von ihm für auf Brieftaschen vertrauende Beteiligte bereitgestellten Zugriffszertifikate erstellt wurden, gegebenenfalls mit den zur Unterscheidung zwischen Zugriffszertifikaten für auf Brieftaschen vertrauende Beteiligte und anderen Zertifikaten erforderlichen Informationen."

(5) Folgender Anhang II Abschnitt 5 wird angefügt:

„5. Notifizierungen von Informationen über Anbieter von Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte

1. Die Mitgliedstaaten übermitteln der Kommission die folgenden Informationen über Anbieter von Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte:

a) den Namen des Anbieters von Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte;

b) gegebenenfalls eine Registriernummer des Anbieters von Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte;

c) den Mitgliedstaat, in dem der Anbieter von Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte niedergelassen ist;

d) die E-Mail-Adresse und die Telefonnummer des Anbieters von Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte zur Kontaktaufnahme in Fragen im Zusammenhang mit den von ihm für auf Brieftaschen vertrauende Beteiligte bereitgestellten Registrierungszertifikaten;

e) gegebenenfalls die URL der Webseite mit zusätzlichen Informationen über den Anbieter von Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte und die von ihm für auf Brieftaschen vertrauende Beteiligte bereitgestellten Registrierungszertifikate;

f) die URL der Webseite mit den Regelungen und Nutzungsbedingungen, die für die Bereitstellung und Nutzung der von dem Anbieter für auf Brieftaschen vertrauende Beteiligte bereitgestellten Registrierungszertifikate gelten;

g) ein oder mehrere Zertifikate, die mit der Norm ETSI EN 319 412-2 V2.4.1 (2025-06) oder der Norm ETSI EN 319 412-3 V1.3.1 (2023-09) im Einklang stehen und zur Überprüfung der Signaturen oder Siegel verwendet werden können, die vom Anbieter von Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte für die von ihm für auf Brieftaschen vertrauende Beteiligte bereitgestellten Registrierungszertifikate erstellt wurden, gegebenenfalls mit den zur Unterscheidung zwischen Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte und anderen Zertifikaten erforderlichen Informationen.

2. Die in Nummer 1 genannten Informationen sind für jeden Anbieter von Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte einzeln anzugeben.“

ANHANG XI

„ANHANG I

Protokolle und Schnittstellen gemäß Artikel 4

Es gilt die technische Spezifikation ETSI TS 119 472-3 V1.1.1 (2026-03) mit den folgenden Anpassungen:

(1) 4.1 General requirements (Allgemeine Anforderungen)

— GEN-REQ-4.1-05: ungültig

— ANMERKUNG: ungültig

(2) 4.2.3 Provision of registration certificates of PID/EAA Provider to EUDI Wallet (Bereitstellung von Registrierungszertifikaten des PID/EAA-Anbieters für die EUDI-Brieftasche)

— ISS-MDATA-REG_CERT-4.2.3-04: Eines der Elemente des Array-Parameters issuer_info enthält das Registrierungszertifikat des PID/EAA-Anbieters.

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

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

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

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

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

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

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

(3) 4.2.4.2 ARF pre-defined PID/EAA reuse policy (vordefinierte PID/EAA-Weiterverwendungsregelung des ARF)

— ISS-MDATA-EAA-REUSE-POL-4.2.4.2-09: Hat das id-Glied den Wert ‚arf_annex_ii' und enthält das dem ‚details'-Label zugeordnete Array den Wert ‚once_only' oder den Wert ‚per-relying-party', so enthält das JSON-Objekt, das dieses dem ‚details'-Label zugeordnete Array enthält, auch eine JSON-Nummer, die dem ‚reissue_trigger_unused'-Label zugeordnet ist.

(4) Anhang A findet keine Anwendung."

ANHANG XII

„ANHANG II

Technische Spezifikationen gemäß Artikel 5

Es gilt die technische Spezifikation in Anhang C der Norm ISO/IEC 18013-7:2025.

