bitkom

Stellungnahme

April 2025

5-Punkte-Papier zu den eIDAS Implementing Acts

Zusammenfassung

Die Durchführungsrechtsakte der novellierten eIDAS-Verordnung sind das entscheidende Puzzleteil, um die grundlegenden Ziele eines europäischen Ökosystems für Digitale Identitäten und Vertrauensdienste zu realisieren. Der Bitkom hat 5 Punkte identifiziert, denen in den Verhandlungen der Implementing Acts besondere Aufmerksamkeit gewidmet werden sollte. Damit möchten wir auf die möglichen Auswirkungen insb. einer uneinheitlichen Umsetzung der eIDAS-Verordnung in Europa hinweisen.

Wir sehen die Durchführungsrechtsakte nicht nur als rein technische Spezifikation für die Umsetzung der eIDAS Verordnung, sondern auch als Gelegenheit, um die Grundlagen eines gemeinsamen homogenen europäischen Ökosystem zu legen und dabei die Erwartungshaltungen bezüglich der EUDI-Wallet zu klären sowie ein gemeinsames Verständnis zu schaffen.

Die Durchführungsrechtsakte sollten:

- Die Grundlage für ein harmonisiertes europäisches Ökosystem legen
- Frei von Interpretationsspielraum sein
- Interoperabilität durch einen gemeinsamen Standardisierungsrahmen schaffen und Sicherheit gewährleisten
- Auf Bestehendem aufbauen
- Zugang zu Authentic Sources sicherstellen.

Die Durchführungsrechtsakte als Grundlage für ein harmonisiertes europäisches Ökosystem

Um ein EU-weit homogen nutzbares Ökosystem zu erreichen, müssen zunächst die Grundlagen der Anforderungen der EU-Verordnung klar erläutert werden. Dabei sollte geregelt werden, was das Zielbild einer homogenen europäischen Wallet ist, und welche Zuständigkeiten die EU und die Mitgliedstaaten in den einzelnen Bereichen haben, bevor kritische Aspekte beleuchtet werden. Dies umfasst Fragen wie z. B. die Gestaltung und Grundordnung des Ökosystems sowie den Betrieb der Wallet. Somit setzen wir uns für die Stärkung der europäischen Souveränität sowie für die Unabhängigkeit von nicht-europäischen marktführenden Plattformen ein.

Interpretationsfehler vermeiden: Das Beispiel des Re-Keying

Einige kritische Aspekte der eIDAS-Verordnung zeigen Inkohärenzen und mangelnde Klarheit, die in den Durchführungsrechtsakten geklärt werden müssen, um Fehlinterpretationen zu vermeiden, die die Bemühungen zur Schaffung eines harmonisierten europäischen Ökosystems beeinträchtigen könnten. Dabei sollten die noch zu erlassenden Implementing Acts möglichst konkret und technisch spezifisch sein.

Beispielsweise erlaubt die europäische ETSI-Norm 319 411-1 das Re-Keying, d. h. die einfache Ausstellung eines qualifizierten Zertifikats für einen Abonnenten, wenn dieses größtenteils mit dem zuvor von derselben Zertifizierungsstelle ausgestellten Zertifikat identisch ist. Dies wird zu erheblichen Vorteilen für Bürgerinnen und Bürger und Unternehmen führen, da unnötige Reibungsverluste bei der Beantragung eines Zertifikats vermieden werden.

Jedoch kann die Formulierung am Anfang vom Artikel 24.1 „[...] bei der Ausstellung eines qualifizierten Zertifikats [...]“ zu der Interpretation führen, dass die QTSP alle Identitätsinformationen jedes Mal neu validieren müssen, wenn ein neues Zertifikat „ausgestellt“ wird. Darüber hinaus kann der Begriff „hohes Maß an Vertrauen“ im Artikel 24, Abs. 1, Buchst. c) mit dem Begriff „hohes Maß an Sicherheit“ verwechselt und falsch interpretiert werden. Wir empfehlen, im Durchführungsakt zu Artikel 24.1 die Praxis des Re-Keying u. a. auf die europäische ETSI-Norm EN 319 411-1 sowie auf die in der im Februar veröffentlichten neuen Version der TS 119 461 zu verweisen, um eine Harmonisierung der Auslegung zu erreichen, die zu einem homogenen und kohärenten Ansatz im Binnenmarkt führen kann.

