Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)56

29.06.2022

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Fragenkatalog

Anhörung Digitale Identitäten – Ausschuss für Digitales
04. Juli 2022

Nationale Ebene

1. Wo steht Deutschland im Bereich der Digitalen Identitäten (eID, SmarteID und Wallet)? Wo sehen Sie die größten Hürden?

Nach den Erfahrungen des BSI ist es notwendig mehr Wissen über das bestehende eID System mit allen seinen Komponenten und Wirkweisen (z.B. Nutzung am NFC-fähigen Smartphone ohne weiterer Hardware) in die Fläche zu bringen. Die bisherige Erfahrung zeigt: Sobald Bürgerinnen und Bürger wissen, dass und wie sie ihren Online-Ausweis nutzen können, verwenden sie ihn.

Das Interesse am Online-Ausweis ist trotzdem erkennbar gestiegen:
- erfolgreiche Transaktionen in 2020: 742.000
- erfolgreiche Transaktionen in 2021: 1,4 Mio.
- erfolgreiche Transaktionen in 2022: 1,8 Mio. bis einschl. Mai

Die Bundesregierung verfolgt – ebenso wie andere Mitgliedstaaten – die evolutionäre Weiternutzung und -entwicklung des vorhandenen eID-Systems. In Deutschland ist das die eID-Infrastruktur des deutschen Personalausweises. Diese Infrastruktur soll um die Nutzungsmöglichkeit der ID-Funktion auf dem Smartphone („Smart-eID"-Funktion) und um eine Wallet-Funktion für weitere Nachweise ergänzt werden. Gleichzeitig sollen die rechtlichen und sicherheitstechnischen Vorgaben der bestehenden Datenschutz- und IT-Sicherheitsstandards erhalten werden. Eine große Herausforderung wird sein ein ausgewogenes Verhältnis von Sicherheit, Datenschutz, Nutzerfreundlichkeit und hoher Anwendungsbreite zu erzielen. Das BSI ist zentraler Bestandteil dieser Bestrebungen.

2. Mit der eID gibt es seit mehr als 12 Jahren eine digitale Identitätslösung. Wie bewerten Sie diese und warum wurde die Lösung vergleichsweise wenig genutzt? Welche Rolle könnte die eID noch in der Zukunft spielen?

Nach Auffassung der Bundesregierung stellt es eine Kernaufgabe des Staates dar, Bürgerinnen und Bürgern sichere Identifizierungsmittel zur Verfügung zu stellen. Mit dem Online-Ausweis existiert eine Technologie,

Zustell- und Lieferanschrift: Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn

durch die der Staat allen Bürgerinnen und Bürgern ein sicheres Verfahren zur elektronischen Identifizierung zur Verfügung stellt.

Nur wenn die angebotenen Produkte einfach zu verwenden sind und gleichzeitig den notwendigen Datenschutz sowie die notwendige IT-Sicherheit bieten, werden sie auf eine breite Akzeptanz stoßen. Die Lösungen sollen zudem auch im europäischen Rahmen skalieren können. Dies betrifft sowohl die Funktionalität als auch die Komplexität bei der Einbindung der ID-Lösungen in die eigenen digitalen Angebote.

Die Gründe für die geringe Nutzung der Online-Ausweisfunktion sind vielfältig. Zu nennen ist hier ein fehlendes Angebot von Dienstleistungen sowohl von privatwirtschaftlicher als auch von öffentlicher Seite. Gerade die öffentliche Seite könnte mit einem vielfältigen Angebot zu einem Durchbruch der Online-Ausweisfunktion beitragen.

Zur Verbesserung der Zugänglichkeit wurde Anfang dieses Jahres der PIN-Rücksetzdienst eingeführt, welcher es Bürgern von zu Hause aus ermöglicht ihren Ausweis zu aktiveren oder ihre PIN neu zu setzen. Um die Nutzerfreundlichkeit der Online-Ausweisfunktion weiter zu erhöhen wird zudem die Smart-eID eingeführt (siehe hierzu Antwort auf Frage 8).

Weitere durchgeführte Verbesserungen sind beispielsweise:

1. Nach langsamen Start sind heute die meisten Smartphones NFC-fähig. NFC ist die Voraussetzung für die Nutzung des Online-Ausweises auf dem Smartphone, wodurch kein Kartenleser mehr angeschafft werden muss.
2. Seit 2021 stehen Plugins für gängige Webserver-Anwendungen (WordPress, Nextcloud usw.) bereit, um das Online-Ausweisen ohne technische Kenntnisse in eigene Webanwendungen zu integrieren.

Die Entwicklung der Online-Ausweisfunktion sehen wir positiv. So ist die eID bereits seit Anbeginn nach dem Prinzip einer Self-Sovereign Identity (SSI) konzipiert und für den Bürger nutzbar – lange bevor das SSI-Konzept in der Öffentlichkeit oder in der Privatwirtschaft diskutiert wurde. Die eID hat sich somit als belastbar gegenüber aufkommenden Anforderungen bewiesen und sie bietet eine zukunftssichere Ausgangslage für ihre Weiterentwicklung.

Die eID wird auch zukünftig eine wichtige Rolle spielen, da nur sie staatlich beglaubigte elektronische Personendaten bescheinigt. Die eID kann somit als Vertrauensanker für unterschiedliche Anwendungen oder abgeleitete eIDs, aus dem privaten oder öffentlichen Sektor, herangezogen werden.

