bitkom

Stellungnahme

Mai 2026

Bitkom-Kommentierung der Entwurfsfassung der TR-03189 zur Zertifizierung der EUDI-Wallet (Version 0.9.1)

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
Übergreifend	Zertifizierung	Die Spezifikation behandelt nicht, ob eine in einem anderen Mitgliedstaat zertifizierte Wallet in Deutschland ohne erneute Zertifizierung gemäß TR-03189 anerkannt wird. Wenn eine eigenständige deutsche Zertifizierung unabhängig von einer EU-Zertifizierung gemäß CIR 2024/2981 erforderlich ist, ergibt sich ein nationaler Zertifizierungsaufwand, der über die EU-Ebene hinausgeht. Wir regen eine ausdrückliche Behandlung des Verhältnisses zwischen EU-weiter und nationaler Zertifizierung an, einschließlich der Frage, welche Nachweise aus der EU-Zertifizierung übernommen werden können.	Fehlende Inhalte
Übergreifend	Geltungsbereich	Die Spezifikation richtet sich primär an die im Inland etablierte Wallet-Provider, PID-Provider und Relying Parties. Die Anforderungen an grenzüberschreitende Aussteller von EAAs, deren regulatorische Heimatzuordnung in einem anderen Mitgliedstaat liegt (Stichwort: Notifizierungspfad in Deutschland), werden nicht explizit behandelt. Wir regen eine Ergänzung an, die das Registrierungs- und Aufsichtsverhältnis grenzüberschreitender EAA-Aussteller gegenüber dem deutschen Ökosystem klarstellt.	Fehlende Inhalte
Übergreifend		Die TR sollte vermeiden, nationale Zusatzanforderungen („Gold-Plating“) einzuführen, die über das eIDAS-Regelwerk	Fehlende Inhalte

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
		hinausgehen und die europäische Interoperabilität sowie den Marktzugang unnötig einschränken.	
Übergreifend		Die TR sollte klarstellen, dass Interoperabilität und Marktzugang für Wallet-Provider, PID-Provider und Relying Parties integrale Ziele sind, sofern die Sicherheitsanforderungen erfüllt werden.	Fehlende Inhalte
1	1	Die Spezifikation schließt Vor-Ort-Szenarien und Offline-Funktionalität explizit aus. Dies steht im Spannungsverhältnis zu Art. 5a Abs. 4 lit. a eIDAS-VO, der die Offline-Nutzung der Wallet als Grundfähigkeit vorsieht. Wir regen an, einen Fahrplan für eine zukünftige Offline-Spezifikation aufzunehmen sowie zu definieren, unter welchen Bedingungen kurzfristige Offline-Token bei eingeschränkter WSCA-Verfügbarkeit zulässig sind. Andernfalls bleiben Anwendungsfälle am stationären POS und im Nahverkehr architektonisch ausgeschlossen.	Fehlende Inhalte
1	2	Die TR wird als zentraler Sicherheits- und Qualitätsrahmen für EUDI-Wallets ausdrücklich begrüßt. Ergänzend sollte klarer hervorgehoben werden, dass die TR einen Mindeststandard definiert und technologieoffene Umsetzungen zulässt, sofern das Vertrauensniveau „hoch“ nach eIDAS nachweislich erreicht wird.	Fehlende Inhalte
1	2	Die TR sollte klarstellen, dass sie den staatlichen Rahmen für Sicherheit und Interoperabilität definiert, ohne einzelne technische Lösungen oder Geschäftsmodelle zu bevorzugen. Wettbewerb, Wahlfreiheit und Beteiligung privater Anbieter sind integraler Bestandteil eines funktionierenden EUDI-Ökosystems.	Fehlende Inhalte
1	3.1	Die Spezifikation definiert ausschließlich die serverseitige HSM-Architektur. Auf eine zukünftige Berücksichtigung gerätegebundener Architekturen (Secure Element / TEE) wird hingewiesen, ohne Zeitplan oder Profil zu nennen. Wir regen an, einen indikativen Zeitplan für die Veröffentlichung eines gerätegebundenen Profils sowie eine Aussage zur Gleichwertigkeit der Zertifizierungspfade zu ergänzen. Ohne diese Planungsgrundlage ist eine mobil-native Wallet-Umsetzung gemäß den vorherrschenden iOS- und Android-Sicherheitsmodellen nicht möglich.	Fehlende Inhalte
1	4.8	Die Lebenszyklus-Darstellung legt eine Sperrfrist von einer Stunde für den Fall des Versterbens des Nutzers fest. Gleichzeitig wird festgestellt, dass der Mechanismus für die Entgegennahme	Inhaltlich prüfen