Auch wenn klar ist, dass eine präzise und detaillierte Festlegung der unter die eIDAS-Verordnung fallenden authentischen Quellen erst auf nationaler Ebene erfolgen kann, sollten die Implementing Acts eine Konkretisierung von Anhang VI vornehmen, der derzeit sehr offen formuliert ist. Dies würde den Mitgliedstaaten als präziser Leitfaden zur Identifikation relevanter Quellen dienen und zugleich zu einer stärkeren Harmonisierung des eIDAS-Ökosystems sowie einer fundierten Vorbereitung der QTSP beitragen.

Schaffung eines sicheren, interoperablen europäischen Ökosystems durch einen gemeinsamen Standardisierungsrahmen

Der Artikel 24.1a, Buchst. a) beschränkt die Ausstellung von qualifizierten Zertifikaten auf eID-Mittel mit hohem Zuverlässigkeitsgrad. Diese Entscheidung wird tiefgreifende restriktive Auswirkungen auf die Prozesse der QTSP haben.

Obwohl viele Mitgliedstaaten eID-Mittel mit einem hohen Zuverlässigkeitsgrad bereitstellen, unterstreichen wir die Dringlichkeit, Prozesse zu erwägen, die die QTSP verwenden können, um die Sicherheit des Identitätsnachweisverfahrens durch zusätzliche Maßnahmen zu verstärken, wie in Artikel 24.1a, Buchst. c) „andere Identifizierungsmethoden, die die Identifizierung einer Person mit einem hohen Maß an Vertrauen gewährleisten und deren Konformität von einer Konformitätsbewertungsstelle bestätigt wird“. Dafür muss der gewählte Standardisierungsrahmen dieses „hohe Maß an Vertrauen“ sicherstellen und europaweit angewendet werden, um überall in Europa eine sichere Umgebung für Digitale Identitäten zu gewährleisten.

Außerdem sollten alle Durchführungsrechtsakte auf europäische Standards ETSI/CEN verweisen, die eine Flexibilität bei technischen Änderungen gewährleisten. Diese Standards sollten zudem bereits final verabschiedet sein. Deshalb halten wir es für wichtig, dass die ETSI TS 119 461 die Grundlage für die Durchführungsrechtsakte bildet. In den Bereichen Archiving und Ledger sollten die entsprechenden Standardisierungen aus CEN TC 468 (Archiving) und CEN JTC 19 (Ledger) angewendet werden. In beiden Gremien befinden sich entsprechende Standards (z. B. CEN TS 18170) momentan noch in der Ausgestaltung, werden aber eine wichtige Referenz für diese Vertrauensdienste sein.

Selbst im Rahmen eines harmonisierten Ansatzes wird es jedoch weiterhin nationale Besonderheiten geben (Art der rechtsgültigen Dokumente, Verbreitungsgrad von eID-Mitteln, digitale Bildung der Bürgerinnen und Bürger). Die QTSPs benötigen ein gewisses Maß an Flexibilität, um darauf eingehen zu können, wobei gleiche Wettbewerbsbedingungen aufrechtzuerhalten und Asymmetrien bei der Einhaltung zu vermeiden sind. Das heißt: Ein Anbieter aus Italien sollte in Deutschland nur mit den gleichen Anforderungen operieren können wie ein deutscher Anbieter. Derzeit besteht hier eine Wettbewerbsverzerrung durch unterschiedliche nationale Richtlinien der QTSPs. Wir fordern, dass QTSPs, sofern sie keinen nationalen Sonderregelungen unterliegen, mit der Novellierung der eIDAS-Verordnung und Standards wie ETSI TS 119 461 (v2.1.1) keinen Wettbewerbsnachteil mehr erleiden werden.

Neben dem Bedarf an Harmonisierung bringt der Einsatz der Wallet zusätzliche Sicherheitsherausforderungen mit sich. Erstens sind datenschutzrechtliche Bedenken seitens der Expertinnen und Experten und der Zivilgesellschaft bekannt, da Relying Parties Zugriff auf Daten erlangen könnten, die sie eigentlich gemäß DSGVO nicht erheben dürften (sog. Überidentifizierung). Daher ist es wichtig, dass der Zugriff durch technische Mittel beschränkt wird, was konkret bedeuten könnte, dass Zugriffsrollen oder Attributsgruppen in den Implementing Acts definiert werden, die dann durch

Abbildung in den Zugriffs- und Registrierungszertifikaten die Steuerung des Datenzugriffs der Relying Parties (beispielsweise durch die sog. PSD2-Lösung) übernehmen.

