Amtsblatt
der Europäischen Union

DE
Reihe L

2024/2979

4.12.2024

# 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**

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) Der durch die Verordnung (EU) Nr. 910/2014 geschaffene europäische Rahmen für die digitale Identität ist eine unverzichtbare Komponente für die Schaffung eines sicheren und interoperablen Ökosystems für die digitale Identität in der gesamten Union. Da die europäischen Brieftaschen für die digitale Identität (im Folgenden „Brieftaschen“) den Eckpfeiler des Rahmens bilden, soll damit der Zugang zu Diensten für natürliche und juristische Personen in allen Mitgliedstaaten erleichtert und gleichzeitig der Schutz personenbezogener Daten und der Privatsphäre gewährleistet werden.

(2) Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([2]) und, sofern anwendbar, die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([3]) gelten für jede Verarbeitung personenbezogener Daten gemäß der vorliegenden Verordnung.

(3) Gemäß Artikel 5a Absatz 23 der Verordnung (EU) Nr. 910/2014 muss die Kommission erforderlichenfalls einschlägige Spezifikationen und Verfahren festlegen. Erreicht wird dies durch vier Durchführungsverordnungen, nämlich über Protokolle und Schnittstellen: Durchführungsverordnung (EU) 2024/2982 der Kommission ([4]), Integrität und Kernfunktionen: Durchführungsverordnung (EU) 2024/2979 der Kommission ([5]), Personenidentifizierungsdaten und elektronische Attributsbescheinigungen: Durchführungsverordnung (EU) 2024/2977 der Kommission ([6]) sowie Notifizierungen an die Kommission: Durchführungsverordnung (EU) 2024/2980 der Kommission ([7]). In der vorliegenden Verordnung werden die einschlägigen Anforderungen an die Integrität und die Kernfunktionen europäischer Brieftaschen für die digitale Identität festgelegt.

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

([2]) 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).

([3]) 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).

([4]) 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).

([5]) 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 ).

([6]) 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).

([7]) 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).

(4) Die Kommission bewertet regelmäßig neue Technologien, Praktiken, Normen oder technische Spezifikationen. Um ein Höchstmaß an Harmonisierung zwischen den Mitgliedstaaten bei der Entwicklung und Zertifizierung der Brieftaschen zu gewährleisten, beruhen die in dieser Durchführungsverordnung festgelegten technischen Spezifikationen auf den Arbeiten, die auf der Grundlage der 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 ([8]) durchgeführt wurden, insbesondere auf der Architektur und dem Referenzrahmen. Nach Erwägungsgrund 75 der Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates ([9]) sollte die Kommission diese Durchführungsverordnung gegebenenfalls überprüfen und aktualisieren, damit sie mit globalen Entwicklungen, der Architektur und dem Referenzrahmen Schritt hält und den bewährten Verfahren des Binnenmarkts folgt.

(5) Um eine präzise Kommunikation, technische Differenzierung und eine klare Zuweisung der Zuständigkeiten zu gewährleisten, muss zwischen verschiedenen Komponenten und Konfigurationen von Brieftaschen unterschieden werden. Unter einer Brieftaschenlösung sollte das vollständige System verstanden werden, das von einem Brieftaschenanbieter bereitgestellt wird und für den Betrieb einer Brieftasche erforderlich ist. Dies umfasst die Software- und Hardwarekomponenten sowie die Dienste, Einstellungen und Konfigurationen, die erforderlich sind, damit die Brieftasche ordnungsgemäß funktioniert. Eine Brieftaschenlösung kann auf den Geräten und in den Umgebungen der Nutzer und auf der Backend-Struktur des Anbieters laufen. Unter einer Einzelbrieftasche sollte eine besondere Einzelkonfiguration der Brieftaschenlösung für einen einzelnen Nutzer verstanden werden. Dies umfasst die auf dem Gerät oder in der Umgebung des Brieftaschennutzers installierte Anwendung, mit der der Brieftaschennutzer direkt interagiert (die „Brieftascheninstanz“), und die erforderlichen Sicherheitsmerkmale zum Schutz der Daten und Transaktionen des Nutzers. Diese Sicherheitsmerkmale sollten spezielle Software oder Hardware zur Verschlüsselung und zum Schutz sensibler Informationen einschließen. Eine Brieftascheninstanz sollte Teil der Einzelbrieftasche sein und es dem Brieftaschennutzer ermöglichen, auf die Funktionen seiner Brieftasche zuzugreifen.