Es gelten die technischen Spezifikationen in den Abschnitten 4.1, 4.2, 5 und 6 der Norm ETSI TS 119 472-2 V1.2.1 (2026-03) mit den folgenden Anpassungen, einschließlich der Einfügung eines neuen Abschnitts 4.3:

(1) 1 Scope (Anwendungsbereich)

— Mit dem vorliegenden Dokument werden zwei Profile von Protokollen festgelegt, die es einem vertrauenden Beteiligten (im Folgenden ‚RP') ermöglichen, EAAPs oder personenbezogene Personenidentifizierungsdaten (im Folgenden ‚PID') bei der EUDI-Brieftasche anzufordern, und die es der EUDI-Brieftasche ermöglichen, die angeforderten EAAPs/PIDs an den RP zu übermitteln. Jedes der Profile unterstützt die beiden folgenden Übertragungsmechanismen: API-vermittelt und nicht API-vermittelt, wie nachstehend dargestellt:

a) Ein Profil baut auf Folgendem auf:

— ISO/IEC 18013-5 [10] nur für nicht API-vermittelte Übertragungsmechanismen und

— Anhang C der Norm ISO/IEC 18013-7 [16] für API-vermittelte Übertragungsmechanismen.

Dieses Profil wird als ISO/IEC-mdoc-Profil bezeichnet und ist in Abschnitt 5 dieses Dokuments definiert.

b) Ein Profil baut auf Folgendem auf:

OpenID4VC-HAIP [11] sowohl für API-vermittelte als auch für nicht API-vermittelte Übertragungsmechanismen wie folgt:

— Abschnitte 5, 5.1, 5.3, 7 und 8 von [11] für die Übertragung über Redirects oder nicht API-vermittelte Übertragungsmechanismen und

— Abschnitte 5, 5.2, 5.3, 7 und 8 von [11] für API-vermittelte Übertragungsmechanismen.

Dieses Profil wird als OpenID4VC-HAIP-Profil bezeichnet und ist in Abschnitt 6 dieses Dokuments definiert.

(2) 2.1 Normative references (Normative Verweise)

— [15] ISO 639: ‚Language code'.

— [16] ISO/IEC 18013-7:2025 – Persönliche Identifizierung – ISO – konformer Führerschein – Teil 7: Zusatzfunktionen für den digitalen Führerschein (mDL).

(3) 4.1 EAAP implementation based on SD-JWT VC (Auf SD-JWT VC gestützte EAAP-Implementierung)

— EAAP-SD-JWT VC-04: ungültig.

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

— EAAP-ISO/IEC-mdoc-01: ungültig.

— *Note2*: ungültig.

— EAAP-ISO/IEC-mdoc-02: ungültig.

(5) 4.3 EAAP implementation with mediating API (EAAP-Implementierung mit vermittelnder API)

— EAAP-API-GEN-01: Die EUDI-Brieftasche unterstützt eine vermittelnde API, die beide in Abschnitt 5.2 von [11] und in Anhang C von [16] definierten Protokolle unterstützt.

— *ANMERKUNG:* Wenn das Gerät, auf dem die EUDI-Brieftasche installiert ist, nicht beide Protokolle unterstützt, kann diese Anforderung nicht erfüllt werden und führt zu einer Nichtkonformität aufgrund der zugrunde liegenden Betriebssysteme und Browser, in denen die erforderlichen Interoperabilitätsmerkmale nicht implementiert sind.

— EAAP-API-GEN-02: Die EUDI-Brieftasche unterstützt eine vermittelnde API zumindest für PIDs und EAA-Typen, die im Katalog der Regelungen gemäß der Durchführungsverordnung (EU) 2025/1569 registriert sind, und mindestens für alle in Anhang II der Durchführungsverordnung (EU) 2024/2979 festgelegten Formate.

