Executive Summary: 1. Monat Ad-Hoc Technical Advisory Group EC - 02.07.2024

Mit der geplanten technischen EU-Spezifikation [1] der eIDAS2 Verordnung [2] sind die in der Verordnung verbrieften Rechte der Bürger*innen nicht umsetzbar [3][4]. Weiterhin werden die Rechte auf pseudonyme Nutzung, auf Unbeobachtbarkeit und auf Unverknüpfbarkeit bei der Nutzung digitaler Identitäten bereits durch die Architektur systemisch verhindert [3][4]. Nach fachlichem Konsens ist eine gesetzeskonforme Umsetzung mit Hilfe einer an die Verhältnisse angepassten Zeitplanung möglich und realistisch [5]. Mit der aktuellen EU-Spezifikation hingegen wird keine gesetzeskonforme Umsetzung möglich sein.

Hier ist darauf hinzuweisen, dass das Gesetzgebungsverfahren der eiDAS2 Verordnung sich von 2021 bis 2024 hinzog. Um den geplanten Go-live in 2026 zu halten, wurden die Zeiträume für die Entwicklung der EU-Spezifikation sowie der darauf aufbauenden Prototypenentwicklung gekürzt. Letztere von Ende 2022 bis Mitte 2025 auf unter sieben Monate[6][1] (Abb. 1.).

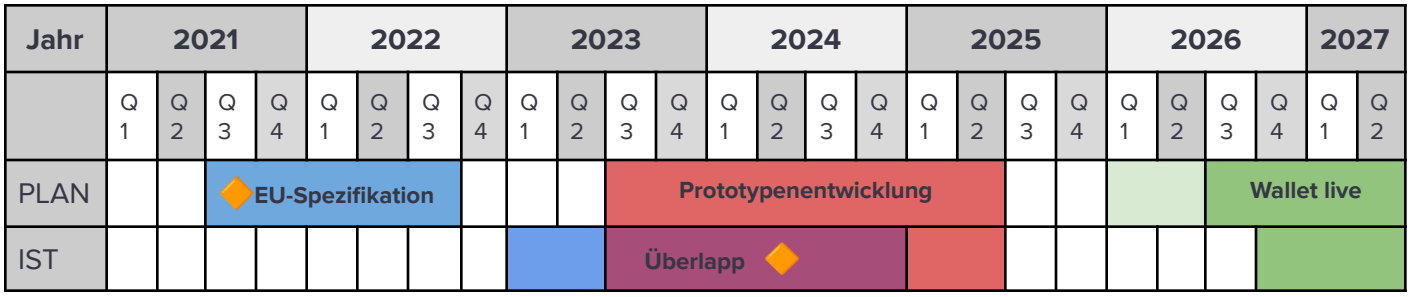

Abbildung 1: Gegenüberstellung Umsetzungsszenarien; 🔸 = Verabschiedung eIDAS 2

Die aktuell vorliegende EU-Spezifikation (sog. Architectural Reference Framework (ARF) V1.4 - Mai ´24) hat den formalen Zustimmungsprozess der eIDAS Expert Group der EU [7] nicht durchlaufen. Es soll auf Technologien zurückgegriffen werden, die für den angedachten Verwendungszweck weder entwickelt wurden noch geeignet sind [5]. Gleichzeitig werden im Entwurfsstadium befindliche Ansätze verfolgt, deren technische Grundlagen seit 2022 nicht mehr unterstützt werden [8].

Die genannten Punkte sind Konsens von Expert*innen aus Akademia [5], internationalen Standardisierungsorganisationen [8] (IETF [9]/W3C[10]) und Zivilgesellschaft [3] (epicenter.woks [11]). Sie sind Teil der öffentlichen Arbeitsergebnisse der Ende Mai 2024 berufenen Ad-Hoc Technical Advisory Group (ATAG) der EU Komission. Die ATAG wurde von der zuständigen Unit CNECT.H4 der Europäischen Kommission Ende Mai berufen, um zum ARF V 1.4 (Mai 2024) Stellung zu beziehen.