3. Was erhoffen Sie sich vom nun geplanten "interministeriellen Laborformat" für digitale Identitäten?

Die Bundesregierung will die Aufgabe (aus Antwort 2) mit einer interministeriellen Arbeitsgruppe angehen, die sich von unmittelbar bei den Nutzerinnen und Nutzern ermittelten Bedarfen leiten lässt. Schwerpunkte der Arbeitsgruppe werden – jeweils unter Beibehaltung strengster Anforderungen an Datenschutz und Datensicherheit – sein:

- Weiterentwicklung des eID-Systems zu mehr Nutzungsfreundlichkeit sowohl für Bürgerinnen und Bürger als auch für Anbieter von digitalen Leistungen,
- Vereinfachung des mobilen Zugangs zu Verwaltungsleistungen,
- Erforschung innovativer Identifizierungsverfahren im Rahmen des Innovationswettbewerbs „Schaufenster Sichere Digitale Identitäten“[1] (unter FF des BMWK),
- Bewerbung für sogenannte Large Scale Pilots im Kontext der Vorgaben der EU zur EU DI-Wallet[2] und der eIDAS 2.0 Novellierung.

4. Welche konkreten rechtlichen, regulatorischen oder ökonomischen Maßnahmen müssen noch in welcher Reihenfolge ergriffen werden, damit eIDs in Deutschland erfolgreich eingesetzt und von den Bürgerinnen und Bürgern angenommen werden (bspw. Wegfall des Schriftformerfordernisses)? Bitte bewerten Sie diese hinsichtlich Kurzfristigkeit/Langfristigkeit der Wirksamkeit und Priorität sowie benennen Sie möglichst präzise den Adressaten. Welche Erweiterungsmöglichkeiten bieten sich mit Blick z.B. auf Führerschein, Gesundheitskarte, Impfnachweise, Betriebsausweise (siehe Hotel Checkin Pilot)? Gibt es noch weitere Potenziale?

Die in der Frage adressierten zu klärenden Punkte sind Bestandteil des Projektauftrages Digitale Identitäten[3]. Ein bestehendes Projektziel ist, dass klare Umsetzungsvorschläge bezüglich der ggf. rechtlichen, regulatorischen und/oder ökonomischen Maßnahmen erarbeitet sind und hinsichtlich der jeweiligen Wirksamkeit priorisiert und umgesetzt wurden.

5. Welche möglichen Interessenkonflikte könnten durch die Verteilung von Entscheidungshoheiten und „Schaufensterprojekten“ zwischen Ministerien, der Privatwirtschaft und der Gesellschaft entstehen? Gibt es mögliche Widersprüche bzw. Konfliktpotenziale zwischen den gesellschaftlichen Zielen und möglichen Gewinnwirtschaftsabsichten?

---

1 https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html

2 Das „DI“ im Namen „EU DI-Wallet“ steht für „Digital Identity“.

3 https://www.personalausweisportal.de/Webs/PA/DE/verwaltung/projekt_digitale_identitaeten/projekt_digitale_identitaeten_node.html

Durch die interministerielle Arbeitsgruppe des Projektes Digitale Identitäten des BMI sollen die offenen Fragen gemeinsam gelöst werden.. Dieser Arbeit möchten wir nicht vorgreifen.

6. Welche Verfahren sind für die Revozierung eines Wallet vorgesehen? Was werden die Folgen für Bürger*innen sein, die den Zugang zu ihrem eID-Wallet nicht mehr haben, etwa weil ein Wallet revoziert (deaktiviert) wurde, weil sie ihre PIN vergessen oder ihr Smartphone verlieren oder es gestohlen wird?

Mit der Ausgestaltung dieser inhaltlichen Fragen auch zu einer Wallet beschäftigt sich das Projekt Digitale Identitäten des BMI. Nach jetzigem Planungstand und Wissen des BSI ist das Befüllen der Wallet durch ein initiales Verwenden von Ausweisdokumenten vorgesehen. So muss bei der Smart e-ID zunächst der Personalausweis über die NFC-Schnittstelle des Smartphones ausgelesen werden, ehe die eID auf dem Secure Element hinterlegt wird. Dies kann bei neuen Geräten – oder nach Deaktivierung auch auf bereits genutzten Geräten – jederzeit erfolgen.

7. Wo sollten staatlich beglaubigte elektronische Personendaten eingesetzt werden dürfen? Wie kann gewährleistet werden, dass bei digitalen Identitäten Offenbarungsverbote (§ 5 Transsexuellengesetz) auch weiterhin eingehalten werden können? Wer legt fest, welche Arten von Attributen die eID dokumentiert und mitteilt (bspw Alter, Gender) und wer legt fest, welche „Werte“ diese Attribute haben können (im Fall von Gender: männlich, weiblich, noch weitere)?

Personenbezogene Daten müssen durch geeignete technische und organisatorische Maßnahmen vor missbräuchlicher Verwendung geschützt werden. Bei der Umsetzung einer elektronischen Identität oder Wallet muss daher darauf geachtet werden, dass erstens persönliche Identitätsattribute nur an seriöse Diensteanbieter mit berechtigtem Interesse übermittelt werden (siehe hierzu auch Antwort zu Frage 16), und dass zweitens die übermittelten Daten für Dritte wertlos sind (siehe hierzu auch Antwort zu Frage 8).

In Falle der Online-Ausweisfunktion wird die Verwendung der Personendaten bereits durch das PAuswG, das AufenthG, das eIDKG, sowie deren nachgelagerte Verordnung gesetzlich reguliert. In diesen sind auch die erlaubten Attribute abschließend benannt, welche im Rahmen der Online-Ausweisfunktion gespeichert und übermittelt werden dürfen. Die notwendigen technischen und organisatorischen Maßnahmen werden durch die in den Gesetzestexten normativ referenzierten Technischen Richtlinien des BSI vorgeben.