— *ANMERKUNG 1:* Wenn zugrunde liegende Betriebssysteme, Browser, vermittelnde APIs oder andere technische Ebenen außerhalb der Kontrolle der EUDI-Brieftasche die Nachweisformate und die im Programmkatalog registrierten PID- und EAA-Typen einschränken, filtern, vorauswählen oder anderweitig beschränken, kann diese Anforderung nicht erfüllt werden. Wenn eine solche Beschränkung die EUDI-Brieftasche daran hindert, einen Typ oder ein Format eines registrierten Zertifikats zu unterstützen, ist die daraus resultierende Nichtkonformität darauf zurückzuführen, dass diese zugrunde liegenden Betriebssysteme, Browser, vermittelnden APIs oder anderen einschlägigen technischen Ebenen die erforderlichen Interoperabilitätsmerkmale nicht bereitstellen.

(6) 4.4 Wallet-relying party validation and overasking checks (Validierung von auf Brieftaschen vertrauenden Beteiligten und Überabfrage-Prüfungen)

— WRP-VALIDATION-01: Die EUDI-Brieftasche validiert das in der Abfrage erhaltene Registrierungszertifikat für auf Brieftaschen vertrauende Beteiligte, bevor sie dem Brieftaschennutzer eine angeforderte PID oder elektronische Attributsbescheinigung zur Genehmigung vorlegt.

— WRP-VALIDATION-02: Ist die Validierung des Registrierungszertifikats für auf Brieftaschen vertrauende Beteiligte nicht erfolgreich, auch wenn das Zertifikat abgelaufen ist, widerrufen wurde, nicht von einem bestehenden vertrauenswürdigen Anbieter von Registrierungszertifikaten für auf Brieftaschen vertrauende Beteiligte ausgestellt wurde, fehlerhaft ist oder nicht kryptografisch überprüft werden kann, so warnt die EUDI-Brieftasche den Brieftaschennutzer, dass der auf Brieftaschen vertrauende Beteiligte nicht validiert werden konnte, und stellt die Abfrage nicht als erfolgreich validiert dar. Der Brieftaschennutzer muss der Abfrage des vertrauenden Beteiligten dann ausdrücklich zustimmen. Keine Antwort oder vorangekreuzte Kästchen reichen für eine ausdrückliche Zustimmung nicht aus.

— WRP-VALIDATION-03: Der Brieftaschenanbieter legt auf der Grundlage seiner Risikoanalyse und seiner Sicherheitsregelung fest, ob und unter welchen Bedingungen bestimmte fehlgeschlagene Validierungsprüfungen vom Brieftaschennutzer übergangen werden können.

— WRP-OVERASKING-01: Die EUDI-Brieftasche gleicht die vom auf Brieftaschen vertrauenden Beteiligten angeforderten Bescheinigungen und Attribute mit den registrierten Bescheinigungen und Attributen im Registrierungszertifikat für auf Brieftaschen vertrauende Beteiligte ab.

— WRP-OVERASKING-02: Fragt der auf Brieftaschen vertrauende Beteiligte PIDs oder elektronische Attributsbescheinigungen oder Aussagen ab, die nicht vom Registrierungszertifikat für auf Brieftaschen vertrauende Beteiligte abgedeckt sind, warnt die EUDI-Brieftasche den Brieftaschennutzer deutlich, bevor eine Offenlegung erfolgt. Aus der Warnung muss hervorgehen, dass der auf Brieftaschen vertrauende Beteiligte mehr Informationen abfragt, als er registriert hat. Der Brieftaschennutzer muss der Abfrage des vertrauenden Beteiligten dann ausdrücklich zustimmen. Keine Antwort oder vorangekreuzte Kästchen reichen für eine ausdrückliche Zustimmung nicht aus.

— WRP-OVERASKING-03: Der Brieftaschenanbieter legt auf der Grundlage seiner Risikoanalyse, seiner Sicherheitsregelung und des geltenden Rechts fest, ob der Brieftaschennutzer trotz einer solchen Warnung fortfahren darf, ob nur der Teil der angeforderten Daten, die vom Registrierungszertifikat abgedeckt sind, offengelegt werden darf oder ob die Abfrage abgelehnt werden muss.

