Amtsblatt
der Europäischen Union

DE
Reihe L

2024/2981

4.12.2024

DURCHFÜHRUNGSVERORDNUNG (EU) 2024/2981 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 Zertifizierung der europäischen 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 5c Absatz 6,

in Erwägung nachstehender Gründe:

(1) Gemäß Artikel 5c der Verordnung (EU) Nr. 910/2014 muss die Zertifizierung europäischer Brieftaschen für die digitale Identität (im Folgenden „Brieftaschen") im Einklang mit funktionalen Anforderungen, Cybersicherheitsanforderungen und Datenschutzanforderungen erfolgen, um ein hohes Maß an Sicherheit und Vertrauen in die Brieftaschen zu gewährleisten. Diese Zertifizierungsanforderungen müssen in allen Mitgliedstaaten harmonisiert werden, um eine Marktfragmentierung zu verhindern und einen soliden Rahmen zu schaffen.

(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 die Verarbeitung personenbezogener Daten gemäß der vorliegenden Verordnung.

(3) 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 Verordnung 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 ([4]) durchgeführt wurden, insbesondere auf der Architektur und dem Referenzrahmen, die Teil davon sind. Nach Erwägungsgrund 75 der Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates ([5]) 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.

(4) Um die Konformität mit den im Zertifizierungsrahmen enthaltenen Cybersicherheitsanforderungen zu bescheinigen, sollte sich die Zertifizierung von Brieftaschenlösungen, soweit verfügbar und relevant, auf die gemäß der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates ([6]) eingerichteten europäischen Systeme (Schemata) für die Cybersicherheitszertifizierung beziehen. In Ermangelung solcher Systeme oder wenn sie Cybersicherheitsanforderungen nur teilweise abdecken, werden in dieser Verordnung die allgemeinen Anforderungen festgelegt, die für nationale Zertifizierungssysteme gelten und funktionale Anforderungen, Cybersicherheitsanforderungen und Datenschutzanforderungen beinhalten.

([1]) ABl. L 257 vom 28.8.2014, S. 73, ELI: http://data.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]) ABl. L 210 vom 14.6.2021, S. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.
([5]) 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).
([6]) Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) Gemäß Artikel 5a Absatz 11 der Verordnung (EU) Nr. 910/2014 sind die Brieftaschen gemäß der Verordnung (EU) Nr. 910/2014 und der Durchführungsverordnung (EU) 2015/1502 der Kommission ([7]) auf dem Sicherheitsniveau „hoch" zu zertifizieren. Die Brieftaschenlösung insgesamt muss diesem Sicherheitsniveau entsprechen. Nach der vorliegenden Verordnung können einige Komponenten der Brieftaschenlösung mit einem niedrigeren Sicherheitsniveau zertifiziert werden, sofern dies hinreichend begründet ist, und unbeschadet dessen, dass mit der Gesamtlösung das Sicherheitsniveaus „hoch" erreicht werden muss.

(6) Alle nationalen Zertifizierungssysteme sollten einen Systeminhaber benennen, der für die Entwicklung und Pflege des Zertifizierungssystems verantwortlich ist. Der Systeminhaber kann eine Konformitätsbewertungsstelle, eine staatliche Stelle oder Behörde, ein Wirtschaftsverband, eine Gruppe von Konformitätsbewertungsstellen oder eine sonstige geeignete Stelle sein und kann eine andere Stelle als diejenige sein, die das nationale Zertifizierungssystem betreibt.

(7) Der Zertifizierungsgegenstand sollte die Softwarekomponenten der Brieftaschenlösung, wie z. B. die Brieftascheninstanz, umfassen. Die sichere Kryptoanwendung für Brieftaschen (*Wallet Secure Cryptographic Application*, „WSCA"), das sichere Kryptomodul für Brieftaschen (*Wallet Secure Cryptographic Device*, WSCD) und die Plattformen, auf denen diese Softwarekomponenten ausgeführt werden, sollten zwar Teil der Betriebsumgebung sein, aber nur dann in den Zertifizierungsgegenstand einbezogen werden, wenn sie von der Brieftaschenlösung bereitgestellt werden. In anderen Fällen, insbesondere wenn diese Module und Plattformen von Endnutzern bereitgestellt werden, sollten die Anbieter Annahmen über die Betriebsumgebung der Brieftaschenlösung, auch auf diesen Modulen und Plattformen, festlegen und Maßnahmen ergreifen, um zu bestätigen, dass diese Annahmen in der Praxis überprüft werden. Zum Schutz der kritischen Werte durch Hardware und Systemsoftware, die zur Verwaltung und zum Schutz kryptografischer Schlüssel, die vom WSCD erstellt, gespeichert oder verarbeitet werden, muss das WSCD hohen Zertifizierungsstandards genügen, die sich in internationalen Normen wie den in der Durchführungsverordnung (EU) 2024/482 der Kommission ([8]) festgelegten Gemeinsamen Kriterien (EUCC) widerspiegeln, und zwar durch einer EAL4-Evaluierung und eine fortgeschrittene methodische Schwachstellenanalyse, z. B. vergleichbar mit AVA_VAN.5. Diese Zertifizierungsstandards sollten spätestens dann angewandt werden, wenn die Zertifizierung der Konformität von Brieftaschen im Anschluss an ein gemäß der Verordnung (EU) 2019/881 angenommenes europäisches System (Schema) für die Cybersicherheitszertifizierung durchgeführt wird.

(8) Vollständig mobile, sichere und benutzerfreundliche Brieftaschen werden durch die Verfügbarkeit standardisierter und zertifizierter manipulationssicherer Lösungen wie etwa eingebetteter sicherer Elemente, externer Geräte (z. B. Chipkarten) oder eingebetteter SIM-Plattformen in Mobilgeräten unterstützt. Es ist wichtig, den zeitnahen Zugang zu eingebetteten sicheren Elementen für nationale eID-Mittel und Brieftaschen sicherzustellen und die Bemühungen der Mitgliedstaaten in diesem Bereich zu koordinieren. Die gemäß Artikel 46e Absatz 1 der Verordnung (EU) Nr. 910/2014 eingesetzte europäische Kooperationsgruppe für die digitale Identität (im Folgenden „Kooperationsgruppe") sollte daher zu diesem Zweck eine spezielle Untergruppe einrichten. Nach Konsultation der einschlägigen Interessenträger sollte sich diese Untergruppe auf einen gemeinsamen Fahrplan für den Zugang zu eingebetteten sicheren Elementen einigen, den die Kommission im Überprüfungsbericht zur Verordnung (EU) Nr. 910/2014 berücksichtigen sollte. Um die Einführung der Brieftasche auf nationaler Ebene zu erleichtern, sollte die Kommission darüber hinaus in Zusammenarbeit mit den Mitgliedstaaten ein Handbuch für Anwendungsfälle als Teil der Architektur und des Referenzrahmens ausarbeiten und kontinuierlich aktualisieren.

(9) Der Zertifizierungsgegenstand nationaler Zertifizierungssysteme sollte auch die Prozesse umfassen, die für die Bereitstellung und den Betrieb der Brieftaschenlösung verwendet werden, auch wenn Dritte mit der Festlegung oder Ausführung dieser Prozesse beauftragt werden. Um nachzuweisen, dass die Prozesse den Anforderungen der Systeme genügen, dürfen Sicherheitsangaben als Nachweis verwendet werden, sofern anhand einer Abhängigkeitsanalyse festgestellt wird, dass solche Sicherheitsangaben ausreichen. Die Sicherheitsangaben werden in vielen unterschiedlichen Formen vorgelegt, darunter als Berichte und Konformitätszertifikate, die privat, national, europäisch oder international sein können, sowie auf der Grundlage von Normen oder technischen Spezifikationen. Ziel der Abhängigkeitsanalyse ist es, die Qualität der verfügbaren Sicherheitsangaben über die Brieftaschenkomponenten zu bewerten.

([7]) 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).

([8]) Durchführungsverordnung (EU) 2024/482 der Kommission vom 31. Januar 2024 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC) (ABl. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) Nach den zu diesem Zweck festgelegten Verfahren sollte die Kooperationsgruppe in der Lage sein, Stellungnahmen und Empfehlungen zu den ihr vorgelegten Entwürfen für nationale Zertifizierungssysteme abzugeben. Solche nationalen Zertifizierungssysteme sollten spezifisch für die Brieftaschenarchitektur sein und für jede einzelne unterstützte Architektur bestimmte Profile vorsehen.

(11) Um ein gemeinsames Verständnis und einen harmonisierten Ansatz für die Bewertung der größten Risiken, die sich auf die Bereitstellung und den Betrieb von Brieftaschen auswirken könnten, zu gewährleisten, sollte ein Register der Risiken und Bedrohungen erstellt werden, das bei der Konzeption von Brieftaschenlösungen unabhängig von ihrer spezifischen Architektur berücksichtigt werden sollte. Bei der Ermittlung, welche Risiken in das Register aufgenommen werden sollten, sollten die in der Verordnung (EU) Nr. 910/2014 beschriebenen Cybersicherheitsziele wie Vertraulichkeit, Unversehrtheit und Verfügbarkeit der Brieftaschenlösung sowie die Privatsphäre der Nutzer und der Datenschutz berücksichtigt werden. Die gebührende Berücksichtigung der Risiken und Bedrohungen, die in diesem Risikoregister verzeichnet sind, sollte Teil der Anforderungen der nationalen Zertifizierungssysteme sein. Um mit der sich ständig weiterentwickelnden Bedrohungslandschaft Schritt zu halten, sollte das Risikoregister in Zusammenarbeit mit der Kooperationsgruppe geführt und regelmäßig aktualisiert werden.

(12) Bei der Einrichtung ihrer Zertifizierungssysteme sollten die Systeminhaber eine Risikobewertung durchführen, um die im Register aufgeführten Risiken und Bedrohungen durch Risiken und Bedrohungen zu präzisieren und zu ergänzen, die für die Architektur oder Umsetzung der Brieftaschenlösung spezifisch sind. Bei der Risikobewertung sollte geprüft werden, wie die bestehenden Risiken und Bedrohungen angemessen behandelt werden können. Brieftaschenanbieter sollten die Risikobewertung des Systems ergänzen, um Risiken und Bedrohungen zu bestimmen, die für ihre Brieftaschenumsetzung spezifisch sind, und geeignete Risikobehandlungsmaßnahmen zur Evaluierung durch die Zertifizierungsstelle vorschlagen.

(13) Zum Nachweis, dass eine Architektur der Brieftaschenlösung den geltenden Sicherheitsanforderungen entspricht, sollte jedes architekturspezifische System oder Profil zumindest eine Beschreibung der Architektur der Brieftaschenlösung, eine Liste der für die Architektur der Brieftaschenlösung geltenden Sicherheitsanforderungen, einen Evaluierungsplan zur Bestätigung, dass eine Brieftaschenlösung auf der Grundlage dieser Architektur diesen Anforderungen entspricht, und eine Risikobewertung enthalten. Die nationalen Zertifizierungssysteme sollten die Brieftaschenanbieter dazu verpflichten, die Übereinstimmung der Konzeption der von ihnen bereitgestellten Brieftaschenlösung mit der Referenzarchitektur nachzuweisen und die Sicherheitskontrollen und Validierungspläne für die jeweilige Brieftaschenlösung im Einzelnen darzulegen. In den nationalen Zertifizierungssystemen sollte auch eine Konformitätsbewertungstätigkeit festgelegt werden, um zu überprüfen, ob die Konzeption der Brieftasche die Referenzarchitektur des ausgewählten Profils angemessen widerspiegelt. Die nationalen Zertifizierungssysteme sollten die Anforderungen des Artikels 51 der Verordnung (EU) 2019/881, mit Ausnahme der Buchstaben e und f, in Bezug auf die Protokollierung erfüllen.

(14) In Bezug auf die Zertifizierung von Produkten sollten Konformitätszertifikate, die im Rahmen des EU-Systems für die Cybersicherheitszertifizierung EUCC ausgestellt wurden, und Konformitätszertifikate, die im Zuge nationaler Zertifizierungssysteme nach der in der Gruppe hoher Beamter für die Sicherheit der Informationssysteme (SOG-IS) getroffenen Vereinbarung über die gegenseitige Anerkennung ausgestellt wurden, verwendet werden dürfen. Darüber hinaus sollten andere nationale Zertifizierungssysteme für weniger sensible Produktkomponenten verwendet werden dürfen, wie z. B. diejenigen, die gemäß der CEN-Norm EN 17640 für die zeitlich festgelegte Cybersicherheitsevaluationsmethodologie eingerichtet wurden.

(15) Das Vertrauenssiegel der europäischen Brieftasche für die digitale Identität (im Folgenden „Vertrauenssiegel“) sollte verwendet werden, um klar, einfach und erkennbar anzugeben, dass eine Brieftasche gemäß der Verordnung (EU) Nr. 910/2014 bereitgestellt wird. Daher sollte es als Konformitätssiegel für eine im Rahmen nationaler Zertifizierungssysteme zertifizierte Brieftaschenlösung betrachtet werden. In den nationalen Zertifizierungssystemen sollten keine anderen Konformitätssiegel festgelegt werden.

(16) Um Betrug zu verhindern, sollten in den nationalen Zertifizierungssystemen Maßnahmen festgelegt werden, die zu ergreifen sind, wenn eine Zertifizierung im Rahmen des Systems in betrügerischer Absicht behauptet wird.

(17) Zur Gewährleistung eines effizienten Managements der Meldung von Schwachstellen sollten Anbieter von Brieftaschenlösungen und das elektronische Identifizierungssystem, in dessen Rahmen diese bereitgestellt werden, Prozesse zur Bewertung der Schwere und der möglichen Auswirkungen von Schwachstellen festlegen und umsetzen. In den nationalen Zertifizierungssystemen sollte ein Schwellenwert festgelegt werden, ab dem die Zertifizierungsstelle benachrichtigt werden muss. Diese Meldepflicht sollte die in den Datenschutzvorschriften und von den Datenschutzbehörden der Mitgliedstaaten festgelegten Kriterien für die Meldung von Verletzungen des Schutzes personenbezogener Daten unberührt lassen. Es könnten mögliche Synergien zwischen der obligatorischen Meldung einer Verletzung oder Beeinträchtigung der Brieftaschenlösungen und der Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 hergestellt werden. Die Bewertung eines Berichts über die Analyse der Auswirkungen der Schwachstelle durch die Zertifizierungsstelle sollte die Bewertung einer Datenschutz-Folgenabschätzung durch eine Datenschutzbehörde gemäß den Artikeln 35 und 36 der Verordnung (EU) 2016/679 unberührt lassen.

(18) Die Anbieter von Brieftaschenlösungen und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt werden, sollten den Systeminhaber über etwaige Gründe für Ausnahmen von der für die Evaluierung des WSCD und der WSCA gemäß Anhang IV erforderlichen Schwachstellenbewertung unterrichten.

(19) Die Aufhebung eines Konformitätszertifikats könnte schwerwiegende Folgen haben, wie z. B. den Widerruf aller eingesetzten Einzelbrieftaschen. Daher sollten Zertifizierungsstellen eine Aufhebung nur dann in Betracht ziehen, wenn eine nicht behobene Schwachstelle die Zuverlässigkeit der Brieftaschenlösung oder die Zuverlässigkeit einer anderen Brieftaschenlösung wahrscheinlich erheblich beeinträchtigt.

(20) Es sollte ein besonderer Prozess für die Aktualisierung der nationalen Zertifizierungssysteme eingeführt werden, um den Übergang zwischen aufeinanderfolgenden Versionen der Systeme zu steuern, insbesondere in Bezug auf Maßnahmen, die der Zertifikatsinhaber in Zukunft in Bezug auf Evaluierungen, Pflege, Neuzertifizierung und Sonderevaluierungen zu ergreifen hat.

(21) Zugunsten einer größeren Transparenz sollten Brieftaschenanbieter Sicherheitsinformationen über ihre Brieftaschenlösung öffentlich zur Verfügung stellen.

(22) Stützen sich nationale Zertifizierungssysteme auf Sicherheitsangaben aus anderen Zertifizierungssystemen oder Quellen, sollte eine Abhängigkeitsanalyse durchgeführt werden, um zu überprüfen, ob die Sicherheitsunterlagen, z. B. Instanzsicherheitsberichte und Konformitätszertifikate, verfügbar und für die Brieftaschenlösungen und das elektronische Identifizierungssystem, in dessen Rahmen diese bereitgestellt werden, angemessen sind. Diese Abhängigkeitsanalyse sollte auf der Risikobewertung der Brieftaschenlösungen und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt werden, beruhen. Bei der Bewertung sollte festgestellt werden, ob die Sicherheitsunterlagen zu einer bestimmten Brieftaschenlösung und dem elektronischen Identifizierungssystem, in dessen Rahmen diese bereitgestellt wird, geeignet sind, um eine der angestrebten Prüftiefe entsprechende Gewähr zu bieten. Im Rahmen der Evaluierung sollte auch die Abhängigkeitsanalyse aktualisiert oder erforderlichenfalls vollständig neu durchgeführt werden.

(23) Die Zertifizierungsstellen sollten Konformitätszertifikate im Rahmen nationaler Zertifizierungssysteme zusammen mit einem öffentlich zugänglichen Zertifizierungsbericht gemäß Artikel 5d Absatz 2 Buchstabe a der Verordnung (EU) Nr. 910/2014 ausstellen. Der zugehörige Bericht über die Bewertung der Zertifizierung sollte der Kooperationsgruppe zur Verfügung gestellt werden.

(24) Die nationalen Zertifizierungssysteme sollten eine jährliche Überwachungsevaluierung vorsehen, um sicherzustellen, dass die Prozesse im Zusammenhang mit der Verwaltung und Pflege der Brieftaschen wirksam, d. h. im Einklang mit den Konzepten zur Festlegung der Prozesse, funktionieren. Die zweijährliche Schwachstellenbeurteilung ist eine Anforderung aus der Verordnung (EU) Nr. 910/2014 und soll sicherstellen, dass die Brieftaschenlösung den im Risikoregister verzeichneten Cybersicherheitsrisiken und -bedrohungen, einschließlich etwaiger Entwicklungen der Bedrohungslage, weiterhin angemessen gerecht wird. Die Begriffe „Überwachungsevaluierungen“, „Evaluierungen der Neuzertifizierung“ und „Sonderevaluierungen“ sollten der Norm EN ISO/IEC 17021-1:2015 entsprechen.