(6) Sichere Kryptoanwendungen für Brieftaschen als separate Spezialkomponenten innerhalb einer Brieftasche werden nicht nur für den Schutz kritischer Werte bzw. Daten wie privater kryptografischer Schlüssel benötigt, sondern sind auch für die Bereitstellung wichtiger Funktionen wie das Vorweisen elektronischer Attributsbescheinigungen erforderlich. Die Verwendung gemeinsamer technischer Spezifikationen kann den Brieftaschenanbietern den Zugang zu eingebetteten sicheren Elementen erleichtern. Sichere Kryptoanwendungen für Brieftaschen können auf unterschiedliche Weise und für verschiedene Arten von sicheren Kryptomodulen für Brieftaschen bereitgestellt werden. Wenn angepasste sichere Kryptoanwendungen für Brieftaschen von Brieftaschenanbietern als Java-Card-Applets für eingebettete sichere Elemente bereitgestellt werden, sollten die Brieftaschenanbieter die in Anhang I aufgeführten Normen oder gleichwertige technische Spezifikationen befolgen.

(7) Einzelbrieftaschen müssen es den Anbietern von Personenidentifizierungsdaten oder elektronischen Attributsbescheinigungen ermöglichen, zu überprüfen, ob sie solche Daten oder Bescheinigungen an echte Einzelbrieftaschen des Brieftaschennutzers ausstellen.

(8) Um den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu gewährleisten, sollten die Brieftaschen mit modernsten bestehenden Techniken zum Schutz der Privatsphäre ausgestattet sein. Diese Merkmale sollten die Möglichkeit bieten, Brieftaschen zu verwenden, ohne dass der Brieftaschennutzer dabei über verschiedene auf Brieftaschen vertrauende Beteiligte hinweg nachverfolgt werden kann, soweit dies in dem Nutzungsszenario von Belang ist. So sollten Brieftaschenanbieter im Zusammenhang mit Einzelbrieftaschenbescheinigungen die Privatsphäre verbessernde Maßnahmen berücksichtigen, die dem neuesten Stand der Technik entsprechen, wie z. B. Verwendung kurzlebiger Brieftaschenbescheinigungen oder Batch-Ausstellung. Darüber hinaus sollten eingebettete Offenlegungsregelungen gewährleisten, dass die Brieftaschennutzer vor einer unangemessenen oder rechtswidrigen Offenlegung von Attributen aus elektronischen Attributsbescheinigungen gewarnt werden.

(9) Einzelbrieftaschenbescheinigungen sollten es den auf Brieftaschen vertrauenden Beteiligten, die Attribute von Einzelbrieftaschen abfragen, ermöglichen, den Gültigkeitsstatus der Einzelbrieftasche, mit der sie kommunizieren, zu überprüfen, da Einzelbrieftaschenbescheinigungen zu widerrufen sind, wenn die Einzelbrieftasche nicht mehr gültig ist. Die Angaben zum Gültigkeitsstatus der Einzelbrieftaschen sollten in interoperabler Weise zur Verfügung gestellt werden, damit sie von allen auf Brieftaschen vertrauenden Beteiligten verwendet werden können. Darüber hinaus sollten Brieftaschenanbieter den Brieftaschennutzern ermöglichen, den Widerruf ihrer Einzelbrieftasche zu veranlassen, falls diese ihre Einzelbrieftasche oder die Kontrolle darüber verloren haben. Um die Privatsphäre und die Unverknüpfbarkeit zu gewährleisten, sollten die Mitgliedstaaten auch für die Einzelbrieftaschenbescheinigung bestimmte Techniken zum Schutz der Privatsphäre einsetzen. Dies kann bedeuten, dass mehrere Einzelbrieftaschenbescheinigungen für unterschiedliche Zwecke verwendet werden, um nur die für eine Transaktion unbedingt erforderlichen relevanten Informationen über die Brieftasche offenzulegen, oder dass die Lebensdauer der Einzelbrieftaschenbescheinigung als Alternative zur Verwendung von Widerrufskennungen begrenzt wird.

([8]) ABl. L 210 vom 14.6.2021, S. 51. ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität (ABl. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(10) Brieftaschen sollten bestimmte vorgegebene Arten von Datenformaten und eine selektive Offenlegung unterstützen, damit alle Brieftaschen technisch in der Lage sind, Personenidentifizierungsdaten und elektronische Attributsbescheinigungen grenzüberschreitend zu empfangen und vorzuweisen, ohne die Interoperabilität zu beeinträchtigen. Nach Maßgabe der Verordnung (EU) Nr. 910/2014 ist die selektive Offenlegung ein Konzept, das den Eigentümer von Daten dazu ermächtigt, nur bestimmte Teile größerer Datensätze offenzulegen, damit der Empfänger nur diejenigen Informationen erhält, die für die Erbringung des von einem Nutzer angeforderten Dienstes notwendig sind. Da die Brieftaschen es dem Nutzer ermöglichen sollen, Attribute selektiv offenzulegen, sollten die in Anhang II aufgeführten Normen so umgesetzt werden, dass dieses Brieftaschenmerkmal ermöglicht wird. Zusätzlich können Brieftaschen noch andere Formate und Funktionen unterstützen, um bestimmte Anwendungsfälle zu erleichtern.