Attribute wie Geschlecht oder Gender bieten für die sichere Identifizierung von Personen nur einen geringen Mehrwert. Aus diesem Grund werden diese Attribute im Personalausweis, dessen Online-Ausweisfunktion und

der hierauf aufbauenden Smart-eID nicht gespeichert und können folglich auch nicht weitergegeben werden.

Für mögliche weitere staatliche oder privatwirtschaftliche Systeme zur Bereitstellung elektronischer Identitäten sollten vergleichbare regulatorische Maßnahmen implementiert werden, bevor diese echte Nutzerdaten verarbeiten dürfen.

Speicherung/ Technologie

8. Wie definieren und bewerten Sie das Self-Sovereign Identity (SSI)-Konzept? Eine Kritik an SSI ist, dass beglaubigte Daten bei den Empfängern gespeichert würden. Wie bewerten Sie die Datensicherheit des SSI-Konzepts? Gibt es aus Ihrer Sicht technische Wege, wie diese Empfangsspeicherung durch SSI vermieden werden kann?

SSI ist zunächst ein Schlagwort, unter welchem mehrere Prinzipien und Paradigmen für Identitätssysteme zusammengefasst werden. Eine einheitliche Definition von SSI existiert bis dato nicht. Häufig werden mindestens die Anforderungen Transparenz, Nutzerkontrolle und Dezentralität genannt. Der Nutzer soll hierbei über die Möglichkeit verfügen, die Verwendung seiner Identitätsdaten vollständig zu kontrollieren, ohne dass es der Erlaubnis eines Vermittlers oder einer zentralen Partei bedarf. Zudem soll er über die Kontrolle verfügen, wie und mit wem seine persönlichen Daten geteilt und verwendet werden.

Das Prinzip der nutzerkontrollierten, souveränen Verwaltung und Weitergabe von Daten begrüßen wir grundsätzlich. Erwähnenswert ist, dass in einem großen Teil der SSI-Community das SSI-Konzept stark mit der Nutzung von Blockchain-Technologie und einer dezentralen Architektur in Verbindung gebracht wird (s. auch Frage 13). Aus Sicht des BSI ist eine derartige Umsetzung jedoch keineswegs zwingend. Stattdessen sollte im Sinne der Technologieneutralität vor der Entscheidung über die technische Umsetzung eine sorgfältige Analyse der tatsächlich benötigten Funktionen und Sicherheitseigenschaften stehen. Zur grundsätzlichen Einschätzung von SSI hat das BSI im Jahr 2021 ein Eckpunktepapier für Self-sovereign Identitites veröffentlicht, das unter *bsi.bund.de → Themen → Unternehmen und Organisationen → Kryptografie → Blockchain → Eckpunktepapier für Self-sovereign Identities (SSI)*[4] abrufbar ist.

Die Datensicherheit des SSI-Konzepts lässt sich nicht pauschal beantworten, da diese von der konkreten Umsetzung abhängt. Hier spielt sowohl die Gesamtarchitektur des Systems eine Rolle als auch die eingesetzten Sicherheitsmaßnahmen auf Software- und Hardwareebene,

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf

ebenso die verwendeten kryptografischen Verfahren. Ein sehr relevanter Aspekt ist dabei unter anderem die Frage, inwiefern die Seriosität von Diensteanbietern sichergestellt wird. Hier unterscheiden sich z. B. die Konzepte von eID und ID-Wallet erheblich.

Die Sorge, dass beglaubigte Daten beim Empfänger gespeichert würden, ist vom Grundsatz her berechtigt. Es muss daher darauf geachtet werden, dass erstens persönliche Daten nur an seriöse Diensteanbieter mit berechtigtem Interesse und einem überzeugenden Datensicherheitskonzept übermittelt werden, und dass zweitens die übermittelten Daten für Dritte wertlos sind.

In vielen Implementierungen von elektronischen Identitäten werden die Identitätsdaten mit einer elektronischen Signatur versehen, um deren Authentizität nachweisen zu können. Diese Signatur wird durch den Ausgeber der jeweiligen eID an den Identitätsdaten angebracht und ist nach jetzigem Kenntnisstand nicht fälschbar, jedoch beliebig vervielfältigbar. In der Folge ist jede Kopie der Kombination aus Identitätsdaten und Signatur vergleichbar mit einer beglaubigten Kopie. Problematisch ist hierbei, dass jede Person, die in den Besitz der Identitätsdaten mit Signatur gelangt, über nachweislich authentische Daten verfügt und dies auch beliebig an Dritte weitergeben kann, ohne dass der Inhaber der Identitätsdaten dies kontrollieren kann.

Daher sollten Daten zum Nachweis ihrer Authentizität nicht einfach mit einer Signatur versehen und an den Empfänger übermittelt werden. Stattdessen sollte, wie bei der Online-Ausweisfunktion des Personalausweises, die Authentizität der Daten durch den Hardware-Chip im Ausweis sichergestellt und implizit während des Identifizierungsvorgangs nachgewiesen werden. Dadurch ist die Echtheit der übermittelten Daten nur innerhalb der Kommunikation zwischen Diensteanbieter und Nutzer überprüfbar. Auf diesem Wege kann der Dienstanbieter weiterhin zweifelsfrei feststellen, dass es sich um eine echte Identität handelt. Sollte er die Daten aber später (unberechtigterweise) an Dritte weitergeben, kann er deren Echtheit nicht mehr beweisen, wodurch diese Daten ihren Wert für Kriminelle und Unbefugte verlieren.