(25) Ein Zertifizierungszyklus endet mit dem Ablauf des Konformitätszertifikats oder mit der Ausstellung eines neuen Konformitätszertifikats nach einer erfolgreichen Evaluierung der Neuzertifizierung. Die Evaluierung der Neuzertifizierung sollte eine Evaluierung aller Komponenten des Zertifizierungsgegenstands, einschließlich einer Evaluierung der Wirksamkeit und gegebenenfalls einer Schwachstellenbeurteilung, umfassen. Während der Neuzertifizierung sollte es möglich sein, die Ergebnisse früherer Evaluierungen von Komponenten, die sich nicht geändert haben, zu übernehmen.

(26) Nachdem ein europäisches System für die Cybersicherheitszertifizierung angenommen worden ist, sollten im Rahmen nationaler Zertifizierungssysteme mit demselben Anwendungsbereich nach einem festgelegten Übergangszeitraum gemäß Artikel 57 Absatz 1 der Verordnung (EU) 2019/881 keine Zertifikate mehr ausgestellt werden.

(27) Die nationalen Zertifizierungssysteme sollten sich auf bestehende Rahmen stützen und gegebenenfalls Nachweise weiterverwenden, um Harmonisierung und Interoperabilität zu gewährleisten. Die Mitgliedstaaten können Vereinbarungen über die grenzüberschreitende Weiterverwendung von Zertifizierungssystemen oder Teilen davon schließen. Die Europäische Kommission und die ENISA sollten die Mitgliedstaaten in Zusammenarbeit mit der Kooperationsgruppe bei der Entwicklung und Pflege ihrer nationalen Zertifizierungssysteme unterstützen, um so den Wissensaustausch und bewährte Verfahren sicherzustellen.

(28) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([9]) angehört und gab am 30. September 2024 seine Stellungnahme ab.

(29) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des in Artikel 48 Absatz 1 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 Referenzstandards sowie Spezifikationen und Verfahren festgelegt, um einen soliden Rahmen für die Zertifizierung von Brieftaschen aufzubauen, der regelmäßig aktualisiert wird, damit er mit den Entwicklungen von Technologie und Normen sowie mit den auf der Grundlage der Empfehlung (EU) 2021/946 für ein gemeinsames Instrumentarium der Union für ein koordiniertes Herangehen an einen Rahmen für die europäische digitale Identität durchgeführten Arbeiten und insbesondere mit der Architektur und dem Referenzrahmen Schritt hält.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck:

1. „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;
2. „Systeminhaber“ eine Organisation, die für die Entwicklung und Pflege eines Zertifizierungssystems verantwortlich ist;
3. „Zertifizierungsgegenstand“ Produkte, Prozesse und Dienste oder eine Kombination davon, für die bestimmte Anforderungen gelten;
4. „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;
5. „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;

([9]) 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).

6. „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;

7. „Risikoregister“ eine Aufzeichnung von Informationen über festgestellte Risiken, die für den Zertifizierungsprozess relevant sind;

8. „Brieftaschenanbieter“ eine natürliche oder juristische Person, die Brieftaschenlösungen bereitstellt;

9. „Zertifizierungsstelle“ eine als Dritte auftretende Konformitätsbewertungsstelle, die Zertifizierungssysteme betreibt;

10. „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;

11. „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;

12. „Brieftaschennutzer“ einen Nutzer, der die Kontrolle über die Einzelbrieftasche hat;

13. „Sicherheitsvorfall“ einen Sicherheitsvorfall im Sinne des Artikels 6 Nummer 6 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates ([10]);

14. „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.

KAPITEL II

NATIONALE ZERTIFIZIERUNGSSYSTEME

Artikel 3

Einrichtung nationaler Zertifizierungssysteme

(1) Die Mitgliedstaaten benennen für jedes nationale Zertifizierungssystem einen Systeminhaber.

(2) Gegenstand der in den nationalen Zertifizierungssystemen festgelegten Zertifizierung sind die Bereitstellung und der Betrieb von Brieftaschenlösungen und der elektronischen Identifizierungssysteme, in deren Rahmen diese bereitgestellt werden.

(3) Gemäß der Durchführungsverordnung (EU) 2015/1502 umfasst der Zertifizierungsgegenstand nationaler Zertifizierungssysteme folgende Elemente:

a) Softwarekomponenten, einschließlich Einstellungen und Konfigurationen von Brieftaschenlösungen und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt werden;

b) Hardwarekomponenten und -plattformen, auf denen die unter Nr. b) genannten Softwarekomponenten laufen oder auf die diese für kritische Vorgänge angewiesen sind, sofern sie direkt oder indirekt von der Brieftaschenlösung und dem elektronischen Identifizierungssystem, in dessen Rahmen diese bereitgestellt wird, zur Verfügung gestellt werden und sofern sie zur Einhaltung des gewünschten Sicherheitsniveaus für diese Softwarekomponenten erforderlich sind. Werden die Hardwarekomponenten und -plattformen nicht vom Brieftaschenanbieter zur Verfügung gestellt, so müssen die nationalen Zertifizierungssysteme Annahmen für die Evaluierung der Hardwarekomponenten und -plattformen formulieren, nach denen Angreifern mit hohem Angriffspotenzial im Einklang mit der Durchführungsverordnung (EU) 2015/1502 widerstanden werden kann, und die Evaluierungstätigkeiten zur Bestätigung dieser Annahmen gemäß Anhang IV angeben;

([10]) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) Prozesse, die die Bereitstellung und den Betrieb einer Brieftaschenlösung unterstützen, einschließlich des in Artikel 5a der Verordnung (EU) Nr. 910/2014 genannten Verfahrens für die Nutzereinbindung, die mindestens die Anmeldung, die Verwaltung elektronischer Identifizierungsmittel und die Organisation gemäß Anhang I Abschnitte 2.1, 2.2 und 2.4 der Durchführungsverordnung (EU) 2015/1502 umfassen.

(4) Die nationalen Zertifizierungssysteme enthalten eine Beschreibung der spezifischen Architektur der Brieftaschenlösungen und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt werden. Umfassen nationale Zertifizierungssysteme mehr als eine spezifische Architektur, müssen sie ein Profil für jede spezifische Architektur enthalten.

(5) Für jedes Profil müssen die nationalen Zertifizierungssysteme mindestens Folgendes festlegen:

a) die spezifische Architektur einer Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen die Lösung bereitgestellt wird;

b) die Sicherheitskontrollen im Zusammenhang mit den Sicherheitsniveaus gemäß Artikel 8 der Verordnung (EU) Nr. 910/2014;

c) einen Evaluierungsplan, der gemäß der Norm EN ISO/IEC 17065:2012 Abschnitt 7.4.1 erstellt wurde;

d) die erforderlichen Sicherheitsanforderungen, um die im Risikoregister gemäß Anhang I der vorliegenden Verordnung verzeichneten Cybersicherheitsrisiken und -bedrohungen bis zum erforderlichen Sicherheitsniveau zu bewältigen und gegebenenfalls die in Artikel 51 der Verordnung (EU) 2019/881 festgelegten Ziele einzuhalten;

e) Zuordnungen zu den Kontrollen gemäß Buchstabe b dieses Absatzes in Bezug auf die Komponenten der Architektur;

f) eine Beschreibung, wie die Sicherheitskontrollen, die Zuordnungen, die Sicherheitsanforderungen und der Evaluierungsplan gemäß den Buchstaben b bis c es den Anbietern von Brieftaschenlösungen und dem elektronischen Identifizierungssystem, in dessen Rahmen diese bereitgestellt werden, ermöglichen, die Cybersicherheitsrisiken und -bedrohungen, die in dem unter Buchstabe d genannten Risikoregister verzeichnet sind, bis zum erforderlichen Sicherheitsniveau auf der Grundlage einer Risikobewertung, anhand der im Risikoregister verzeichneten Risiken und Bedrohungen, die durch architekturspezifische Risiken und Bedrohungen präzisiert und ergänzt werden, angemessen zu behandeln.

(6) In dem in Absatz 5 Buchstabe c genannten Evaluierungsplan werden Evaluierungstätigkeiten aufgeführt, die bei der Evaluierung der Brieftaschenlösungen und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt werden, zu berücksichtigen sind.

(7) Im Rahmen der in Absatz 6 genannten Evaluierungstätigkeit müssen Anbieter von Brieftaschenlösungen und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt werden, Informationen gemäß den Anforderungen in Anhang II bereitstellen.

Artikel 4

Allgemeine Anforderungen

(1) Die nationalen Zertifizierungssysteme müssen funktionale Cybersicherheits- und Datenschutzanforderungen abdecken, indem — soweit verfügbar und anwendbar — die folgenden Zertifizierungssysteme verwendet werden:

a) europäische Systeme (Schemata) für die Cybersicherheitszertifizierung gemäß der Verordnung (EU) 2019/881, einschließlich des EUCC-Systems;

b) nationale Systeme für die Cybersicherheitszertifizierung, die gemäß Artikel 49 der Durchführungsverordnung (EU) 2024/482 unter das EUCC-System fallen.

(2) Soweit verfügbar und anwendbar, können sich nationale Zertifizierungssysteme zusätzlich auf Folgendes stützen:

a) andere einschlägige nationale Zertifizierungssysteme,

b) internationale, europäische und nationale Normen,

c) technische Spezifikationen, die die Anforderungen des Anhangs II der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates ([11]) erfüllen.

(3) Die nationalen Zertifizierungssysteme

a) führen die in Abschnitt 6.5 der Norm EN ISO/IEC 17067:2013 aufgeführten Elemente auf;

b) werden gemäß EN ISO/IEC 17067:2013 Abschnitt 5.3.8 als System des Typs 6 umgesetzt.

(4) Die nationalen Zertifizierungssysteme müssen den folgenden Anforderungen genügen:

a) Nur den Anbietern gemäß Artikel 5a Absatz 2 der Verordnung (EU) Nr. 910/2014 dürfen Zertifikate im Rahmen der nationalen Zertifizierungssysteme ausgestellt werden;

b) nur das Vertrauenssiegel wird als Konformitätssiegel verwendet;

c) Anbieter von Brieftaschenlösungen und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt werden, verweisen auf die Verordnung (EU) Nr. 910/2014 und die vorliegende Verordnung, wenn sie auf das System Bezug nehmen;

d) Anbieter von Brieftaschenlösungen und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt werden, ergänzen die Risikobewertung des Systems gemäß Artikel 3 Absatz 5 Buchstabe f, um spezifische Risiken und Bedrohungen für ihre Umsetzung zu ermitteln und geeignete Behandlungsmaßnahmen für alle relevanten Risiken und Bedrohungen vorzuschlagen;

e) die Zuständigkeiten und rechtlichen Schritte werden festgelegt und enthalten Verweise auf die geltenden nationalen Rechtsvorschriften, in denen die Zuständigkeiten und möglichen rechtlichen Schritte für den Fall festgelegt sind, dass die Zertifizierung im Rahmen des Systems in betrügerischer Absicht verwendet wird.

(5) Die Bewertung gemäß Absatz 4 Buchstabe d wird der Zertifizierungsstelle zur Evaluierung übermittelt.

Artikel 5

Sicherheitsvorfall- und Schwachstellenmanagement

(1) Nationale Zertifizierungssysteme enthalten Anforderungen an das Sicherheitsvorfall- und Schwachstellenmanagement gemäß den Absätzen 2 bis 9.

(2) Der Inhaber eines Konformitätszertifikats einer Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt wird, meldet seiner Zertifizierungsstelle unverzüglich jeden Verstoß oder jede Beeinträchtigung in Bezug auf eine Brieftaschenlösung oder das elektronische Identifizierungssystem, in dessen Rahmen diese bereitgestellt wird, die sich auf deren/dessen Konformität mit den Anforderungen der nationalen Zertifizierungssysteme auswirken könnten.

(3) Der Inhaber eines Konformitätszertifikats muss ein Konzept und Verfahren für das Schwachstellenmanagement festlegen, aufrechterhalten und anwenden und dabei die Verfahren berücksichtigen, die in bestehenden europäischen und internationalen Normen, einschließlich der Norm EN ISO/IEC 30111:2019, festgelegt sind.

(4) Der Inhaber des Konformitätszertifikats meldet der ausstellenden Zertifizierungsstelle die Schwachstellen und Änderungen, die sich auf die Brieftaschenlösung auswirken, auf der Grundlage der für die Auswirkungen dieser Schwachstellen und Veränderungen festgelegten Kriterien.

(5) Der Inhaber des Konformitätszertifikats erstellt einen Bericht über die Analyse der Auswirkungen von Schwachstellen, die sich auf die Softwarekomponenten der Brieftaschenlösung auswirken. Der Bericht umfasst folgende Informationen:

a) die Auswirkungen der Schwachstelle auf die zertifizierte Brieftaschenlösung;

b) mögliche Risiken im Zusammenhang mit der Nähe oder Wahrscheinlichkeit einer Angriffsmöglichkeit;

([11]) Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) ob die Schwachstelle mit den verfügbaren Mitteln behoben werden kann;

d) falls die Schwachstelle mit den verfügbaren Mitteln behoben werden kann, Möglichkeiten zur Behebung der Schwachstelle.

(6) Ist eine Meldung nach Absatz 4 erforderlich, übermittelt der Inhaber des Konformitätszertifikats der Zertifizierungsstelle unverzüglich den Bericht über die Analyse der Auswirkungen der Schwachstelle gemäß Absatz 5.

(7) Der Inhaber eines Konformitätszertifikats muss ein Konzept für das Schwachstellenmanagement festlegen, aufrechterhalten und anwenden, das die Anforderungen des Anhangs I der Cyberresilienz-Verordnung ([12]) erfüllt.

(8) In den nationalen Zertifizierungssystemen werden Anforderungen an die Offenlegung von Schwachstellen festgelegt, die für Zertifizierungsstellen gelten.

(9) Der Inhaber eines Konformitätszertifikats legt alle öffentlich bekannten und behobenen Schwachstellen in der Brieftaschenlösung offen oder trägt sie in eines der in Anhang V genannten Online-Register ein.

Artikel 6

Pflege nationaler Zertifizierungssysteme

(1) Die nationalen Zertifizierungssysteme müssen einen Prozess zur regelmäßigen Überprüfung ihrer Funktionsweise vorsehen. Ziel dieses Prozesses ist es, ihre Angemessenheit zu bestätigen und unter Berücksichtigung der Rückmeldungen der Interessenträger verbesserungsbedürftige Aspekte zu ermitteln.

(2) Die nationalen Zertifizierungssysteme müssen Bestimmungen über ihre Pflege enthalten. Dieser Prozess umfasst zumindest folgende Anforderungen:

a) Vorschriften für die Leitung der Festlegung und der Anforderungen der nationalen Zertifizierungssysteme;

b) Festlegung von Fristen für die Ausstellung von Zertifikaten nach der Annahme aktualisierter Versionen der nationalen Zertifizierungssysteme, sowohl für neue als auch für zuvor ausgestellte Konformitätszertifikate;

c) eine regelmäßige Überprüfung der nationalen Zertifizierungssysteme, damit die entsprechenden Anforderungen einheitlich angewandt werden, wobei mindestens folgende Aspekte zu berücksichtigen sind:

— an den Systeminhaber gerichtete Klarstellungsersuchen in Bezug auf die Anforderungen des nationalen Zertifizierungssystems;

— Rückmeldungen von Beteiligten und anderen interessierten Kreisen;

— Reaktionsfähigkeit des Inhabers des nationalen Zertifizierungssystems auf Anfragen;

d) Vorschriften für die Überwachung von Referenzdokumenten und Verfahren für die Weiterentwicklung der Referenzversionen der nationalen Zertifizierungssysteme, zumindest mit Übergangszeiträumen;

e) ein Prozess, mit dem sichergestellt wird, dass die jeweils jüngsten Cybersicherheitsrisiken und -bedrohungen, die im Risikoregister gemäß Anhang I dieser Verordnung verzeichnet sind, abgedeckt werden;

f) ein Prozess zur Verwaltung anderer Änderungen der nationalen Zertifizierungssysteme.

([12]) Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) (ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(3) Die nationalen Zertifizierungssysteme enthalten Anforderungen an die Durchführung von Evaluierungen derzeit zertifizierter Produkte innerhalb eines bestimmten Zeitraums nach der Überarbeitung des Systems oder nach der Veröffentlichung neuer Spezifikationen oder Normen oder neuer Fassungen davon, denen die Brieftaschenlösungen und das elektronische Identifizierungssystem, in dessen Rahmen diese bereitgestellt werden, entsprechen müssen.

KAPITEL III

ANFORDERUNGEN AN SYSTEMINHABER

Artikel 7

Allgemeine Anforderungen

(1) Die Systeminhaber entwickeln und pflegen nationale Zertifizierungssysteme und regeln ihren Betrieb.

(2) Die Systeminhaber können ihre Aufgaben ganz oder teilweise an Dritte übertragen. Bei der Vergabe von Unteraufträgen an einen privaten Auftragnehmer legen die Systeminhaber die Pflichten und Verantwortlichkeiten aller Beteiligten vertraglich fest. Die Systeminhaber bleiben für alle an Unterauftragnehmer übertragenen Tätigkeiten verantwortlich.

(3) Die Systeminhaber nehmen ihre Überwachungstätigkeiten gegebenenfalls zumindest auf der Grundlage der folgenden Informationen wahr:

a) Informationen von Zertifizierungsstellen, nationalen Akkreditierungsstellen und zuständigen Marktüberwachungsbehörden;

b) Informationen aus eigenen Prüfungen und Untersuchungen und denen anderer Behörden;

c) Beschwerden und Einsprüche gemäß Artikel 15.

(4) Die Systeminhaber unterrichten die Kooperationsgruppe über Änderungen der nationalen Zertifizierungssysteme. Diese Meldungen enthalten angemessene Informationen, damit die Kooperationsgruppe Empfehlungen an die Systeminhaber und Stellungnahmen zu den aktualisierten nationalen Zertifizierungssystemen abgeben kann.

KAPITEL IV

ANFORDERUNGEN AN ANBIETER VON BRIEFTASCHENLÖSUNGEN UND DAS ELEKTRONISCHE IDENTIFIZIERUNGSSYSTEM, IN DESSEN RAHMEN DIESE BEREITGESTELLT WERDEN

Artikel 8

Allgemeine Anforderungen

(1) Die nationalen Zertifizierungssysteme enthalten Cybersicherheitsanforderungen auf der Grundlage einer Risikobewertung jeder spezifischen unterstützten Architektur. Diese Cybersicherheitsanforderungen zielen darauf ab, die ermittelten Cybersicherheitsrisiken und -bedrohungen, die in dem in Anhang I genannten Risikoregister verzeichnet sind, zu behandeln.