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
		entsprechender Sterbemeldungen noch nicht abschließend definiert ist. Eine SLA ohne definierten Meldemechanismus erzeugt eine operative Verpflichtung, die nicht planbar umgesetzt werden kann. Wir regen an, die SLA bis zur Definition des Meldemechanismus zurückzustellen oder die zulässigen Meldequellen (z. B. Standesamt-Schnittstellen) und eine Schnittstellenspezifikation zu ergänzen.	
1	5 (PKI.WUA.Revo.5 / PKI.PIDCr.Revo.7)	Die maximale Bearbeitungszeit für Sperrvorgänge von 24 Stunden in Verbindung mit der Pflicht zur Gültigkeitsprüfung der WUA bei jedem WSCA-Zugriff (PKI.WUA.Revo.3) ergibt eine permanente Online-Liveness-Abhängigkeit. Wir regen an klarzustellen, ob für definierte Anwendungsfälle (z. B. Wiederholpräsentationen innerhalb einer kurzen Zeitspanne) eine begrenzte Zwischenspeicherung des Sperrstatus zulässig ist, und falls ja, mit welcher maximalen Cache-Lebensdauer.	unklar
1	5	Die maximale Gültigkeitsdauer der Zertifikate für PID-Provider und Wallet-Provider beträgt sechs Monate. Eine Spezifikation der Erneuerungsfristen sowie der Vorlaufzeiten für die Bereitstellung neuer Zertifikate ist nicht enthalten. Wir regen eine Klarstellung an, dass Erneuerungen mit einer Mindestvorlaufzeit (z. B. 60 Tage) bereitgestellt werden und dass eine definierte Übergangsphase nach Ablauf des alten Zertifikats vorgesehen wird, um Betriebsunterbrechungen zu vermeiden.	Anforderung schärfen
2	3.3.1.3 (WI.Backup.O.BLOCK)	Die Spezifikation verbietet den Export bzw. die Wiederherstellung von PID-Credentials und personengebundenen EAAs. Bei jedem Gerätewechsel ist eine Neuausstellung sämtlicher personengebundener EAAs durch alle betroffenen Aussteller erforderlich. Wir regen an, die Spezifikation um eine Empfehlung zur ausstellerseitigen Erkennung von Gerätewechseln sowie um eine Klarstellung zur Behandlung verwaister Credentials auf nicht mehr aktiven Geräten (Bereinigung der Sperrlisten) zu ergänzen.	Fehlende Inhalte
2	3.3.1.4 (WI.Log.F.DATAb / WI.Pres.Req.LOG)	Sämtliche Präsentationsversuche werden in der Wallet protokolliert, einschließlich gescheiterter Versuche. Eine Unterscheidung zwischen technischen Fehlern (z. B. Verbindungsabbruch) und Policy-Ablehnungen (z. B. Ablehnung einer überschießenden Attributanfrage) ist nicht vorgesehen. Wir regen eine Differenzierung im Log an, damit Relying Parties Konfigurationsfehler in ihrer Registrierung erkennen können.	Anforderung schärfen