9. Eine sichere Lösung zum Speichern der Daten auf dem Smartphone ist die Nutzung eines Secure Elements. Hieran ist jedoch eine soziale Frage geknüpft: Bisher haben nur neue, teure Smartphones die NFC-Schnittstelle und Secure Elements. Wie bewerten Sie dieses Problem heute sowie mittel- oder langfristig? Wie könnten sozialverträgliche Lösungen aussehen – auch für diejenigen, die gar kein Smartphone besitzen? Eine weitere technische Lösung ist die Nutzung der Secure-Enclave Ebene, die in mehr Smartphones zur Verfügung steht. Wie bewerten Sie diese Ebene in Bezug auf die Sicherheit und Performanz?

Die Speicherung von Identitätsdaten auf dem Smartphone ist zunächst eine Komfort-Funktion für die Verwendung des deutschen eID-Systems, bei welcher der Nutzer/ die Nutzerin nicht mehr die Ausweiskarte an einen NFC-Leser halten muss. Die Möglichkeit der Verwendung des Kartenausweises soll jedoch nicht abgeschafft werden, so dass auch in Zukunft die Nutzbarkeit des eID-Systems auf dem höchsten Vertrauensniveau für Nutzer ohne ein geeignetes Smartphone gewährleistet ist. Perspektivisch wird zudem in den nächsten Jahren eine zunehmende Verbreitung von geeigneten Secure Elements und eUICCs erwartet, so dass diese flächendeckend in Mobilgeräten verfügbar sind.

Die Secure Enclave ist eine durch die Firma Apple entwickelte und in die Geräte der Firma Apple verbaute Sicherheitsebene. Sie ist bei Apple Geräten seit mehreren Generationen in unterschiedlich tiefgehender Ausprägung vorhanden. Android Smartphones haben mit StrongBox ein ähnliches System. Bei beiden Lösungen steht jeweils die Abhängigkeit vom Entwickler und Anbieter der Ebene im Raum, eine grundlegende Aussage zur Performanz und Sicherheit kann daher immer nur im Einzelfall und auch nur für den aktuellen Zeitpunkt getroffen werden. Die durch beide Lösungen bereitgestellten Sicherheitsfunktionen sind zudem seitens der Hersteller in ihrem Umfang stark eingeschränkt. In der Folge sind wesentliche notwendige Funktionen, welche für die Realisierung der deutschen eID notwendig sind, nicht durch die Secure Enclave oder StrongBox abbildbar. Diese können dementsprechend nur durch Implementierungen in Software realisiert werden, wodurch schlussendlich nur ein niedrigeres Vertrauensniveau für eine Secure Enclave bzw. StrongBox basierte eID erreicht werden kann.

10. Als alternative Lösung wird eine verschlüsselte Speicherung auf dem Hauptspeicher des Smartphones anvisiert. Wie bewerten Sie diese Ebene in Bezug auf die Sicherheit und Performanz?

Ein solche Lösung würde die Sicherheit der Identitätsdaten und die Vertrauenswürdigkeit des Identifizierungsvorgangs lediglich durch software-basierte Mechanismen absichern können. Diese haben zum einen starke Abhängigkeit von dem zugrundeliegenden Mobil-Betriebssystem des Smartphones und sind zum anderen auch deutlich gefährdeter gegenüber Angriffen durch Schadsoftware. In der Konsequenz lässt sich hiermit absehbar nur ein niedriges Vertrauensniveau erreichen.

11. Eine weitere diskutierte Lösung für die Speicherung der Daten ist die eSIM auf den Smartphones. Wie bewerten Sie dabei die Rolle der Anbieter, die sich teilweise sperren, die eSIM für die staatlichen Lösungen zu öffnen? Inwieweit könnte der Digital Markets Act diese Gatekeeper-Handlung verhindern?

Die Sicherheit der Speicherung der Daten auf einer eSIM ist technisch ähnlich zu bewerten wie die Speicherung auf einem Secure Element. Bei der Verbreitung von eSIMs wird im Laufe der nächsten Jahre mit einem

deutlichen Anstieg gerechnet. Allerdings ist nicht jede eSIM für die Speicherung von zusätzlichen Daten geeignet.
Derzeit ist neben der technischen Eignung der eSIM auch die Mitwirkung der MNOs (Mobile Network Operator) nötig, um z.B. eID-Daten in einem MNO-Profil auf der eSIM ablegen zu können. Ein dedizierter Speicherbereich auf der eSIM, als Alternative zu der Nutzung der MNO-Profile, befindet sich momentan in der Standardisierung und wird mittelfristig zur Verfügung stehen. Die Zuständigkeit für die Provisionierung von Anwendungen in diesem Speicherbereich ist aktuell noch in Klärung.
Für die Nutzung der eSIM sind somit zwei Dinge nötig, eine technisch geeignete eSIM sowie der Zugang zu einem MNO-Profil oder (perspektivisch) dem dedizierten Speicherbereich. Initiativen wie der Digital Markets Act können hier starke Akzente setzen.

12. Wie schätzen Sie die Gefahr von Identitätsdiebstählen ein, wenn entsprechende Identifikationsdaten in einer Wallet auf Smartphones gespeichert werden und wie kann diese reduziert werden?

