Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Stellungnahme

Implementing Acts zur eIDAS 2.0 (Integrität und Kernfunktionen, Personenidentifizierungsdaten und elektronische Attributsbescheinigungen, Zu unterstützende Protokolle und Schnittstellen, Zertifizierung)

Lobbyregister-Nr. R001459
EU-Transparenzregister-Nr. 52646912360-95

Kontakt:
Tim Kremer
Telefon: +49 30 20225-5314
E-Mail: tim.kremer@dsgv.de

Berlin, 25. September 2024

Federführer:
Deutscher Sparkassen- und Giroverband e. V.
Charlottenstraße 47 | 10117 Berlin
Telefon: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

I. Vorbemerkung:

Wir bedanken uns für die Gelegenheit zur Stellungnahme. Mit dem vorliegenden Papier übermitteln wir einige grundsätzliche Erwägungen und geben zusätzliche Anregungen.

Die Implementing Acts sind insgesamt zu allgemein gehalten. Es muss sichergestellt werden, dass europaweite technische und rechtliche Interoperabilität sichergestellt wird und europaweit gleiche Bedingungen für Bereitstellung und Nutzung der Wallet gelten. Es sollte verhindert werden, dass sogenannte technische und rechtliche Vermittler („Konverter") zwischen den Ländern notwendig werden. Es darf insbesondere nicht zu einem sog. „gold-plating" kommen, bei dem in einem Mitgliedsstaat strengere Anforderungen gelten, als in einem anderen.

Die Entwürfe für die Implementing Acts sind erkennbar unfertig. Sie müssen konkreter werden und wesentliche Vorgaben direkt enthalten, so könnten z.B. Teile des Architecture and Reference Frameworks (ARF) in die Implementing Acts überführt werden. Dort werden bereits etablierte Begriffe, Definitionen und technischen Beschreibungen verwendet, die sich in den vorliegenden Entwürfen nicht wiederfinden. Beispielsweise sollte der Begriff „Wallet Secure Cryptographic Device" (WSCD), der in jedem der Implementing Acts definiert ist, dahingehend präzisiert werden, dass das WSCD als Remote WSCD, Local External WSCD oder Local WSCD implementiert werden kann.

Darüber hinaus arbeiten die europäischen Normungsorganisationen CEN TC/224 und ETSI ESI gemeinsam an der Entwicklung einer Reihe von Normen zur Unterstützung des eIDAS2-Rechtsrahmens im Allgemeinen und der EU Digital Identity Wallet im Besonderen. Der Gesetzgebungsprozess zur Ausarbeitung der Implementing Acts sollte diese Normungsarbeiten berücksichtigen.

Zu den einzelnen Implementing Acts nehmen wir wie folgt Stellung:

1. Integrität und Kernfunktionen

- Ein EU-weiter Standard ist insbesondere für eine technische Interoperabilität erforderlich und ist auch Basis für die Akzeptanz und Verbreitung der EU Digital Identity Wallets.

- Die Kernfunktionen müssen genauer beschrieben werden. Beispielweise ist nicht klar, was es konkret bedeutet, dass die in Art. 6 Abs. 3 d Mechanismen für die Authentifizierung der „wallet user" von den „wallet units" unabhängig sein sollen; vgl. Art. 6 Abs. 3 e.

- Bei den Transaction Logs sollte je nach Anwendungsfall unterschieden werden können: Es wird nicht immer gewollt sein, dass sämtliche Transaction Logs mit allen Informationen zu Verfügung stehen. Hier bietet sich eine optional vom Anwender einzustellende Version an. Genauso kann es Anwendungsfälle geben, in denen ein Komplett-Log verpflichtend sein sollte. Zwei Beispiele:

  1) Aus Datenschutzgründen entscheidet sich eine natürliche Person dafür, nicht alles loggen zu wollen. Risiken (Wiederherstellung der Daten nicht möglich) kennt sie.

  2) Es handelt sich um eine Organisations-Wallet. Hier sollten sämtliche logs geschrieben werden und verfügbar sein - von allen Bevollmächtigten.

- Es werden noch sehr unterschiedliche Optionen zur Erstellung einer QES aufgezeigt. Das spiegelt vermutlich den aktuellen Arbeitsstand wider. Es wäre wünschenswert, wenn es hier zeitnah Spezifizierungen geben würde.

2. Personenidentifizierungsdaten und elektronische Attributsbescheinigungen

- Die eIDAS-VO sieht nach unserem Verständnis explizit die Bereitstellung von EUDI-Wallets für natürliche Personen, juristische Personen und auch natürliche Personen, die juristische oder natürliche Personen vertreten, vor. Es fehlt bisher vollständig an Regelungen Juristische Personen und Vollmachts- bzw. Vertretungsverhältnisse. Wann und wo sollen die erforderlichen Regelungen aufgenommen werden?