(11) Die Protokollierung von Transaktionen ist ein wichtiges Hilfsmittel zur Gewährleistung von Transparenz, weil so der Brieftaschennutzer einen Überblick über die Transaktionen erhält. Darüber hinaus sollten Protokolle verwendet werden, um bei einem verdächtigen Verhalten von auf Brieftaschen vertrauenden Beteiligten auf Veranlassung des Brieftaschennutzers eine rasche und einfache Weitergabe bestimmter Informationen an die gemäß Artikel 51 der Verordnung (EU) 2016/679 eingerichteten zuständigen Aufsichtsbehörden zu ermöglichen.

(12) Damit ein Brieftaschennutzer elektronisch unterzeichnen kann, sollte ihm ein qualifiziertes Zertifikat ausgestellt werden, das an eine qualifizierte elektronische Signaturerstellungseinheit gebunden ist. Der Brieftaschennutzer sollte Zugang zu einer Signaturerstellungsanwendung haben. Die Ausstellung qualifizierter Zertifikate ist zwar eine Dienstleistung qualifizierter Vertrauensdiensteanbieter, jedoch sollten Brieftaschenanbieter oder andere Einrichtungen in der Lage sein, die anderen Komponenten bereitzustellen. Beispielsweise können qualifizierte elektronische Signaturerstellungseinheiten von qualifizierten Vertrauensdiensteanbietern als Dienst verwaltet werden oder sie können lokal im Gerät des Brieftaschennutzers vorhanden sein, z. B. als Chipkarte. Ebenso können Signaturerstellungsanwendungen in die Brieftascheninstanz integriert sein, als separate App auf dem Gerät des Brieftaschennutzers installiert sein oder aus der Ferne bereitgestellt werden.

(13) Objekte für Datenexport und Datenübertragbarkeit können die an eine bestimmte Einzelbrieftasche ausgestellten Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen protokollieren. Mithilfe dieser Objekte können Brieftaschennutzer die relevanten Daten aus ihrer Einzelbrieftasche extrahieren, um ihr Recht auf Datenübertragbarkeit zu stärken. Brieftaschenanbieter werden dazu ermuntert, mit denselben technischen Lösungen auch Backup- und Wiederherstellungsverfahren für Einzelbrieftaschen einzurichten, damit gegebenenfalls verlorene Einzelbrieftaschen wiederhergestellt oder Informationen von einem Brieftaschenanbieter an einen anderen übermittelt werden können, sofern dies möglich ist, ohne das Recht auf Datenschutz und die Sicherheit des Ökosystems für die digitale Identität zu beeinträchtigen.

(14) Durch die Generierung spezifischer Pseudonyme für verschiedene auf Brieftaschen vertrauende Beteiligte sollte es den Brieftaschennutzern ermöglicht werden, sich selbst zu authentifizieren, ohne den auf Brieftaschen vertrauenden Beteiligten unnötige Informationen zu übermitteln. Nach Maßgabe der Verordnung (EU) Nr. 910/2014 dürfen Brieftaschennutzer nicht daran gehindert werden, beim Zugang zu Diensten ein Pseudonym zu verwenden, wenn die rechtliche Identität für die Authentifizierung nicht vorgeschrieben ist. Deshalb sollten die Brieftaschen eine Funktion zum Generieren von nutzergewählten und nutzerverwalteten Pseudonymen für die Authentifizierung beim Zugang zu Online-Diensten enthalten. Durch die Umsetzung der in Anhang V genannten Spezifikationen sollten diese Funktionsmerkmale entsprechend ermöglicht werden. Außerdem dürfen auf Brieftaschen vertrauende Beteiligte von den Nutzern nur die Daten verlangen, die im Register der vertrauenden Beteiligten für die beabsichtigte Verwendung der Brieftaschen verzeichnet sind. Die Brieftaschennutzer sollten die Registrierungsdaten vertrauender Beteiligter jederzeit überprüfen können.

(15) Die Verordnung (EU) 2024/1183 sieht vor, dass die Mitgliedstaaten den Zugang natürlicher oder juristischer Personen, die sich gegen die Verwendung der Brieftaschen entscheiden, zu öffentlichen oder privaten Diensten weder direkt noch indirekt beschränken dürfen und alternative Lösungen zur Verfügung stellen müssen.

(16) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([10]) angehört und gab am 30. September 2024 seine Stellungnahme ab.

([10]) 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).

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

HAT FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

**ALLGEMEINE BESTIMMUNGEN**

*Artikel 1*

**Gegenstand und Anwendungsbereich**

Mit dieser Verordnung werden Vorschriften für die Integrität und die Kernfunktionen der Brieftaschen festgelegt, die regelmäßig zu aktualisieren sind, damit sie mit den Entwicklungen von Technologie und Normen sowie mit den auf der Grundlage der Empfehlung (EU) 2021/946 der Kommission durchgeführten Arbeiten und insbesondere mit der Architektur und dem Referenzrahmen Schritt halten.