Zweitens sollten Schutzmechanismen gegen Quishing und QR-Hijacking entwickelt werden – beispielsweise durch Absicherung der QR-Codes durch QWAC, die eine verifizierte Identität der Relying Party nutzerfreundlich anzeigen können.

Drittens sollten in den Implementing Acts Bestimmungen aufgenommen werden, die das Erfordernis einer funktionalen Trennung der Erbringung von QEAA-Diensten von Artikel 45h, Abs. 3 präzisieren. Diese funktionale Trennung könnte durch die Erstellung getrennter Teamstrukturen, ein speziell für die QEAA zuständiges Mitglied der Leitungsebene und getrennte Berichtswege zu diesem Mitglied erreicht werden.

Der letzte Punkt betrifft Artikel 24, Abs. 2, Buchst. h), der QTSPs verpflichtet, alle ausgegebenen Daten für die Zeit aufzubewahren, die für die Beweisführung vor Gericht relevant ist. Wir halten es für wichtig, dass dies für QEAA nur die Transaktionsdaten und ausdrücklich nicht den Inhalt der elektronischen Attribute umfasst. Andernfalls würde dies dazu führen, dass der QTSP faktisch ein zentrales Register verifizierter Nutzerattributdaten schafft, was potenziell hohe Angriffs- und Missbrauchsrisiken mit sich bringen würde.

Auf Bestehendem aufbauen: Harmonisierung mit bestehenden Regelungen und Referenzierung bestehender Vertrauensdienste

Einige Aufsichtsstellen – wie z. B. die niederländische Aufsichtsstelle – verlangen eine Haager Apostille auf Dokumenten (z. B. aus einem Unternehmensregister oder einer Vollmacht) für juristische Personen, die in verschiedenen EU- oder Nicht-EU-Mitgliedsstaaten registriert sind, bevor sich ein QTSP auf solche Dokumente verlassen kann.

Wir bitten um eine klare Anleitung zu den Umständen, unter denen diese Haager Apostille im Zusammenhang mit der ersten Identitätsprüfung erforderlich ist, und welche Alternativen angemessen sind oder bestehen könnten.

Zudem sollten in den Implementing Acts mehr auf die Anwendung bestehender Vertrauensdienste referenziert werden, die den Vorteil darstellen, dass sie bereits reguliert, standardisiert und bereits etabliert sind, und nur noch etwaig für den konkreten Anwendungszweck angepasst werden müssten. Außerdem würde eine solche Referenzierung den europäischen Vertrauensraum stärken und die Nutzungsmöglichkeiten von Vertrauensdiensten erweitern.

Zugang zu Authentic Sources und zu Polizeidatenbanken gestohlener Ausweise

Wenn sich Attribute auf authentische Quellen innerhalb des öffentlichen Sektors stützen, muss es qualifizierten Vertrauensdiensteanbietern von elektronischen Bescheinigungen von Attributen erlaubt sein, diese Attribute in Übereinstimmung mit Artikel 45e zu überprüfen. Viele Informationen, die von authentischen Quellen zur Verfügung gestellt werden, können sogar für die Überprüfung der Identität bei der Ausstellung von Zertifikaten sehr wichtig sein.

Außerdem fordern wir, im Durchführungsrechtsakt einen programmatischen Zugang zum Business Register Interconnection System (BRIS) für QTSPs vorzusehen, der bei der Validierung der Identitätsinformationen helfen könnte, bevor ein Zertifikat ausgestellt wird. Insgesamt fordern wir eine konsequente Öffnung aller Register, die Daten nach Anhang VI der eIDAS-Verordnung beinhalten.

Insbesondere ist es auch notwendig, dass qualifizierte Vertrauensdiensteanbieter die Identifizierung von Personen und bzw. die Gültigkeit von Personalausweisen und Reisepässen mit Hilfe der Interpol/API überprüfen können, wie dies heute für Fluggesellschaften und Kreuzfahrten erlaubt ist. Wir fordern klare Vorgaben für den Zugang von QTSPs zu dieser Datenbank und generell zu allen Registern, die notwendig sind, um das Vertrauen und die Sicherheit der Identifizierung zu erhöhen und den Bürgerinnen und Bürgern das beste Schutzniveau auf dem digitalen Markt zu bieten.

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 +49 30 27576-157| l.slous@bitkom.org

Verantwortliches Bitkom-Gremium

AK Anwendung elektronischer Vertrauensdienste
AK Digitale Identitäten

Copyright

Bitkom 2025 | Version 2

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.