(2) Im Einklang mit Artikel 5a Absatz 23 der Verordnung (EU) Nr. 910/2014 müssen die nationalen Zertifizierungssysteme dafür sorgen, dass Brieftaschenlösungen und die elektronischen Identifizierungssysteme, in deren Rahmen diese bereitgestellt werden, auf dem Sicherheitsniveau „hoch“ widerstandsfähig gegen Angreifer mit hohem Angriffspotenzial gemäß der Durchführungsverordnung (EU) 2015/1502 sind.

(3) In den nationalen Zertifizierungssystemen müssen Sicherheitskriterien festgelegt werden, die folgende Anforderungen umfassen:

a) soweit zutreffend die Anforderungen der Cyberresilienz-Verordnung oder andere Anforderungen, die der Erreichung der in Artikel 51 der Verordnung (EU) 2019/881 festgelegten Sicherheitsziele dienen;

b) Festlegung und Umsetzung von Konzepten und Verfahren für das Risikomanagement im Zusammenhang mit dem Betrieb einer Brieftaschenlösung, einschließlich der Ermittlung und Bewertung von Risiken und der Minderung der ermittelten Risiken;

c) Festlegung und Umsetzung von Konzepten und Verfahren für das Änderungsmanagement und das Schwachstellenmanagement gemäß Artikel 5 der vorliegenden Verordnung;

d) Festlegung und Umsetzung von Konzepten und Verfahren für das Personalmanagement, einschließlich Anforderungen an Fachwissen, Zuverlässigkeit, Erfahrung, Sicherheitsschulung und Qualifikationen des an der Entwicklung oder dem Betrieb der Brieftaschenlösung beteiligten Personals;

e) Anforderungen an die Betriebsumgebung der Brieftaschenlösung, auch in Form von Annahmen über die Sicherheit der Geräte/Module und Plattformen, auf denen die Softwarekomponenten der Brieftaschenlösung betrieben werden, einschließlich WSCDs, und gegebenenfalls Konformitätsbewertungsanforderungen, um zu bestätigen, dass diese Annahmen in Bezug auf die betreffenden Geräte und Plattformen überprüft werden;

f) für jede Annahme, die auf kein Konformitätszertifikat oder andere annehmbare Sicherheitsangaben gestützt wird, eine Beschreibung des Mechanismus, mit dem der Brieftaschenanbieter das Zutreffen der Annahme nachweisen kann, sowie eine Begründung, dass der Mechanismus ausreicht, um sicherzustellen, dass das Zutreffen der Annahme überprüft wird;

g) Festlegung und Durchführung von Maßnahmen zur Gewährleistung der Verwendung einer derzeit zertifizierten Version der Brieftaschenlösung.

(4) Die nationalen Zertifizierungssysteme enthalten für die in Anhang III aufgeführten Vorgänge funktionale Anforderungen in Bezug auf Aktualisierungsmechanismen für jede Softwarekomponente der Brieftaschenlösungen und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt werden.

(5) Die nationalen Zertifizierungssysteme verlangen, dass der Antragsteller der Zertifizierungsstelle folgende Informationen und Unterlagen übermittelt oder auf andere Weise zur Verfügung stellt:

a) Nachweise für die in Anhang IV Nummer 1 genannten Informationen, gegebenenfalls mit Einzelheiten über die Brieftaschenlösung und ihren Quellcode, einschließlich

— *Informationen über die Architektur*: für jede Komponente der Brieftaschenlösung (einschließlich Produkt-, Prozess- und Dienstkomponenten) eine Beschreibung ihrer wesentlichen Sicherheitseigenschaften und ihrer externen Abhängigkeiten;

— *Kontrollen und Sicherheitsniveaus*: für jede Sicherheitskontrolle der Brieftaschenlösung eine Beschreibung der Kontrolle und des erforderlichen Sicherheitsniveaus auf der Grundlage des Anhangs der Durchführungsverordnung (EU) 2015/1502, in dem eine Reihe technischer Spezifikationen und Verfahren festgelegt sind, die für die verschiedenen mit den elektronischen Identifizierungsmitteln durchgeführten Kontrollen gelten;

— *Zuordnung der Kontrollen zu Architekturkomponenten*: eine Beschreibung, wie die Kontrollen der Brieftaschenlösung unter Verwendung der verschiedenen Komponenten der Brieftaschenlösung durchgeführt werden, basierend auf einer Erklärung für die Notwendigkeit eines bestimmten Sicherheitsniveaus, und wie die Kontrollen mit allen erforderlichen Sicherheitsaspekten auf dem angemessenen Niveau durchgeführt werden;

— *Erklärung und Begründung der Risikoabdeckung*: eine Begründung für

  — die Zuordnung der Kontrollen zu Komponenten,

  — die Eignung des vorgeschlagenen Evaluierungsplans, um alle Kontrollen angemessen abzudecken,

  — die Abdeckung der im Risikoregister verzeichneten Cybersicherheitsrisiken und -bedrohungen durch die Kontrollen, ergänzt durch Kontrollen von für die Umsetzung spezifischen Risiken und Bedrohungen, auf dem angemessenen Sicherheitsniveau;

b) die in Anhang V aufgeführten Informationen;

c) eine vollständige Liste der Konformitätszertifikate und sonstigen Sicherheitsangaben, die bei den Evaluierungstätigkeiten als Nachweis verwendet wurden;

d) sonstige Informationen, die für die Evaluierungstätigkeiten relevant sind.

KAPITEL V

ANFORDERUNGEN AN ZERTIFZIERUNGSSTELLEN

Artikel 9

Allgemeine Anforderungen

(1) Die Zertifizierungsstellen werden von nationalen Akkreditierungsstellen, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates ([13]) benannt wurden, gemäß der Norm EN ISO/IEC 17065:2012 akkreditiert, sofern sie die Anforderungen der nationalen Zertifizierungssysteme gemäß Absatz 2 erfüllen.

(2) Für die Zwecke der Akkreditierung müssen die Zertifizierungsstellen alle folgenden Kompetenzanforderungen erfüllen:

a) detaillierte und technische Kenntnisse der einschlägigen Architekturen einer Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt wird, sowie der Bedrohungen und Risiken, die für diese Architekturen relevant sind;

b) Kenntnis der verfügbaren Sicherheitslösungen und ihrer Eigenschaften gemäß dem Anhang der Durchführungsverordnung (EU) 2015/1502;

c) Kenntnis der Tätigkeiten, die aufgrund von Konformitätszertifikaten in Bezug auf Komponenten der Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt wird, als Zertifizierungsgegenstand durchgeführt werden;

d) detaillierte Kenntnis des anwendbaren nationalen Zertifizierungssystems gemäß Kapitel II.

(3) Die Zertifizierungsstellen führen ihre Überwachungstätigkeiten insbesondere auf der Grundlage der folgenden Informationen durch:

a) Informationen von nationalen Akkreditierungsstellen und zuständigen Marktüberwachungsbehörden;

b) Informationen aus ihren eigenen Prüfungen und Untersuchungen und denen anderer Behörden;

c) Beschwerden und Einsprüche gemäß Artikel 15.

Artikel 10

Vergabe von Unteraufträgen

Die Zertifizierungsstellen können gemäß Artikel 13 Dritte mit den Evaluierungstätigkeiten beauftragen. Werden Unterauftragnehmer mit den Evaluierungstätigkeiten beauftragt, so müssen die nationalen Zertifizierungssysteme Folgendes festlegen:

1. Alle Unterauftragnehmer der Zertifizierungsstelle, die Evaluierungstätigkeiten durchführen, müssen, soweit zutreffend und für die durchzuführenden Tätigkeiten angemessen, die Anforderungen harmonisierter Normen wie EN ISO/IEC 17025:2017 für Prüfungen, EN ISO/IEC 17020:2012 für Inspektionen, EN ISO/IEC 17021-1:2015 für Audits und EN ISO/IEC 17029:2019 für die Validierung und Verifizierung erfüllen;

2. die Zertifizierungsstellen übernehmen die Verantwortung für alle Evaluierungstätigkeiten, die an andere Stellen ausgelagert werden, und weisen nach, dass sie während ihrer Akkreditierung geeignete Maßnahmen ergriffen haben, gegebenenfalls auch durch Rückgriff auf eine eigene Akkreditierung ihrer Unterauftragnehmer;

3. das Ausmaß, in dem vorab bei den Systeminhabern oder dem Kunden, dessen Brieftaschenlösung im Rahmen des Zertifizierungssystems zertifiziert wird, die Zustimmung einer erforderlichen Auslagerung eingeholt werden muss.

([13]) Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Artikel 11

Meldung bei der Aufsichtsstelle

Die Zertifizierungsstellen melden der in Artikel 46a Absatz 1 der Verordnung (EU) Nr. 910/2014 genannten Aufsichtsstelle die Ausstellung, Aussetzung und Aufhebung von Konformitätszertifikaten der Brieftaschenlösungen und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt werden.

Artikel 12

Sicherheitsvorfall- und Schwachstellenmanagement

(1) Die Zertifizierungsstellen setzen die Konformitätszertifikate für die Brieftaschenlösungen und das elektronische Identifizierungssystem, in dessen Rahmen diese bereitgestellt werden, unverzüglich aus, nachdem sie bestätigt haben, dass sich die gemeldete Sicherheitsverletzung oder -beeinträchtigung auf die Konformität mit den Anforderungen der nationalen Zertifizierungssysteme, der Brieftaschenlösung oder des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt wird, auswirkt.

(2) Die Zertifizierungsstellen heben das Konformitätszertifikat, das infolge einer nicht rechtzeitig behobenen Sicherheitsverletzung oder -beeinträchtigung ausgesetzt wurde, auf.

(3) Die Zertifizierungsstellen heben Konformitätszertifikate gemäß Artikel 5c Absatz 4 und Artikel 5e Absatz 2 der Verordnung (EU) Nr. 910/2014 auf, wenn eine festgestellte Schwachstelle nicht in angemessenem Verhältnis zu ihrer Schwere und ihren potenziellen Auswirkungen behoben wurde.

KAPITEL VI

KONFORMITÄTSBEWERTUNGSTÄTIGKEITEN

Artikel 13

Evaluierungstätigkeiten

(1) Nationale Zertifizierungssysteme müssen Methoden und Verfahren enthalten, die von den Konformitätsbewertungsstellen bei der Durchführung ihrer Evaluierungstätigkeiten gemäß der Norm EN ISO/IEC 17065:2012 anzuwenden sind und mindestens folgende Aspekte abdecken:

a) die Methoden und Verfahren für die Durchführung von Evaluierungstätigkeiten, einschließlich solcher im Zusammenhang mit dem WSCD, gemäß Anhang IV;

b) die Prüfung der Umsetzung der Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt wird, auf der Grundlage des Risikoregisters gemäß Anhang I und erforderlichenfalls ergänzt durch die Betrachtung umsetzungsspezifischer Risiken;

c) Funktionstests, die, soweit verfügbar und angemessen, auf Testreihen beruhen, die gemäß technischen Spezifikationen oder Normen definiert sind;

d) Bewertung des Vorhandenseins und der Eignung von Pflegeprozessen, zumindest mit Versions-, Aktualisierungs- und Schwachstellenmanagement;

e) Bewertung der operativen Wirksamkeit von Pflegeprozessen, zumindest mit Versions-, Aktualisierungs- und Schwachstellenmanagement;

f) vom Brieftaschenanbieter vorgelegte Abhängigkeitsanalyse, einschließlich einer Methodik zur Bewertung der Zulässigkeit der Sicherheitsangaben, die die in Anhang VI aufgeführten Elemente umfasst;

g) Schwachstellenbeurteilung auf dem angemessenen Niveau, einschließlich

— Überprüfung der Konzeption der Brieftaschenlösung und gegebenenfalls ihres Quellcodes,

— Prüfung der Widerstandsfähigkeit der Brieftaschenlösung gegenüber Angreifern mit hohem Angriffspotenzial für das Sicherheitsniveau „hoch“ gemäß Abschnitt 2.2.1 des Anhangs der Durchführungsverordnung (EU) 2015/1502;

h) Bewertung der Entwicklung des Bedrohungsumfelds und der Auswirkungen auf die Abdeckung der Risiken durch die Brieftaschenlösung, um festzustellen, welche Evaluierungstätigkeiten für die verschiedenen Komponenten der Brieftaschenlösung erforderlich sind.

(2) Die nationalen Zertifizierungssysteme umfassen eine Evaluierung zur Feststellung, ob die Umsetzung von Brieftaschenlösungen und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt werden, der Architektur gemäß Artikel 3 Absatz 5 Buchstabe a entspricht, sowie eine Evaluierung zur Feststellung, ob der zusammen mit der Umsetzung vorgeschlagene Evaluierungsplan dem in Artikel 3 Absatz 5 Buchstabe c genannten Evaluierungsplan entspricht.

(3) Die nationalen Zertifizierungssysteme enthalten Probenahmevorschriften, um die Wiederholung identischer Evaluierungstätigkeiten zu vermeiden und sich auf Tätigkeiten zu konzentrieren, die für eine bestimmte Variante spezifisch sind. Diese Probenahmevorschriften ermöglichen die Durchführung von Funktions- und Sicherheitsprüfungen an nur einer Stichprobe von Varianten einer Zielkomponente einer Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt wird, sowie an einer Stichprobe von Zielmodulen. Die nationalen Zertifizierungssysteme verlangen von allen Zertifizierungsstellen, dass sie ihre Stichprobenverwendung begründen.

(4) Die nationalen Zertifizierungssysteme verlangen von der Zertifizierungsstelle, dass sie die WSCA auf der Grundlage der in Anhang IV aufgeführten Methoden und Verfahren evaluiert.

Artikel 14

Zertifizierungstätigkeiten

(1) Die nationalen Zertifizierungssysteme legen eine Bescheinigungstätigkeit für die Ausstellung eines Konformitätszertifikats gemäß Abschnitt V Buchstabe a Tabelle 1 der Norm EN ISO/IEC 17067:2013 fest, die folgende Aspekte umfasst:

a) den Inhalt des Konformitätszertifikats gemäß Anhang VII;

b) wie die Ergebnisse der Evaluierung im öffentlichen Zertifizierungsbericht anzugeben sind, zumindest mit einer Zusammenfassung des vorläufigen Prüfungs- und Validierungsplans gemäß Anhang VIII;

c) den Inhalt der im Zertifizierungsbericht angegebenen Evaluierungsergebnisse, einschließlich der in Anhang VIII aufgeführten Elemente.

(2) Der Bericht über die Bewertung der Zertifizierung kann der Kooperationsgruppe und der Kommission zur Verfügung gestellt werden.

Artikel 15

Beschwerden und Einsprüche

Die nationalen Zertifizierungssysteme enthalten Verfahren oder Verweise auf die geltenden nationalen Rechtsvorschriften, in denen der Mechanismus für die wirksame Einreichung und Bearbeitung von Beschwerden und Einsprüchen im Zusammenhang mit der Umsetzung des Zertifizierungssystems oder einem ausgestellten Konformitätszertifikat festgelegt ist. Diese Verfahren umfassen Information des Beschwerdeführers über den Stand des Verfahrens und die getroffene Entscheidung sowie die Belehrung des Beschwerdeführers über die Möglichkeit eines wirksamen gerichtlichen Rechtsbehelfs. Die nationalen Zertifizierungssysteme sehen vor, dass alle Beschwerden und Einsprüche, die von der Zertifizierungsstelle nicht beigelegt werden oder nicht beigelegt werden können, dem Systeminhaber zur Bewertung und Beilegung übermittelt werden.

Artikel 16

Überwachungstätigkeiten

(1) Die nationalen Zertifizierungssysteme verpflichten die Zertifizierungsstellen zur Durchführung von Überwachungstätigkeiten, die in der Überwachungsevaluierung von Prozessen in Verbindung mit stichprobenartigen Tests oder Kontrollen bestehen.

(2) Die nationalen Zertifizierungssysteme enthalten Anforderungen an die Systeminhaber in Bezug auf die Überwachung der Einhaltung der Verpflichtungen gemäß der Verordnung (EU) Nr. 910/2014 und gegebenenfalls gemäß den nationalen Zertifizierungssystemen durch die Zertifizierungsstellen.

(3) Die nationalen Zertifizierungssysteme enthalten Anforderungen an die Zertifizierungsstellen, Folgendes zu überwachen:

a) dass die Inhaber von Konformitätszertifikaten, die im Rahmen nationaler Zertifizierungssysteme ausgestellt wurden, ihren Verpflichtungen in Bezug auf die Zertifizierung gemäß der Verordnung (EU) Nr. 910/2014 und den nationalen Zertifizierungssystemen nachkommen,

b) dass die zertifizierte Brieftaschenlösung die Anforderungen der nationalen Zertifizierungssysteme erfüllt.

Artikel 17

Folgen von Verstößen

In den nationalen Zertifizierungssystemen werden die Folgen von Verstößen einer zertifizierten Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt wird, gegen die Anforderungen dieser Verordnung festgelegt. Diese Folgen umfassen die folgenden Aspekte:

1. die Verpflichtung der Zertifizierungsstelle, den Inhaber des Konformitätszertifikats über Verstöße zu unterrichten und ihn zur Ergreifung von Abhilfemaßnahmen aufzufordern;

2. die Verpflichtung der Zertifizierungsstelle, andere einschlägige Marktüberwachungsbehörden zu unterrichten, wenn der Verstoß einschlägige Rechtsvorschriften der Union betrifft;

3. die Bedingungen für die Durchführung von Abhilfemaßnahmen durch den Inhaber des Konformitätszertifikats;

4. die Bedingungen für die Aussetzung eines Konformitätszertifikats durch die Zertifizierungsstelle und für die Wiederherstellung des Konformitätszertifikats nach Behebung des Verstoßes;

5. die Bedingungen für die Aufhebung eines Konformitätszertifikats durch die Zertifizierungsstelle;

6. die Folgen eines Verstoßes gegen die Anforderungen des nationalen Zertifizierungssystems durch die Zertifizierungsstelle.

KAPITEL VII

ZERTIFIZIERUNGZYKLUS

Artikel 18

Zertifizierungszyklus

(1) Die Gültigkeit von Konformitätszertifikaten, die im Rahmen nationaler Zertifizierungssysteme ausgestellt wurden, unterliegt regelmäßigen Evaluierungen durch die Zertifizierungsstelle, die gemäß den Anforderungen in Anhang IX durchgeführt werden.

