bitkom

Stellungnahme

Oktober 2025

Kommentierung der Entwurfsfassung der TR-03189 - EUDI Wallet

Kapitelname	Zeile	Kurzbeschreibung (max. 250 Zeichen)	Kommentar & Änderungsvorschlag
Teil 1 4. Begriffsdefinitionen 5.1 Nutzer	"Die Nutzer der EUDI-Wallet sind natürliche oder juristische Personen, die die Wallet-Instanz verwenden, um PID-Credentials und elektronische Attributsbescheinigungen zu empfangen, zu speichern und vorzuzeigen und ihre Identität nachzuweisen."	Der Begriff der juristischen Person wird an zahlreichen Stellen verwendet, aber zuvor nicht definiert. Dies könnte zu Missverständnissen führen, da die deutsche (v. a. keine Personengesellschaften; oHG/KG) von der europäischen Auslegung abweicht.	Definitionsvorschlag (auch mit Blick auf die Fortentwicklung zur European Business Wallet): Juristische Person im Sinne der eIDAS-Verordnung sind alle Einheiten, denen ein Recht zustehen kann, unabhängig von ihrer genauen nationalen Einordnung; eine eigene bzw. gesonderte Rechtspersönlichkeit wird nicht vorausgesetzt. Eine juristische Person ist damit zusätzlich jede Einheit, unabhängig von ihrer Rechtsform, die eine wirtschaftliche Tätigkeit ausübt. Dazu gehören insbesondere auch jene Einheiten, die Tätigkeiten als Einpersonen ausüben, sowie Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen (vgl. Art. 1 des Anhangs der Empfehlung 2003/361/EG der Kommission).
Teil 1 5.1 Anbieter qualifizierter elektronischer Signaturen und Siegeln	"Nach Artikel 5a lit. g müssen alle natürlichen Personen diese Möglichkeit kostenlos erhalten."	Es wird ausgeführt, dass nach Art. 5a lit. g alle natürlichen Personen diese Möglichkeiten kostenlos erhalten müssen. Dies ist rechtlich ungenau (Zitierweise und Inhalt).	Art. 5a Abs. 5 UAbs. 1 Buchst. g eIDAS-Verordnung sieht zwar vor, dass die EUDI-Wallet allen natürlichen Personen die Möglichkeit bieten muss, mittels qualifizierter elektronischer Signaturen kostenlos zu unterzeichnen. Dieser Rechtssatz wird allerdings durch Art. 5a Abs. 5 UAbs. 2 eIDAS-Verordnung relativiert. Danach können die Mitgliedstaaten verhältnismäßige Maßnahmen vorsehen, um sicherzustellen, dass die kostenlose Verwendung qualifizierter elektronischer Signaturen durch natürliche Personen auf nichtgewerbliche Zwecke beschränkt wird.