Die Verlängerung der Prototypenentwicklung, den sog. Large Scale Pilots und eine Aufstockung der EU-Mittel ist rechtlich möglich [12], eine realistische Zeitschiene bedarf politischer Unterstützung.

Im Folgenden werden das Verhältnis des ARF V 1.4 zur Arbeit der eIDAS Expert Group und Eingaben aus dem Kontext der ATAG dargestellt. Die ausgewählten Beiträge aus der ATAG basieren und auf dem fachlichen Konsens relevanter Expert*innen aus Akademia (14 Lehrstühle für Kryptographie), internationaler Standardisierungsorganisationen (IETF / W3C) und Zivilgesellschaft (Federführung von epicenter.works).

Gregor Bransky gregor.bransky@inoeg.de – Tel: 0176 209 66 393

Einzelbetrachtungen der Arbeitsergebnisse der ATAG:

Zivilgesellschaft: Technische Umsetzung nicht Gesetzeskonform

Im Rahmen der Stellungnahme von epicenter.works wird aufgezeigt, dass die aktuelle Spezifikation des ARF sieben zentrale Rechte aus der eiDAS2 Verordnung nicht erreicht:

- **Recht auf Pseudonymität**
  Im Rahmen des ARF V 1.4 ist eine neue Rolle der sog. "Pseudonym Provider" vorgesehen, diese findet sich nicht im Gesetzestext der eIDAS Verordnung. Im Rahmen eines geleakten "Pseudoym Rule Book" vom 17. Oktober 2023 [4] sollen "Pseudonym Provider" verpflichtet werden, im Dienste von Strafverfolgungsbehörden Pseudonyme rückwirkend aufzulösen. Ähnlich der Ende-zu-Ende Verschlüsselung in der Diskussion um die Chatkontrolle ist hier unklar, wieso das Auflösen von Pseudonymen - wenn durch Dritte technisch möglich - ausschließlich den "Pseudonym Providern" vorbehalten sein soll und dies nur im Dienste von Strafverfolgungsbehörden vorgenommen werden soll.

- **Regulierung der Use-cases**
  Artikel 5a und 5b der eIDAS Regulierung sehen vor, dass sog. relying parties transparent machen, welche Daten sie aus der Wallet aus welchen Gründen abrufen und dies für die Nutzer*innen der Wallet unabhängig überprüfbar ist. Das ARF V 1.4 sieht keinen solchen Mechanismus vor. Es scheint absehbar, dass sich eine äquivalente Situation zu den gemeinhin bekannten "Cookie-Bannern" entwickelt.

- **Privacy Dashboard**
  Die eIDAS Regulierung sieht vor, dass Nutzer*innen stets einen Überblick darüber haben, welche Parteien aktuell über welche ihrer Daten verfügen. In Abschnitt 4.2.1. wird die Verpflichtung der Parteien hierfür digital ansprechbar zu sein, grundlegend verworfen und die Verantwortung auf die Wallet Lösung zugedacht. Ein Recht auf Datenlöschung ohne eine technische Grundlage zur digitalen Datenabfrage oder digitalen Anforderung der Datenlöschung scheint nicht im Sinne der eIDAS Verordnung. Den Nutzer*innen bliebe der Griff zum Telefon, das Schreiben eines Briefes, oder das Senden eines Faxes oder einer Mail. Wie auf diesen Wegen die Nutzer*innen nachweisen sollen, dass es sich um ihre Daten handelt, da die Nutzung der EUdI-Wallet nicht gewährleistet ist, erscheint unklar.

- **Unbeobachtbarkeit**
  Politische Motivation der EUdI-Wallet ist es, der Bevölkerung der EU zu ermöglichen sich digital zu bewegen, ohne auf die Dienste großer Plattformanbieter zurückzugreifen [14]. In der eIDAS Regulierung mehrfach explizit ausgeführt, dass es Anbietern nicht möglich sein soll die Nutzung nachzuvollziehen. Der Anspruch einer privacy-by-design-Architektur findet sich im ARF nicht.