(2) Die nationalen Zertifizierungssysteme enthalten einen Prozess für die Neuzertifizierung von Brieftaschenlösungen und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt werden, vor Ablauf des ursprünglichen Konformitätszertifikats auf Antrag des Inhabers des Konformitätszertifikats. Dieser Prozess für die Neuzertifizierung beinhaltet eine umfassende Evaluierung der Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt wird, einschließlich einer Schwachstellenbeurteilung, gemäß den in Anhang IX festgelegten Grundsätzen.

(3) Die nationalen Zertifizierungssysteme enthalten einen Prozess für die Verwaltung von Änderungen in der Brieftaschenlösung und dem elektronischen Identifizierungssystem, in dessen Rahmen diese bereitgestellt wird. Dieser Prozess umfasst Vorschriften für die Feststellung, ob eine Änderung durch eine Sonderevaluierung gemäß Absatz 4 oder durch die Überprüfung der operativen Wirksamkeit von Pflegeprozessen gemäß Anhang IV abzudecken ist.

(4) Die nationalen Zertifizierungssysteme müssen einen Prozess für Sonderevaluierungen gemäß der Norm EN ISO/IEC 17065:2012 enthalten. Dieser Prozess für Sonderevaluierungen umfasst eine Auswahl von Tätigkeiten, die durchzuführen sind, um das spezifische Problem anzugehen, das die Sonderevaluierung ausgelöst hat.

(5) Die nationalen Zertifizierungssysteme enthalten Vorschriften für die Aufhebung eines Konformitätszertifikats.

KAPITEL VIII

AUFZEICHNUNG UND SCHUTZ VON INFORMATIONEN

Artikel 19

Aufbewahrung von Aufzeichnungen

(1) Die nationalen Zertifizierungssysteme enthalten Anforderungen an Zertifizierungsstellen in Bezug auf ein Aufzeichnungssystem für alle relevanten Informationen, die im Zusammenhang mit den von ihnen durchgeführten Konformitätsbewertungstätigkeiten gewonnen werden, einschließlich der Daten, die von Anbietern von Brieftaschenlösungen und der elektronischen Identifizierungssysteme, in deren Rahmen diese bereitgestellt werden, herausgegeben und empfangen werden. Die Aufzeichnungen dieser Informationen werden auf sichere Weise gespeichert. Die Aufzeichnungen können elektronisch aufbewahrt werden und bleiben so lange zugänglich, wie dies nach Unionsrecht oder nationalem Recht vorgeschrieben ist, mindestens aber fünf Jahre lang nach Aufhebung oder Ablauf des betreffenden Konformitätszertifikats.

(2) Die nationalen Zertifizierungssysteme enthalten Anforderungen an den Inhaber des Konformitätszertifikats, nach denen er die folgenden Informationen für die Zwecke dieser Verordnung und für einen Zeitraum von mindestens fünf Jahren nach der Aufhebung oder dem Ablauf des betreffenden Konformitätszertifikats sicher speichern muss:

a) Aufzeichnungen der Informationen, die der Zertifizierungsstelle oder ihren Unterauftragnehmern während des Zertifizierungsprozesses übermittelt wurden;

b) Muster von Hardware-Komponenten, die in den Anwendungsbereich der Zertifizierung der Brieftaschenlösung einbezogen wurden.

(3) Die nationalen Zertifizierungssysteme verpflichten den Inhaber des Konformitätszertifikats, die in Absatz 1 genannten Informationen auf Anfrage der Zertifizierungsstelle oder der Aufsichtsstelle gemäß Artikel 46a Absatz 1 der Verordnung (EU) Nr. 910/2014 zur Verfügung zu stellen.

Artikel 20

Schutz von Informationen

Im Rahmen nationaler Zertifizierungssysteme müssen alle Personen oder Organisationen, denen bei der Durchführung von Tätigkeiten im Rahmen des nationalen Zertifizierungssystems Zugang zu Informationen gewährt wird, die Sicherheit und den Schutz von Geschäftsgeheimnissen und anderen vertraulichen Informationen sowie die Wahrung der Rechte des geistigen Eigentums gewährleisten und hierzu die erforderlichen und geeigneten technischen und organisatorischen Maßnahmen ergreifen, um diese Vertraulichkeit zu sicherzustellen.

KAPITEL IX

SCHLUSSBESTIMMUNGEN

Artikel 21

Übergang zu einem europäischen System für die Cybersicherheitszertifizierung

Diese Verordnung wird bei der Annahme des ersten europäischen Systems für die Cybersicherheitszertifizierung für Brieftaschenlösungen und die elektronischen Identifizierungssysteme, in deren Rahmen diese bereitgestellt werden, überprüft, um dem Beitrag eines solchen europäischen Systems für die Cybersicherheitszertifizierung zur Gesamtzertifizierung von Brieftaschenlösungen und zu den elektronischen Identifizierungssystemen, in deren Rahmen sie bereitgestellt werden, Rechnung zu tragen.

Artikel 22

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

RISIKOREGISTER FÜR EUROPÄISCHE BRIEFTASCHEN FÜR DIE DIGITALE IDENTITÄT

Einführung

Im Risikoregister werden die wichtigsten Risiken und Bedrohungen für die Sicherheit und den Schutz der Privatsphäre, die Brieftaschen betreffen und die in jeder Architektur und Umsetzung von Brieftaschen angemessen berücksichtigt werden müssen, beschrieben. Die **übergeordneten Risiken** (Abschnitt I) sind mit der Verwendung von Brieftaschen durch Nutzer und vertrauende Beteiligte verbunden und stehen im Zusammenhang mit direkten Bedrohungen, die sich gegen die Brieftaschenwerte und -daten richten. Darüber hinaus werden einige **Risiken auf Systemebene** (Abschnitt II) für Brieftaschen aufgeführt, die sich in der Regel aus einer Kombination von Bedrohungen für das gesamte Brieftaschensystem ergeben.

Art des Risikos	Risikokennung	Bezeichnungen der entsprechenden Risiken
Übergeordnete Risiken für die Brieftaschen	R1	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels
	R2	Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels
	R3	Erstellung oder Verwendung gefälschter Attribute
	R4	Identitätsdiebstahl
	R5	Datendiebstahl
	R6	Offenlegung von Daten
	R7	Datenmanipulation
	R8	Datenverlust
	R9	Unbefugte Transaktionen
	R10	Transaktionsmanipulation
	R11	Zurückweisung
	R12	Offenlegung von Transaktionsdaten
	R13	Störung des Dienstes
	R14	Überwachung
Systembezogene Risiken	SR1	Pauschalüberwachung
	SR2	Rufschädigung
	SR3	Rechtsverstoß

In dem Register werden auch **technische Bedrohungen** (Abschnitt III) verzeichnet, die sich gegen die Umsetzung der Brieftaschenlösung richten. Diese Bedrohungen sind insofern mit den übergeordneten Risiken verbunden, als jede von ihnen zahlreiche übergeordnete Risiken auslösen könnte.

Art der Bedrohung	Kennung der Bedrohung	Bezeichnungen der entsprechenden Bedrohungen	Unterkategorien von Bedrohungen
Technische Bedrohungen	TT1	Physische Angriffe	1.1. *Diebstahl*
			1.2. *Durchsickern von Informationen*
			1.3. *Verfälschung*
	TT2	Fehler und Fehlkonfigurationen	2.1. *Fehler beim Management eines IT-Systems*
			2.2. *Fehler oder Verwendungsfehler auf Anwendungsebene*
			2.3. *Entwicklungsfehler und Fehlkonfigurationen des Systems*

Art der Bedrohung	Kennung der Bedrohung	Bezeichnungen der entsprechenden Bedrohungen	Unterkategorien von Bedrohungen
	TT3	Verwendung unzuverlässiger Ressourcen	3.1. *Fehlerhafte Verwendung oder Konfiguration der Brieftaschenkomponenten*
	TT4	Fehler und Ausfälle	4.1. *Fehler oder Fehlfunktion von Geräten, Modulen oder Systemen*
			4.2. *Verlust von Ressourcen*
			4.3. *Ausfall unterstützender Dienste*
	TT5	Böswillige Handlungen	5.1. *Abfangen von Informationen*
			5.2. *Phishing und Spoofing*
			5.3. *Wiedereinspielen von Nachrichten (Replay-Angriff)*
			5.4. *Brute-Force-Angriffe*
			5.5. *Softwareschwachstellen*
			5.6. *Lieferkettenangriffe*
			5.7. *Schadsoftware*
			5.8. *Zufallszahlenvorhersage*

Schließlich sind im Register **direkte Bedrohungen für die Brieftaschen aufgeführt**, und jede davon ist mit einer (nicht erschöpfenden) Auswahl von Risiken verbunden (Abschnitt IV).

ABSCHNITT I

Übergeordnete Risiken für die Brieftaschen

R1. Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels

Die Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels wird definiert als die Erstellung einer elektronischen Identität, die es in Wirklichkeit gibt und einem anderen Nutzer gehört, in einer Brieftasche. Im Wesentlichen führt dieses Risiko zu den Risiken „Identitätsdiebstahl“ (R4) und „Unbefugte Transaktionen“ (R9).

R2. Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels

Die Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels wird definiert als die Erstellung einer elektronischen Identität, die es in Wirklichkeit nicht gibt, in einer Brieftasche.

R3. Erstellung oder Verwendung gefälschter Attribute

Die Erstellung oder Verwendung gefälschter Attribute wird definiert als die Erstellung oder Verwendung von Attributen, deren Ausstellung durch den genannten Anbieter nicht validiert werden kann und die nicht vertrauenswürdig sind.

R4. Identitätsdiebstahl

Identitätsdiebstahl wird definiert als der unbefugte Erwerb der Einzelbrieftasche oder Verlust von Authentifizierungsfaktoren, die es ermöglichen, sich als eine andere Person auszugeben.

R5. Datendiebstahl

Datendiebstahl wird definiert als die unbefugte Extraktion von Daten. Datendiebstahl steht auch im Zusammenhang mit Bedrohungen wie dem Abfangen von Daten (unbefugte Erfassung von Daten während der Übermittlung) und der Datenentschlüsselung (unbefugte Entschlüsselung verschlüsselter Daten), die in einigen Fällen zur Offenlegung von Daten (R6) führen dürften.

R6. Offenlegung von Daten

Die Offenlegung von Daten wird definiert als die unbefugte Offenlegung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten. Das Risiko einer Verletzung der Privatsphäre ist sehr ähnlich, wenn es nicht unter dem Gesichtspunkt der Sicherheit, sondern unter dem Gesichtspunkt der Privatsphäre betrachtet wird.

R7. Datenmanipulation

Datenmanipulation wird definiert als die unbefugte Veränderung von Daten.

R8. Datenverlust

Datenverlust wird definiert als die Situation, in der in der Brieftasche gespeicherte Daten durch Missbrauch oder böswillige Handlungen verloren gehen. Dieses Risiko ist häufig ein sekundäres Risiko der „Datenmanipulation" (R7) oder „Störung des Dienstes" (R13), bei dem die Daten ganz oder teilweise nicht wiederhergestellt werden können.

R9. Unbefugte Transaktionen

Unbefugte Transaktionen werden definiert als Vorgänge, die ohne Erlaubnis oder Wissen des Brieftaschennutzers durchgeführt werden. In vielen Fällen kann eine unbefugte Transaktion zu „Identitätsdiebstahl" (R4) oder zur „Offenlegung von Daten" (R6) führen. Dies steht auch mit unbefugten Transaktionen wie dem Missbrauch kryptografischer Schlüssel im Zusammenhang.

R10. Transaktionsmanipulation

Transaktionsmanipulation wird definiert als die unbefugte Veränderung von Vorgängen in der Brieftasche. Die Manipulation von Transaktionen ist ein Angriff auf die Integrität und steht mit der Verletzung der Datenintegrität im Zusammenhang.

R11. Zurückweisung

Die Zurückweisung wird definiert als eine Situation, in der ein Beteiligter die Durchführung einer Handlung oder die Beteiligung an einer Transaktion verweigert und andere Beteiligte nicht über geeignete Nachweise verfügen, um dem zu widersprechen.

R12. Offenlegung von Transaktionsdaten

Die Offenlegung von Transaktionsdaten wird definiert als die Offenlegung von Informationen über eine Transaktion zwischen Beteiligten.

R13. Störung des Dienstes

Die Störung des Dienstes wird definiert als Unterbrechung oder Beeinträchtigung des normalen Betriebs der Brieftasche. Eine bestimmte Art der Störung des Dienstes ist die Aussperrung des Nutzers, d. h. dass ein Nutzer nicht auf sein Konto oder seine Brieftasche zugreifen kann.

R14. Überwachung

Überwachung oder Monitoring wird definiert als die unbefugte Verfolgung oder Beobachtung der Aktivitäten, Kommunikation oder Daten eines Brieftaschennutzers. Die Überwachung steht häufig im Zusammenhang mit Schlussfolgerungen, die definiert werden als Ableitung sensibler oder personenbezogener Daten aus scheinbar unverfänglichen Daten.

ABSCHNITT II

Systembezogene Risiken

Diese Risiken werden in der Liste der Bedrohungen nicht berücksichtigt, da sie in der Regel die Folge mehrerer Bedrohungen sind, die so wiederholt auftreten, dass sie zur Bedrohung für das gesamte System werden.

SR1. Pauschalüberwachung

Pauschalüberwachung wird definiert als die Verfolgung oder Beobachtung der Aktivitäten vieler Nutzer durch die Überwachung der Kommunikation oder der Daten ihrer Brieftaschen. Pauschalüberwachung wird häufig mit „Überwachung" (R14) und mit Rückschlüssen auf globaler Ebene in Verbindung gebracht, bei denen Informationen über viele Nutzer kombiniert werden, um sensible oder personenbezogene Daten über Nutzer abzuleiten oder statistische Trends zu ermitteln, die für die Konzeption weiterer Angriffe verwendet werden können.

SR2. Rufschädigung

Rufschädigung wird definiert als der Schaden, der dem Ansehen einer Organisation oder Regierungsstelle zugefügt wird. Rufschädigung ergibt sich auch aus anderen Risiken, wenn die Medien über einen Verstoß oder Sicherheitsvorfall berichten und die Organisation in ungünstigem Licht erscheinen lassen. Rufschädigung kann zu weiteren Risiken führen, wie z. B. Vertrauensverlust aufgrund der berechtigten Zweifel der Nutzer und Verlust des Ökosystems, wenn das gesamte Ökosystem zusammenbricht.

SR3. Rechtsverstoß

Rechtsverstoß wird definiert als eine Situation, in der die einschlägigen Gesetze, Vorschriften oder Normen nicht eingehalten werden können. Da im Zusammenhang mit der Brieftasche die Sicherheit und der Schutz der Privatsphäre der Brieftaschenlösung rechtliche Anforderungen darstellen, dürften alle Bedrohungen zu einer Art des Verstoßes gegen Rechtsvorschriften führen.

ABSCHNITT III

Technische Bedrohungen

Die technischen Bedrohungen sind nicht allesamt mit spezifischen Risiken für die Brieftaschen verbunden, denn viele von ihnen können als Mittel zur Durchführung möglicher Angriffe eingesetzt werden könnten, die vielen unterschiedlichen Risiken entsprechen.

TT1. Physische Angriffe

1.1. *Diebstahl*

Diebstahl wird definiert als Diebstahl von Geräten/Modulen, die das ordnungsgemäße Funktionieren der Brieftasche beeinträchtigen können (wenn das Gerät/Modul gestohlen wird und die Einzelbrieftasche nicht angemessen geschützt ist). Dies kann zu vielen Risiken beitragen, darunter „Identitätsdiebstahl“ (R4), „Datendiebstahl“ (R5) und „Unbefugte Transaktionen“ (R9).

1.2. *Durchsickern von Informationen*

Durchsickern von Information wird definiert als unbefugter Zugriff, unbefugte Informationsverbreitung oder Weitergabe nach physischem Zugriff auf die Brieftasche. Dies kann insbesondere zur „Offenlegung von Daten“ (R6) und „Datendiebstahl“ (R5) beitragen.

1.3. *Verfälschung*

Verfälschung wird definiert als Verletzung der Integrität einer oder mehrerer Komponenten der Brieftasche oder der Komponenten, auf die sich die Einzelbrieftasche stützt, z. B. des Geräts des Nutzers oder dessen Betriebssystems. Dies kann insbesondere zu „Datenmanipulation“ (R7), „Datenverlust“ (R8) und „Transaktionsmanipulation“ (R10) beitragen. Werden Softwarekomponenten verfälscht, kann dies zu vielen Risiken beitragen.

TT2. Fehler und Fehlkonfigurationen

2.1. *Fehler beim Management eines IT-Systems*

Fehler beim Management eines IT-Systems werden definiert als Durchsickern und Weitergabe von Informationen oder Schäden durch den Missbrauch von IT-Werten durch Nutzer (mangelnde Kenntnis der Anwendungsmerkmale) oder durch die unsachgemäße Konfiguration oder das unsachgemäße Management von IT-Werten.

2.2. *Fehler oder Verwendungsfehler auf Anwendungsebene*

Fehler oder Verwendungsfehler auf Anwendungsebene werden definiert als Fehlfunktionen der Anwendung, die auf einen Fehler in der Anwendung selbst oder auf einen Fehler eines Nutzers (Brieftaschennutzer und vertrauende Beteiligte) zurückzuführen sind.

2.3. *Entwicklungsfehler und Fehlkonfigurationen des Systems*

Entwicklungsfehler und Fehlkonfigurationen des Systems werden definiert als Fehlfunktionen oder Schwachstellen, die durch nicht ordnungsgemäß entwickelte oder konfigurierte IT-Werte oder Geschäftsprozesse verursacht werden (unzureichende Spezifikationen von IT-Produkten, unzureichende Nutzbarkeit, unsichere Schnittstellen, unsachgemäße Konzept- und Verfahrensabläufe, Konzeptionsfehler).

TT3. Verwendung unzuverlässiger Ressourcen

Die Verwendung unzuverlässiger Ressourcen wird definiert als Tätigkeit, die zu unbeabsichtigtem Schaden aufgrund schlecht definierter Vertrauensbeziehungen führt, wie z. B. Vertrauen in einen Drittanbieter ohne ausreichende Sicherheitsgarantien.

3.1. *Fehlerhafte Verwendung oder Konfiguration der Brieftaschenkomponenten*

Eine fehlerhafte Verwendung oder Konfiguration der Brieftaschenkomponenten wird definiert als unbeabsichtigte Beschädigung von Brieftaschenkomponenten aufgrund einer fehlerhaften Verwendung oder Konfigurationen durch Brieftaschennutzer oder durch nicht ausreichend geschulte Entwickler oder aufgrund mangelnder Anpassung an Veränderungen in der Bedrohungslandschaft, in der Regel durch die Verwendung anfälliger Komponenten Dritter oder von Runtime-Plattformen.