Die Gefahr von Identitätsdiebstählen aus einer Wallet hängt maßgeblich von der Ausgestaltung und Implementierung selbiger ab. Auf technischer Ebene muss hierbei einerseits ein geeignetes sicheres Speichermedium für die Speicherung und Verwendung der Identitätsdaten eingesetzt und andererseits sichere und vertrauenswürdige Protokolle implementiert werden, welche den Zugriff auf die gespeicherten Daten absichern. Eine anschließende Evaluierung und Zertifizierung der Komponenten und Funktionen der Wallet erbringt dann den Nachweis über die Eignung der Sicherheitseigenschaften. Gleichzeitig muss für den Betrieb der Wallet ein geeignetes Sicherheitskonzept für das gesamte System vorliegen und die Wallet muss im Rahmen wohldefinierteter Vorgaben betrieben werden (siehe hierzu auch Antwort auf Frage 7).
In der Betriebsphase muss die Wallet zudem sicherstellen, dass Identitätsdaten nur an seriöse Diensteanbieter mit berechtigtem Interesse übermittelt werden (siehe hierzu auch Antwort zu Frage 16), und dass zweitens die übermittelten Daten für Dritte wertlos sind (siehe hierzu auch Antwort zu Frage 8).

13. In Bezug auf die ID-Wallet-App weist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in seinem 30. Tätigkeitsbericht für das Jahr 2021 auf noch offene datenschutzrechtliche Fragestellungen beim Einsatz der Blockchain-Technologie hin. Wie bewerten Sie den Nutzen und die Erfordernis der Blockchain-Technologie in Konzepten digitaler Identitäten wie ID-Wallets?

Der Begriff SSI wird z.T. in derselben Community diskutiert und vorangetrieben, die sich auch mit Blockchain-Technologien befasst. Dennoch gibt es aus technischer Sicht keinen zwingenden Grund, SSI und digitale Identitäten mithilfe von Blockchain-Technologien umzusetzen (siehe auch Frage 8).

Derzeitige SSI-Ansätze sehen vor, dass gewisse Daten, die die Richtigkeit der vom Nutzer vorgelegten Identitätsattribute bezeugen, in manipulationssicheren, öffentlich einsehbaren Registern verwaltet werden. Blockchains können hier eine Möglichkeit zur Umsetzung eines solchen Registers darstellen; dabei werden oft Dezentralität, Manipulationssicherheit und hohe Verfügbarkeit als Vorteil genannt. Allerdings sind diese Eigenschaften kein Alleinstellungsmerkmal der Blockchain-Technologie. Andere Strukturen, die ebenfalls eine hohe Verfügbarkeit und Integritätsschutz bieten, sind ebenso denkbar. Technologische Beispiele sind unter anderem signierte Daten in verteilten Datenbanken oder Public-Key-Infrastrukturen (PKI).

Andere Eigenschaften von Blockchains können auch hinderlich sein: So ist z. B. die Löschung von Daten aus einer Blockchain technisch nicht vorgesehen, aber die dauerhafte Aufbewahrung längst abgelaufener Informationen ist inhaltlich meist überflüssig und erzeugt große Datenmengen. Die Transparenzanforderung an Register erfordert es, technisch sicherzustellen, dass keine Rückschlüsse auf sensible Inhalte und auch keine Verlinkungsangriffe ermöglicht werden. Das Sicherheitsrisiko ist insbesondere mit Blick auf die angesprochenen datenschutzrechtlichen Fragestellungen sorgfältig abzuwägen. Eine Übersicht zu den entsprechenden Fragen im Blockchain-Kontext hat das BSI bereits im Jahr 2019 unter Mitarbeit des BfDI veröffentlicht unter: *bsi.bund.de → Themen → Unternehmen und Organisationen → Kryptografie → Blockchain → Blockchain sicher gestalten - Konzepte, Anforderungen, Bewertungen (Blockchain sicher gestalten, Kapitel 9)*[5].

Ferner fehlen Sicherheitsempfehlungen für Blockchains insbesondere dort, wo neuartige Funktionen durch wenig untersuchte Protokolle und kryptographische Verfahren umgesetzt werden sollen (z. B. für Konsens und Widerruf).

Es sei angemerkt, dass das deutsche eID-System bereits seit über zehn Jahren zeigt, wie man einige der wesentlichen SSI-Paradigmen realisieren und dabei völlig ohne Blockchain-Technologie auskommen kann.

Basierend auf den obigen Ausführungen stand das BSI einer Nutzung von Blockchain-Technologie im Rahmen der ID-Wallet skeptisch gegenüber und hat die Verantwortlichen frühzeitig darüber informiert. Insbesondere war der Nutzen der Blockchain-Technologie aus Sicht des BSI unklar, erhöhte jedoch die Komplexität und damit einhergehend die grundsätzliche Anfälligkeit für Sicherheitslücken des gesamten Systems. In diesem Kontext hatte das BSI auch auf die fehlenden belastbaren

---

5 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf

Sicherheitsgarantien für neuartige kryptografische Verfahren (s. auch oben) hingewiesen.

14. Die derzeitige Beschreibung des eID-Systems lässt noch technische Details offen. Weitere Verfeinerungen können einen Einfluss auf Datenschutz und Sicherheit haben. So könnte eine auf der Wallet basierende Architektur, bei der die Wallet immer dann mit einem zentralen Cloud-Anbieter interagiert, wenn sich die oder der Nutzer*in bei einem Dienst authentifiziert, zu unerwünschtem Informationsverlust führen (etwa, wann und bei welchem Dienst die Wallet verwendet wird). Wird dies berücksichtigt? Nach welchem Verfahren werden diese technischen Einzelheiten festgelegt, und welches Maß an demokratischer Kontrolle ist vorgesehen?

Das aktuelle eID System der Online-Ausweisfunktion ist in den Technischen Richtlinien des BSI spezifiziert. Hier sei insbesondere die TR-03127 stellvertretend genannt, die ihrerseits auf einige weitere TRs verweist. Im aktuellen System wird beispielsweise durch ein dienste- und kartenspezifisches Pseudonym (siehe Kapitel 4.4.2 TR-03127) sowie die generelle Dezentralität des Systems die Nichtverkettbarkeit über Diensteanbietergrenzen hinweg abgesichert.