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
2	3.3.3.1 (WI.RPIdent.Req.ACCEmpty / WI.RPIdent.Req.CERTa)	Eine Präsentationsanfrage ohne gültiges Zugangszertifikat wird durch die Wallet ohne Übergangsfrist zwingend abgelehnt. Wir regen an, eine kurze Toleranzphase nach Ablauf des Zertifikats (z. B. 48 Stunden) für laufende Transaktionen vorzusehen, um Dienstunterbrechungen während der Zertifikatserneuerung zu vermeiden. Ergänzend sollte die Wallet den Nutzer im Falle eines abgelaufenen RP-Zertifikats über den konkreten Grund informieren, statt einen generischen Fehler anzuzeigen.	Anforderung lockern
2	3.3.3.1 (WI.RPIdent.Req.REGEmpty)	Die Spezifikation verweist auf das Register des Registrars für die Registrierungsinformationen einer Relying Party, ohne den Registrar für Deutschland zu benennen oder Prozess, Fristen und Schnittstellen zu beschreiben. Wir regen an, die zuständige Stelle, das Registrierungsverfahren und den Zeitplan für die Betriebsbereitschaft des Registrars zu ergänzen, da die RP-Registrierung eine harte Voraussetzung für jede Präsentation ist.	Fehlende Inhalte
2	3.3.3.2 (WI.RequV.Req.PSEUD)	Die Wallet ist verpflichtet zu prüfen, ob eine Identifikation rechtlich erforderlich ist, und andernfalls die Nutzung eines Pseudonyms anzubieten. Die Spezifikation lässt offen, anhand welcher Felder in der Registrierungsbescheinigung die Wallet diese Bestimmung trifft. Wir regen eine Präzisierung des Inhalts und der Struktur der Rechtsgrundlage-Felder in der RP-Registrierung an, einschließlich einer Behandlung von Pflichten nach VO (EU) 2024/1620 (AMLR), bei denen die Rechtsgrundlage für die Identifikation eindeutig vorliegt.	unklar
2	3.3.3.3 (WI.Discl.Req.USE / WI.Discl.Req.DISCL)	Das Disclosure-Authorization-Modul prüft die eingebettete Offenlegungs-Policy einer EAA gegen die RP-Registrierung. Die Spezifikation lässt offen, wie sich Policies vom Typ „nur autorisierte Relying Parties" auf Intermediär-Konstellationen nach Art. 5b Abs. 10 eIDAS-VO auswirken. Wir regen eine Klarstellung an, ob ein Intermediär in die Liste der autorisierten Relying Parties aufgenommen werden muss oder ob die zugrundeliegende End-RP für die Berechtigungsprüfung maßgeblich ist.	unklar
2	3.3.4.3	Die Spezifikation stellt fest, dass eine Offline-Funktionalität gemäß Art. 5a Abs. 4 lit. a eIDAS-VO aufgrund der Remote-WSCA-Architektur nicht anwendbar ist. Damit entfällt die Eignung der deutschen Wallet für eine Vielzahl von Anwendungsfällen am stationären Point-of-Sale. Wir regen an, eine Aussage zur Behandlung dieser Lücke gegenüber den eIDAS-Anforderungen aufzunehmen und einen Pfad für eine zukünftige Offline-Fähigkeit zu skizzieren.	Fehlende Inhalte

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
2	3.3.8.6 (WI.EAAEnrol.Req.BATCH)	Die Mehrfach-Ausstellung von EAAs wird als optional („KANN") definiert. Für eine planbare Skalierung der Ausstellung benötigen EAA-Provider Klarheit darüber, ob zertifizierte Wallets diese Funktion unterstützen. Wir regen entweder eine Hebung auf „MUSS" an oder die Pflicht der Wallet, ihre Batch-Unterstützung in maschinenlesbarer Form zu veröffentlichen, damit Aussteller ihre Ausstellungsprozesse entsprechend gestalten können.	Anforderung schärfen
2	3.3.8.6 (WI.EAAEnrol.Req.AUTHa)	Personengebundene EAAs erfordern eine starke Nutzerauthentifizierung (Strong User Authentication) je Ausstellung. In der Remote-WSCA-Architektur bedeutet dies einen Backend-Roundtrip je EAA, was bei mehreren Ausstellungsvorgängen zu erheblicher kumulativer Reibung führt. Wir regen an, ein Sitzungsmodell zuzulassen, in dem mehrere personengebundene EAAs innerhalb einer einzigen Authentifizierungssitzung mit getrennter Einwilligung je Credential ausgestellt werden können.	Anforderung lockern
2	3.3.9 (WI.WUI.Req.REAUTH)	Die Empfehlung einer Wallet-Reauthentifizierung nach maximal fünf Minuten Inaktivität kann zu Reibungen mit den SCA-Sitzungsdauern nach PSD2/PSD3 führen, insbesondere bei Zahlungsabläufen, die nach kurzer Inaktivität fortgesetzt werden. Wir regen eine Klarstellung an, wie das Verhältnis zwischen Wallet-Reauthentifizierungszeit und SCA-Sitzungsgültigkeit harmonisiert werden soll, um doppelte Authentifizierungen zu vermeiden.	unklar
3	2 Betriebsumgebung	Die Anforderung, WSCA und WSCD im selben Serverraum desselben Rechenzentrums zu betreiben, ist restriktiv formuliert und schließt geographisch verteilte sowie cloud-native Architekturen aus, ohne dass das zugrundeliegende Schutzziel zwingend eine physische Raumgrenze erfordert. Wir regen an, die Anforderung präziser zu fassen, sodass auch kryptographisch isolierte WSCA-WSCD-Paare an voneinander getrennten zertifizierten Standorten zulässig sind, sofern eine dokumentierte Bedrohungsanalyse die Gleichwertigkeit nachweist.	Anforderung lockern
3	4 Zertifizierung	EUCC EAL4 mit AVA_VAN.5 wird für die WSCD über alle drei Implementierungsvarianten hinweg gefordert. Damit verlieren die Varianten ihre differenzierende Wirkung, und der Markt verfügbarer Produkte sowie Anbieter wird auf eine sehr kleine Auswahl reduziert. Wir regen an klarzustellen, ob die Varianten in ihrem Zertifizierungsumfang differenziert werden sollten (z. B. niedrigere Assurance für Orchestrierungskomponenten in Variante 3, sofern die	Inhaltlich prüfen