TT4. Fehler und Ausfälle

4.1. *Fehler oder Fehlfunktion von Geräten, Modulen oder Systemen*

Ein Fehler oder eine Fehlfunktion von Geräten wird definiert als unbeabsichtigte Beschädigung von IT-Anlagen aufgrund einer Störung oder Fehlfunktion der Geräte, einschließlich der Infrastruktur des Anbieters und der Nutzergeräte.

4.2. *Verlust von Ressourcen*

Der Verlust von Ressourcen wird definiert als Störung oder Fehlfunktion aufgrund der Nichtverfügbarkeit solcher Ressourcen, z. B. von Ersatzteilen.

4.3. *Ausfall unterstützender Dienste*

Der Ausfall unterstützender wird definiert als Ausfall oder Fehlfunktion aufgrund der Nichtverfügbarkeit unterstützender Dienste, die für den ordnungsgemäßen Betrieb des Systems erforderlich sind, einschließlich der Netzanbindung der Infrastruktur des Anbieters und der Nutzergeräte.

TT5. Böswillige Handlungen

5.1. *Abfangen von Informationen*

Das Abfangen von Informationen wird definiert als das Abfangen von Informationen, die bei der Übermittlung nicht ordnungsgemäß gesichert waren, einschließlich Man-in-the-Middle-Angriffen.

5.2. *Phishing und Spoofing*

Phishing wird definiert als das Erlangen von Informationen, die nach einer irreführenden Interaktion vom Nutzer selbst bereitgestellt werden und häufig mit dem Spoofing rechtmäßiger Kommunikationsmittel und Websites in Verbindung stehen. Solche Bedrohungen richten sich gegen den Nutzer und tragen in der Regel zu „Identitätsdiebstahl" (R4) und „Unbefugten Transaktionen" (R9) bei, häufig durch „Datendiebstahl" (R5) oder „Offenlegung von Daten" (R6).

5.3. *Wiedereinspielen von Nachrichten (Replay-Angriff)*

Das Wiedereinspielen von Nachrichten (Replay-Angriff) wird definiert als die Wiederverwendung zuvor abgefangener Nachrichten zur Durchführung unbefugter Transaktionen, häufig auf Protokollebene. Diese technische Bedrohung trägt hauptsächlich zu unbefugten Transaktionen bei, die dann je nach Transaktion zu weiteren Risiken führen können.

5.4. *Brute-Force-Angriffe*

Brute-Force-Angriffe werden definiert als Verletzung der Sicherheit und oft der Vertraulichkeit, die dadurch erreicht wird, dass eine sehr große Zahl von Interaktionen durchgeführt wird, bis die erhaltenen Antworten wertvolle Informationen liefern.

5.5. *Softwareschwachstellen*

Die Bedrohung im Zusammenhang mit Softwareschwachstellen wird definiert als eine Sicherheitsverletzung durch Ausnutzung einer Softwareschwachstelle in den Brieftaschenkomponenten oder in den bei der Umsetzung der Brieftasche verwendeten Software- und Hardwarekomponenten, einschließlich bekannter und unbekannter (Zero-Day-) Schwachstellen.

5.6. *Lieferkettenangriffe*

Ein Lieferkettenangriff wird definiert als eine Sicherheitsverletzung durch Angriffe auf den Lieferanten des Brieftaschenanbieters oder auf dessen Nutzer, um danach weitere Angriffe auf die Brieftasche selbst zu ermöglichen.

5.7. *Schadsoftware*

Schadsoftware wird definiert als Sicherheitsverletzung durch böswillige Anwendungen, die unerwünschte und unrechtmäßige Handlungen in der Brieftasche durchführen.

5.8. *Zufallszahlenvorhersage*

Die Zufallszahlenvorhersage wird definiert als die Ermöglichung von Brute-Force-Angriffen durch teilweise oder vollständige Vorhersage generierter Zufallszahlen.

ABSCHNITT IV

Bedrohungen für die Brieftaschen

Dieser letzte Abschnitt enthält eine Auswahl typischer Bedrohungsszenarien für Brieftaschen, die den oben aufgeführten damit verbundenen übergeordneten Risiken zugeordnet sind. In dieser Liste sind Bedrohungen aufgeführt, die abgedeckt werden müssen, es handelt sich jedoch um keine erschöpfende Liste von Bedrohungen, die in hohem Maße von der Architektur der ausgewählten Brieftaschenlösung und der Entwicklung des Bedrohungsumfelds abhängen. Darüber hinaus kann der Brieftaschenanbieter bei der Risikobewertung und den vorgeschlagenen Maßnahmen nur für die Komponenten verantwortlich sein, die in den Anwendungsbereich der Zertifizierung fallen (*).

Kennung *Kennung*	Beschreibung der Bedrohung *Beschreibung der ermittelten Bedrohung (*)*	Bezeichnung der Risiken *Verbundene Risiken*
TR1	Ein Angreifer kann Pseudonyme ohne triftigen Grund widerrufen.	Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels (R2)
TR2	Ein Angreifer kann gefälschte elektronische Identitäten ausstellen, die es nicht gibt.	Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels (R2)
TR3	Ein Angreifer kann unbefugt Personenidentifizierungsdaten (PID) ausstellen.	Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels (R2)
TR4	Ein Angreifer kann einen Administrator dazu veranlassen, einen falschen PID-Anbieter in die Liste vertrauenswürdiger PID-Anbieter aufzunehmen.	Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels (R2)
TR5	Ein Angreifer kann den Fernidentitätsnachweisdienst umgehen.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels (R2)
TR6	Ein Angreifer kann den physischen Identitätsnachweisdienst umgehen.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels (R2)
TR7	Ein Angreifer kann den Identitätsnachweisdienst im Zusammenhang mit der Nutzung eines (qualifizierten) Fernzertifikats umgehen.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels (R2)
TR8	Ein Angreifer kann Zugang zu einer Brieftasche erhalten, die an keine Person gebunden ist.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels (R2)
TR9	Ein Angreifer kann technische und verfahrenstechnische Kontrollen überwinden, um falsche PID zu erstellen.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels (R2)
TR10	Ein Angreifer kann eine neue Brieftasche mit einem ungültigen WSCD aktivieren.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels (R2)
TR11	Ein Angreifer kann den Identitätsnachweisdienst im Zusammenhang mit der Nutzung bestehender eID-Mittel umgehen.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Identitätsdiebstahl (R4) / Unbefugte Transaktionen (R9)
TR12	Ein Angreifer kann die Überprüfung durch den PID-Anbieter, ob die Brieftasche von ihrem Nutzer kontrolliert wird, umgehen und PID an eine beeinträchtigte, vom Angreifer kontrollierte Brieftasche ausstellen lassen.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Identitätsdiebstahl (R4) / Unbefugte Transaktionen (R9)

Kennung *Kennung*	Beschreibung der Bedrohung *Beschreibung der ermittelten Bedrohung (*)*	Bezeichnung der Risiken *Verbundene Risiken*
TR13	Ein Angreifer kann gültige PID in eine ungültige Einzelbrieftasche einschleusen.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Identitätsdiebstahl (R4) / Unbefugte Transaktionen (R9)
TR14	Ein PID-Anbieter kann gefälschte Identifizierungsmittel für die Identität einer existierenden Person ausstellen.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Identitätsdiebstahl (R4) / Unbefugte Transaktionen (R9)
TR15	Ein Angreifer kann PID mit der falschen Brieftasche verknüpfen, da der PID-Anbieter nicht in der Lage ist, die PID mit der richtigen Brieftasche zu verknüpfen.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Identitätsdiebstahl (R4) / Unbefugte Transaktionen (R9)
TR16	Ein Angreifer kann den Nutzer dazu bringen, der Aktivierung einer neuen Einzelbrieftasche/Brieftascheninstanz unter der Kontrolle des Angreifers zuzustimmen — auch mit anschließender Kontrolle der Bescheinigungen.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Erstellung oder Verwendung eines gefälschten elektronischen Identifizierungsmittels (R2) / Identitätsdiebstahl (R4) / Unbefugte Transaktionen (R9)
TR17	Ein Angreifer kann PID eines anderen Staates ausstellen, um auf Daten/digitale Werte der betroffenen Bürger zuzugreifen.	Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1) / Identitätsdiebstahl (R4) / Unbefugte Transaktionen (R9)
TR18	Ein Angreifer kann technische und verfahrenstechnische Kontrollen überwinden, um falsche (qualifizierte) elektronische Attributsbescheinigungen ((Q)EAAs) zu erstellen.	Erstellung oder Verwendung gefälschter Attribute (R3)
TR19	Ein Angreifer kann (Q)EAAs vorweisen, die ihm nicht rechtsgültig ausgestellt wurden.	Erstellung oder Verwendung gefälschter Attribute (R3)
TR20	Ein Angreifer kann den kryptografischen Mechanismus der Brieftasche zur Verknüpfung der PID und einer nicht an ihn ausgestellten (Q)EAA angreifen.	Erstellung oder Verwendung gefälschter Attribute (R3)
TR21	Ein Angreifer kann eine (Q)EAA in einer Brieftasche verwenden, obwohl das physische Gegenstück zur (Q)EAA abgelaufen oder ungültig ist.	Erstellung oder Verwendung gefälschter Attribute (R3)
TR22	Ein Angreifer kann die Überprüfung durch den (Q)EAA-Anbieter, ob die Brieftasche von ihrem Nutzer kontrolliert wird, umgehen und eine (Q)EAA an eine beeinträchtigte, vom Angreifer kontrollierte Brieftasche ausstellen lassen.	Erstellung oder Verwendung gefälschter Attribute (R3)
TR23	Ein Angreifer kann elektronische Attributsbescheinigungen fälschen.	Erstellung oder Verwendung gefälschter Attribute (R3)
TR24	Ein Angreifer kann gefälschte elektronische Attributsbescheinigungen in eine Brieftasche einschleusen.	Erstellung oder Verwendung gefälschter Attribute (R3)
TR25	Die Brieftasche kann einem vertrauenden Beteiligten ohne Zustimmung eines Nutzers Attribute vorweisen.	Offenlegung von Daten (R6)
TR26	PID, (Q)EAAs oder Pseudonyme können einem falschen vertrauenden Beteiligten vorgewiesen werden.	Offenlegung von Daten (R6)
TR27	Ein Angreifer kann eine böswillige Erneuerung elektronischer Attributsbescheinigungen (EAAs) einleiten.	Offenlegung von Daten (R6)
TR28	Ein Angreifer kann einen Nutzer dazu bringen, einer Abfrage elektronischer Attributsbescheinigungen fälschlicherweise zuzustimmen (Phishing oder Sonstiges).	Offenlegung von Daten (R6)

Kennung *Kennung*	Beschreibung der Bedrohung *Beschreibung der ermittelten Bedrohung (*)*	Bezeichnung der Risiken *Verbundene Risiken*
TR29	Ein Angreifer kann Attribute aus der Brieftasche abgreifen und den Brieftaschennutzer identifizieren, obwohl keine Identifizierung erforderlich/zulässig ist.	Offenlegung von Daten (R6)
TR30	Ein Angreifer kann technische und verfahrenstechnische Kontrollen überwinden, um Daten zu extrahieren.	Offenlegung von Daten (R6)
TR31	Eine Abfrage kann einem Angreifer zugespielt werden.	Offenlegung von Daten (R6)
TR32	Ein Angreifer kann Kenntnis von der eingebetteten Offenlegungsregelung für Attribute erlangen und Attribute vorweisen, die in der aktuellen Abfrage von Einzelbrieftaschen enthalten sind.	Offenlegung von Daten (R6)
TR33	Ein Angreifer kann Protokolle oder Teile davon extrahieren.	Offenlegung von Daten (R6)
TR34	Ein Angreifer kann in Erfahrung bringen, ob eine Brieftasche auf demselben Gerät, das er verwendet, oder auf einem anderen Gerät installiert ist, und Informationen darüber sammeln.	Offenlegung von Daten (R6)
TR35	Ein Angreifer kann an einen Wissensfaktor gelangen, der für die Authentifizierung des Nutzers in der WSCA verwendet wird.	Offenlegung von Daten (R6)
TR36	Die elektronische Attributsbescheinigung einer Person, die in mehreren Transaktionen mit einem vertrauenden Beteiligten oder zwischen verschiedenen vertrauenden Beteiligten vorgewiesen wird, ermöglicht es unbeabsichtigt, mehrere Transaktionen mit der betreffenden Person zu verknüpfen.	Offenlegung von Daten (R6)
TR37	Eine öffentliche Liste widerrufener Bescheinigungen/vertrauender Beteiligter kann Informationen über die Verwendung der Bescheinigung durch den Nutzer enthalten (z. B. Standort, IP-Adresse usw.).	Offenlegung von Daten (R6)
TR38	Wenn vertrauende Beteiligte nicht in der Lage sind, die Zustimmung des Nutzers zur Verwendung gemeinsamer Attribute nachzuweisen, kann dies die Integrität der Protokolle beeinträchtigen.	Offenlegung von Daten (R6)
TR39	Ein Angreifer kann die Aktivitäten von Brieftaschennutzer mithilfe eindeutiger/nachverfolgbarer Kennungen unrechtmäßig verfolgen.	Offenlegung von Daten (R6) / Überwachung (R14)
TR40	Ein vertrauender Beteiligter, der aus mehreren Einheiten/Einrichtungen besteht, die jeweils einen anderen Anwendungsbereich in Bezug darauf haben, was sie abfragen/verarbeiten dürfen, kann ohne rechtmäßige Grundlage Daten abfragen und verarbeiten.	Offenlegung von Daten (R6) / Unbefugte Transaktionen (R9)
TR41	Ein Angreifer kann die Integritäts- und Authentizitätsprüfungen von PID durch die Brieftasche aushebeln, sodass stets eine positive Bestätigung erfolgt.	Datenmanipulation (R7)
TR42	Ein Angreifer kann die Durchführung von Prüfungen durch die Brieftasche, mit denen die Integrität und Authentizität der abgefragten Attribute überprüft werden, umgehen oder aushebeln, sodass stets eine positive Bestätigung erfolgt.	Datenmanipulation (R7)
TR43	Ein Angreifer kann die Durchführung von Prüfungen durch die Brieftasche, mit denen überprüft wird, ob alle abgefragten Attribute zu demselben Nutzer gehören, umgehen oder aushebeln, sodass stets eine positive Bestätigung erfolgt.	Datenmanipulation (R7)
TR44	Ein Angreifer kann die Durchführung von Prüfungen durch die Brieftasche, mit denen die Gültigkeit der PID und deren Ausstellung durch einen vertrauenswürdigen PID-Anbieter überprüft werden, umgehen oder aushebeln, sodass stets eine positive Bestätigung erfolgt.	Datenmanipulation (R7)

Kennung *Kennung*	Beschreibung der Bedrohung *Beschreibung der ermittelten Bedrohung (*)*	Bezeichnung der Risiken *Verbundene Risiken*
TR45	Ein Angreifer kann die Durchführung von Prüfungen durch die Brieftasche, mit denen die Gültigkeit einer QEAA und deren Ausstellung durch einen qualifizierten, für die Ausstellung der QEAA registrierten Vertrauensdiensteanbieter überprüft werden, umgehen oder aushebeln, sodass stets eine positive Bestätigung erfolgt.	Datenmanipulation (R7)
TR46	Ein Angreifer kann die Durchführung von Prüfungen durch die Brieftasche, mit denen überprüft wird, ob die PID durch den PID-Anbieter widerrufen wurden, umgehen oder aushebeln, sodass stets eine positive Bestätigung erfolgt.	Datenmanipulation (R7)
TR47	Ein Angreifer kann die Durchführung von Prüfungen durch die Brieftasche, mit denen überprüft wird, ob die (Q)EAA durch den (Q) EAA-Anbieter widerrufen wurden, umgehen oder aushebeln, sodass stets eine positive Bestätigung erfolgt.	Datenmanipulation (R7)
TR48	Ein Angreifer kann den Inhalt von Sicherungs- und Wiederherstellungsdaten ändern, die ausschließlich der Kontrolle des Nutzers unterliegen sollten.	Datenmanipulation (R7) / Datenverlust (R8)
TR49	Ein Angreifer kann den Transaktionsverlauf für eine bestimmte Brieftascheninstanz aus den Tätigkeitsprotokollen ändern.	Datenmanipulation (R7) / Datenverlust (R8)
TR50	Ein Angreifer kann die Verbindung der Brieftasche zu den vertrauenden Beteiligten abhören.	Datendiebstahl (R5) / Offenlegung von Daten (R6)
TR51	Ein Angreifer kann einen Nutzer dazu bringen, unabsichtlich personenbezogene Daten (d. h. PID, EAAs, Pseudonyme, elektronische Signaturen, Protokolle und andere Daten) an den Angreifer oder einen Dritten weiterzugeben.	Datendiebstahl (R5) / Offenlegung von Daten (R6)
TR52	Ein Angreifer kann den Transaktionsverlauf für eine bestimmte Brieftascheninstanz aus den Tätigkeitsprotokollen auslesen.	Datendiebstahl (R5) / Offenlegung von Daten (R6)
TR53	Ein Angreifer kann kryptografische Schlüssel aus dem WSCD exportieren oder extrahieren.	Datendiebstahl (R5) / Offenlegung von Daten (R6) / Unbefugte Transaktionen (R9)
TR54	Ein Angreifer kann den Inhalt von Sicherungs- und Wiederherstellungsdaten auslesen, die ausschließlich der Kontrolle des Nutzers unterliegen sollten.	Datendiebstahl (R5) / Offenlegung von Daten (R6)
TR55	Ein Angreifer kann die Nutzerauthentifizierungsmethode umgehen, um ein von einer Einzelbrieftasche erzeugtes Pseudonym zu verwenden.	Identitätsdiebstahl (R4)
TR56	Ein Angreifer kann eine Anwendung anbieten, die für die Nutzer eine bestimmte rechtmäßige Brieftasche nachbildet.	Identitätsdiebstahl (R4)
TR57	Ein Angreifer kann Brieftaschendaten, einschließlich PID, (Q)EAAs oder Protokolle exportieren.	Identitätsdiebstahl (R4)
TR58	Ein Angreifer kann Elemente einer kryptografischen Bindung exportieren.	Identitätsdiebstahl (R4)
TR59	Ein Angreifer kann über die kryptografischen Schlüssel der Brieftasche die Kontrolle über Identitäten übernehmen.	Identitätsdiebstahl (R4)
TR60	Ein Angreifer kann die persönliche Einzelbrieftasche eines anderen Nutzers auf seinem eigenen Gerät duplizieren und verwenden.	Identitätsdiebstahl (R4) / Erstellung oder Verwendung eines bestehenden elektronischen Identifizierungsmittels (R1)