(7) 5.1 Introduction (Einleitung)

— In Abschnitt 5 und dessen Unterabschnitten wird ein Profil für ein Protokoll festgelegt, das es einem RP ermöglicht, EAAPs oder PIDs bei der EUDI-Brieftasche anzufordern, und das es der EUDI-Brieftasche ermöglicht, die angeforderten EAAPs/PIDs an den RP zu übermitteln, entweder mit einem nicht API-vermittelten Übermittlungsmechanismus, der auf der Norm ISO/IEC 18013-5 [10] beruht, oder mit einem API-vermittelten Übermittlungsmechanismus, der auf Anhang C der Norm ISO/IEC 18013-7 [16] beruht, um die in der Norm ISO/IEC 18013-5 [10] definierten Datenstrukturen entsprechend zu übertragen.

— Der Rest von Abschnitt 5 ist wie folgt aufgebaut:

  — In Abschnitt 5.2 werden Anforderungen an die Unterstützung des Profils und der Übertragungsmechanismen durch RPs und die EUDI-Brieftasche festgelegt;

  — Abschnitt 5.3 enthält Anforderungen, die speziell für den nicht API-vermittelten Übertragungsmechanismus gelten;

  — Abschnitt 5.4 und dessen Unterabschnitte enthalten Anforderungen, die speziell für den API-vermittelten Übertragungsmechanismus gelten.

(8) 5.2 Requirements on EUDI Wallet and RP support (Anforderungen an die EUDI-Brieftasche und die RP-Unterstützung)

— ISO/IEC 18013-SUPPORT-01: Einzelbrieftaschen, PID-Anbieter, Bescheinigungsanbieter, Brieftaschenanbieter und vertrauende Beteiligte unterstützen keinen Serverabruf gemäß der Norm ISO/IEC 18013-5 [10] für die Abfrage und Vorlage von PID oder Bescheinigungsattributen.

— ISO/IEC 18013-SUPPORT-02: Die EUDI-Brieftasche erfüllt die in den Abschnitten 5.3 und 5.4 dieses Dokuments festgelegten Anforderungen.

— ISO/IEC 18013-SUPPORT-04: Ein vertrauender Beteiligter sollte das in Abschnitt 5.4 dieses Dokuments definierte Profil umsetzen.

(9) 5.3.2 ISO/IEC-mdoc EAAP Request contents (Inhalte von EAAP-Antworten für ISO/IEC-mdoc)

— ISO/IEC 18013-5-REQ-04: An EUDI-Brieftaschen übermittelte Geräteabfragen enthalten das Schlüsselwertpaar ‚requestInfo' gemäß Abschnitt 8.3.2.1.2.1 von [10]. Der Wert dieses Paares entspricht dem RequestInfo-Typ.

— ISO/IEC 18013-5-REQ-05: Der RequestInfo-Typ entspricht der nachstehenden CDDL-Definition.

```
RequestInfo = {

    'euWrprc': bstr ; enthält ein Registrierungszertifikat (siehe nachstehende Anforderungen)

}
```

— ISO/IEC 18013-5-REQ-06: Das genannte requestInfo-Glied muss ein Glied mit dem Label ‚euWrprc' enthalten.

— ISO/IEC 18013-5-REQ-07: Der ‚euWrprc'-Wert ist ein CBOR-kodiertes Registrierungszertifikat.

— ISO/IEC 18013-5-REQ-08: ungültig.

— *ANMERKUNG 3:* ungültig.

— ISO/IEC 18013-5-REQ-09: ungültig.

— ISO/IEC 18013-5-REQ-10: ungültig.

— ISO/IEC 18013-5-REQ-11: ungültig.

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

— In diesem Abschnitt werden die Anforderungen an den DeviceResponse-Meldungstyp festgelegt, die beiden Arten von Übertragungsmechanismen (API-vermittelt und nicht API-vermittelt) gemeinsam sind.