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
		WSCA selbst keine Schlüsseloperationen ausführt), und die jeweiligen Grenzen explizit zu dokumentieren.	
3	7.4 Authentifizierung (WSCA.AUTHF.O.2)	Die Anforderung verbietet den Einsatz biometrischer Verfahren als direkten Authentifizierungsfaktor gegenüber der WSCA; Biometrie darf lediglich einen Besitzfaktor freischalten. Diese Festlegung weicht von etablierten Verbraucher-Authentifizierungsmustern ab, in denen hardwaregebundene Biometrie als starker dynamischer Besitznachweis dient. Wir regen an, Biometrie unter dokumentierten Bedingungen als direkten Faktor zuzulassen, sofern das biometrische Matching geräteseitig in einer hardwareisolierten Umgebung erfolgt, das Template das Gerät nie verlässt und Fehlerraten durch veröffentlichte Plattformspezifikationen begrenzt sind.	Anforderung lockern
3	7.4 Authentifizierung (WSCA.AUTHF.O.1 / WSCA.AUTHF.O.4)	Nach drei Fehlversuchen wird das KFVM unwiderruflich gesperrt; die Wiederherstellung erfordert eine vollständige Neu-Ausstellung sämtlicher Credentials. Diese harte Sperrlogik erzeugt einen erheblichen operativen Aufwand für Aussteller und Nutzer, wenn Sperrungen durch Nutzerverhalten und nicht durch Sicherheitsereignisse ausgelöst werden. Wir regen an, eine gestaffelte Sperrlogik (zeitliche Verzögerung statt sofortiger destruktiver Sperrung) vorzusehen sowie einen Wiederherstellungspfad zu definieren, der Aussteller-Vertrauensbeziehungen erhält, auch wenn Nutzerschlüssel neu erzeugt werden müssen.	Anforderung lockern
3	2 Architektur (WSCA.Target.4)	Die Spezifikation untersagt jeden parallelen Sicherheitspfad für LoA-High-Operationen außerhalb der WSCA. Hybride Architekturen mit Fallback-Pfaden zur Verbesserung von Verfügbarkeit oder Resilienz sind damit ausgeschlossen. Wir regen eine Klarstellung an, ob Hochverfügbarkeits-Konfigurationen mit redundanten zertifizierten WSCA-Instanzen zulässig sind, und falls ja, unter welchen Bedingungen.	unklar
3	5.2 Mehrmandantenfähigkeit (WSCA.LCR.Base.3)	Die Trennung der Nutzerbereiche auf mehrmandantenfähigen Plattformen wird gefordert, ohne dass das Partitionierungsschema, die Performanz-Eigenschaften oder die Zertifizierungs-Geltungsgrenzen technisch spezifiziert werden. Bei nationaler Skalierung auf gemeinsam genutzter Infrastruktur entstehen erhebliche Umsetzungsunsicherheiten, die erst im Zertifizierungsdialog mit dem BSI geklärt würden. Wir regen an, ein	Fehlende Inhalte

