bitkom

Stellungnahme

November 2025

Bitkom-Kommentierung der Entwurfsfassung der TR-03189 zur Zertifizierung der EUDI-Wallet (Teil 5)

Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
	Allgemeine Anmerkungen: Die in der TR 03189 beschriebenen Anforderungen zu EAA und QEAA sind sehr redundant zu den bestehenden europäischen Regelungen bzw. zu den eIDAS-Vorgaben, den dazugehörigen Implementing Acts sowie den einschlägigen ETSI-Normen. Darüber hinaus besteht Klärungsbedarf hinsichtlich der Zielgruppe dieser TR und der Frage, ob bzw. in welchem Umfang Auditoren sie berücksichtigen sollen/werden.	Inhaltlich prüfen
1 bis 4.4	Die gesamte TR-03189-5 ist noch einmal auf die deutsche Rechtschreibung zu überprüfen. Es sind zahlreiche Fehler beim Lesen aufgefallen (Kommasetzung, fehlerhafte Wörter etc.), welche an dieser Stelle nicht einzeln aufgeführt werden. Dabei sollten auch die Schreibweisen angeglichen werden (Beispiel: PubEAA versus PUB-EAA). Zudem fehlen teilweise auch die Satzzeichen (Punkte) am Satzende (siehe vor allem die Tabellen).	Editorisches
4 (erster Absatz)	Das gewählte Beispiel für ein EAA ist nicht wirklich passend, weil die Fahrerlaubnis praktisch immer ein QEAA/PubEAA sein wird. Besser wäre ein Beispiel, welches in allen drei Formen denkbar wäre, zB eine Organisationszugehörigkeit einer Person.	Inhaltlich prüfen
4 (zweiter Absatz)	EAAs werden im Dokument als Grundfall behandelt, QEAA/PubEAA als Spezialität. Fraglich ist, ob dies sinnvoll ist. So sind einige technische Anforderungen an EAA (z.B. für Integritätsschutz) noch ungeklärt, sodass Anforderungen an EAA denkbar wären, die für QEAA und PubEAA dann nicht gelten. Der zu kommentierende Entwurf selbst kann diese Grundfall-	Inhaltlich prüfen

Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
	Spezialfall-Systematik nicht durchhalten, so werden in Kapitel 4.2.2 dieselben Risiken für QEAA und EAA erfasst. Hilfreich wären an der Stelle auch eine Beschreibung der Gründe, warum manche EAA als QEAA oder PubEAA ausgegeben werden.	
4 (fünfter Absatz, letzter Satz)	Die Attributsbescheingungsregelungen enthalten auch für das Ökosystem sehr wichtige Regelungen zu Zusammensetzung des Attributs und Berechtigung zur Ausstellung. Daher sollten diese beiden Punkte neben "Vorschriften für Erstellung und Nutzung von elektronischen Attributsbescheinigungen" aufgenommen werden.	Editorisches
4 (sechster Absatz)	Die Ausnahmeregelungen sind unseres Erachtens nicht schlüssig. Gemäß Art 45g eIDAS müssen EAAs in die EUDI-Wallet ausgegeben werden können und für QEAA müssen QTSP immer eine Schnittstelle zur EUDIW bereitstellen. Daraus folgen zwei Dinge: 1. Alle EAAs müssen immer EUDI-Wallet-kompatibel sein 2. Alle EAA-Typen sind nicht an die EUDI-Wallet gebunden, sondern können immer unabhängig davon ausgestellt, genutzt, weitergegeben und validiert werden. Die TR sollte daher beide Umstände im Blick behalten, beispielsweise dadurch, dass nicht nur ein Walletbinding bei allen EAA-Typen stattfindet, sondern auch immer ein PID-Binding bei der EUDI-Wallet stattfinden kann. Es kann daher nicht wirklich zwischen EAAs außerhalb der EUDIW und innerhalb differenziert werden.	Inhaltlich prüfen
4.1. (Überschrift)	Es muss hier QEAA statt EAA heißen.	Editorisches
4.1. (erster Absatz)	Hier wäre eine Klarstellung sinnvoll, dass QEAA nicht nur über authentische Quellen und den Mechanismus aus Art 45e eIDAS verifiziert und ausgestellt werden können, sondern auch gemäß der allgemeinen Regeln aus Art 24 Abs. 1a eIDAS, um falsche Interpretationen der TR (zB nur QEAA aus Art 45e eIDAS können in die EUDIW ausgegeben werden) zu vermeiden.	Editorisches
4.1. (erster Absatz, letzter Satz)	Ist mit der Formulierung "in diesem Kontext" der Prozess des Ausstellens der QEAA (vgl. Art. 24 Abs. 1 eIDAS-Verordnung) oder die Überprüfung ohne Ausstellen (vgl. Art. 45e Abs. 1 eIDAS-Verordnung) gemeint? Oder sind davon beide Fälle umfasst (siehe auch 4.3)? Wen adressiert der Text, wenn darin von Nutzerin bzw. Nutzer gesprochen wird? Den Nutzer des QTSP - oder ist der QTSP als Nutzer gemeint? Das ergibt sich aus dem Text nicht eindeutig. Daher sollte der Zusatz "auf Verlangen der Nutzerin bzw. des Nutzers" im Sinne der Eindeutigkeit konkretisiert werden -	unklar

Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
	es kann sich nur um den Nutzers des QTSP handeln. Ist die oben angeführte Äußerung auch dahingehend zu interpretieren, dass jeder QTSP als QEAA-Provider QEAA basierend auf authentischen Quellen jederzeit und ohne Bedingung (beispielsweise Rücksprache mit der öffentlichen Stelle, welche für die authentische Quelle zuständig ist) ausstellen kann? Das könnte den schützenswerten Interessen der öffentlichen Stellen, die für die Verwaltung authentischer Quellen zuständig sind, zuwiderlaufen - und ginge auch über die Anforderungen des Art. 24 Abs. 1 eIDAS-Verordnung hinaus. In diesem Artikel werden insbesondere die Anforderungen an die Ausstellung von QEEA geregelt (siehe auch 4.3). Wir schlagen die nachfolgende Formulierung vor: "Eine öffentliche Stelle, die für die Verwaltung einer authentischen Quelle zuständig ist, a) ermöglicht auf Verlangen des Nutzers eines qualifizierten Vertrauensdiensteanbieters den hierfür von der zuständigen öffentlichen Stelle ausdrücklich berechtigten qualifizierten Vertrauensdiensteanbietern die Ausstellung von QEAAs auf Basis der von ihnen verwalteten authentischen Quellen und b) ermöglicht es hiervon unabhängig allen qualifizierten Vertrauensdiensteanbietern, Attribute auf Verlangen des Nutzers eines qualifizierten Vertrauensdiensteanbieters mit elektronischen Mitteln zu überprüfen, soweit diese Attribute auf der authentischen Quelle der öffentlichen Stelle beruhen."	
4.1.(zweiter Absatz)	Wann ist dies nach dem BSI der Fall? Welche Anforderungen müssen hier an die öffentlichen Stellen gestellt werden? Typischerweise werden die öffentlichen Stellen die Ausstellung nicht selbst vornehmen, sondern technische Dienstleister (gegebenenfalls aus der Privatwirtschaft) einbeziehen. An welches Subjekt (öffentliche Stelle oder technischer Dienstleister) sind dann diese Anforderungen zu stellen? Muss der technische Dienstleister zertifiziert werden oder die öffentliche Stelle? Oder wird an beide Rechtssubjekte als Gesamteinheit angeknüpft? Oder ist die Heranziehung eines technischen Dienstleisters bei der Ausstellung von PuB-EAA nicht möglich (dann würden die Ausführungen unter 4.3 "beauftragte Vermittler" missverständlich sein)?	unklar
4.1.(zweiter Absatz)	Besser eigenes Kapitel, weil PubEAA-Provider rechtlich ausdrücklich nicht QTSP sind (insbesondere nicht unter der Aufsicht der nationalen Behörde stehen), sondern nur eklektisch entsprechend Vorschriften einhalten müssen und nur ein vergleichbares Schutzniveau haben. Öffentliche Stellen, die PuB-EAA ausstellen, sind keine QTSP im Sinne der eIDAS-Verordnung.	Editorisches

Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
4.2.1. EAA.F.FUNCT	Klarstellung erforderlich, um fehlerhafte Interpretation zu vermeiden. Nach Art 4 Abs. 2 Durchführungsbeschluss (EU) 2025/1569 sind Anbieter qualifizierter elektronischer Attributsbescheinigungen und Anbieter elektronischer Attributsbescheinigungen, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder in deren Namen ausgestellt werden, die einzigen Stellen, die die von ihnen ausgestellten elektronischen Attributsbescheinigungen widerrufen können dürfen. Der Nutzer selbst hat nur einen Anspruch den Widerruf zu verlangen, kann aber selbst nicht widerrufen, ebenso kann der Walletbetreiber das QEAA/PubEAA nicht selbst widerrufen.	unklar
4.2.1. EAA.F.CLVCL	Die Anforderung lässt die exakte Natur der zu erfüllenden Aufgabe nicht eindeutig erkennen. Die vorliegende Untersuchung befasst sich mit der Fragestellung, ob eine Multiuser-Funktionalität für eine Wallet als zwingend erforderlich zu betrachten ist.	Inhaltlich prüfen
4.2.2. TR 21	Unseres Erachtens außerhalb des Anwendungsbereichs der TR. Dies ist ein Risiko für den QTSP nicht für die Wallet. Der QTSP trägt alleine die Gewähr und Haftung für die Richtigkeit des QEAA innerhalb der Gültigkeit nach Ausstellung vgl. Art 4 Abs. 3 lit. b) Durchführungsbeschluss (EU) 2025/1569 und Art 13 eIDAS. TR 21 sollte somit gestrichen werden. Rückwärtsgewandte Bedrohung: Diese Anforderung sollte nur zutreffen, wenn es ein physisches Gegenstück dazu gibt.	Inhaltlich prüfen
4.2.2. TR 32	Wir bitten um Beschreibung des Risiko in einer alternativen Formulierung. Die Verständlichkeit der aktuellen Beschreibung ist nicht gegeben.	unklar
4.2.2. TR 43	Klarstellung und Berücksichtigung erforderlich, um fehlerhafte Interpretation zu vermeiden. Ein Binding kann immer auch an die Identitätsdaten des Nutzers (PID-Binding) erfolgen. Nicht nur über den Walletkey.	Inhaltlich prüfen
4.2.2. TR 45	Redundant, da durch gewählte Systematik (QEAA=EAA + spezielle Anforderungen) deckungsgleich zur TR 42. Somit zu streichen.	Inhaltlich prüfen
4.2.2. TR 71	Redundant, da durch gewählte Systematik (QEAA=EAA + spezielle Anforderungen) deckungsgleich zur TR 70. Zudem unpräzise, da zu einem Widerruf nicht die Zustimmung des Nutzers erforderlich ist, vgl. zB Art 4 Abs. 3 lit. b) Durchführungsbeschluss (EU) 2025/1569. Somit zu streichen.	Inhaltlich prüfen

Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
4.2.2. TR 137	Redundant, da durch gewählte Systematik (QEAA=EAA + spezielle Anforderungen) deckungsgleich zur TR 136. Somit zu streichen.	Inhaltlich prüfen
4.2.4. & 4.2.5.	Warum definiert die TR-03189 in Kap. 4.2.4, und 4.2.5 Anforderungen an QEAA, wenn die Zertifizierung von QTSP zur Ausstellung von QEAA gem. Implementing Act zu Art. 20 (4) eiDAS (Commission Implementing Regulation (EU) 2025/2162) zwingend folgende Standards durch die CAB anzuwenden sind: - ETSI TS 119 471 - ETSI EN 301 549 - ETSI TS 119 461 - ETSI EN 319 401 Kap. 4.2.4 und 4.2.5 der TR-031389 sollten gestrichen werden, da die den Implementing Acts widersprechen.	Inhaltlich prüfen
4.2.4. EAA.Req.3	Klarstellung und Berücksichtigung erforderlich, um fehlerhafte Interpretation zu vermeiden. Ein Binding kann immer auch an die Identitätsdaten des Nutzers (PID-Binding) erfolgen. Es folgt aus dieser Anforderung kein mandatorisches Walletbinding für EAAs, EAAs können auch außerhalb der EUDIW ausgegeben werden. Kryptografische Bindung des EAAs an die Wallet ist immer nur eine zusätzliche Maßnahme.	Inhaltlich prüfen
4.2.4. EAA.Req.17	Woraus folgt diese Anforderung? Unseres Erachtens ist es keine gesetzliche (inkl. Implementing Acts) Anforderung. Als zusätzliche, freiwillige Anforderung zu streichen oder zumindest in ein "KANN" umzuwandeln, da so unnötige Komplexität geschaffen wird. In vielen Fällen technisch schwierig bis unmöglich und für Anwendungen (Einmal-Nutzungen, Kurzzeit QEAA) gar nicht erforderlich. Zudem schlagen wir vor, die Anforderunge wie folgend anzupassen: "[...] zur Erneuerung eines EAAs beim TSP anzufragen."	Inhaltlich prüfen
4.2.8.	4.2.8 Inhalte von QEAA der TR-03189 widerspricht Art .45 d (3) eIDAS. Dieser definiert: "Qualified electronic attestations of attributes shall not be subject to any mandatory requirement in addition to the requirements laid down in Annex V." Die Vorgaben von Kap. 4.2.8 der TR sind in Annex V eIDAS nicht enthalten und damit rechtswidrig.	Inhaltlich prüfen
4.3. vierter Absatz	Ist mit der Formulierung "in diesem Kontext" der Prozess des Ausstellens der QEAA (vgl. Art. 24 Abs. 1 eIDAS-Verordnung) oder die Überprüfung ohne	unklar

Kapitelnummer	Kommentar & Änderungsvorschlag	Aktion
	Ausstellen (vgl. Art. 45e Abs. 1 eIDAS-Verordnung) gemeint? Oder sind davon beide Fälle umfasst (siehe bereits 4.1)?	
4.3. letzter Absatz	ETSI TS 119 478 ist noch in Arbeit, zudem noch nicht gesetzlich referenziert. Bessere Formulierung daher: "Derzeit wird mit ETSI TS 119 478 an einem Standard gearbeitet, der Vorgaben an die Spezifikation eines Interfaces zur Anbindung von Authentic Sources beinhaltet."	Inhaltlich prüfen
4.3. letzter Absatz	Wir regen eine eigene, separate TR zum Thema Anbindung QTSP an authentic source (Art 45e eIDAS) an, da die Anforderungen aus eIDAS und Durchführungsbeschluss (EU) 2025/1569 zu allgemein sind, und auf technischer Ebene nicht ausreichend sind. Diese TR sollte nicht redudant zu ETSI TS 119 478.	Fehlende Inhalte
4.4.	Je nachdem, wie der weitere Aufbau der TR aussieht: Gegebenenfalls macht es Sinn, diese Begrifflichkeit in der Gliederung nach vorne zu ziehen.	Editorisches
4.4.	Vor allem auf die Vorgaben aus Art. 45h eIDAS-Verordnung sollten behandelt werden, um der Praxis eine Einschätzung zu den hierfür notwendigen Maßnahmen zu geben.	Fehlende Inhalte

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
AK Digitale Identitäten