Kapitelname	Zeile	Kurzbeschreibung (max. 250 Zeichen)	Kommentar & Änderungsvorschlag
Teil 1 5.2.1 Komponenten der Wallet-Services	"die Identifizierung des Nutzers auf Basis der Online-Ausweisfunktion um die Ausstellung eines PID-Credentials zu ermöglichen"	Nach den Ausführungen erfolgt die Identifizierung des Nutzers auf Basis der Online-Ausweisfunktion um die Ausstellung eines PID-Credentials zu ermöglichen.	Der Begriff Nutzer umfasst natürliche und juristische Personen. Eine Online-Ausweisfunktion existiert allerdings nur für natürliche Personen, weswegen unklar ist, ob die Formulierung dies bereits auf diesen Personenkreis verengen soll. Falls mit Online-Ausweisfunktion auch ein künftiges Ausweismittel für juristische Personen gemeint ist, sollte der Begriff Online-Ausweisfunktion zuvor definiert werden (Formulierungsbeispiel: bereits und künftig bestehende Identitätsnachweise).
Teil 1 5.2.1 Komponenten der Wallet-Services Teil 2 2.2.2.1 Registrierung und Identifizierung Teil 3 3.1.2 eID-Client	"die Identifizierung des Nutzers auf Basis der Online-Ausweisfunktion um die Ausstellung eines PID-Credentials zu ermöglichen" 2) "Die Identifizierung des Nutzers gegenüber dem PID-Provider MUSS mit der Online-Ausweisfunktion auf Vertrauensniveau „hoch“ durchgeführt werden." 1) " Der eID-Client bietet eine Schnittstelle zur Online-Ausweisfunktion."	Nach den Ausführungen erfolgt die Identifizierung des Nutzers auf Basis der Online-Ausweisfunktion um die Ausstellung eines PID-Credentials zu ermöglichen. Ein eID-Client ist erforderlich.	Es sollten auch andere Einrichtungsmöglichkeiten eingeführt werden abseits der Online-Ausweisfunktion. 1) Die Einrichtung der Wallet kann auch bei der Ausgabe des Ausweises erfolgen und so dem Nutzer eine einfache Möglichkeit zur Einrichtung geben. Man hat in diesem Prozess, die Möglichkeit, den Benutzer vorab zu informieren, so dass er weiterhin auch die Chance hat zum Beispiel eine Wallet vorab zu informieren und zur Einrichtung bereit zu halten. 2) Auch ist eine Einrichtung bei der Beantragung eines neuen Ausweises denkbar und in den Prozess integrierbar. Beides hat den Vorteil, die Hürde für den Einstieg in die Wallet-Nutzung zu senken und somit das Benutzererlebnis und die Akzeptanz zu steigern. Weiterhin kann dies auch den Aufwand auf Behördenseite verringern, in dem man keine weiteren (Zwischen)Schritte für die Einrichtung der Online-Ausweisfunktion benötigt. Zudem legt die eIDAS-Richtlinie Kriterien für sichere Identifizierung von Personen fest. Jedes nach eIDAS als hoch sicher geprüfte Verfahren sollte neben der Online-Ausweisfunktion zum Einsatz kommen können. Die eIDAS-Novelle sieht explizit vor, dass auch andere Verfahren zulässig sind, sofern sie von einer akkreditierten Konformitätsbewertungsstelle (KBS) zertifiziert wurden, z.B.: - eIDAS LoA „high“, - ETSI TS 119 461 Extended LoIP (Entspricht dem eIDAS-Vertrauensniveau „hoch“) - oder eIDAS-konforme qualifizierte elektronische Signaturen (QES; vgl. Artikel 24 Abs. 1a Buchst. c eIDAS-VO), Nur so kann die notwendige technologische Offenheit, Nutzerfreundlichkeit und Innovationskraft für die EUDI-Wallet gewährleistet werden.

Kapitelname	Zeile	Kurzbeschreibung (max. 250 Zeichen)	Kommentar & Änderungsvorschlag
Teil 2 2.2.1 Provisionierung	2) "Im provisionierten Zustand DARF die Wallet NICHTS anderes können, als die Registrierung zu starten."	Frisch provisionierte Wallet darf nur Registrierungen starten.	Diese Anforderung schränkt die Nutzerfreundlichkeit von EUDI-Wallet-Lösungen stark ein. Es ist nach dieser Vorgabe nicht erlaubt, dem Nutzer eine Applikation anzubieten, die über den Rahmen einer reinen EUDI-Wallet hinaus nützlich ist. Es ist insbesondere nicht möglich eine Applikation anzubieten, die eine EUDI-Wallet-Funktion als Modul oder Komponente beinhaltet.
Teil 2 2.2.2 Personalisierung	5) "Ein Authentisierungsfaktor „Wissen“ MUSS festgelegt werden."	Ein Authentifizierungsfaktor "Wissen" MUSS festgelegt werden.	Die Einschränkung auf Wissensfaktoren ist nicht nachvollziehbar und schränkt die Nutzerfreundlichkeit ein. Ein biometrischer Faktor kann für ausreichende Sicherheit sorgen und sollte ebenfalls erlaubt sein.
Teil 2 2.2.2.2 Aktivierung Teil 3 3.1.3.2 Aktivierung	2) "Der Nutzer MUSS eine Nutzer-PIN setzen und MUSS dazu den Aktivierungscode verwenden." 1) "Die Aktivierung einer Wallet-Instanz MUSS über das Wallet User Interface und nach Erhalt des Aktivierungscodes angestoßen werden."	Der Nutzer muss den Aktivierungscode aktiv verwenden.	Die Eingabe eines Aktivierungscodes durch den Nutzer ist keine angenehme User Experience. Wenn die Registrierung und Aktivierung in einem Prozess erfolgen, sollte kein Prozessbruch dieser zwei Schritte erfolgen, da dies für den Nutzer nicht nachvollziehbar ist und keinen Sicherheitsvorteil bietet. Es sollte möglich sein, Registrierung und Aktivierung in einem Prozess abzubilden, ohne dass der Nutzer Aktivierungscodes oder ähnliches selbst handhaben muss.
Teil 2 2.3.1 Ziele - Widerruf	9) "Der Nutzer MUSS innerhalb von 12h über spezielle sichere Kanäle über den Widerruf und die Gründe des Widerrufes in klarer und einfacher Sprache informiert werden."	Der Nutzer muss über den Widerruf seiner Credentials innerhalb von 12h informiert werden.	Die Richtlinie spricht von "speziellen sicheren Kanälen", definiert aber keine Anforderungen dafür und gibt keine Beispiele. Es ist nicht ersichtlich was einen Kanal speziell oder sicher macht. Dies sollte konkretisiert werden, um angemessene Lösung anbieten zu können. Dazu muss geklärt werden, in welcher Zeitzone die Frist gerechnet wird und ab wann die Frist genau beginnt.
Teil 3 4 WSCD, WSCA und Hardwaresicherheit	"Das Remote Wallet Secure Cryptographic Device (WSCD) ist ein gehärtetes Hardwaremodul, das zur Absicherung der kritischen Assets und Operationen von dem Wallet Secure Cryptographic Application	Die Einführung beschreibt das WSCD - eine Einschränkung auf ein Remote WSCD ist nicht erforderlich	"Remote" streichen in "Das Remote Wallet Secure Cryptographic Device (WSCD)...". Kapitel 4 sollte technologieoffen formuliert werden und die Möglichkeiten aus dem ARF zu WSCA (Trusted Service App, JavaCard Applet, OS) und WSCD (Remote-HSM, Local External-Smart Card, Local-eSIM/eSE und Local native) beinhalten.