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
		bestehendes Standardverfahren zu referenzieren oder die Anforderung detaillierter zu spezifizieren.	
3	2 Security Target	Die Spezifikation verlangt die Veröffentlichung eines WSCA Security Target als zentrale Zertifizierungsgrundlage, gibt jedoch über die Funktionsverteilung zwischen WSCA und WSCD hinaus weder Umfang, Format noch Inhalt vor. Für Erst-Antragsteller besteht damit ein erhebliches Risiko divergierender erster Einreichungen. Wir regen an, eine Vorlage, ein annotiertes Beispiel oder eine detaillierte Inhaltscheckliste für das Security Target zu ergänzen.	Fehlende Inhalte
3	7 Verfügbarkeit	Die Spezifikation enthält keine Anforderungen an Verfügbarkeit (SLA), Wiederherstellungszeit (RTO) oder Disaster-Recovery für WSCA und WSCD. Aus Art. 5b eIDAS-VO ergeben sich Verpflichtungen zur Dienstkontinuität, ohne dass ein technisches Mindestmaß spezifiziert ist. Wir regen an, eine Mindest-Verfügbarkeit (z. B. 99,9 Prozent monatlich mit definierten Ausnahmen), eine maximale RTO sowie Anforderungen an die Standort-Redundanz zu spezifizieren.	Fehlende Inhalte
4.1	2.2.3.3 WP.WRevoc	Die Spezifikation sieht vor, dass der Wallet-Provider den PID-Provider bei Sperrungen der WUA informieren kann. Eine entsprechende Verpflichtung gegenüber EAA-Ausstellern fehlt. EAA-Aussteller können Sperrungen nur durch Polling der öffentlichen Statusliste erkennen, was bei latenzkritischen Präsentationsabläufen problematisch ist. Wir regen an, eine Push-Benachrichtigungs-Schnittstelle vom Wallet-Provider zu abonnierten EAA-Ausstellern zu definieren, beschränkt auf Sperrereignisse, die deren Credentials betreffen.	Fehlende Inhalte
4.1	2.2.5.3 WP.WIDB (WP.WIDB.Req.INAKT)	Nach WSCA-Registrierung wird die Wallet mit einer Aktivierungsfrist von einem Monat in den inaktiven Zustand versetzt. Bleibt die Aktivierung aus, kann die Wallet keine PIDs oder EAAs entgegennehmen. Die Spezifikation legt nicht fest, wie Aussteller diesen Zustand erkennen können; Ausstellungsversuche scheitern in einer für den Aussteller nicht von transienten Fehlern unterscheidbaren Weise. Wir regen eine Spezifikation der Fehlerantwort und des Fehlercodes für Ausstellungsversuche gegenüber inaktiven Wallets an.	Fehlende Inhalte
4.1	2.2.2.5 WP.DevHealth	Die Kriterien des Device Health Attestation Moduls werden durch den Wallet-Provider kontrolliert und mindestens täglich aktualisiert. Aussteller und Relying Parties haben keine Einsicht in die	Fehlende Inhalte

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
		ausgewerteten Signale und können daraus resultierende WUA-Sperrungen in ihren eigenen Risikomodellen nicht antizipieren. Wir regen an, kategorisierte Übersichten der ausgewerteten Signale zu veröffentlichen sowie standardisierte Reason-Codes in Sperrereignissen aufzunehmen, damit abhängige Parteien ihre Risikomodelle anpassen können.	
4.1	2.2.4.1 WP.WSCAReg (WP.WSCAReg.Req.AKTCHAN)	Der WSCA-Aktivierungscode muss über einen vom Personalisierungskanal getrennten Kanal übermittelt werden, ohne dass der konkrete Kanal definiert wird. Übliche Interpretationen (SMS, E-Mail, Postweg) weisen sehr unterschiedliche Sicherheitseigenschaften auf. Wir regen an, die zulässigen Kanäle und deren jeweilige Sicherheitseigenschaften zu spezifizieren, damit Umsetzende konforme Kanäle mit Rechtssicherheit auswählen können.	Anforderung schärfen
4.1	2.2.1.4 WP.Wdev (WP.WDev.Req.PINNING)	Die Pflicht zum Zertifikats-Pinning des PID-Providers in der Wallet-App setzt eine eindeutige architektonische Trennung zwischen PID-Provider-Endpunkten und EAA-Aussteller-Endpunkten voraus. Wir regen eine ergänzende Klarstellung an, wie OID4VCI-Konfigurationen von EAA-Ausstellern gestaltet sein müssen, um nicht versehentlich als PID-Provider-Flow interpretiert zu werden und stille Fehlschläge zu vermeiden.	Anforderung schärfen
4.1	2.1 WP.F.COLLECT / WP.F.DATA	Die strikten Datensparsamkeits-Anforderungen an den Wallet-Provider stehen potenziell im Spannungsverhältnis zu legitimen Betrugspräventions- und Sicherheitsaufgaben (z. B. Mustererkennung über mehrere RPs hinweg zur Erkennung kompromittierter Geräte). Wir regen eine Klarstellung an, welche Verarbeitungen zu Sicherheits- und Betrugspräventionszwecken zulässig sind und welche Schutzmaßnahmen (z. B. Pseudonymisierung) dabei einzuhalten sind.	unklar
4.1	2.1 WP.Req.BACKUP	Die Anforderung an ein Backup-Verfahren ist optional. In Kombination mit dem Verbot der Übertragbarkeit personengebundener EAAs (TR-03189-2 WI.Backup.O.BLOCK) führt dies zu obligatorischer Neu-Ausstellung bei jedem Gerätewechsel. Wir regen an, die Auswirkungen dieser Konstellation für die Aussteller-Ökonomie und Nutzererfahrung explizit zu beschreiben sowie zu klären, ob eine geräteübergreifende Wiederherstellung nicht-personengebundener Credentials zulässig ist.	unklar