*Artikel 2*

**Begriffsbestimmungen**

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „sichere Kryptoanwendung für Brieftaschen“ (*Wallet Secure Cryptographic Application*) eine Anwendung, die kritische Werte verwaltet und dabei mit den kryptografischen und nicht-kryptografischen Funktionen eines sicheren Kryptomoduls für Brieftaschen verknüpft ist und diese nutzt;
2. „Einzelbrieftasche“ eine einzigartige Konfiguration einer Brieftaschenlösung, die Brieftascheninstanzen, sichere Kryptoanwendungen für Brieftaschen und sichere Kryptomodule für Brieftaschen umfasst, die einem einzelnen Brieftaschennutzer von einem Brieftaschenanbieter bereitgestellt werden;
3. „kritische Werte“ Werte bzw. Daten innerhalb oder im Zusammenhang mit einer Einzelbrieftasche, die so außerordentlich wichtig sind, dass die Beeinträchtigung ihrer Verfügbarkeit, Vertraulichkeit oder Integrität eine sehr schwerwiegende, beeinträchtigende Wirkung auf die verlässliche Verwendbarkeit der Einzelbrieftasche hätte;
4. „Anbieter von Personenidentifizierungsdaten“ eine natürliche oder juristische Person, die für die Ausstellung und den Widerruf der Personenidentifizierungsdaten verantwortlich ist und sicherstellt, dass die Personenidentifizierungsdaten eines Nutzers kryptografisch an eine Einzelbrieftasche gebunden sind;
5. „Brieftaschennutzer“ einen Nutzer, der die Kontrolle über die Einzelbrieftasche hat;
6. „auf Brieftaschen vertrauender Beteiligter“ einen vertrauenden Beteiligten, der beabsichtigt, zur Erbringung öffentlicher oder privater Dienste mittels digitaler Interaktion auf Einzelbrieftaschen zu vertrauen;
7. „Brieftaschenanbieter“ eine natürliche oder juristische Person, die Brieftaschenlösungen bereitstellt;
8. „Einzelbrieftaschenbescheinigung“ ein Datenobjekt, das die Komponenten der Einzelbrieftasche beschreibt oder die Authentifizierung und Validierung dieser Komponenten ermöglicht;
9. „einbettete Offenlegungsregelung“ eine Reihe von Vorschriften, die ein Anbieter in seine elektronische Attributsbescheinigung einbettet und die angibt, welche Bedingungen ein auf Brieftaschen vertrauender Beteiligter erfüllen muss, um auf die elektronische Attributsbescheinigung zugreifen zu können;
10. „Brieftascheninstanz“ die Anwendung, die als Bestandteil einer Einzelbrieftasche auf dem Gerät oder in der Umgebung eines Brieftaschennutzers installiert und konfiguriert ist und die der Brieftaschennutzer verwendet, um mit der Brieftasche zu interagieren;
11. „Brieftaschenlösung“ eine Kombination aus Software, Hardware, Diensten, Einstellungen und Konfigurationen, einschließlich Brieftascheninstanzen, einer oder mehreren sicheren Kryptoanwendungen für Brieftaschen und einem oder mehreren sicheren Kryptomodulen für Brieftaschen;
12. „sicheres Kryptomodul für Brieftaschen“ (*Wallet Secure Cryptographic Device*) eine manipulationssichere Vorrichtung, die eine Umgebung bietet, die mit der sicheren Kryptoanwendung für Brieftaschen verknüpft ist und von dieser genutzt wird, um kritische Werte zu schützen und kryptografische Funktionen für die sichere Ausführung kritischer Vorgänge bereitzustellen;

13. „Kryptovorgang in der Brieftasche“ (*Wallet Cryptographic Operation*) einen kryptografischen Mechanismus, der im Zusammenhang mit der Authentifizierung des Brieftaschennutzers und der Ausstellung oder Vorweisung von Personenidentifizierungsdaten oder elektronischen Attributsbescheinigungen erforderlich ist;

14. „Zugriffszertifikat für auf Brieftaschen vertrauende Beteiligte“ ein Zertifikat für elektronische Siegel oder Signaturen, mit dem auf Brieftaschen vertrauende Beteiligte authentifiziert und validiert werden und das von einem Anbieter von Zugriffszertifikaten für auf Brieftaschen vertrauende Beteiligte ausgestellt wird;

15. „Anbieter von Zugriffszertifikaten für auf Brieftaschen vertrauende Beteiligte“ eine natürliche oder juristische Person, die von einem Mitgliedstaat beauftragt wurde, Zugriffszertifikate für auf Brieftaschen vertrauende Beteiligte auszustellen, die in diesem Mitgliedstaat registriert sind.