Gregor Bransky gregor.bransky@inoeg.de – Tel: 0176 209 66 393

- **Unverknüpfbarkeit**
  Die Artikel 5a(16)(a) und Punkt (b) stellen weiterhin sicher, dass - solange keine gesetzliche Grundlage (bspw. Geldwäsche und Terrorismusbekämpfung) dem entgegensteht - es dritten Parteien nicht möglich sein soll, unterschiedliche Fälle der Nutzung der Wallet zu verknüpfen. Weder bei wiederholter Interaktion mit der selben Nutzer*in (bspw. Zigarettenautomaten) noch der Abgleich zwischen unterschiedlichen Parteien. Mit den aktuell in der EU-Spezifikation vorgesehenen Technologien ist es nicht möglich, diese Anforderungen zu erfüllen. Entsprechende Ansätze, bspw. für Zero-Knowledge Proofs, sind seit 20 Jahren erprobte Techniken, siehe u.a.[3][5]. Es droht sonst sog. Overidentification. Darauf hat unter anderem der CCC hat in den Anhörungen im Innenausschuss 2021 [15] und im Digitalauschuss 2022 [16] hingewiesen.

- **Abstreitbarkeit und sog. signed credentials**
  Authentizität von Daten wird regelmäßig durch die Verwendung digitaler Signaturen hergestellt, welche eine lange und starke Beweiskraft besitzen, mitunter leider auch in Identifizierungskontexten. Mit dem Merkmal „Abstreitbarkeit“ wird sichergestellt, dass die Partei, gegenüber der sich Nutzer:innen authentifiziert haben, nicht in der Lage ist, die Authentizität der Identifizierungsinformation gegenüber Dritten zu beweisen. Mit anderen Worten können Nutzer:innen die bereits erfolgte Identifizierung gegenüber Dritten stets abstreiten. Im Falle signierter Identifizierungsinformationen ist dies nicht möglich. Der Einsatz abstreitbarer Lösungen würde zudem verhindern, dass Datenhändler in der Lage sind, einen Markt langlebiger kryptographisch signierter Datensätze aufzubauen. Der CCC hat in Anhörungen im Innenausschuss 2021 [14] und im Digitalauschuss 2022 [15] explizit auf das Risiko staatlich signierter Identitätsdaten hingewiesen. Ein tagesaktuelles Beispiel (01.07.2024), dass es sich um ein realistisches Szenario handelt, zeigt die illegal vom Anbieter BinDoc betriebene Falldatenbank im Gesundheitsbereich [17]. Google und Mozilla haben es 2022 im Rahmen des W3C abgelehnt (formal Objection), die für im ARF referenzierten Spezifikationen grundlegende DID Spezifikation in ihren Browsern zu implementieren. Das entsprechende Gremium sieht ausschließlich einstimmige Entscheidungen vor.

- **Portabilität der Daten**
  Der Anspruch die Wallet Anbieter*in zu wechseln, findet sich im ARF nicht wieder.

Gregor Bransky gregor.bransky@inoeg.de – Tel: 0176 209 66 393

eIDAS expert group: Nicht konsultiert

Die im Mai publizierte V 1.4 des ARF stellen nach aktuellem Stand Drafts dar und haben bisher nicht den formalen Zustimmungsprozess der eIDAS Expert Group durchlaufen, der letzte Termin der eIDAS Expert Group fand im Februar 2024 statt [7]. Die aktuelle Version von der EUC in Zusammenarbeit mit einem Dienstleister, basierend auf Diskussionen und Dokumenten der eIDAS Expert Group entwickelt. Der Expert Group wurde für die Kommentierung der letzten Version ARF V 1.3 eine sehr kurze Frist eingeräumt und es wurde lediglich die Definition von roten Linien zugestanden. Eine Zustimmung scheint unwahrscheinlich.

Im Fall weiteren Interesses sei an die Vertreter*innen des BSI als Teil der eIDAS expert group verwiesen.