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
4.1	2.2.4.9. Nutzer-Authentisierung	Die TR legt aktuell einen starken Fokus auf wissensbasierte Faktoren (z. B. PIN). Ergänzend sollten biometrische Faktoren als gleichwertige Alternative vorgesehen werden, insbesondere für Aktivierungs-, Wiederherstellungs- und Freigabeprozesse.	Anforderung anpassen
4.1	2.2.4.8 Aktivierung	Die verpflichtende Nutzung manueller Aktivierungscodes kann zu Medienbrüchen und Akzeptanzproblemen führen. Die TR sollte alternative, gleichwertig sichere Aktivierungsverfahren innerhalb eines durchgängigen digitalen Prozesses zulassen.	Anforderung anpassen
4.2	2.3.2	Die verpflichtenden PID-Attribute umfassen Familienname, Vorname, Geburtsdatum, Geburtsort und Staatsangehörigkeit. Die Wohnadresse ist optional. Die VO (EU) 2024/1620 (AMLR) verlangt im Rahmen der Kundensorgfaltspflichten regelmäßig die Verifikation der Wohnadresse. Wenn die deutsche PID die Adresse nicht verpflichtend führt, können Relying Parties im Finanzdienstleistungsbereich ihre AMLR-Pflichten nicht allein auf Basis der PID erfüllen. Wir regen an, die Wohnadresse als Pflichtattribut aufzunehmen oder eine definierte PubEAA-Adressbescheinigung derselben autoritativen Quelle vorzusehen, deren Vertrauenseigenschaften die Kombination mit der PID als funktional gleichwertig zu einem vollständigen Identitätspaket im Sinne der AMLR ausweisen.	Anforderung schärfen
4.2	2.3.2.4	Die Spezifikation hält fest, dass die Ausstellung von PIDs für juristische Personen derzeit nicht empfohlen wird. Mit dem absehbaren European Business Wallet (EBW) entsteht jedoch Bedarf an einer juristischen Person-Identität. Wir regen einen Fahrplan für die juristische Person-Identität in Deutschland an sowie eine Aussage, welcher Standard zwischenzeitlich für Attestierungen juristischer Personen verwendet werden soll (z. B. LEI-basierte Bezeichner über PubEAA), damit Ökosystem-Teilnehmer auf ein bekanntes Ziel hin entwickeln können.	Fehlende Inhalte
4.2	2.2.1.7 Wallet-Akzeptanz (PIDP.Req.WALLET / PIDP.WVeri.F.ACCEPT)	Der PID-Provider akzeptiert WUAs nur von Wallets auf seiner zugelassenen Liste. Die Aufnahme in diese Liste erscheint als gesonderter, von der TR-03189-Zertifizierung verschiedener Schritt, dessen Kriterien und Zeitplan nicht spezifiziert sind. Wir regen an, die Aufnahmekriterien, die zu erwartende Bearbeitungsdauer von der Zertifizierungsabschluss bis zur Listenaufnahme sowie das Verhältnis zur EU-Vertrauensliste gemäß CIR 2024/2981 explizit zu beschreiben.	Fehlende Inhalte