— *ANMERKUNG 1:* Wird ein nicht API-vermittelter Mechanismus auf der Grundlage der Norm ISO/IEC 18013-5 [10] verwendet, ist eine EAAP-Antwort genau eine DeviceResponse-Instanz gemäß dem Profil im vorliegenden Abschnitt. Wird ein API-vermittelter Mechanismus auf der Grundlage des Anhangs C der Norm ISO/IEC 18013-7 [16] verwendet, so entspricht dies einer DeviceRequest-Instanz gemäß Anhang C von [16].

— ISO/IEC 18013-5-RESP-02: Der Anbieter von Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen darf keine Datenelemente in die KeyAuthorizations-Zuordnung im mobilen Sicherheitsobjekt der von ihm ausgestellten Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen aufnehmen, mit Ausnahme von Datenelementen, die vom auf Brieftaschen vertrauenden Beteiligten in den Transaktionsdaten in der von der Einzelbrieftasche mit dem privaten Schlüssel der Personenidentifizierungsdaten oder elektronischen Attributsbescheinigungen zu unterzeichnenden oder zu besiegelnden mdoc-Abfrage bereitgestellt werden.

— *ANMERKUNG 2:* Folglich können Einzelbrieftaschen den auf Brieftaschen vertrauenden Beteiligten keine vom Gerät signierten Datenelemente vorlegen, mit Ausnahme der Signierdaten, die der auf Brieftaschen vertrauende Beteiligte bereitgestellt hat, z. B. in Anwendungsfällen für eine sichere Nutzerauthentifizierung.

— *ANMERKUNG 3:* In der Norm ISO/IEC 18013-5:2021 ist nicht festgelegt, wie auf Brieftaschen vertrauende Beteiligte Transaktionsdaten in eine mdoc-Abfrage aufnehmen können. Die Aufnahme von Transaktionsdaten in eine mdoc-Abfrage erfolgt unter Hinzufügung technischer Spezifikationen.

— ISO/IEC 18013-5-RESP-03: Anbieter von Personenidentifizierungsdaten dürfen nicht zulassen, dass mit dem privaten Schlüssel der Personenidentifizierungsdaten Datenelemente unterzeichnet werden, die vom auf Brieftaschen vertrauenden Beteiligten in den Transaktionsdaten in der mdoc-Abfrage bereitgestellt werden.

(11) 5.4 Requirements for API mediated mechanism (Anforderungen für API-vermittelten Mechanismus)

5.4.1 ISO/IEC 18013-7-related requirements (Anforderungen in Bezug auf ISO/IEC 18013-7)

In diesem Abschnitt werden Anforderungen an API-vermittelte Übertragungsmechanismen im Zusammenhang mit den in Anhang C von [16] festgelegten Anforderungen festgelegt.

— ISO/IEC 18013-7-API-01: Das Profil, das API-vermittelte Vorlagen unterstützt, entspricht den Anforderungen in Anhang C der Norm ISO/IEC 18013-7 [16], wie in den Abschnitten 5.3 und 5.4 dieses Dokuments weiter ausgeführt.

— ISO/IEC 18013-7-API-02: Alle in Anhang C von [16] festgelegten obligatorischen Anforderungen gelten wie in den Abschnitten 5.3 und 5.4 dieses Dokuments weiter ausgeführt.

— ISO/IEC 18013-7-API-03: Alle in Anhang C von [16] festgelegten fakultativen Anforderungen bleiben fakultativ, sofern in diesem Dokument nicht anders angegeben.

(12) 5.4.2 Additional requirements (Zusätzliche Anforderungen)

— Im vorliegenden Abschnitt werden zusätzliche Anforderungen an API-vermittelte Übertragungsmechanismen festgelegt.

— ISO/IEC 18013-ADD-API-01: Die EUDI-Brieftasche legt standardmäßig das Vorhandensein aller gespeicherten Typen elektronischer Attributsbescheinigungen gegenüber der vermittelnden API offen, die gemäß Anhang C von [16] funktioniert, sie darf jedoch nicht die Attribute und deren Werte in diesen elektronischen Attributsbescheinigungen offenlegen.