KAPITEL II

## INTEGRITÄT EUROPÄISCHER BRIEFTASCHEN FÜR DIE DIGITALE IDENTITÄT

*Artikel 3*

### Integrität der Einzelbrieftasche

(1) Einzelbrieftaschen dürfen die in Artikel 5a Absatz 4 der Verordnung (EU) Nr. 910/2014 aufgeführten Funktionen — mit Ausnahme der Authentifizierung des Brieftaschennutzers für den Zugriff auf die Einzelbrieftasche — erst ausführen, nachdem die Einzelbrieftasche den Brieftaschennutzer erfolgreich authentifiziert hat.

(2) Brieftaschenanbieter müssen für jede Einzelbrieftasche mindestens eine den Anforderungen des Artikels 6 genügende Einzelbrieftaschenbescheinigung unterzeichnen oder besiegeln. Das zur Unterzeichnung oder Besiegelung der Einzelbrieftaschenbescheinigung verwendete Zertifikat muss anhand eines Zertifikats ausgestellt worden sein, das in der Vertrauensliste gemäß der Durchführungsverordnung (EU) 2024/2980 aufgeführt ist.

*Artikel 4*

### Brieftascheninstanzen

(1) Brieftascheninstanzen müssen für die Verwaltung kritischer Werte mindestens ein sicheres Kryptomodul für Brieftaschen verwenden.

(2) Die Brieftaschenanbieter gewährleisten die Integrität, Authentizität und Vertraulichkeit der Kommunikation zwischen Brieftascheninstanzen und sicheren Kryptoanwendungen für Brieftaschen.

(3) Wenn kritische Werte im Zusammenhang mit der elektronischen Identifizierung auf dem Sicherheitsniveau „hoch“ stehen, werden die Kryptovorgänge in der Brieftasche oder andere Vorgänge, bei denen kritische Werte verarbeitet werden, im Einklang mit den Anforderungen an die Merkmale und die Gestaltung elektronischer Identifizierungsmittel auf dem Sicherheitsniveau „hoch“ gemäß der Durchführungsverordnung (EU) 2015/1502 der Kommission ([11]) durchgeführt.

*Artikel 5*

### Sichere Kryptoanwendungen für Brieftaschen

(1) Brieftaschenanbieter stellen sicher, dass sichere Kryptoanwendungen für Brieftaschen

a) Kryptovorgänge in der Brieftasche, die kritische Werte betreffen, mit Ausnahme solcher, die zur Authentifizierung des Brieftaschennutzers durch die Einzelbrieftasche erforderlich sind, nur dann durchführen, wenn diese Anwendungen die Brieftaschennutzer zuvor erfolgreich authentifiziert haben;

([11]) Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (ABl. L 235 vom 9.9.2015, S. 7. ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

b) wenn sie Brieftaschennutzer im Zusammenhang mit der elektronischen Identifizierung auf dem Sicherheitsniveau „hoch“ authentifizieren, die Authentifizierung der Brieftaschennutzer gemäß den Anforderungen an die Merkmale und die Gestaltung elektronischer Identifizierungsmittel auf dem Sicherheitsniveau „hoch“ gemäß der Durchführungsverordnung (EU) 2015/1502 durchführen;

c) auf sichere Weise neue kryptografische Schlüssel erzeugen können;

d) kritische Werte sicher löschen können;

e) einen Nachweis über den Besitz privater Schlüssel erstellen können;

f) die von solchen sicheren Kryptoanwendungen für Brieftaschen erzeugten privaten Schlüssel während der Geltungsdauer der Schlüssel schützen;

g) den Anforderungen an die Merkmale und die Gestaltung elektronischer Identifizierungsmittel auf dem Sicherheitsniveau „hoch“ gemäß der Durchführungsverordnung (EU) 2015/1502 genügen;

h) die einzigen Komponenten sind, die Kryptovorgänge in der Brieftasche oder andere Vorgänge, bei denen kritische Werte verarbeitet werden, im Zusammenhang mit der elektronischen Identifizierung auf dem Sicherheitsniveau „hoch“ durchführen können.

(2) Wenn Brieftaschenanbieter beschließen, eine sichere Kryptoanwendung für Brieftaschen für ein eingebettetes sicheres Element bereitzustellen, stützen sie ihre technische Lösung auf die in Anhang I aufgeführten technischen Spezifikationen oder auf andere gleichwertige technische Spezifikationen.

*Artikel 6*

**Echtheit und Gültigkeit der Einzelbrieftasche**

(1) Die Brieftaschenanbieter stellen sicher, dass jede Einzelbrieftasche Einzelbrieftaschenbescheinigungen enthält.