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
4.2	2.2.1.4 Ausstellung von PID-Credentials	Die TR sollte nicht zwingend voraussetzen, dass die Personalisierung und die Ausstellung von PID Credentials ausschließlich über die Online Ausweisfunktion erfolgen. Die derzeitige aktive Nutzung der eID Funktion in Deutschland dürfte für eine breite Wallet Adoption ohne alternative Onboarding Pfade nicht ausreichen. Daher sollte die TR ausdrücklich zulassen, dass PID Credentials auch auf Basis anderer gleichwertiger und zertifizierter Identifizierungsverfahren ausgestellt werden können, insbesondere für Personen, die noch keine eID erhalten können. Als mögliche Bootstrap Pfade sollten hochwertige Identifizierungsverfahren, etwa videobasierte Identifizierung im Einklang mit bestehenden AML Vorgaben, spezifiziert werden. Mindestens sollte ein Übergangspfad vorgesehen werden, der mit steigenden eID Aktivierungsraten schrittweise angepasst werden kann. Ergänzend sollte die TR die Nutzung international verbreiteter Identitätsdokumente (z. B. eMRTD/Reisepass mit NFC-Schnittstelle) als interoperablen Onboarding-Pfad stärker berücksichtigen. Dies ist insbesondere für grenzüberschreitende Nutzungsszenarien sowie für nicht-eID-aktive Nutzergruppen von zentraler Bedeutung.	Fehlende Inhalte
4.2	2.2.1 Onboarding-Prozesse	Bei den Anforderungen an das Onboarding sollte stärker berücksichtigt werden, dass bundesweite Skalierbarkeit und gleichbleibende Qualität insbesondere durch digitalisierte, remote-fähige Verfahren erreicht werden. Remote-fähige Identifizierungsverfahren sollten nicht nur als alternative Option zur Online-Ausweisfunktion betrachtet werden, sondern als zentrale Voraussetzung für eine flächendeckende Nutzung der EUDI-Wallet. Ohne vollständig digitale Onboarding-Prozesse ist eine breite Adoption insbesondere in mobilen und grenzüberschreitenden Nutzungsszenarien nicht erreichbar.	Inhaltlich prüfen
4.2	2.2.2.2 PIDP.WMon (PIDP.WMon.Req.CHECK / Req.REVOKE)	Der PID-Provider prüft die WUA-Sperrliste mindestens täglich und sperrt im Sperrfall sämtliche PIDs in den betroffenen Wallets. Es ist nicht festgelegt, ob die tägliche Prüfung die Untergrenze darstellt oder zeitnähere Prüfungen zulässig sind, und ob ein Wallet-Provider eine Sperrung als zielgerichtet (ein Nutzer) oder systemisch (eine Wallet-Klasse) deklarieren kann. Wir regen eine Differenzierung an, damit der PID-Provider verhältnismäßige Kaskaden-Reaktionen vornehmen kann.	unklar
4.2	2.2.2.4 PIDP.Status (PIDP.Status.Req.DATA / Req.USE)	Die Sperrstatusliste muss Datenschutz wahren und Rückschlüsse auf Nutzungsmuster verhindern. Eine konkrete empfohlene Implementierungstechnik (z. B. Status List 2021 mit Bitmap-Struktur)	Fehlende Inhalte

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
		wird nicht genannt. Wir regen die Aufnahme einer empfohlenen Referenzimplementierung an, damit Ökosystem-Teilnehmer interoperabel umsetzen und nicht auf undokumentierte Eigenentwicklungen ausweichen.	
4.3	3	Die Spezifikation führt das Konzept der „personengebundenen EAA" ein, das eine hardwaregebundene Bindung an dieselbe Sicherheitshardware wie die PID voraussetzt. Eine Abbildung dieses Konzepts auf die EU-Taxonomie (QEAA / PubEAA / EAA gemäß CIR 2024/2981 und CIR 2025/1569) ist nicht enthalten. Wir regen eine explizite Zuordnung an, einschließlich der Frage, ob eine auf EU-Ebene zertifizierte EAA automatisch als personengebunden anerkannt wird und welche technischen Bindungsnachweise erforderlich sind.	unklar
4.3	3	Die Abgrenzung zwischen EAA-Provider und QEAA-Provider wird in Kapitel 3 nicht abschließend gezogen; insbesondere bleibt offen, unter welchen Bedingungen eine privatwirtschaftliche Zahlungsattestierung der QEAA-Kategorie (und damit dem QTSP-Status) zugeordnet werden könnte. Wir regen eine ausdrückliche Klarstellung an, dass privatwirtschaftliche Zahlungsattestierungen unter den definierten Bedingungen unter die reguläre EAA-Kategorie fallen können, sofern die technischen Anforderungen erfüllt sind.	Inhaltlich prüfen
4.3	4	Die Anforderung, dass jede Relying Party sich bei einem nationalen Registrar registrieren muss, steht im Spannungsverhältnis zum Grundsatz der einmaligen Registrierung im Heimat-Mitgliedstaat gemäß CIR 2025/848. Wir regen eine ausdrückliche Klarstellung an, ob eine in einem anderen Mitgliedstaat etablierte Relying Party eine zusätzliche Registrierung beim deutschen Registrar benötigt, und falls ja, in welchem Umfang sich die Inhalte gegenüber der Heimatstaat-Registrierung unterscheiden.	unklar
4.3	5	Die Risikotabelle in Kapitel 5 weist Bedrohungen den Rollen Relying Party und EAA-Provider zu, jedoch nur teilweise mit Verweis auf konkrete Anforderungen in den Teilen 1 bis 4.3. Wir regen die Ergänzung einer vollständigen Rückverfolgbarkeitsmatrix von jeder Bedrohung zu den jeweils mitigierenden Anforderungen an, damit Umsetzende die erwarteten Design-Kontrollen vollständig erkennen können.	Fehlende Inhalte