Die technische Ausgestaltung einer europäischen Wallet findet aktuell in Arbeitsgruppen der EU-Kommission unter Mitarbeit der Mitgliedsstaaten statt. Hierbei werden die dafür üblichen Beteiligungen der verschiedenen Ressorts etc. eingehalten. Auch das BSI ist hier aktiv beteiligt. Wie die Entwicklungen anderer Wallet Umsetzungen, abseits der europäischen Lösungen, umgesetzt werden kann das BSI nicht beantworten. Zum Beispiel werden schon jetzt verschiedene (zentrale und auch dezentrale) Lösungsalternativen auch im Hinblick auf Datenschutz und Datensicherheit betrachtet und diskutiert

15. Sollten aus Ihrer Sicht alle Funktionen einer eID-Wallet auch offline verfügbar sein?

Auch auf EU Ebene ist die „offline Verfügbarkeit“ noch nicht ausreichend definiert. Hier wären verschiedene Szenarien vorstellbar (eID und Verifier offline, oder nur einer von beiden), die unterschiedliche Anforderungen mit sich bringen. Sicher ist, dass eine überprüfende Stelle in Vor-Ort Szenarien andere Möglichkeiten hat, als in einem Online-Szenario. In ersterem wäre z.B. ein Gesichtsbildabgleich möglich, um eine Personenbindung herzustellen. Gleichzeitig ist es in vollständigen Offline-Fall Fall nicht möglich auf externe Vertrauensanker zuzugreifen. Alle Funktionen wären in diesem Sinne nicht nutzbar.

Laut dem aktuellen Entwurf der eIDAS VO soll die eID-Wallet auch für obengenannte Anwendungsfälle nutzbar sein. So sollen beispielsweise bei Fahrschein- oder Führerscheinkontrollen oder auch bei gesundheitlichen Notfällen die Funktionen einer eID-Wallet auch offline zur Verfügung stehen.

Die Nutzbarkeit und Sicherheit von Offline-Funktionen hängt stark von der Anwendung und auch der Implementierung ab. So ist auch in diesem Kontext bei (z.B. hoheitlichen) Anwendungen mit einem hohen Sicherheitsbedarf sicherzustellen, dass z.B. keine Kopien (wie bei der Übertragung über QR-Codes) angefertigt werden können. Des Weiteren wäre z.B. im Kontext eines Führerscheinnachweises auch die Aktualität des Nachweises nicht zu garantieren. Daneben können Formate so gewählt werden, dass ein Zeitstempel die letzte Aktualisierung der Daten/Attribute anzeigt; dadurch kann der Überprüfer selbst entscheiden, ob ihm die Aktualität der Attributdaten genügt.

16. Wie bewerten Sie Berechtigungszertifikate, die verhindern sollen, dass bei einfachen Logins (bspw. Online-Shopping, Social Media) immer der Personalausweis vorgezeigt wird? Wer stellt diese Zertifikate aus? Wie schätzen Sie allgemein die Sicherheitsrisiken in diesem Kontext ein? Welche alternativen Möglichkeiten zur Verhinderung von Over-Identification gibt es? Bitte unterscheiden Sie diese nach technischen und regulatorischen Ansätzen.

Dem ersten Satz der Fragestellung kann inhaltlich nicht gefolgt werden, da der Zweck von Berechtigungszertifikaten im eID Kontext nicht darin liegt, die Nutzung der Online-Ausweisfunktion für bestimmte Situationen grundsätzlich zu beschränken. Vielmehr stellen die Berechtigungszertifikate sicher, dass die anfragende Stelle eindeutig identifiziert werden kann und nur die zuvor beantragten Datenfelder auslesen darf. Zusätzlich können diese Berechtigungen im Missbrauchsfall auch wieder entzogen werden.

Da beim Login personenbezogene Daten übertragen werden, ist es für den Nutzer wichtig die Identität seines Kommunikationspartners, bzw. des Diensteanbieters, sowie die zu übertragenden Personendaten vorab zu kennen. Ohne diese anbieterseitige Identitätsangabe könnten Diensteanbieter anonym die Identitätsdaten des Nutzers auslesen oder sich sogar gegenüber dem Nutzer mit einer frei gewählten Anbieter-Identität ausgeben. Der Nutzer könnte daher schlussendlich nicht sicher beurteilen, mit wem er kommuniziert. Bei Konzeption eines eID Systems ist es daher aus Sicht des BSI notwendig, auf eine angemessene Identifizierung der Diensteanbieter zu achten und nicht auf diese zu verzichten.

Bei der Verwendung der Online-Ausweisfunktion muss der Diensteanbieter dem Nutzer ein Berechtigungszertifikat vorlegen, aus welchem der Nutzer die Identität des Diensteanbieters feststellen kann. Für die Beantragung des Zertifikates muss sich der Anbieter vorab bei der Vergabestelle für Berechtigungszertifikate identifizieren. Zudem muss der Diensteanbieter erklären, welche Attribute er erheben möchte und zu welchem Zweck er diese benötigt.

Aus technischer Sicht ist das Zertifikat eine elektronische Bescheinigung, die nach Berechtigung seitens der Vergabestelle für Berechtigungszertifikate durch eine nach Vorgaben des Bundes betriebene Public-Key-Infrastruktur ausgestellt wird. Die Root-CA dieser PKI wird hierbei durch das BSI betrieben. Im Zertifikat ist zudem festgelegt, welche personen- und ausweisbezogenen Daten der Anbieter eines Dienstes aus dem Personalausweis einer sich ausweisenden Person (maximal) abfragen darf.