(2) Die Brieftaschenanbieter stellen sicher, dass die in Absatz 1 genannten Einzelbrieftaschenbescheinigungen öffentliche Schlüssel enthalten und dass die zugehörigen privaten Schlüssel durch ein sicheres Kryptomodul für Brieftaschen geschützt werden.

(3) Die Brieftaschenanbieter

a) informieren die Brieftaschennutzer über ihre Rechte und Pflichten in Bezug auf ihre Einzelbrieftasche;

b) stellen von Einzelbrieftaschen unabhängige Mechanismen für die sichere Identifizierung und Authentifizierung der Brieftaschennutzer bereit;

c) stellen sicher, dass Brieftaschennutzer das Recht haben, mittels der in Buchstabe b genannten Authentifizierungsmechanismen den Widerruf ihrer Einzelbrieftaschenbescheinigungen zu veranlassen.

*Artikel 7*

**Widerruf von Einzelbrieftaschenbescheinigungen**

(1) Nur die Brieftaschenanbieter können die Einzelbrieftaschenbescheinigungen für von ihnen bereitgestellte Einzelbrieftaschen widerrufen.

(2) Die Brieftaschenanbieter stellen eine öffentlich zugängliche Regelung auf, in der sie die Bedingungen und Fristen für den Widerruf von Einzelbrieftaschenbescheinigungen festlegen.

(3) Wenn Brieftaschenanbieter Einzelbrieftaschenbescheinigungen widerrufen haben, informieren sie die betroffenen Brieftaschennutzer innerhalb von 24 Stunden über den Widerruf ihrer Einzelbrieftaschen und nennen dabei Gründe für den Widerruf und die Folgen für den Brieftaschennutzer. Diese Informationen müssen auf präzise und leicht zugängliche Weise und in klarer und einfacher Sprache bereitgestellt werden.

(4) Wenn Brieftaschenanbieter Einzelbrieftaschenbescheinigungen widerrufen haben, machen sie den Gültigkeitsstatus der Brieftaschenbescheinigungen unter Wahrung der Privatsphäre öffentlich bekannt und beschreiben in der Einzelbrieftaschenbescheinigung, wo diese Informationen abrufbar sind.

KAPITEL III

**KERNFUNKTIONEN UND KERNMERKMALE EUROPÄISCHER BRIEFTASCHEN FÜR DIE DIGITALE IDENTITÄT**

*Artikel 8*

**Formate für Personenidentifizierungsdaten und elektronische Attributsbescheinigungen**

Die Brieftaschenanbieter stellen sicher, dass Brieftaschenlösungen die Verwendung von Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen, die nach den im Normenverzeichnis in Anhang II aufgeführten Normen ausgestellt wurden, unterstützen.

*Artikel 9*

**Transaktionsprotokolle**

(1) Unabhängig davon, ob eine Transaktion erfolgreich abgeschlossen wird oder nicht, protokollieren Brieftascheninstanzen alle Transaktionen mit auf Brieftaschen vertrauenden Beteiligten und mit anderen Einzelbrieftaschen, einschließlich der elektronischen Unterzeichnung und Besiegelung.

(2) Die protokollierten Informationen müssen zumindest Folgendes enthalten:

a) das Datum und die Uhrzeit der Transaktion;

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, oder — im Falle anderer Einzelbrieftaschen — einschlägige Informationen aus der Einzelbrieftaschenbescheinigung;

c) die Art(en) der in der Transaktion angeforderten und vorgewiesenen Daten;

d) bei nicht abgeschlossenen Transaktionen den Grund für den Nichtabschluss.

(3) Die Brieftaschenanbieter gewährleisten die Integrität, Authentizität und Vertraulichkeit der protokollierten Informationen.

(4) Brieftascheninstanzen protokollieren die Berichte, die Brieftaschennutzer mit ihren Einzelbrieftaschen an die Datenschutzbehörden übermitteln.

(5) Die in den Absätzen 1 und 2 genannten Protokolle sind auf der Grundlage einer ausdrücklichen vorherigen Zustimmung des Brieftaschennutzers für den Brieftaschenanbieter zugänglich, soweit dies für die Erbringung von Brieftaschendiensten erforderlich ist.

(6) Die in den Absätzen 1 und 2 genannten Protokolle bleiben so lange zugänglich, wie sie nach Unionsrecht oder nationalem Recht erforderlich sind.

(7) Die Brieftaschenanbieter ermöglichen es den Brieftaschennutzern, die in Absatz 2 genannten protokollierten Informationen zu exportieren.

*Artikel 10*

**Eingebettete Offenlegung**

(1) Die Brieftaschenanbieter stellen sicher, dass die von ihnen bereitgestellten Einzelbrieftaschen elektronische Attributsbescheinigungen mit gemeinsamen eingebetteten Offenlegungsregelungen gemäß Anhang III verarbeiten können.