— *ANMERKUNG 1:* Die Attributswertbeschränkung gilt auch dann, wenn eine solche Offenlegung die vom Betriebssystem für die EUDI-Brieftasche bereitgestellten Dienste verbessern würde, z. B. die Auswahl von Bescheinigungen im Zusammenhang mit der vermittelnden API.

— Es gibt Erwägungen im Zusammenhang mit Betriebssystemen und Browsern, die nicht der Kontrolle der Implementierer unterliegen und die gemäß den folgenden Anmerkungen 2 bis 4 berücksichtigt werden können:

— *ANMERKUNG 2:* Eine Vorlageabfrage eines den Anhang C von [16] unterstützenden vertrauenden Beteiligten kann vom Browser und/oder Betriebssystem verarbeitet werden, um verfügbare EAAs zu suchen, Betrug gegen den Nutzer zu verhindern oder Probleme zu beheben.

— *ANMERKUNG 3:* Es wird erwartet, dass eine Vorlageabfrage eines den Anhang C von [16] unterstützenden vertrauenden Beteiligten vom Browser und/oder Betriebssystem für die Zwecke der Sicherheit des Nutzers verarbeitet wird.

— *ANMERKUNG 4:* Es wird erwartet, dass eine Vorlageabfrage eines den Anhang C von [16] unterstützenden vertrauenden Beteiligten vom Browser und/oder Betriebssystem nicht für Marktanalysezwecke (auch nicht als Nebenzweck) oder für die internen Zwecke des Browsers und/oder des Betriebssystems verarbeitet wird.

— ISO/IEC 18013-ADD-API-02: Falls eine EUDI-Brieftasche auf Veranlassung des Nutzers PID oder eine EAA löscht, die zuvor gegenüber der vermittelnden API offengelegt wurde, die gemäß Anhang C von [16] funktioniert, so muss die EUDI-Brieftasche gegenüber der vermittelnden API offenlegen, dass diese PID oder EAA nicht mehr gespeichert ist/sind.

— ISO/IEC 18013-ADD-API-03: Wenn der Nutzer seine EUDI-Brieftasche deinstalliert, so legt die EUDI-Brieftasche gegenüber der vermittelnden API, die gemäß Anhang C der [16] funktioniert, offen, dass keine zuvor offengelegte(n) PID oder EAA mehr gespeichert ist/sind.

— ISO/IEC 18013-ADD-API-04: Die EUDI-Brieftasche bietet eine allgemeine Nutzereinstellung, um die Offenlegung gespeicherter EAAs über eine vermittelnde API, die gemäß ISO/IEC 18013-ADD-API-01 funktioniert, zu deaktivieren. Wenn diese Einstellung deaktiviert ist, darf die EUDI-Brieftasche keine API-vermittelte Vorlage- oder Ausstellungsabfragen anbieten oder beantworten.

— ISO/IEC 18013-ADD-API-05: EUDI-Brieftaschen überprüfen bei geräteübergreifenden Abläufen unter Verwendung der vermittelnden API, ob sich das interagierende Gerät in unmittelbarer räumlicher Nähe zur EUDI-Brieftasche befindet, und verwenden dazu einen sicheren, direkten und nutzervermittelten lokalen Kommunikationskanal, z. B. Drahtloskommunikationstechnik mit geringer Reichweite zur Prüfung der physischen räumlichen Nähe.

— *ANMERKUNG:* CTAP 2.3 ermöglicht die Verwendung von BLE für die Durchführung der Prüfung der räumlichen Nähe und, wenn sie von beiden Geräten implementiert wird, auch die Übertragung der Daten zwischen den Geräten über Übertragungstechnik mit geringer Reichweite. Sowohl die Prüfung der räumlichen Nähe als auch die Datenübertragung zwischen den beiden Geräten über einen lokalen Kommunikationskanal mithilfe von CTAP 2.3 sollten von den zugrunde liegenden Betriebssystemen, Browsern, vermittelnden APIs oder anderen technischen Ebenen außerhalb der Kontrolle der EUDI-Brieftasche gegenüber der Nutzung von CTAP-Hybridtunneldiensten bevorzugt werden.