Kapitelname	Zeile	Kurzbeschreibung (max. 250 Zeichen)	Kommentar & Änderungsvorschlag
	(WSCA) verwendet werden kann."		
Teil 3 4.2 Funktionsumfang	"Damit kann die hohe Sicherheit der Hardwareplattform (WSCD) kombiniert werden mit der besseren Ansprechbarkeit eines gehärteten Servers (WSCA)."	Die Hardewareplattform (WSCD) mit einem gehärteten Server (WSCA) ist nur eine Ausprägung.	Weitere Möglichkeiten ergänzen
Teil 3 4.3 Zertifizierung	"Damit ergeben sich folgende minimale Anforderungen an die Plattform: - Konformität zu PP.EN.419.221.5, in Kombination mit PP.EN.419.241.2, vgl. CIR.2024.482, Annex II - Einsatz in einer sicheren Umgebung, die nach IT-Grundschutz des BSI zertifiziert ist"	Den Einsatz verschiedener WSCDs zulassen. Die Anforderungen für die Zertifizierung des WSCD offen für alle im ARF genannten Ausprägungen beschreiben.	Die Zertifzierung sollte offen für weitere WSCD Ausprägungen aus dem ARF sein. Im ARF werden neben dem Remote WSCD (HSM) auch Local External (Smart Cards), Local (eSIM/eSE) und Local native als WSCDs genannt. Neben den Anforderungen für ein Remote WSCD, sollte eine Zertifizierung dieser Komponenten (zukünftig) möglich sein und ergänzt werden.
Teil 4 3.3.3 Sperrdienst	1) "Vor Sperrung einer Wallet-Unit MUSS der Antrag erfolgreich authentifiziert werden"	Der Nutzer muss bei Anträgen auf Sperrung authentifiziert werden.	Die Authentifizierungsmöglichkeiten, die vorgeschrieben sind lassen Lücken, die im aktiven Betrieb zu Problemen führen werden: Der Nutzer braucht Zugriff entweder auf die Wallet-Instanz oder das zur Aktivierung verwendete Identifikationsmittel. In alltäglichen Situationen werden beide gleichzeitig nicht mehr Verfügbar sein, bspw. im Falle von Diebstahl oder Verlust einer Handtasche. Die Authentifizierungsmethoden für Nutzer zur Sperrung der Wallet-Unit sollten alltägliche Situation mit berücksichtigen.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Lorène Slous | Referentin Vertrauensdienste & Digitale Identitäten
T 030 27576-157 | l.slous@bitkom.org

Verantwortliches Bitkom-Gremium

AK Anwendung elektronischer Vertrauensdienste