Die Menge an übermittelten Daten kann und soll also auch abhängig vom jeweiligen Dienst oder sogar Anwendungsfall sein. Neben der Anzeige gegenüber dem Nutzer oder der Nutzerin wird die Zulässigkeit der jeweiligen Datenabfrage auch bei jedem Lesevorgang durch den Chip des Personalausweises überprüft. Wenn es beispielsweise um einen Login geht, kann üblicherweise z.B. auf das Pseudonym zurückgegriffen und auf weitere Daten verzichtet werden, sodass kein vollständiger Satz an Ausweisdaten übermittelt wird. Dem Risiko einer übermäßigen Sammlung von Informationen wird so technisch und organisatorisch Einhalt geboten und der übermittelte Datensatz auf den Bedarf des Dienstes und nach der Auswahl des Nutzers/der Nutzerin reduziert.

Aus Sicht des BSI gewähren die Berechtigungszertifikate dem Nutzer die maximale Transparenz , wer genau welche Daten von diesem anfragt. Der Nutzer hat somit die Hoheit über seine Daten auch im Sinne des SSI-Ansatzes.

17. Wie kann aus Ihrer Sicht die Benutzerfreundlichkeit bei digitalen Identitäten noch besser berücksichtigt werden?

Die Benutzerfreundlichkeit von Anwendungen wird oft daran gemessen, ob diese mit möglichst wenigen Klicks/Aktionen zum Erfolg führen. Bei hoheitlichen digitalen Identitäten spielt jedoch auch die Sicherheit und Verlässlichkeit dieser Identitäten eine wichtige Rolle. Es stellt daher eine Herausforderung dar ein ausgewogenes Verhältnis zwischen diesen beiden Aspekten herzustellen. Das BSI setzt sich dafür ein, dass sichere und gleichzeitig benutzerfreundliche Lösungen realisiert werden. Ebenso legt das BSI Wert darauf bestehende Lösungen auf Ihre Benutzerfreundlichkeit zu überprüfen und diese stetig zu verbessern.

Eine einfache Einrichtung der digitalen Identität mit wenigen analogen Hürden bringt hohe Vorteile in der Benutzerfreundlichkeit. Die Einrichtung der Anwendung muss eine Erleichterung zum bisherigen Prozess darstellen und die persönlichen Ziele der NutzerInnen schneller erreichbar werden. Dies beinhaltet ebenfalls, dass der zukünftige Nutzen hoch erscheint und die Selbstverständlichkeit der Nutzung eintritt. Aus Sicht des BSI kann dieses Ziel nur erreicht werden, wenn es eine große Anzahl an Anwendungen gibt, die mittels digitaler Identitäten nutzbar sind und ein langfristiger Nutzen der digitalen Identität für die Bevölkerung sichtbar ist. Diese Anwendungen müssen in der Bevölkerung bekannt

sein und auch einen relevanten Nutzen für die Bevölkerung haben und deren Bedürfnisse treffen.
Durch Werbung können die Vorteile von (hoheitlichen) digitalen Identitäten den Bürgerinnen und Bürgern bekannt gemacht werden. Auch sollten Behörden und Wirtschaftsunternehmen informiert werden, damit deren Anwendungen und Geschäftsprozesse auf die Nutzung (hoheitlicher) digitaler Identitäten umgestellt werden könnten.
Dabei könnten standardisierte Abläufe, geeignete Tutorials und erklärende Videos hilfreich sein.

Europäische Ebene

18. Wie bewerten Sie die Beratungen und Diskussionen um die eIDAS Verordnung auf europäischer Ebene? An welcher Stelle der VO müsste nachgebessert werden?

Die Überarbeitung der eIDAS-VO ist derzeit im Rat noch nicht abgeschlossen. Der erste Entwurf beinhaltet als wesentliche Änderung die Einführung eines Identitätenökosystems mit der „EU-DI-Wallet“ als Kern. Daneben gibt es ebenso neue Vertrauensdienste und noch andere Anpassungen der alten eIDAS-VO. Neben dem in 2021 veröffentlichten Entwurf der Überarbeitung der eIDAS-VO, wurden im Rat bereits mehrere darauf aufbauende Kompromissvorschläge vorgestellt und diskutiert. In diesem Sinne ist der aktuelle Stand, dass die Diskussionen noch nicht abgeschlossen sind.

In den aktuellen Entwürfen gibt es noch einige offene Punkte, die klargestellt werden müssen, wie zum Beispiel hinsichtlich eines geforderten einheitlichen persistenten Identifiers, sowie der Frage ob die Wallet ein eID Mittel ist, oder eines enthält. Mit Blick auf die Architektur des eID Systems erscheint beispielsweise ersteres nicht notwendig, da die eID ohne einen solchen Identifier auskommt und stattdessen mit dem dienste- und kartenspezifischen Kennzeichen Maßstäbe in Bezug auf Datenschutz und Datensicherheit setzt.

Daneben sieht der aktuelle Entwurf vor, dass die Wallet zertifiziert werden muss, um u.a. die Erfüllung von Vertrauensniveau hoch nachzuweisen. Aus Sicht des BSI sollte dieser Prozess jedoch nicht die in eIDAS 1.0 vorgesehenen Peer Reviews ersetzen, sondern diese lediglich vereinfachen, um den vertrauensbildenden Charakter der Peer Reviews zu erhalten.