Kennung *Kennung*	Beschreibung der Bedrohung *Beschreibung der ermittelten Bedrohung (*)*	Bezeichnung der Risiken *Verbundene Risiken*
TR61	Behörden eines anderen Staates können den Nutzer auffordern, alle Brieftaschendaten vorzuweisen und/oder weiterzugeben, wenn er sich in der Nähe dieses Staates befindet, z. B. beim Überschreiten seiner Grenze.	Identitätsdiebstahl (R4) / Überwachung (R14)
TR62	Nutzer können ihre Transaktionsprotokolle nach einem Fehler eines Nutzergeräts nicht übertragen, was die Rückverfolgung früherer Transaktionen auf der neuen Brieftasche unmöglich macht.	Zurückweisung (R11)
TR63	Nutzer können ihre Transaktionsprotokolle nach einem Fehler eines Nutzergeräts nicht wiederherstellen, was die Rückverfolgung auf der neuen Brieftasche unmöglich macht.	Zurückweisung (R11)
TR64	Vertrauende Beteiligte können Schwierigkeiten haben, die Zustimmung zu elektronischen Fernsignaturen nachzuweisen.	Zurückweisung (R11)
TR65	Ein Angreifer kann die Verbindung(en) zu vertrauenden Beteiligten mit Abfragen überlasten.	Störung des Dienstes (R13)
TR66	Ein Angreifer kann einen Statusbereitstellungsdienst mit Verbindungen zu vertrauenden Beteiligten überlasten.	Störung des Dienstes (R13)
TR67	Ein Angreifer kann die Attributsvorweisung als strittig/abgelehnt darstellen, obwohl sich die Attributsvorweisung als gültig ausweist.	Störung des Dienstes (R13)
TR68	Ein Angreifer kann PID ohne triftigen Grund widerrufen.	Störung des Dienstes (R13)
TR69	Ein Angreifer kann PID ohne Zustimmung des Nutzers widerrufen.	Störung des Dienstes (R13)
TR70	Ein Angreifer kann eine (Q)EAA ohne triftigen Grund widerrufen.	Störung des Dienstes (R13)
TR71	Ein Angreifer kann eine (Q)EAA ohne Zustimmung des Nutzers widerrufen.	Störung des Dienstes (R13)
TR72	Ein Angreifer kann mehrere Identifizierungsabfragen auslösen, ohne dass sie als absichtlich verwaiste Abfragen erkannt werden.	Störung des Dienstes (R13)
TR73	Ein Angreifer kann mehrere Abfragen ohne Folgetransaktion senden.	Störung des Dienstes (R13)
TR74	Ein Angreifer kann es ermöglichen, dass ein vertrauender Beteiligter eine Identität ohne entsprechende Identifizierung (Antwort) und vollständige Kontrolle abfragt.	Störung des Dienstes (R13)
TR75	Ein Angreifer kann eine Antwort auf eine Abfrage nach deren Beendigung oder in ähnlichen Situationen versenden, was zu einer Störung des Dienstes führt.	Störung des Dienstes (R13)
TR76	Ein vertrauender Beteiligter kann mehrere ungültige Abfragen senden.	Störung des Dienstes (R13)
TR77	Ein Angreifer kann mehrere ungültige Abfragen an einen Brieftaschenanbieter senden.	Störung des Dienstes (R13)
TR78	Ein Angreifer kann es einem Mitgliedstaat unmöglich machen, einen nicht vertrauenswürdigen PID-Anbieter aus der Liste vertrauenswürdiger PID-Anbieter zu streichen.	Störung des Dienstes (R13)
TR79	Ein Angreifer kann die Aussetzung oder den Widerruf einer Brieftasche verhindern.	Störung des Dienstes (R13)

Kennung *Kennung*	Beschreibung der Bedrohung *Beschreibung der ermittelten Bedrohung (*)*	Bezeichnung der Risiken *Verbundene Risiken*
TR80	Ein Angreifer kann Transaktionen durch vertrauende Beteiligte, Nutzer und/oder PID-Anbieter blockieren.	Störung des Dienstes (R13)
TR81	Ein Angreifer kann ein WSCD deaktivieren oder unzugänglich machen.	Störung des Dienstes (R13)
TR82	Ein Angreifer kann es dem PID-Anbieter unmöglich machen, PID zu widerrufen oder auszusetzen.	Störung des Dienstes (R13) / Unbefugte Transaktionen (R9)
TR83	Ein vertrauender Beteiligter kann die Identitätsdaten des Nutzers über die mit ihm ausgetauschten Daten hinaus ableiten.	Überwachung (R14)
TR84	Eine Gruppe vertrauender Beteiligter oder von PID-Anbietern kann die Identitätsdaten des Nutzers über die ihnen bekannten Daten hinaus ableiten.	Überwachung (R14)
TR85	Ein Angreifer kann einen Nutzer anhand dessen Personenidentifizierungsdaten ausfindig machen und verfolgen, obwohl eine Identifizierung des Nutzers nicht erforderlich ist.	Überwachung (R14)
TR86	Ein Angreifer kann eine „gefälschte“ Vorweisung von (Q) EAA-Kombinationen zusammenfügen.	Transaktionsmanipulation (R10)
TR87	Ein Angreifer kann die Brieftasche ohne ausdrückliche Zustimmung oder alleinige Kontrolle des Nutzers aus der Ferne aktivieren/übernehmen (z. B. eine Bank-App, in die eine Authentifizierungs- oder Bescheinigungsabfrage eingebettet ist), ohne dass der Nutzer davon Kenntnis hat (z. B. nachts) oder ohne dass der Nutzer den vertrauenden Beteiligten sehen kann.	Transaktionsmanipulation (R10)
TR88	Angreifer können Änderungen an den Metadaten einer Abfrage (Dienstname, Verwendung usw.) vornehmen.	Transaktionsmanipulation (R10)
TR89	Angreifer können Änderungen an den Antwortinformationen (Dienstzustand, Nonce usw.) vornehmen.	Transaktionsmanipulation (R10)
TR90	Angreifer können Änderungen an den Attributinformationen einer Abfrage (Überabfrage usw.) vornehmen.	Transaktionsmanipulation (R10)
TR91	Ein vertrauender Beteiligter kann Elemente einer früheren Sitzung in einer anderen Sitzung wiedergeben.	Transaktionsmanipulation (R10)
TR92	Ein Angreifer kann PID während ihrer Übertragung vom PID-Anbieter an die Einzelbrieftasche ersetzen oder ändern.	Transaktionsmanipulation (R10)
TR93	Ein Angreifer kann PID während ihrer Übertragung von einer Einzelbrieftasche an den vertrauenden Online-Beteiligten ersetzen oder ändern.	Transaktionsmanipulation (R10)
TR94	Ein Angreifer kann PID während ihrer Übertragung von einer Einzelbrieftasche an den vertrauenden Offline-Beteiligten ersetzen oder ändern.	Transaktionsmanipulation (R10)
TR95	Ein Angreifer kann PID ohne Zustimmung des Nutzers ausstellen.	Unbefugte Transaktionen (R9)
TR96	Ein Angreifer kann widerrufene oder ungültige eingebettete Offenlegungsregelungen verwenden, möglicherweise ohne Wissen der vertrauenden Beteiligten.	Unbefugte Transaktionen (R9)
TR97	Ein Angreifer kann die Brieftasche täuschen, sodass sie falsche elektronische Signaturen überprüft.	Unbefugte Transaktionen (R9)
TR98	Ein Angreifer kann die Brieftasche außerhalb der Kontrolle des Nutzers verwenden.	Unbefugte Transaktionen (R9)

Kennung *Kennung*	Beschreibung der Bedrohung *Beschreibung der ermittelten Bedrohung (*)*	Bezeichnung der Risiken *Verbundene Risiken*
TR99	Ein Angreifer kann einen Nutzer dazu bringen, Transaktionen mit einem Angreifer oder einem unbefugten Dritten zu authentifizieren und zu genehmigen.	Unbefugte Transaktionen (R9)
TR100	Ein Angreifer kann einen Nutzer zu einer elektronischen Unterschrift veranlassen, ohne dem Nutzer den Inhalt vorzuweisen oder nachdem er falsche Inhalte vorgewiesen hat.	Unbefugte Transaktionen (R9)
TR101	Ein Angreifer kann die Zugangskontrolle des Nutzerkontos beim Brieftaschenanbieter umgehen.	Unbefugte Transaktionen (R9)
TR102	Ein Angreifer kann sich während der Verbindung zu vertrauenden Beteiligten als vertrauender Beteiligter ausgeben.	Unbefugte Transaktionen (R9) / Offenlegung von Daten (R6)
TR103	Der Nutzer bei der Verbindung zwischen dem vertrauenden Beteiligten und dem Browser kann sich von dem Nutzer bei der Verbindung zwischen dem vertrauenden Beteiligten und der Brieftasche unterscheiden.	Unbefugte Transaktionen (R9) / Offenlegung von Daten (R6) / Identitätsdiebstahl (R4)
TR104	Ein Angreifer kann den Nutzer dazu bringen, seine Brieftasche ohne Grund zu widerrufen.	Unbefugte Transaktionen (R9) / Störung des Dienstes (R13)
TR105	Ein Angreifer kann Man-in-the-Middle-Angriffe durchführen.	Unbefugte Transaktionen (R9) / Offenlegung von Daten (R6) / Überwachung (R14)
TR106	Ein Angreifer kann ungültige oder widerrufene Attribute aus einer Brieftasche vorweisen, die nicht regelmäßig mit dem Netz verbunden ist.	Auswirkung auf verschiedene Risiken
TR107	Ein Angreifer kann Informationen von einem Nutzer stehlen, indem er eine Brieftasche spooft.	Auswirkung auf verschiedene Risiken
TR108	Ein Angreifer kann sich durch das Wiedergeben (Replay)/Nachahmen einer Datenabfrage (z. B. Authentifizierung), die als gültig erscheint, als Nutzer ausgeben.	Auswirkung auf verschiedene Risiken
TR109	Ein Angreifer kann eine eingebettete Offenlegungsregelung gegenüber einem Nutzer wiedergeben, um eine genehmigte Abfrage nachzuahmen.	Auswirkung auf verschiedene Risiken
TR110	Ein Angreifer kann den Informationsmangel der Brieftaschennutzer oder unangemessene Verzögerungen nach einer Sicherheitsverletzung oder -beeinträchtigung ausnutzen.	Auswirkung auf verschiedene Risiken
TR111	Ein Angreifer kann eine zuvor installierte rechtmäßige Brieftascheninstanz ändern, um böswillige Merkmale hinzuzufügen.	Auswirkung auf verschiedene Risiken
TR112	Ein Angreifer kann eine rechtmäßige Brieftascheninstanz ändern und sie den Nutzern als rechtmäßige Instanz anbieten.	Auswirkung auf verschiedene Risiken
TR113	Ein Angreifer kann den Nutzerauthentifizierungsmechanismus selbst überwinden, um die Authentifizierung des Brieftaschennutzers zu umgehen.	Auswirkung auf verschiedene Risiken
TR114	Ein Angreifer kann während der Auslieferung an das Gerät des Nutzers böswillige Codes oder Hintertüren in den Brieftaschencode einschleusen.	Auswirkung auf verschiedene Risiken
TR115	Ein Angreifer kann während der Entwicklung böswillige Codes oder Hintertüren in den Brieftaschencode einschleusen.	Auswirkung auf verschiedene Risiken
TR116	Ein Angreifer kann die Generierung von Zufallszahlen verfälschen, um deren Entropie ausreichend zu verringern, sodass Angriffe ermöglicht werden.	Auswirkung auf verschiedene Risiken

Kennung *Kennung*	Beschreibung der Bedrohung *Beschreibung der ermittelten Bedrohung (*)*	Bezeichnung der Risiken *Verbundene Risiken*
TR117	Ein Angreifer kann Nutzergeräte in der Lieferkette manipulieren, um Codes oder Konfigurationen aufzunehmen, die die Bedingungen für die Verwendung der Brieftasche nicht erfüllen.	Auswirkung auf verschiedene Risiken
TR118	Ein Angreifer kann eine Einzelbrieftasche unter Verwendung eines von den Angreifern kontrollierten WSCD aktivieren.	Auswirkung auf verschiedene Risiken
TR119	Ein Angreifer kann die an die WSCA und/oder das WSCD übermittelten Informationen auslesen.	Auswirkung auf verschiedene Risiken
TR120	Ein Angreifer kann willkürliche Informationen an die WSCA senden.	Auswirkung auf verschiedene Risiken
TR121	Ein Angreifer kann Informationen stehlen, indem er die Kommunikation zwischen der WSCA und dem WSCD abfängt.	Auswirkung auf verschiedene Risiken
TR122	Ein Angreifer kann willkürliche Informationen an das WSCD übermitteln.	Auswirkung auf verschiedene Risiken
TR123	Ein Angreifer kann Informationen an das WSCD senden und damit die WSCA umgehen.	Auswirkung auf verschiedene Risiken
TR124	Ein Angreifer kann Phishing nutzen, um Nutzer zu einer gefälschten Brieftasche und PID-Webanwendung zu führen.	Auswirkung auf verschiedene Risiken
TR125	Ein Angreifer kann die Schlüssel einer Brieftasche durch andere Schlüssel ersetzen, um Nachrichten zu erstellen, die dann bei einem anderen Angriff verwendet werden sollen.	Auswirkung auf verschiedene Risiken
TR126	Ein Angreifer kann die Schlüssel einer Brieftasche verändern oder zerstören, wodurch einige Funktionen der Brieftasche unbrauchbar werden.	Auswirkung auf verschiedene Risiken
TR127	Ein Angreifer kann eine Schadsoftware kontrollieren, um auf die in der Brieftasche gespeicherten Daten zuzugreifen.	Auswirkung auf verschiedene Risiken
TR128	Ein Angreifer kann auf die in der Brieftasche generierten Nachweise zugreifen.	Auswirkung auf verschiedene Risiken
TR129	Brieftaschenanbieter können auf Objekte in der Brieftasche zugreifen.	Auswirkung auf verschiedene Risiken
TR130	Brieftaschenanbieter können auf die in der Brieftasche generierten Nachweise zugreifen.	Auswirkung auf verschiedene Risiken
TR131	Ein Angreifer kann eine ungesperrte Brieftasche stehlen.	Auswirkung auf verschiedene Risiken
TR132	Ein Angreifer kann das System manipulieren, um zu verhindern, dass bestimmte Ereignisse protokolliert werden.	Auswirkung auf verschiedene Risiken
TR133	Ein Angreifer kann die Kommunikation zwischen Brieftascheninstanz und WSCA abfangen oder Nutzeraktionen wiedergeben/nachahmen (z. B. durch Übernahme des Authentifizierungsmechanismus).	Auswirkung auf verschiedene Risiken

ANHANG II

KRITERIEN ZUR BEWERTUNG DER ZULÄSSIGKEIT DER SICHERHEITSANGABEN

Bezeichnung	Gegenstand	Zu beachtende Punkte
EUCC	IKT-Produkte	Zum Aussteller: keine (akkreditierte Zertifizierungsstellen) Zum Anwendungsbereich: — Prüfung des Schutzprofils und des Sicherheitsziels — Prüfung des Sicherheitsniveaus der Evaluierung und der Erweiterungen Zur Sicherheit: — Prüfung der Beschränkungen in der Nutzerdokumentation — Für die Zusammensetzung kann der Zugang zum technischen Evaluierungsbericht erforderlich sein.
EUCS (soweit verfügbar)	Cloud-Dienste	Zum Aussteller: keine (akkreditierte Zertifizierungsstellen) Zum Anwendungsbereich: — Prüfung der Beschreibung des Cloud-Dienstes — Prüfung des Evaluierungsniveaus und der Erweiterungsprofile Zur Sicherheit: — Prüfung der Transparenzinformationen und erforderlichenfalls der Angaben zur Zusammensetzung
In der EU betriebene auf den Gemeinsamen Kriterien beruhende Systeme, einschließlich SOG-IS-Systeme	IKT-Produkte	Zum Aussteller: keine (Mitgliedstaaten) Zum Anwendungsbereich: — Prüfung des Schutzprofils und des Sicherheitsziels — Prüfung des Sicherheitsniveaus der Evaluierung und der Erweiterungen Zur Sicherheit: — Prüfung der Beschränkungen in der Nutzerdokumentation — Für die Zusammensetzung kann der Zugang zum technischen Evaluierungsbericht erforderlich sein.
EN 17640:2018 (FITCEM, einschließlich CSPN, BSZ, LINCE, BSZA)	IKT-Produkte	Zum Aussteller: — Prüfung des Systems und der Anforderungen an Zertifizierungsstellen Zum Anwendungsbereich: — Prüfung der Produktbeschreibung — Prüfung der Sicherheitsaussagen — Prüfung des Sicherheitsniveaus Zur Sicherheit: — Prüfung der durchgeführten Tätigkeiten und der Feststellungen im Bericht
Zertifizierungssysteme qualifizierter Signaturerstellungseinheiten (*Qualified Signature Creation Devices*, QSCD) gemäß Artikel 30 der Verordnung (EU) Nr. 910/2014	QSCD	Zum Aussteller: — Prüfung des Systems und der Anforderungen an Zertifizierungsstellen Zum Anwendungsbereich: — Prüfung der Produktbeschreibung — Prüfung der Sicherheitsaussagen — Prüfung des Sicherheitsniveaus Zur Sicherheit: — Prüfung der durchgeführten Tätigkeiten

Bezeichnung	Gegenstand	Zu beachtende Punkte
EN ISO/IEC 27001:2022	ISMS	Zum Aussteller: keine (akkreditierte Zertifizierungsstellen) Zum Anwendungsbereich: — Prüfung der Beschreibung des Managementsystems — Prüfung der Erklärung zur Anwendbarkeit Zur Sicherheit: — Prüfung der durchgeführten Tätigkeiten
SOC2	Organisationen	Zum Aussteller: — Prüfung des Wirtschaftsprüferstatus Zum Anwendungsbereich: — Prüfung der Managementerklärung und der Beschreibung der Kontrollen — Prüfung der Erklärung zur Anwendbarkeit Zur Sicherheit: — Prüfung der Feststellungen im Bericht — Prüfung der Bridge-Letter (bei Bedarf)
MDSCert (GSMA) (soweit verfügbar)	Mobilgeräte	Zum Aussteller: — Prüfung der Anforderungen an Zertifizierungsstellen Zum Anwendungsbereich: — Prüfung des Sicherheitsniveaus — Prüfung der Systemanforderungen Zur Sicherheit: — Prüfung der Tätigkeiten und der Feststellungen im Bericht
Andere Systeme	Alle Komponenten	Zum System: — Prüfung der Relevanz und Bestimmungen des Systems Zum Aussteller: — Prüfung der Anforderungen an Zertifizierungsstellen Zum Anwendungsbereich: — Prüfung der Systemanforderungen — Prüfung des Sicherheitsziels oder eines ähnlichen Dokuments, in dem die Anforderungen an sicherheitsbezogene Funktionen und an das Sicherheitsniveau beschrieben werden — Prüfung der Produktbeschreibung und ausgewählter Anforderungen an die funktionale Sicherheit Zur Sicherheit: — Prüfung der Tätigkeiten und der Feststellungen im Bericht

ANHANG III

FUNKTIONALE ANFORDERUNGEN AN BRIEFTASCHENLÖSUNGEN

Gemäß Artikel 5a Absätze 4, 5, 8 und 14 der Verordnung (EU) Nr. 910/2014 umfassen die funktionalen Kriterien, die eine zertifizierte Brieftaschenlösung und das elektronische Identifizierungssystem, in dessen Rahmen diese bereitgestellt wird, erfüllen müssen, die funktionalen Anforderungen für die folgenden Vorgänge:

1. Durchführungsverordnung (EU) 2024/2979 der Kommission ([1]) 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,
2. Durchführungsverordnung (EU) 2024/2982 der Kommission ([2]) 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,
3. Durchführungsverordnung (EU) 2024/2977 der Kommission ([3]) 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.