(2) Die Brieftascheninstanzen müssen die in Absatz 1 genannten eingebetteten Offenlegungsregelungen in Verbindung mit Daten, die vom abfragenden auf Brieftaschen vertrauenden Beteiligten empfangen werden, verarbeiten und vorweisen können.

(3) Die Brieftascheninstanzen müssen überprüfen, ob der auf Brieftaschen vertrauende Beteiligte den Anforderungen der eingebetteten Offenlegungsregelung genügt, und den Brieftaschennutzer über das Ergebnis informieren.

*Artikel 11*

**Qualifizierte elektronische Signaturen und Siegel**

(1) Die Brieftaschenanbieter stellen sicher, dass Brieftaschennutzer qualifizierte Zertifikate für qualifizierte elektronische Signaturen oder Siegel erhalten können, die mit qualifizierten Signatur- oder Siegelerstellungseinheiten verknüpft sind, die in Bezug auf die Brieftascheninstanzen entweder lokal, extern oder entfernt (remote) eingerichtet sind.

(2) Die Brieftaschenanbieter stellen sicher, dass Brieftaschenlösungen über eine sichere Schnittstelle mit einer der folgenden Arten qualifizierter Signatur- oder Siegelerstellungseinheiten verbunden werden können: lokal, extern oder entfernt (remote) verwaltete qualifizierte Signatur- oder Siegelerstellungseinheiten zwecks Verwendung der in Absatz 1 genannten qualifizierten Zertifikate.

(3) Die Brieftaschenanbieter stellen sicher, dass Brieftaschennutzer, die natürliche Personen sind, zumindest für nichtgewerbliche Zwecke kostenlos Zugang zu Signaturerstellungsanwendungen haben, die es ermöglichen, kostenlos qualifizierte elektronische Signaturen unter Verwendung der in Absatz 1 genannten Zertifikate zu erstellen.

*Artikel 12*

**Signaturerstellungsanwendungen**

(1) Die von Einzelbrieftaschen verwendeten Signaturerstellungsanwendungen können entweder von Brieftaschenanbietern, von Vertrauensdiensteanbietern oder von auf Brieftaschen vertrauenden Beteiligten bereitgestellt werden.

(2) Signaturerstellungsanwendungen haben folgende Funktionen:

a) Unterzeichnen und Besiegeln der von Brieftaschennutzern bereitgestellten Daten;

b) Unterzeichnen und Besiegeln der von auf Brieftaschen vertrauenden Beteiligten bereitgestellten Daten;

c) Erstellen von Signaturen oder Siegeln in mindestens den in Anhang IV genannten obligatorischen Formaten;

d) Information der Brieftaschennutzer über das Ergebnis des Signatur- oder Siegelerstellungsprozesses.

(3) Signaturerstellungsanwendungen können entweder in Brieftascheninstanzen integriert oder extern eingerichtet sein. Auf qualifizierten Fernsignaturerstellungseinheiten beruhende und in Brieftascheninstanzen integrierte Signaturerstellungsanwendungen müssen die in Anhang IV genannte Anwendungsprogrammierschnittstelle unterstützen.

*Artikel 13*

**Datenexport und Datenübertragbarkeit**

Sofern dies technisch machbar ist und keine kritischen Werte betrifft, müssen Einzelbrieftaschen — in einer Weise, die die Einhaltung des in der Durchführungsverordnung (EU) 2015/1502 festgelegten Sicherheitsniveaus „hoch“ gewährleistet — den sicheren Export und die Übertragbarkeit personenbezogener Daten des Brieftaschennutzers unterstützen, damit der Brieftaschennutzer zu einer Einzelbrieftasche einer anderen Brieftaschenlösung wechseln kann.

*Artikel 14*

**Pseudonyme**

(1) Einzelbrieftaschen unterstützen die Generierung von Pseudonymen für Brieftaschennutzer nach den technischen Spezifikationen in Anhang V.

(2) Einzelbrieftaschen unterstützen auf Veranlassung eines auf Brieftaschen vertrauenden Beteiligten die Generierung eines Pseudonyms, das für diesen Beteiligten spezifisch und eindeutig ist, und stellen diesem auf Brieftaschen vertrauenden Beteiligten dieses Pseudonym entweder selbstständig oder in Verbindung mit von ihm angeforderten Personenidentifizierungsdaten oder elektronischen Attributsbescheinigungen bereit.