Akademia: Spezifikation nicht Stand der Technik

In Summe haben sechzehn namhafte Kryptographie Lehrstühle (u.a. Anna Lysyanskaya, Brown University, Carmela Troncoso, EPFL) in Konsens dargelegt, dass mit den in der ARF V 1.4 verwendeten kryptographischen Verfahren, die in der eIDAS Verordnung festgeschriebenen Ziele nicht erreichbar sind und sich dies nicht mit kleineren Modifikationen erreichen lässt, sondern ein kryptographisches Redesign auf seit 20 Jahren etablierte Zero-Knowledge Proofs mit überschaubarem Aufwand umsetzbar scheint. Weiterhin ist aufgrund bestehender wissenschaftlicher Erkenntnisse im Bereich der Zero-Knowledge Proofs gesichert, dass sich der Stand der Technik auf absehbare Zeit zukunftsweisend weiterentwickeln wird.

Zitat: "*Unfortunately, we believe that some of the currently suggested design aspects of the EUDI and its credential mechanism fall short of the privacy requirements that were explicitly defined after extensive debate in the Digital Identity regulation. The main reason for this shortcoming in the current proposal is that it relies on cryptographic methods that were never designed for such requirements. We do not see a way to fix the proposed solution to meet all the privacy features as required by the regulation; we believe that a larger redesign is in order.* " [5].

Im Fall weiteren Interesses sei hier an Anja Lehmann vom Hasso-Platter-Institut und der Universität Potsdam als Leitautorin verwiesen.

Gregor Bransky gregor.bransky@inoeg.de – Tel: 0176 209 66 393

IETF: Grundlegende Spezifikationen - End of life

Google und Mozilla haben es 2022 im Rahmen des W3C abgelehnt (formal Objection), die für im ARF referenzierten Spezifikationen grundlegende DID Spezifikation in ihren Browsern zu implementieren. Es sind keine Anzeichen von Arbeiten im Rahmen von Standardisierungsprozessen allgemein bekannt, die darauf schließen lassen, dass eine Implementierung absehbar ist. Damit ist das Ziel eines “login in mit EUID Wallet” Features in den für 447 Millionen Europäer handelsüblichen Browsern (Chrome, Firefox) mit dem ARF 1.4 vermutlich nicht gegeben.

Zitat: “*All major browser vendors ultimately blocked further DID specification in 2022 and there is no reason to assume that there will be any support from them in the future: …*” [8]

Im Fall weiteren Interesses sei hier an Dr. Henk Birkholz vom Fraunhofer SIT verwiesen, er ist u.a. Subject Matter Expert für das National Security Telecommunications Advisory Committee des US-Präsidenten.

Gregor Bransky gregor.bransky@inoeg.de – Tel: 0176 209 66 393

Quellen:

[1] Revision of the eIDAS Regulation – European Digital Identity (EUid)
[2] eudi-doc-architecture-and-reference-framework/docs/arf.md at main · eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework · GitHub
[3] eIDAS Architecture Reference Framework 1.4 - epicenter.works
[4] EUDI-Wallet: Eine Brieftasche voller Schlupflöcher
[5] Cryptographers' Feedback on the EU Digital Identity's ARF · Issue #200
[6] European Digital Identity Wallet
[7] Register of Commission expert groups and other similar entities
[8] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/issues/205
[9] IETF
[10] W3C
[11] Epicenter.works
[12] Feb 15, 2022 Support to the implementation of the European Digital Identity Framework and the implementation of the Once Only System under the Single Digital Gateway Regulation ID: DIGITAL-2022-DEPLOY-02-ELECTRONIC-ID
[13] https://www.cisa.gov/sites/default/files/2023-04/NSTAC_Strategy_for_Increasing_Trust_Report_%282-21-23%29_508_0.pdf
[14] Europäische digitale Identität
[15] https://www.ccc.de/de/updates/2021/gemeinsame-stellungnahme-zum-eid-gesetz-entwurf
[16] https://www.bundestag.de/dokumente/textarchiv/2022/kw27-pa-digitales-identitaeten-901172
[17] https://www.heise.de/news/Gutachter-IT-Dienstleister-BinDoc-betreibt-illegale-Krankenhaus-Falldatenbank-9785718.html

Gregor Bransky gregor.bransky@inoeg.de – Tel: 0176 209 66 393