([1]) 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).

([2]) 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).

([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).

ANHANG IV

METHODEN UND VERFAHREN FÜR EVALUIERUNGSTÄTIGKEITEN

1. **Prüfung der Umsetzung einer Brieftaschenlösung**

Eine Konformitätsbewertungstätigkeit besteht in der Auswahl bestimmter Evaluierungstätigkeiten.

Die nationalen Zertifizierungssysteme legen eine Evaluierungstätigkeit zur Bewertung der bereitgestellten Informationen fest, die mindestens Folgendes umfasst:

a) eine Analyse der vorgelegten Informationen, um zu bestätigen, dass sie für eine der in den nationalen Zertifizierungssystemen festgelegten Architekturen geeignet sind,

b) eine Analyse der Abdeckung der im Risikoregister gemäß Anhang I verzeichneten Cybersicherheitsrisiken und -bedrohungen durch die beschriebenen Sicherheitskontrollen.

Die unter den Buchstaben a und b genannte Analyse stützt sich auf die Erklärung und Begründung des Brieftaschenanbieters.

2. **Evaluierungstätigkeiten in Verbindung mit dem sicheren Kryptomodul für Brieftaschen**

1. Kritische Vorgänge, einschließlich kryptografischer Berechnungen, müssen nicht vollständig im WSCD umgesetzt werden. Der im WSCD umgesetzte Teil muss jedoch beim Betrieb als Teil der Brieftaschenlösung den Schutz kritischer Vorgänge vor Angriffen durch Angreifer mit hohem Angriffspotenzial gemäß der Durchführungsverordnung (EU) 2015/1502 der Kommission ([1]) gewährleisten.

2. Das WSCD kann ganz oder teilweise Gegenstand der Zertifizierung sein, wenn es vom Zertifikatinhaber oder Antragsteller bereitgestellt wird, oder außerhalb des Zertifizierungsgegenstands liegen, wenn es in ein vom Endnutzer bereitgestelltes Gerät eingebettet ist. Darüber hinaus sind in den nationalen Zertifizierungssystemen die Evaluierungstätigkeiten zur Überprüfung der Eignung des WSCD in den beiden folgenden Fällen festzulegen:

   a) Hängt die WSCA vom jeweiligen WSCD ab (d. h. wenn sie als zusammengesetztes Produkt auf der Grundlage des WSCD bewertet werden muss), dann ist für die Bewertung der WSCA der Zugang zu zusätzlichen Informationen im Zusammenhang mit der WSCD-Zertifizierung, insbesondere zum technischen Evaluierungsbericht, erforderlich;

   b) wenn für eine als Teil des Systems betrachtete Architektur mehrere WSCD verwendet werden oder wenn einige Vorgänge in Bezug auf kritische Werte außerhalb des WSCD durchgeführt werden, müssen die nationalen Zertifizierungssysteme Evaluierungstätigkeiten umfassen, um sicherzustellen, dass die Gesamtlösung das erwartete Sicherheitsniveau bietet.

3. Als Voraussetzung für die Zertifizierung im Rahmen nationaler Zertifizierungssysteme wird das WSCD anhand der in der Durchführungsverordnung (EU) 2015/1502 festgelegten Anforderungen an das Sicherheitsniveau „hoch“ bewertet.

   Sind die Bedingungen in Artikel 3 Absatz 3 Buchstabe b erfüllt, so umfasst die Evaluierung des WSCD oder eines Teils davon eine Schwachstellenbeurteilung gemäß EN ISO/IEC 15408-3:2022 auf Stufe AVA_VAN.5 gemäß Anhang I der Durchführungsverordnung (EU) 2024/482 der Kommission ([2]), es sei denn, es wird gegenüber der Zertifizierungsstelle hinreichend begründet, dass die Sicherheitsmerkmale der WSCA es ermöglichen, ein niedrigeres Bewertungsniveau anzuwenden und gleichzeitig das in der Durchführungsverordnung (EU) 2015/1502 festgelegte Gesamtsicherheitsniveau „hoch“ einzuhalten.

([1]) 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).

([2]) Durchführungsverordnung (EU) 2024/482 der Kommission vom 31. Januar 2024 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC) (ABl. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

4. In den Unterlagen zu jeder einzelnen spezifischen Architektur müssen die nationalen Zertifizierungssysteme darüber hinaus Annahmen für diese Evaluierung des Kryptomoduls für Brieftaschen formulieren, nach denen Angreifern mit hohem Angriffspotenzial gemäß der Durchführungsverordnung (EU) 2015/1502 der Kommission widerstanden werden kann, und die Evaluierungstätigkeiten zur Bestätigung dieser Annahmen sowie zur Bestätigung, dass diese Annahmen nach Ausstellung des Zertifikats nach wie vor überprüft sind, angeben. Die nationalen Systeme verpflichten die Zertifizierungskandidaten, diese Annahmen für ihre spezifische Umsetzung zu verfeinern und die Maßnahmen zu beschreiben, mit denen sichergestellt wird, dass die Annahmen während des gesamten Zertifizierungszyklus überprüft werden.

5. In jedem Fall umfassen die nationalen Zertifizierungssysteme eine Evaluierungstätigkeit, mit der überprüft wird, ob die für das WSCD verfügbaren Sicherheitsangaben für die Zwecke der Brieftaschenlösung geeignet sind, und zwar durch eine Analyse der Sicherheitsangaben, wie z. B. des Sicherheitsziels für EUCC-Zertifikate, einschließlich der folgenden Tätigkeiten:

   a) Überprüfung, ob der Anwendungsbereich der Evaluierung angemessen ist, was z. B. für EUCC-Zertifikate bedeutet, dass für die Sicherheitsziele die Konformität mit einem der im EUCC empfohlenen Schutzprofile geltend gemacht wird,

   b) Überprüfung, ob die Annahmen über die Betriebsumgebung mit der Brieftaschenlösung vereinbar sind, was z. B. für EUCC-Zertifikate bedeutet, dass diese Annahmen im Sicherheitsziel zu finden sind,

   c) Überprüfung, ob die Empfehlungen in der Nutzerleitlinien oder -dokumentation mit den Bedingungen vereinbar sind, unter denen das WSCD in der Brieftaschenlösung verwendet werden soll,

   d) Überprüfung, ob die im nationalen Zertifizierungssystem für WSCDs getroffenen Annahmen überprüft und in den Sicherheitsangaben berücksichtigt sind.

6. In Fällen, in denen einige der Überprüfungen nicht vollständig schlüssig sind, verpflichten die nationalen Zertifizierungssysteme die Zertifizierungsstellen, Kompensationsanforderungen für die auf dem WSCD basierende Kryptoanwendung für Brieftaschen (WSCA) festzulegen, die in die Evaluierung der WSCA aufzunehmen sind. Ist dies nicht möglich, beurteilen die nationalen Zertifizierungssysteme die WSCD als ungeeignet, d. h. für die Brieftaschenlösung wird kein Konformitätszertifikat ausgestellt.

3. **Evaluierungstätigkeiten in Verbindung mit sicheren Kryptoanwendungen für Brieftaschen (WSCA)**

1. Die nationalen Zertifizierungssysteme verlangen, dass eine WSCA als Teil einer Brieftaschenlösung mindestens anhand der in der Durchführungsverordnung (EU) 2015/1502 festgelegten Anforderungen an das Sicherheitsniveau „hoch“ bewertet wird.

2. Diese Evaluierung umfasst eine Schwachstellenbeurteilung gemäß der Norm EN ISO/IEC 15408-3:2022 auf Stufe AVA_VAN.5 gemäß Anhang I der Durchführungsverordnung (EU) 2024/482, es sei denn, es wird gegenüber der Zertifizierungsstelle hinreichend begründet, dass die Sicherheitsmerkmale der WSCA es ermöglichen, ein niedrigeres Bewertungsniveau anzuwenden und gleichzeitig das in der Durchführungsverordnung (EU) 2015/1502 festgelegte Gesamtsicherheitsniveau „hoch“ einzuhalten.

3. Wird die WSCA nicht vom Brieftaschenanbieter bereitgestellt, müssen die nationalen Zertifizierungssysteme Annahmen für diese Evaluierung der WSCA formulieren, nach denen Angreifern mit hohem Angriffspotenzial gemäß der Durchführungsverordnung (EU) 2015/1502 widerstanden werden kann, und die Evaluierungstätigkeiten zur Bestätigung dieser Annahmen sowie zur Bestätigung, dass diese Annahmen nach Ausstellung des Zertifikats nach wie vor überprüft sind, angeben. Die nationalen Systeme verpflichten die Zertifizierungskandidaten, diese Annahmen für ihre spezifische Umsetzung zu verfeinern und die Maßnahmen zu beschreiben, mit denen sichergestellt wird, dass die Annahmen während des gesamten Zertifizierungszyklus überprüft werden.

4. In jedem Fall umfassen die nationalen Zertifizierungssysteme eine Evaluierungstätigkeit, mit der überprüft wird, ob die für die WSCA verfügbaren Sicherheitsangaben für die Zwecke der Brieftaschenlösung geeignet sind, und zwar durch eine Analyse der Sicherheitsangaben, wie z. B. des Sicherheitsziels für EUCC-Zertifikate, einschließlich der folgenden Tätigkeiten:

   a) Überprüfung, ob der Anwendungsbereich der Evaluierung angemessen ist, was z. B. für EUCC-Zertifikate bedeutet, dass für die Sicherheitsziele die Konformität mit einem der im EUCC empfohlenen Schutzprofile geltend gemacht wird,

   b) Überprüfung, ob die Annahmen über die Betriebsumgebung mit der Brieftaschenlösung vereinbar sind, was z. B. für EUCC-Zertifikate bedeutet, dass diese Annahmen im Sicherheitsziel zu finden sind,

c) Überprüfung, ob die Empfehlungen in der Nutzerleitlinien oder -dokumentation mit den Bedingungen vereinbar sind, unter denen die WSCA in der Brieftaschenlösung verwendet werden soll,

d) Überprüfung, ob die im nationalen Zertifizierungssystem für WSCAs getroffenen Annahmen überprüft und in den Sicherheitsangaben berücksichtigt sind.

5. Die nationalen Zertifizierungssysteme verlangen, dass die Evaluierung der WSCA alle von dieser WSCA durchgeführten Sicherheitskontrollen umfasst.

4. **Evaluierungstätigkeiten in Verbindung mit dem Endgerät**

Da im Risikoregister gemäß Anhang I dieser Verordnung Risiken verzeichnet sind, die in direktem Zusammenhang mit der Sicherheit des Endgeräts stehen, werden in den nationalen Zertifizierungssystemen Sicherheitsanforderungen für Endgeräte festgelegt. Da diese Geräte jedoch vom Endnutzer und nicht vom Brieftaschenanbieter bereitgestellt werden, müssen diese Anforderungen durch Annahmen abgedeckt werden.

Für jede Annahme muss die Brieftaschenlösung einen Mechanismus umfassen, mit dem für jede Einzelbrieftasche überprüft wird, ob das zugrunde liegende Endgerät die Annahme erfüllt. Solche Mechanismen gelten als Sicherheitskontrollen und sind Gegenstand von Evaluierungstätigkeiten, um sowohl ihre Eignung als auch ihre Wirksamkeit auf dem entsprechenden Sicherheitsniveau nachzuweisen.

Nachstehend sind zwei Beispiele aufgeführt:

a) Ein Endgerät kann ein zertifiziertes WSCD umfassen, was nachzuweisen ist. In der Regel würde dies mithilfe eines kryptografischen Mechanismus erfolgen, um zu überprüfen, ob im zertifizierten WSCD ein kryptografisches Geheimnis vorhanden ist, das ausschließlich im zertifizierten WSCD verfügbar ist. In diesem Fall sollte dieses kryptografische Geheimnis als kritischer Wert betrachtet werden und unter die Zertifizierung des WSCD und/oder der WSCA fallen.

b) Eine typische Anforderung für Endgeräte wäre, dass die Geräte Sicherheitsaktualisierungen erhalten müssen. Da sich diese Anforderung auf die Brieftascheninstanz bezieht, muss der Mechanismus zur Überprüfung der Verfügbarkeit von Sicherheitsaktualisierungen nur durch Evaluierungstätigkeiten mit einem für die Brieftasche geeigneten Sicherheitsniveau abgedeckt werden, insbesondere da dieser wahrscheinlich in die Brieftasche integriert sein wird.

5. **Evaluierungstätigkeiten in Verbindung mit der Brieftascheninstanz**

1. Bei der Evaluierung der Brieftascheninstanz werden die beiden folgenden wichtigen Herausforderungen berücksichtigt:

   a) Die Brieftascheninstanz wird wahrscheinlich in einer Reihe von Varianten derselben Basisanwendung vorkommen, wobei jede Variante auf eine bestimmte Kategorie von Endgeräten zugeschnitten ist;

   b) die verschiedenen Varianten der Brieftascheninstanz werden wahrscheinlich häufig aktualisiert werden müssen, um mit der Entwicklung der zugrunde liegenden Sicherheitsplattform Schritt zu halten, z. B. wenn Schwachstellen festgestellt werden, die Änderungen an den Anwendungen erfordern.

2. Bei der Evaluierung der Brieftascheninstanz sind diese spezifischen Herausforderungen zu berücksichtigen. Eine der unmittelbaren Folgen besteht darin, dass der Rahmen für Gemeinsame Kriterien möglicherweise nicht in allen Fällen geeignet ist. Daher sind erforderlichenfalls alternative Evaluierungsmethoden in Betracht zu ziehen. Nationale Zertifizierungssysteme berücksichtigen die Anwendung der Methodik der Norm EN 17640:2018 für Folgendes:

   a) als Teil des Systems selbst;

   b) durch nationale, auf der Methodik basierende Systeme;

   c) durch nationale Systeme, die auf ähnlichen Grundsätzen beruhen, aber vor der Aufstellung der Methodik der Norm EN 17640:2018 eingerichtet wurden.

3. Da die Durchführung einer umfassenden speziellen Evaluierung jeder Variante möglicherweise nur einen begrenzten Mehrwert bietet, sollten die nationalen Zertifizierungssysteme darüber hinaus die Festlegung von Kriterien für die Durchführung von Stichproben in Erwägung ziehen, um eine Wiederholung identischer Evaluierungstätigkeiten zu vermeiden und sich auf Tätigkeiten zu konzentrieren, die für eine bestimmte Variante spezifisch sind. Die nationalen Zertifizierungssysteme verpflichten alle Zertifizierungsstellen, ihre Stichprobenverwendung zu begründen.

4. Die nationalen Zertifizierungssysteme müssen Aktualisierungen der Brieftascheninstanz in dem für die Brieftaschenlösung festgelegten allgemeinen Änderungsmanagementprozess umfassen. Sie legen auch Vorschriften für die Verfahren, die der Brieftaschenanbieter für jede Aktualisierung durchzuführen hat (z. B. Analyse der Auswirkungen der Änderungen auf die Sicherheitskontrollen), und für die Evaluierungstätigkeiten fest, die die Zertifizierungsstelle bei Aktualisierungen unter bestimmten Bedingungen durchzuführen hat (z. B. Bewertung der operativen Wirksamkeit einer geänderten Sicherheitskontrolle). Der Änderungsmanagementprozess gehört zu den Prozessen, deren operative Wirksamkeit gemäß Artikel 18 Absatz 3 jährlich überprüft werden muss.

6. **Evaluierungstätigkeiten in Verbindung mit Diensten und Prozessen für die Bereitstellung und den Betrieb der Brieftaschenlösung**

1. Für die Evaluierung von Diensten und Prozessen, die bei der Bereitstellung und dem Betrieb der Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt wird, eine Rolle spielen, sammelt das Evaluierungsteam Nachweise, indem es Evaluierungstätigkeiten durchführt, die Audit-, Inspektions-, Verifizierungs- und Validierungstätigkeiten umfassen können.

2. Die Zertifizierungsstelle vergewissert sich, dass die Nachweise ausreichend und angemessen sind, um eine hinreichende Gewähr dafür zu bieten, dass die Dienste und Prozesse die Zertifizierungsanforderungen erfüllen, indem sie Folgendes bestätigt:

   a) die Richtigkeit der in der Beschreibung der Prozesse und Dienste enthaltenen Informationen,

   b) die Eignung der Konzeption und der Kontrollen der Prozesse und Dienste zur Erfüllung der Evaluierungskriterien,

   c) die operative Wirksamkeit der Durchführung dieser Kontrollen während eines bestimmten Zeitraums vor der Evaluierung.

