Secure Elements in eIDAS

Regulatorische Weichenstellung in der EU

Bundesamt
für Sicherheit in der
Informationstechnik

Anforderungen an die EUDI Wallet

Offline Fähigkeit

Zertifizierung

Trackingschutz

Kostenfrei

Große Herausforderungen für Backend/Cloud basierte Lösungen

Secure Element Architekturen in der eIDAS Verordnung

(19) […] Authentifizierung im **Offline-Modus wäre in vielen Sektoren wichtig**, […]. Unter Rückgriff auf das Sicherheitsniveau „hoch“ […] sollten europäische Brieftaschen für die Digitale Identität das Potenzial nutzen, das durch **manipulationssichere Lösungen wie sichere Elemente** geboten wird, um die Sicherheitsanforderungen dieser Verordnung zu erfüllen. […]

(29) Das Ziel dieser Verordnung ist es, den Nutzern eine vollständig mobile, sichere und benutzerfreundliche europäische Brieftasche für die Digitale Identität zur Verfügung zu stellen. Als **Übergangsmaßnahme** bis zur Verfügbarkeit **zertifizierter manipulationssicherer Lösungen, etwa sicherer Elemente innerhalb der Geräte der Nutzer**, sollten europäische Brieftaschen für die Digitale Identität auf zertifizierte **externe sichere Elemente** für den Schutz von kryptografischem Material und anderen sensiblen Daten oder auf **notifizierte elektronische Identifizierungsmittel** mit dem Sicherheitsniveau „hoch“ zurückgreifen können […]

Dezentrale Architektur explizites Ziel für eIDAS Verordnung

Zugang zu Secure Elements

(49) Um das ordnungsgemäße Funktionieren von europäischen Brieftaschen für die Digitale Identität zu gewährleisten, benötigen Anbieter von europäischen Brieftaschen für die Digitale Identität effektive Interoperabilität und **faire, angemessene und diskriminierungsfreie** Bedingungen für den **Zugang** […] zu **spezifischen Hardware- und Softwarefunktionen** mobiler Geräte. Diese Komponenten könnten insbesondere Nahfeldkommunikationsantennen und **sichere Elemente** […] umfassen. […]

Artikel 12b

Zugang zu Hardware- und Software-Funktionen

Wenn Anbieter von europäischen Brieftaschen für die Digitale Identität und Aussteller notifizierter elektronischer Identifizierungsmittel, […] dazu zentrale […] im Zuge der Bereitstellung von Diensten im Zusammenhang mit der europäischen Brieftasche für die Digitale Identität und elektronischen Identifizierungsmitteln an Endnutzer verwenden […] so **ermöglichen Torwächter** ihnen insbesondere wirksame Interoperabilität mit — und **Zugang für Zwecke der Interoperabilität** zu — denselben **Betriebssystem-, Hardware- oder Software-Funktionen**. Im Sinne von Artikel 6 Absatz 7 der Verordnung (EU) 2022/1925 werden diese wirksame **Interoperabilität und der Zugang kostenlos** […] ermöglicht. […]

Secure Element Subgroup

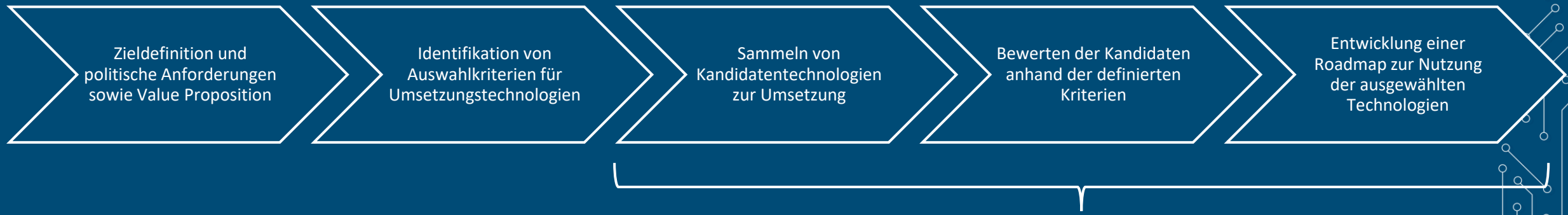
CIR 2024/2981

(8) Vollständig mobile, sichere und benutzerfreundliche Brieftaschen werden durch die Verfügbarkeit **standardisierter und zertifizierter manipulationssicherer Lösungen** wie etwa **eingebetteter sicherer Elemente** […] oder **eingebetteter SIM-Plattformen** in Mobilgeräten unterstützt. Es ist wichtig, den **zeitnahen Zugang zu eingebetteten sicheren Elementen** [..] zu koordinieren. Die […] eingesetzte **europäische 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** […] ausarbeiten und kontinuierlich aktualisieren.

- **Gründung der SE-Subgroup und Auftaktmeeting in Oktober 2025**
- **Mandat:**
  - **Entwicklung einer Roadmap um Zugang zu Secure Elements zu ermöglichen**
  - **Austausch und Zusammenarbeit mit Herstellern zur Identifikation von Barrieren und notwendigen legislativen Änderungen**
- **Ziele:**
  - **Breiten Zugang zu Secure Elements schaffen**
  - **Standards zum Bereitstellen von Applets auf eSE und eSIM identifizieren**
  - **Bereitstellen von PKI Infrastruktur für Provisionierung**

Vision: SE-Subgroup

- **Deutschland übernimmt koordinierende Rolle in der SE-Subgroup**
- **Positionen abgestimmt in Resort übergreifender Arbeitsgruppe unter Leitung des BMDS**
  - **Mit BMG, BMF, BMWK, BSI, etc.**
- **Vorschlag eines Step-by-Step Ansatz für die Arbeit in der Subgroup**



Secure Element Technologien in eIDAS

CIR 2024/2979

Artikel 5

Sichere Kryptoanwendungen für Brieftaschen

[…]

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

Technologien nach Anhang I

SAM.01 Secured Applications for Mobile — Requirements for supporting 3rd party Applets on eSIM and eSE via SAM. v1.1 2023, GSMA;	GPC_GUI_217 GlobalPlatform SAM Configuration Technical specification for implementation of SAM v1.0 2024-04;
GPC_SPE_034 GlobalPlatform Card Specification Technical specification for smart cards v2.3.1 2018-03;	GPC_SPE_007 GlobalPlatform Amendment A Confidential Card Content Management v1.2 2019-07;
GPC_SPE_013 GlobalPlatform Amendment D Secure Channel Protocol 03 v1.2 2020-04;	GPC_SPE_093 GlobalPlatform Amendment F Secure Channel Protocol 11 v1.4 2024-03;
GPD_SPE_075 Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices. v3.3 2018-08, GlobalPlatform.	