(13) 6.2 Requirements on EUDI Wallet and RP support (Anforderungen an die EUDI-Brieftasche und die RP-Unterstützung)

— OIDFVP-HAIP-SUPPORT-02: Die EUDI-Brieftasche entspricht den in Abschnitt 6.5 dieses Anhangs festgelegten Anforderungen.

— OIDFVP-HAIP-SUPPORT-03: Die EUDI-Brieftasche sollte den in Abschnitt 6.4 genannten auf Redirects beruhenden Mechanismus für geräteübergreifende Vorlageflüsse nicht unterstützen.

— *ANMERKUNG 3:* Die Nutzung dieses Mechanismus ist anfällig für Angriffe wie Sitzungsfixierung. Die Eindämmung solcher Angriffe obliegt den vertrauenden Beteiligten. Die Umsetzung dieses Mechanismus sollte nicht zur Nichtkonformität führen.

— OIDFVP-HAIP-SUPPORT-05: Ein vertrauender Beteiligter muss die in Abschnitt 6.5 dieses Anhangs festgelegten Anforderungen erfüllen.

— *ANMERKUNG 5:* ungültig.

(14) 6.3.1 General requirements (Allgemeine Anforderungen)

— OIDFVP-HAIP-GEN-01: Es gelten alle obligatorischen Anforderungen der Abschnitte 5, 5.3, 7 und 8 von HAIP [11].

— *ANMERKUNG 1:* ‚HAIP [11] Abschnitt 5' bezieht sich ausschließlich auf die Anforderungen direkt unter der Überschrift von Abschnitt 5. Dies umfasst nicht die Abschnitte 5.1, 5.2 und 5.3.

— OIDFVP-HAIP-GEN-03: Wird durch diesen Anhang eine Anforderung in OpenID4VC-HAIP [11] geändert, so hat die geänderte Anforderung in diesem Anhang Vorrang.

— *ANMERKUNG 2:* Dies würde es beispielsweise ermöglichen, eine fakultative Anforderung aus OpenID4VC-HAIP [11] zu einer obligatorischen Anforderung zu machen oder obligatorische Anforderungen auszuweiten.

— OIDFVP-HAIP-GEN-04: Wenn das Format der angeforderten Bescheinigung mit [10] übereinstimmt, halten vertrauende Beteiligte und EUDI-Brieftaschen das ‚ISO mdocs'-Profil in Abschnitt 6 von [11] ein.

— *ANMERKUNG 3:* Der Klarheit halber: Das ‚ISO mdocs'-Profil in HAIP bedeutet, dass die vertrauenden Beteiligten und EUDI-Brieftaschen den geltenden Anforderungen in Anhang B.2 von [7] entsprechen müssen.

— OIDFVP-HAIP-GEN-05: Wenn das Format der angeforderten Bescheinigung mit [2] übereinstimmt, halten vertrauende Beteiligte und EUDI-Brieftaschen das ‚IETF SD-JWT VCs'-Profil in Abschnitt 6 von [11] ein.

— *ANMERKUNG 4:* Der Klarheit halber: Das ‚IETF SD-JWT VC'-Profil bedeutet, dass die vertrauenden Beteiligten und EUDI-Brieftaschen den Anforderungen in Anhang B.3 in [7] sowie den Anforderungen in Abschnitt 6.1 in [11] entsprechen müssen.

(15) 6.3.2.1 General requirements (Allgemeine Anforderungen)

— OIDFVP-HAIP-COMMON-REQ-01: ungültig.

(16) 6.3.2.2 Requirements for the Request Object (Anforderungen für das Abfrageobjekt)

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

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

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

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

— OIDFVP-HAIP-COMMON-REQ-RO-06: ungültig.