  Es sollte ein europaweit einheitlich verpflichtendes (QEAA-) Datenset geben, welches z.B. alle verpflichtenden Angaben gemäß der EU-Geldwäsche-Verordnung umfasst, um einen standardisierten EU-einheitlichen Identifizierungsprozess des Vertragspartners (KYC) zu gewährleisten. Die angestrebten Use Cases (u.a. Legitimation zur Kontoeröffnung) müssen mit den in der Wallet verfügbaren Daten (rechts-) sicher erreicht werden können, entweder als PID- oder in Kombination mit QEAA Datenset auf ausreichendem Vertrauensniveau.

  Da es in diesem Implementing Act A um die Personenidentifizierungsdaten (PID) und qualifizierte elektronische Attributsbescheinigungen (QEAA) geht, wäre es sinnvoll, die PID/QEAA-Anforderungen aus dem Implementing Acts Entwurf für EUDIW-Integrität und Kernfunktionalitäten in den Entwurf für EUDIW-Personenidentifizierungsdaten und elektronische Attributsbescheinigungen zu verschieben. Die CEN TC/224 WG20 arbeitet derzeit an einer Norm mit Leitlinien für das Onboarding der PID in die EUDIW. Es wird daher empfohlen, die CEN-Norm als Referenz zu diesem Implementing Act zu betrachten.

- Es gibt Überschneidungen zwischen mandatory und optional data in den im Annex gelisteten Attributen: birth_place (mandatory, Attribute und Datenanforderung nur unzureichend spezifiziert/standardisiert) und drei differenzierte aber nur optionale Datenfelder für birth_city, birth_state, birth_country. Eine Aufteilung des „birth_place" in einzelne Attribute (Birth_country, Birth_City) inkl. Konkretisierung der Data Specification ist für mandatory Attribute der vorzuziehen. Die Zusammenfassung von bis zu drei Attribut-Angaben (city, state, country) in einem Attribut ohne weitere Spezifikation ist nicht zielführend und trägt nicht zu sinnvoll verwendbaren Daten bei.

  Die Implementing Acts sind auch in Bezug auf die PID nicht hinreichend konkret. Es ist u.a. unklar, wie mit den folgenden Konstellationen umgegangen werden soll:

  - Namens- oder ausweisrechtlichen rechtlichen Besonderheiten (Adels- und akademische Titel, Fehlen eines Vornamens o.ä.). Ebenso ist offen, wie mit Mehrstaatlern und Staatenlosen umgegangen werden soll.

  - Das Feld Ablaufdatum ist verpflichtend, es gibt jedoch Ausweise (z.B. griechischer Pass), die kein Ablaufdatum haben. Es ist nicht klar, was hier übermittelt werden soll.

- Warum kann der Countrycode in der Issuing_Authority eventuell vorhanden sein, wenn es doch dafür ein separates Feld gibt? Auch hier stellt sich die Frage nach der Aufteilung des Strings.

- Revokation der PID und von EAAs:

- Wenn eine PID aufgrund von Identitätsbetrug bei Ausstellung der eID revoziert wird, erhalten dann Relying Party mit berechtigtem Interesse (= Banken) auch aktiv diese Information?

- Allgemein: welche Anforderungen gibt es an den Revokationsprozess aus einer Userperspektive? Wie muss sich der User identifizieren oder wie wird sichergestellt, dass die Wallet nicht durch unberechtigte dritte Personen widerrufen werden kann?

- Wenn Provider auch nicht-staatliche Stellen sein können, wie erfolgt dann ein Widerruf von einer PID, die auf Basis einer falsch ausgegebenen eID ausgestellt wurde. Damit ist gemeint, dass unter Vorspiegelung falscher Tatsachen ein echter Ausweis ausgestellt wird. Hier muss in allen Fällen, in jedem Land, der Link zum Ausgangsdokument bestehen, bzw. sofern der Provider einer PID einer staatlichen Stelle entspricht, muss auch hier immer gewährleistet sein, dass mit Verlust des Originals mindestens keine neue PID auf dieser Basis ausgestellt werden kann oder beim Melden eines Missbrauchs die PID revoziert wird.

- Warum sollen EAA-Issuer die ausgestellten Credentials widerrufen können, wenn die wallet unit widerrufen wurde? Die Credentials sind an das Gerät und an die Wallet gebunden. Wird die Wallet deaktiviert, hat man so oder so keinen Zugriff auf die Credentials. Was ist mit Credentials, die geteilt wurden, z.B. Fahrzeugscheine? Und woher soll der EAA-Issuer technisch gesehen wissen, dass eine wallet unit revoziert wurde?

- Soll es die Möglichkeit einer temporären Sperre geben, z.B. beim mutmaßlichen Verlust des Smartphones?

3. <u>Zu unterstützende Protokolle und Schnittstellen:</u>

- Die Protokolle und Interfaces sind unzureichend beschrieben, um eine Implementierung darauf aufsetzen zu können. Sie sollten besser mit dem ARF synchronisiert werden. Einheitliche technische Standards sind Grundvoraussetzung für die Umsetzung und damit obligatorisch zu definieren. Standards sollten Varianten, Lokalisierungen und Optionen zur Gewährleistung der bestmöglichen Kompatibilität möglichst vermeiden.

- In den Annexen wird auf ISO/IEC 18013-5:2021 sowie W3C Verifiable Credential Data Model verweisen. Allerdings fehlen insbesondere Issuing Protokolle wie OpenID4VCI. Auch hier sollten die Implementing Acts besser mit dem ARF synchronisiert werden.