3. Die Richtigkeit der Beschreibung und der operativen Wirksamkeit eingerichteter Kontrollen kann als Prüfziele (im Sinne der Norm ISO/IEC 17000:2020) in Bezug auf die entsprechenden Aussagen des Brieftaschenanbieters (d. h. Bestätigung der Fairness von Ereignissen, die bereits eingetreten sind, oder bereits erzielte Ergebnisse) betrachtet werden, während die Eignung der Konzeption und der Kontrollen der Dienste und Prozesse zur Erfüllung der Evaluierungskriterien als Validierungsziel (im Sinne der Norm ISO/IEC 17000:2020) in Bezug auf die entsprechenden Aussagen des Brieftaschenanbieters (d. h. Bestätigung der Plausibilität einer beabsichtigten künftigen Verwendung oder eines erwarteten Ergebnisses) angesehen werden kann.

4. Da eine Brieftaschenlösung vor ihrer Zertifizierung nicht betrieben werden darf, kann die operative Wirksamkeit nicht auf der Grundlage des tatsächlichen Betriebs der Lösung bestätigt werden. Dies muss daher anhand von Nachweisen bestätigt werden, die bei Tests oder in Pilotprojekten gesammelt wurden.

5. Nationale Zertifizierungssysteme können bereits für bestimmte Dienste und Prozesse bestehen, z. B. für die Einbindung von Nutzern. Die nationalen Zertifizierungssysteme ziehen gegebenenfalls die Nutzung solcher Systeme in Betracht.

7. **Evaluierungstätigkeiten in Verbindung mit IKT-Diensten für die Bereitstellung und den Betrieb der Brieftaschenlösung**

1. Einige Brieftaschenarchitekturen können für die Bereitstellung und den Betrieb einer Brieftaschenlösung auf spezielle IKT-Dienste, einschließlich Cloud-Dienste, angewiesen sein, und diese Dienste können sensible Daten sowie sensible Vorgänge beinhalten. In diesem Fall werden in den nationalen Zertifizierungssystemen Sicherheitsanforderungen für solche IKT-Dienste festgelegt.

2. Es gibt bereits viele Zertifizierungssysteme für IKT-Dienste, Cloud-Dienste und andere Quellen von Sicherheitsangaben, einschließlich der in Anhang II aufgeführten. Die nationalen Zertifizierungssysteme stützen sich, soweit verfügbar und anwendbar, auf diese bestehenden Mechanismen durch einen der folgenden Mechanismen:

   a) Verpflichtung zur Nutzung eines bestimmten Systems oder einer Auswahl von Systemen, indem die Bedingungen festgelegt werden, unter denen die IKT- oder Cloud-Dienste, die diese Systeme nutzen, zu bewerten sind,

   b) die Wahl der Bewertungsweise wird dem Brieftaschenanbieter überlassen und die Abhängigkeitsanalyse wird genutzt, um die Eignung der durch diese Bewertungen gesammelten Sicherheitsangaben zu analysieren.

3. In beiden Fällen müssen die nationalen Zertifizierungssysteme zusätzliche Evaluierungstätigkeiten festlegen, die erforderlich sind, um die im Rahmen dieser Systeme gewonnenen Informationen zu analysieren oder zu ergänzen.

ANHANG V

VERZEICHNIS ÖFFENTLICH VERFÜGBARER INFORMATIONEN ÜBER BRIEFTASCHEN

1. Die gemäß Artikel 8 Absatz 5 zu veröffentlichenden Informationen umfassen mindestens Folgendes:
   a) etwaige Beschränkungen der Verwendung einer Brieftaschenlösung,
   b) Leitlinien und Empfehlungen des Brieftaschenanbieters zur Unterstützung der Endnutzer bei der sicheren Konfiguration, Installation, Einrichtung, dem Betrieb und der Wartung der Brieftaschen,
   c) Zeitraum, während dessen den Endnutzern eine Sicherheitsunterstützung angeboten wird, insbesondere in Bezug auf die Verfügbarkeit von cybersicherheitsbezogenen Aktualisierungen,
   d) Kontaktangaben des Herstellers oder Anbieters und zulässige Verfahren für den Erhalt von Informationen über Sicherheitslücken von Endnutzern und im Bereich der IT-Sicherheit tätigen Wissenschaftlern;
   e) Verweis auf Online-Register mit öffentlich offengelegten Sicherheitslücken in Bezug auf Brieftaschen und gegebenenfalls relevante Cybersicherheitsratgeber.

2. Die in Absatz 1 genannten Informationen werden allen Personen, die eine Brieftaschenlösung verwenden wollen, in klarer, umfassender und leicht zugänglicher Weise an einer öffentlich zugänglichen Stelle zur Verfügung gestellt.

ANHANG VI

METHODIK ZUR BEWERTUNG DER ZULÄSSIGKEIT DER SICHERHEITSANGABEN

1. Bewertung der Verfügbarkeit von Sicherheitsunterlagen

Die Gutachter führen alle verfügbaren Sicherheitsunterlagen für jede Komponente der Brieftaschenlösung und des elektronischen Identifizierungssystems, in deren Rahmen diese bereitgestellt wird, auf. Anschließend bewerten die Gutachter die Gesamtrelevanz aller Sicherheitsunterlagen für die Abhängigkeitsüberprüfung.

In der Analyse werden folgende Aspekte berücksichtigt:

1. zu den Sicherheitsunterlagen selbst:

   a) Art der Sicherheitsunterlagen mit allen erforderlichen Einzelheiten

   (Beispiele für solche Unterlagen sind Konformitätszertifikate nach EN ISO/IEC 27001:2022 oder Typ 1 oder Typ 2 für ISAE-Berichte),

   b) abgedeckter Zeitraum oder Gültigkeitsdauer

   (dieser Zeitraum kann durch einen Bridge-Letter (ein Dokument, das einen Zeitraum zwischen dem Ende des Berichtszeitraums des aktuellen ISAE-Berichts und der Veröffentlichung eines neuen ISAE-Berichts abdeckt) oder eine ähnliche Erklärung ergänzt werden),

   c) anwendbarer Rahmen (z. B. bestehende Norm),

   d) ob die Sicherheitsunterlagen Angaben zu den Anforderungen des Systems umfasst;

2. fachliche Kompetenz und Unparteilichkeit des Ausstellers des Sicherheitsberichts:

   a) Name der Zertifizierungsstelle und — sofern verfügbar — Name des federführenden Gutachters,

   b) Nachweis der Kompetenz der Zertifizierungsstelle und des Gutachters (z. B. Akkreditierung, persönliche Zertifizierung usw.),

   c) Nachweis der Unparteilichkeit der Zertifizierungsstelle und des Gutachters (z. B. Akkreditierung usw.).

2. Sicherheitsbewertung in Verbindung mit Einzelanforderungen

Die Gutachter überprüfen, ob die für die Brieftaschenlösung und das elektronische Identifizierungssystem, in dessen Rahmen diese bereitgestellt wird, zur Verfügung stehenden Sicherheitsunterlagen geeignet sind, um festzustellen, ob die Brieftaschenlösung den Erwartungen in Bezug auf die Einzelanforderungen des Zertifizierungssystems entspricht.

Diese Bewertung wird für alle relevanten Komponenten der Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt wird, durchgeführt, indem eine Annahme zu den Sicherheitskontrollen der Brieftasche formuliert wird.

Für jede dieser Annahmen prüft das Evaluierungsteam, ob die in den verfügbaren Sicherheitsunterlagen gegebene Gewähr angemessen ist.

Die Feststellung, dass die Sicherheitsgewähr angemessen ist, stützt sich auf Folgendes:

1. Die erforderlichen Informationen mitsamt dem erwarteten Sicherheitsniveau sind in den Sicherheitsunterlagen verfügbar;

2. die in den Sicherheitsunterlagen verfügbaren Informationen decken nicht den gesamten Anwendungsbereich der Anforderung ab, aber zusätzliche Kontrollen oder kompensierende Kontrollen (d. h. interne Kontrollen, die das Risiko bestehender oder potenzieller Kontrollschwächen verringern), die in der Brieftaschenlösung oder im elektronischen Identifizierungssystem, in dessen Rahmen diese bereitgestellt wird, umgesetzt werden, ermöglichen den Gutachtern die Feststellung, dass die Informationen angemessen sind;

3. die in den Sicherheitsunterlagen verfügbaren Informationen bieten nicht das erwartete Sicherheitsniveau, aber die Kontrollen zur Bewertung und Überwachung des Brieftaschenanbieters ermöglichen den Gutachtern die Feststellung, dass die Informationen angemessen sind;
4. werden in den Sicherheitsunterlagen Nichtkonformitäten bei der Konzeption oder Durchführung der Kontrollen der Erfüllung einer Annahme erwähnt, so müssen die vom Brieftaschenanbieter vorgeschlagenen und umgesetzten und von seinen Gutachtern überprüften Abhilfemaßnahmen angemessen sein, um zu gewährleisten, dass die Annahme tatsächlich erfüllt wird.

ANHANG VII

INHALT DES KONFORMITÄTSZERTIFIKATS

1. Eine eindeutige Kennung, die von der Zertifizierungsstelle, die das Zertifikat ausstellt, vergeben wird;

2. Informationen über die zertifizierte Brieftaschenlösung und die elektronischen Identifizierungssysteme, in deren Rahmen diese bereitgestellt wird, und über den Inhaber des Konformitätszertifikats, einschließlich der folgenden Angaben:

   a) Name der Brieftaschenlösung,

   b) Name der elektronischen Identifizierungssysteme, in deren Rahmen die Brieftaschenlösung bereitgestellt wird,

   c) Version der Brieftaschenlösung, die evaluiert wurde,

   d) Name, Anschrift und Kontaktangaben des Inhabers des Konformitätszertifikats,

   e) Link zur Website des Inhabers des Konformitätszertifikats mit den Informationen, die öffentlich zugänglich zu machen sind.

3. Informationen über die Evaluierung und Zertifizierung der Brieftaschenlösung und der elektronischen Identifizierungssysteme, in deren Rahmen diese bereitgestellt wird, einschließlich der folgenden Angaben:

   a) Name, Anschrift und Kontaktangaben der Zertifizierungsstelle, die das Konformitätszertifikat ausgestellt hat,

   b) falls es sich nicht um die Zertifizierungsstelle handelt, Name der Konformitätsbewertungsstelle, die die Evaluierung durchgeführt hat, zusammen mit Angaben zu ihrer Akkreditierung,

   c) Name des Systeminhabers,

   d) Verweise auf die Verordnung (EU) Nr. 910/2014 und die vorliegende Verordnung,

   e) Verweis auf den Zertifizierungsbericht in Bezug auf das Konformitätszertifikat,

   f) Verweis auf den Bericht über die Bewertung der Zertifizierung in Bezug auf das Konformitätszertifikat,

   g) Verweis auf die für die Evaluierung verwendeten Normen, einschließlich ihrer Versionen,

   h) Datum der Ausstellung des Konformitätszertifikats und

   i) Gültigkeitsdauer des Konformitätszertifikats.

ANHANG VIII

INHALT DES ÖFFENTLICHEN ZERTIFIZIERUNGSBERICHTS UND DES BERICHTS ÜBER DIE BEWERTUNG DER ZERTIFIZIERUNG

1. Der öffentliche Zertifizierungsbericht muss mindestens folgende Aspekte umfassen:
   a) Zusammenfassung,
   b) Bestimmung der Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt wird,
   c) Beschreibung der Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen diese bereitgestellt wird,
   d) öffentlich zugänglich zu machende Sicherheitsinformationen gemäß Anhang V oder Verweis auf diese Informationen,
   e) Zusammenfassung des vorläufigen Audit- und Validierungsplans,
   f) Zusammenfassung der Überprüfung und der Zertifizierungsentscheidung.

2. Der Bericht über die Bewertung der Zertifizierung muss mindestens Folgendes enthalten:
   a) eine Beschreibung der Konzeption der Brieftaschenlösung, des Identifizierungssystems und des Einbindungsprozesses zusammen mit der Risikobewertung und dem spezifischen Validierungsplan;
   b) eine Beschreibung, wie die Brieftaschenlösung den Anforderungen des Sicherheitsniveaus „hoch“ entspricht und wie dies durch die Ergebnisse der gemäß dieser Verordnung durchgeführten Zertifizierungsbewertung der Brieftaschenlösung nachgewiesen wird;
   c) eine Beschreibung des Ergebnisses der Bewertung der Konformität der Brieftaschenlösung und des elektronischen Identifizierungssystems, in dessen Rahmen die entsprechenden Einzelbrieftaschen bereitgestellt werden, insbesondere der Konformität mit
      — den in Artikel 5a Absätze 4, 5 und 8 der Verordnung (EU) Nr. 910/2014 festgelegten Anforderungen,
      — der Anforderung der logischen Trennung gemäß Artikel 5a Absatz 14 der Verordnung (EU) Nr. 910/2014,
      — gegebenenfalls den in Artikel 5a Absatz 24 der Verordnung (EU) Nr. 910/2014 genannten Normen und technischen Spezifikationen, wobei zu beschreiben ist, in welchem Verhältnis diese Anforderungen zu den entsprechenden normativen Anforderungen stehen, die von den nationalen Zertifizierungssystemen festgelegt werden;
   d) eine Zusammenfassung der Ergebnisse der Durchführung des Validierungsplans, einschließlich aller festgestellten Nichtkonformitäten.

ANHANG IX

ZEITPLAN FÜR OBLIGATORISCHE ÜBERWACHUNGSEVALUIERUNGEN

1. In Artikel 18 sind die Anforderungen an den Zertifizierungszyklus, insbesondere die Durchführung regelmäßiger Evaluierungstätigkeiten, festgelegt. Diese Aktivitäten umfassen mindestens Folgendes:

   a) eine vollständige Bewertung des Gegenstands der Konformitätsbewertung in der Erstevaluierung und bei jeder Evaluierung zur Neuzertifizierung, einschließlich eines Aktualisierungsmerkmals aller Produktkomponenten;

   b) eine Schwachstellenbeurteilung in der Erstevaluierung und bei jeder Evaluierung zur Neuzertifizierung und mindestens alle zwei Jahre bei Überwachungsevaluierungen, die mindestens die Änderungen des Gegenstands der Konformitätsbewertung und die Veränderungen des Bedrohungsumfelds seit der letzten Schwachstellenbeurteilung umfasst;

   c) zusätzliche Tätigkeiten wie Penetrationstests im Falle eines erhöhten Risikoniveaus oder des Auftretens neuer Bedrohungen;

   d) mindestens einmal jährlich eine Evaluierung der operativen Wirksamkeit der Pflegeprozesse bei Überwachungs- und Neuzertifizierungsevaluierungen, die mindestens die letzten Versionsverwaltungs-, Aktualisierungs- und Schwachstellenmanagementprozesse umfasst;

   e) nach einer erfolgreichen Überprüfungs- und Zertifizierungsentscheidung die Ausstellung eines Konformitätszertifikats nach der Erstevaluierung und nach jeder Evaluierung zur Neuzertifizierung.

2. In Tabelle 1 ist ein Referenzzeitplan auf der Grundlage eines Vierjahreszyklus festgelegt, wobei

   a) Jahr 1 mit der erstmaligen Ausstellung des Konformitätszertifikats beginnt und

   b) alle Evaluierungstätigkeiten innerhalb von 12 Monaten nach der Evaluierung des Vorjahres durchgeführt werden.

3. Der Zeitplan in Tabelle 1 ist eine Empfehlung, um eine rechtzeitige Neuzertifizierung zu gewährleisten und Störungen bei der Bereitstellung der Brieftaschenlösung zu vermeiden. Andere Zeitpläne können möglich sein, sofern die Gültigkeitsdauer des Konformitätszertifikats fünf Jahre nicht überschreitet, wie in Artikel 5c Absatz 4 der Verordnung (EU) Nr. 910/2014 festgelegt.

4. Zusätzlich zu den regelmäßigen Evaluierungen könnte auf Veranlassung der Zertifizierungsstelle oder des Inhabers des Konformitätszertifikats nach einer wesentlichen Änderung des Zertifizierungsgegenstands oder des Bedrohungsumfelds eine Sonderevaluierung ausgelöst werden.

5. Jede Evaluierung, einschließlich Überwachungs- und Sonderevaluierungen, kann zur Ausstellung einem neuen Konformitätszertifikat führen, insbesondere im Falle wesentlicher Änderungen des Zertifizierungsgegenstands, jedoch mit demselben Ablaufdatum wie das ursprüngliche Konformitätszertifikat.

Tabelle 1

Ein vollständiger vierjähriger Evaluierungszyklus

Zeitpunkt	Art der Evaluierung	Tätigkeiten
Jahr 0	Anfänglich	— Vollständige Evaluierung des Gegenstands der Zertifizierung, einschließlich Schwachstellenbeurteilung — — Einschließlich einer Funktion für die Durchführung von Aktualisierungen jeder Softwarekomponente — Evaluierung der Pflegeprozesse, mit Ausnahme ihrer operativen Wirksamkeit — Ausstellung des Konformitätszertifikats und Beginn des Vierjahreszyklus
Jahr 1	Überwachung	— Evaluierung der operativen Wirksamkeit der Pflegeprozesse — — Zumindest Versionsprüfung, Aktualisierungs- und Schwachstellenmanagement — Evaluierung der Änderungen, die sich auf die Sicherheit des Produkts auswirken

Zeitpunkt	Art der Evaluierung	Tätigkeiten
Jahr 2	Überwachung	— Schwachstellenbeurteilung für die Gesamtlösung — Evaluierung der operativen Wirksamkeit der Pflegeprozesse — — Zumindest Versionsverwaltung, Aktualisierungs- und Schwachstellenmanagement — Evaluierung der Änderungen, die sich auf die Sicherheit des Produkts auswirken
Jahr 3	Überwachung	— Evaluierung der operativen Wirksamkeit der Pflegeprozesse — — Zumindest Versionsprüfung, Aktualisierungs- und Schwachstellenmanagement — Evaluierung der Änderungen, die sich auf die Sicherheit des Produkts auswirken
Jahr 4	Neuzertifizierung	1. Vollständige Evaluierung des Gegenstands der Zertifizierung, einschließlich Schwachstellenbeurteilung 2. Vereinfachte Evaluierung für Merkmale/Prozesse, die unverändert geblieben sind 3. Einschließlich einer Funktion für die Durchführung von Aktualisierungen jeder Softwarekomponente 4. Evaluierung der Pflegeprozesse, einschließlich ihrer operativen Wirksamkeit 5. Ausstellung eines neuen Konformitätszertifikats