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
4.3	5 (SR1 / SR2 / SR3)	Die systemischen Risiken (SR1 flächendeckende Überwachung, SR2 Reputationsschäden, SR3 Rechtsverstoß) werden nicht auf konkrete Anforderungen abgebildet. Damit verbleibt die Risikobehandlung vollständig auf der Implementierungsebene, was insbesondere für SR1 zu uneinheitlichen Lösungen führen kann. Wir regen die Aufnahme von Mindest-Design-Anforderungen für die systemischen Risiken auf RP- und Aussteller-Seite an.	Fehlende Inhalte
Annex	1.1 Risikobetrachtung	Das Risiko geringer Nutzerakzeptanz durch hohe Einstiegshürden (z. B. zwingende eID-Nutzung, PIN-Kenntnis) sollte explizit berücksichtigt werden.	Fehlende Inhalte
Annex	1.2 Risikoregister (TR40)	Die Bedrohung TR40 (mehrentitätenbasierte RP-Anfragen über die jeweilige Rechtsgrundlage hinaus) ist insbesondere für EU-Dienstleister relevant, die unter einer gemeinsamen Marke mehrere regulierte Entitäten betreiben. Die RP-Registrierungsarchitektur bietet derzeit kein klares Muster für die Abbildung dieser Entitätsgrenzen. Wir regen eine Spezifikation an, ob jede regulierte Entität separat registriert werden muss oder ob eine einzelne Registrierung mit entitätsbezogener Eingrenzung der Attributanfragen zulässig ist.	Fehlende Inhalte
Annex	1.2 Risikoregister (TR36)	Die Anforderung an Unverknüpfbarkeit (Unlinkability) der Präsentationen über verschiedene Relying Parties hinweg ist als Bedrohung definiert, jedoch ohne empfohlene kryptographische Umsetzungstechnik (z. B. BBS+-Signaturen). Wir regen die Aufnahme einer empfohlenen Referenztechnik an, damit Wallet-Implementierungen interoperabel die Anforderung erfüllen und die Verträglichkeit mit Aussteller-vermittelter Entschlüsselung dokumentiert wird.	Fehlende Inhalte
Annex	1.2 Risikoregister (TR37)	Die Bedrohung TR37 (Datenschutzleckage über Sperrstatuslisten) wird benannt, ohne dass eine konkrete Implementierungsempfehlung gegeben wird. Wir regen die Aufnahme einer empfohlenen Referenzarchitektur (etwa Status List 2021) sowie eine Behandlung der Abfragehäufigkeit und der zulässigen Cache-Dauer auf RP-Seite an.	Anforderung schärfen
Annex	1.2 Risikoregister (TR26 / TR102 / TR103)	Die Bedrohungen rund um die Authentifizierung der Relying Party gegenüber dem Nutzer setzen einen ordnungsgemäßen Lebenszyklus von Zugangszertifikaten voraus. Die Spezifikation enthält keine standardisierten Erneuerungsfristen und keine	Fehlende Inhalte

TR-Teil	Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
		definierte Übergangsphase nach Ablauf. Wir regen die Aufnahme einer Mindest-Vorlaufzeit für die Erneuerung sowie einer kurzen Übergangsfrist für laufende Präsentationen an, um Dienstunterbrechungen während der Zertifikatserneuerung zu vermeiden.	
Annex	1.2 Risikoregister (DSGVO_04)	Die DSGVO-Bedrohung adressiert, dass Relying Parties Wallets ausschließlich über den registrierten API-Kanal ansprechen und keine Umgehungs-Architekturen nutzen dürfen. Für Intermediär-Konstellationen nach Art. 5b Abs. 10 eIDAS-VO entstehen damit konkrete Anforderungen an die Architektur. Wir regen eine ausdrückliche Beschreibung an, welche Integrationsmuster für Intermediäre als konform gelten und welche als Umgehung des zertifizierten Kanals einzuordnen sind.	unklar

Bitkom vertritt mehr als 2.300 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 700 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

Ansprechpartnerin

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

Verantwortliches Bitkom-Gremium

AK Anwendung elektronischer Vertrauensdienste
AK Digitale Identitäten