- Es wird empfohlen, den Implementing Act und den entsprechenden Anhang entsprechend dem im ARF dargestellten Ökosystem zu organisieren. Darüber hinaus kann der Normentwurf ETSI TS 119 462 „Wallet interfaces for trust services and signing” im Hinblick auf die für die

verschiedenen Arten von Schnittstellen zu verwendenden APIs und Protokolle berücksichtigt werden.

- Für die Interoperabilität sollten praxisnah mindestens die folgenden Technologien Berücksichtigung finden (QR-Code, NFC, Bluetooth, Datenprotokolle wie Interprotokolle). Auch hier sollten die Implementing Acts besser mit dem ARF synchronisiert werden.

- Die Protokolle und Interfaces sollten kompatibel sein zu anderen großen EU/EZB-Tech-Initiativen oder auf diese jeweils referenzieren, z.B. der Digitale Euro, um ein einheitliches Digitales Ökosystem zu gewährleisten.

- Darüber hinaus wirft der IA-Entwurf noch weitere Fragen auf:

  - Es ist vorgesehen, dass für spezifische Use Cases weitere Protokolle und Schnittstellen genutzt werden können, ohne die Anwendungsfälle näher zu beschreiben.

  - Es ist nicht klar, wer die „provider of wallet relying party access certificates" sein werden. Diese müssen selbst auch zertifiziert sein.

  - Nicht jede Relying Party kann potentiell jedes Credential erhalten/anfragen, sondern der Herausgeber bestimmt welche Gruppe der Relying Parties seine Credentials lesen/empfangen darf. Dies ist einerseits sinnvoll, andererseits erhöht es die Umsetzungskomplexität und widerspricht dem Self Sovereign Ansatz der eIDAS. Ein analoges Dokument hat diese Einschränkung nicht.

  - Über welches Protokoll sollen Anfragen zur Datenlöschung an Relying Parties übermittelt werden?

  - In welchen Fällen wäre es nicht erforderlich bzw. anwendbar anzuzeigen, welche Information (Attributes) die Relying Party fordert?

  - Was ist, wenn die Wallet gewechselt wird. In diesem Fall könnte die neue Wallet nicht dazu verwendet werden, um eine Relying Party bitten, die zuvor (mit der alte Wallet) geteilten Daten zu löschen? Wie soll das geregelt werden, wenn das die Absicht der Datenschutzfunktion ist?

  - Wenn z.B. eine deutsche Wallet benutzt wird, würde der Nutzer die deutschen Behörden über eine sich falsch verhaltende Relying Party informieren, auch wenn diese aus einem anderen Mitgliedstaat stammt? Wie sollen die Backend-Prozesse der Behörden funktionieren und was wird das Ergebnis einer solchen Meldung sein? Wird das auf EU-Ebene festgelegt?

4. <u>Zertifizierung</u>

- Die einzelnen Zertifizierungs-Schemes und Aufsichtsbehörden sind nicht ausreichend harmonisiert. Es existiert daher kein europaweit einheitliches Level Playing Field für die Zertifizierungs-Schemes.

- Die EUDIW-Zertifizierungsempfehlungen im ARF und der von ENISA herausgegebenen EUDIW-Zertifizierungsanalysebericht sollten bei der Entwicklung der IAs berücksichtigt werden.

- Es gibt keine gemeinsame Verlässlichkeit in Sachen Datenschutz-Konformität. Eine für die Mitgliedstaaten optionale datenschutzrechtliche Zertifizierung würde zu einem unterschiedlichen Datenschutzniveau führen.

- Eine einheitliche Prüfung der Funktionalitäten und Anforderungen (Datensets, etc.) über alle zertifizierten Wallets, bzw. alle Zertifizierungs-Schemes ist aus den aktuellen Implementing Acts nicht erkennbar. Die eIDAS-VO sieht grundsätzlich für bestimmte Anwendungsfälle und Branchen Akzeptanzpflichten vor. In Bezug auf diese wäre – an geeigneter Stelle – eine abschließende und klare Definition der hierunter fallenden Anwendungsfälle wünschenswert oder der Verweis auf entsprechende Stelle, an der diese Aspekte geregelt werden. Dies auch, da weitere Vorgaben auf diese aufsetzen (können) z.B. im Falle darauf anwendbare Aufbewahrungsfristen (vgl. hierzu Art. 18 Abs. 1 des Durchführungsrechtsakts im Entwurf „laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets" mit Verweis auf nationales Recht oder Rechtsakte der EU betreffend maßgeblicher Aufbewahrungsfristen.

- Wie würden Wallet-Nutzer davon erfahren, wenn die Zertifizierungsstellen das Konformitätszertifikat einer Wallet unverzüglich aussetzt, nachdem eine Sicherheitsverletzung oder Kompromittierung der Wallet sich auf ihre Konformität mit den Anforderungen der nationalen Zertifizierungssysteme auswirkt. Oder über eine bevorstehende Annullierung des Konformitätszertifikats informiert wird?