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

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

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

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

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

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

— *Anmerkung 2:* ungültig

— OIDFVP-HAIP-COMMON-REQ-RO-13: Eines der Elemente des verifier_info-Parameters enthält das Registrierungszertifikat.

— OIDFVP-HAIP-COMMON-REQ-RO-23: Das in Abschnitt 5.9.3 von OpenID4VP genannte Leaf-Zertifikat zur Verwendung mit dem x509_hash Client Identifier Prefix ist ein RP-Zugriffszertifikat gemäß ETSI TS 119 475 [14].

(17) 6.3.3 Authorization Response (EAAP response) profile (EAAP-Genehmigungsantwortprofil)

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

(18) 6.4.1 General requirements (Allgemeine Anforderungen)

— OIDFVP-HAIP-REDIRECTS-04: ungültig.

— *ANMERKUNG:* ungültig.

(19) 6.5.2 Additional requirements (Zusätzliche Anforderungen)

— OIDFVP-HAIP-ADD-API-01: Die EUDI-Brieftasche legt standardmäßig das Vorhandensein aller gespeicherten EAA-Typen gegenüber der vermittelnden API offen, die gemäß Abschnitt 5.2 von [11] funktioniert, sie darf jedoch nicht die Attribute und deren Werte in diesen EAAs offenlegen.

— OIDFVP-HAIP-ADD-API-04: Wenn die EUDI-Brieftasche eine vermittelnde API unterstützt, die gemäß OIDFVP-HAIP-ADD-API-01 funktioniert, so bietet sie eine allgemeine Nutzereinstellung, um die Offenlegung gespeicherter EAAs über die vermittelnde API zu deaktivieren. Wenn die Offenlegung deaktiviert ist, sollte die EUDI-Brieftasche es dem Nutzer anschließend ermöglichen, einzelne Bescheinigungen auszuwählen, die gegenüber der vermittelnden API offengelegt werden sollen.

— OIDFVP-HAIP-ADD-API-05: EUDI-Brieftaschen überprüfen bei geräteübergreifenden Abläufen unter Verwendung der vermittelnden API, ob sich das interagierende Gerät in unmittelbarer räumlicher Nähe zur EUDI-Brieftasche befindet, und verwenden dazu einen sicheren, direkten und nutzervermittelten lokalen Kommunikationskanal, z. B. eine Drahtloskommunikationstechnik mit geringer Reichweite zur Prüfung der physischen räumlichen Nähe.

— *ANMERKUNG 5:* CTAP 2.3 ermöglicht die Verwendung von BLE für die Durchführung der Prüfung der räumlichen Nähe und, wenn sie von beiden Geräten implementiert wird, auch die Übertragung der Daten zwischen den Geräten über Übertragungstechnik mit geringer Reichweite. Sowohl die Prüfung der räumlichen Nähe als auch die Datenübertragung zwischen den beiden Geräten über einen lokalen Kommunikationskanal mithilfe von CTAP 2.3 sollten von den zugrunde liegenden Betriebssystemen, Browsern, vermittelnden APIs oder anderen technischen Ebenen außerhalb der Kontrolle der EUDI-Brieftasche gegenüber der Nutzung von CTAP-Hybridtunneldiensten bevorzugt werden.

(20) 6.5.3 Specific requirements when requesting ISO/IEC 18013-5 EAAP (Besondere Anforderungen an EAAP-Abfragen nach ISO/IEC 18013-5)

— OIDFVP-HAIP-ISO/IEC_18013_5_REQ-02: Alle in diesem Dokument festgelegten Anforderungen für die in ISO/IEC 18013-5 festgelegten Strukturen für Geräteabfragen und -antworten gelten auch, wenn von der EUDI-Brieftasche über einen API-vermittelten Mechanismus gemäß Abschnitt C.1 von [16] eine ISO/IEC mdoc-Vorlageabfrage erhält.“