KAPITEL IV

**SCHLUSSBESTIMMUNGEN**

*Artikel 15*

**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 28. November 2024

*Für die Kommission*
*Die Präsidentin*
Ursula VON DER LEYEN

*ANHANG I*

**VERZEICHNIS DER NORMEN GEMÄß ARTIKEL 5**

— SAM.01 Secured Applications for Mobile — Requirements for supporting 3rd party Applets on eSIM and eSE via SAM. v1.1 2023, GSMA;

— GPC_GUI_217 GlobalPlatform SAM Configuration Technical specification for implementation of SAM v1.0 2024-04;

— GPC_SPE_034 GlobalPlatform Card Specification Technical specification for smart cards v2.3.1 2018-03;

— GPC_SPE_007 GlobalPlatform Amendment A Confidential Card Content Management v1.2 2019-07;

— GPC_SPE_013 GlobalPlatform Amendment D Secure Channel Protocol 03 v1.2 2020-04;

— GPC_SPE_093 GlobalPlatform Amendment F Secure Channel Protocol 11 v1.4 2024-03;

— GPD_SPE_075 Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices. v3.3 2018-08, GlobalPlatform.

*ANHANG II*

**VERZEICHNIS DER NORMEN GEMÄß ARTIKEL 8**

— ISO/IEC 18013-5:2021;

— „Verifiable Credentials Data Model 1.1“ (Datenmodell für überprüfbare Nachweise), W3C-Empfehlung, 3. März 2022.

*ANHANG III*

**LISTE DER GEMEINSAMEN EINGEBETTETEN OFFENLEGUNGSREGELUNGEN GEMÄß ARTIKEL 10**

1. „Keine Regelung“ bedeutet, dass für die elektronischen Attributsbescheinigungen keine Regelungen gelten.
2. Regelung „Nur an autorisierte vertrauende Beteiligte“ bedeutet, dass Brieftaschennutzer elektronische Attributsbescheinigungen nur gegenüber authentifizierten vertrauenden Beteiligten offenlegen dürfen, die in den Offenlegungsregelungen ausdrücklich aufgeführt sind.
3. „Spezifische Vertrauenswurzel“ bedeutet, dass Brieftaschennutzer die betreffende elektronische Attributsbescheinigung nur an authentifizierte auf Brieftaschen vertrauende Parteien weitergeben sollten, die ihrerseits Zugriffszertifikate für auf Brieftaschen vertrauende Beteiligte besitzen, die von einer bestimmten Wurzel (oder einer Liste bestimmter Wurzeln) oder von einem oder mehreren bestimmten Zwischenzertifikaten abgeleitet sind.

*ANHANG IV*

**SIGNATUR- UND SIEGELFORMATE GEMÄß ARTIKEL 12**

1. Vorgeschriebenes Format für Signaturen und Siegel:

   a) PAdES (*PDF Advanced Electronic Signature* — fortgeschrittene elektronische Signatur für PDF) gemäß ETSI EN 319142-1 V1.1.1 (2016-04) — Elektronische Signaturen und Infrastrukturen (ESI) — PAdES digitale Signaturen — Teil 1: Bausteine und PAdES-Basissignaturen.

2. Liste der fakultativen Formate für Signaturen oder Siegel:

   a) XAdES gemäß ETSI EN 319132-1 V1.2.1 (2022-02) — Elektronische Signaturen und Infrastrukturen (ESI) — XAdES digitale Signaturen — Teil 1: Bausteine und XAdES-Basissignaturen (für die Unterzeichnung des XML-Formats);

   b) JAdES gemäß ETSI TS 119182-1 V1.2.1 (2024-07) Elektronische Signaturen und Infrastrukturen (ESI) — JAdES digitale Signaturen — Teil 1: Bausteine und JAdES-Basissignaturen (für die Unterzeichnung des JSON-Formats);

   c) CAdES (*CMS Advanced Electronic Signature* — fortgeschrittene elektronische Signatur für PDF) gemäß ETSI EN 319122-1 V1.3.1 (2023-06) Elektronische Signaturen und Infrastrukturen (ESI) — CAdES digitale Signaturen — Teil 1: Bausteine und CAdES-Basissignaturen (für die Unterzeichnung des CMS-Formats);

   d) ASiC (*Associated Signature Container* — Container für zugeordnete Signaturen) gemäß ETSI EN 319162-1 V1.1.1 (2016-04) — Elektronische Signaturen und Infrastrukturen (ESI) — Container für zugeordnete Signaturen — Teil 1: Bausteine und ASiC-Basiscontainer und ETSI EN 319162-2 V1.1.1 (2016-04) Elektronische Signaturen und Infrastrukturen (ESI) — Container für zugeordnete Signaturen — Teil 2: Zusätzliche ASiC-Basiscontainer (für die Unterzeichnung von Containern).

3. Anwendungsprogrammierschnittstelle:

   — Spezifikation des *Cloud Signature Consortium* (CSC) V2.0 (20. April 2023).

*ANHANG V*

**TECHNISCHE SPEZIFIKATIONEN FÜR DIE GENERIERUNG VON PSEUDONYMEN GEMÄß ARTIKEL 14**

Technische Spezifikationen:

— WebAuthn — W3C-Empfehlung, 8. April 2021, Level 2, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.