Weiterhin sieht die neue eIDAS-VO die Einführung von "electronic ledgers" zur Speicherung von Daten vor. Deren Aufgabe wird aus der VO aber nicht klar und die betreffenden Artikel sind noch nicht fertig überarbeitet. Insbesondere zeigt sich an vielen Stellen ein nicht technologieneutraler Ansatz, der eine explizite Bevorzugung der Blockchain-Technologie verankern würde. Hier scheint eine Struktur aufgebaut zu werden, die in Bezug auf Vertrauensbildung keineswegs mit

dem Niveau der übrigen eIDAS-Inhalte mithalten kann, da auf belastbare Authentizitätsprüfungen weitestgehend verzichtet werden soll. Das BSI setzt sich daher hier für Nachbesserungen ein.

19. Wie positionieren Sie sich zur Frage, ob es eine einheitliche technische Lösung geben soll, oder (lediglich) einheitliche Standards zur Sicherstellung der Interoperabilität?

Die eIDAS-VO sieht nach unserem Verständnis lediglich vor, dass einheitliche Standards/Spezifikationen gesetzt werden sollen insbesondere auch in Bezug auf notwendige Schnittstellen, schreibt aber nicht fest, bis zu welchem Detailgrad diese festgelegt sein müssen.

Aus Sicht des BSI ist es vorteilhaft für verschiedene Implementierungen in verschiedenen Mitgliedstaaten Freiräume zu lassen, während die äußeren Schnittstellen möglichst einheitlich sind. Dies ermöglicht Mitgliedstaaten (und damit auch Deutschland) bestehende Lösungen evolutionär weiterzuentwickeln und in der nationalen Implementierung zu berücksichtigen (z.B. die Smart-eID), nicht zuletzt um Konkurrenzsituationen zu vermeiden. Gleichzeitig stellen einheitliche äußere Schnittstellen sicher, dass Diensteanbieter nicht jede nationale Implementation einzeln anbinden müssen.

20. Wie schätzen Sie die Verhandlungen zur eIDAS-Verordnung im Kontext der deutschen eID-Strategie ein? Wie wird beides zeitlich aufeinander abgestimmt?

Die Verhandlungen der eIDAS-Verordnung sind noch laufend, sodass ein Ende der Verhandlungen gerade schwer absehbar ist. Es wird aber erst am Ende bis ins Detail feststehen, was die eIDAS-VO ausmacht. Eine deutsche eID-Strategie muss daher flexibel sein und auf Änderungen/Verzögerungen der eIDAS-VO auf EU-Ebene reagieren. Im Rahmen des Projekts Digitale Identitäten des BMI werden auch diese externen Einflüsse von Seiten der EU berücksichtigt.

21. Wie bewerten Sie den Plan der EU KOM, in sogenannten „Large Scale Pilots“ die „European Digital Identity Wallet“ zu testen? Wie schätzen Sie die Chancen ein, dass in jenen Pilots Standards – auch zum Datenschutz und der IT-Sicherheit gesetzt – werden?

Das BSI ist an den deutschen Bestrebungen beteiligt ein eigenes Konsortium zu bilden. Mit FR zusammen wurden nun bereits 17 Mitgliedstaaten (inklusive der Ukraine) in ein gemeinsames Konsortium (‚POTENTIAL‘) aufgenommen, das verschiedene Anwendungsfälle grenzüberschreitend abdecken soll. Hierzu zählen z.B. die Identifikation im eGovernment aber auch die Nutzung eines Führerscheinnachweises. Sowohl die Anzahl der am Konsortium teilnehmenden Staaten als auch die der umzusetzenden Anwendungsfälle kann noch größer werden, da hier permanent Gespräche geführt werden und es eine sehr positive Dynamik gibt.

Der Plan die Wallet im Kontext von LSPs zu testen und damit gleichzeitig schon zukünftig mit der Wallet nutzbare Dienste zu fördern, ist aus Sicht des BSI zu begrüßen. Für die verschiedenen Mitgliedstaaten bietet dies auch die Möglichkeit die notwenige Infrastruktur anzupassen oder aufzubauen. Dies ermöglicht mit einer Wallet auf Basis bestehender nationaler eID-Systeme sehr hohe Datenschutz-Anforderungen zu gewährleisten und die Wallet gleichzeitig nutzerfreundlich in alltäglichen Anwendungsfällen nutzbar zu machen.
Die Piloten werden indes sicher im Kontext der Verhandlungen der eIDAS-VO im Rat und auch bei den Verhandlungen der technischen Grundlagen in der eIDAS Expert Group berücksichtigt, die Standards werden allerdings in der letztgenannten Gruppe festgelegt bzw. zusammengetragen und ihre Auswahl schon jetzt diskutiert.

22. Auf europäischer Ebene wird darüber diskutiert, die technische Ermöglichung von Zero-Knowledge-Proofs (ZKP), also sich rechtssicher auszuweisen ohne Daten preiszugeben, als verpflichtenden Standard in die eIDAS-VO aufzunehmen. Wie bewerten Sie das?

Diskussionen zur Verankerung von Zero-Knowledge-Proofs (ZKP) im Rahmen der eIDAS-VO als verpflichtender Standard sind dem BSI bisher nicht bekannt. Das BSI ist bisher mit Vorschlägen zur Nutzung von ZKP lediglich im Rahmen der Vorarbeiten für die EU-Wallet in Kontakt gekommen.

ZKP basieren auf nicht langjährig untersuchten und erprobten Protokollen und kryptografischen Verfahren. Im Gegensatz zu vom BSI empfohlenen kryptografischen Primitiven existieren aus Sicht des BSI für ZKP bisher keine hinreichend belastbaren Sicherheitsgarantien bzw. Sicherheitsnachweise. Das BSI steht daher einer Aufnahme von ZKP in die eIDAS-VO aus fachlicher Sicht ablehnend gegenüber. Darüber hinaus würde die Aufnahme expliziter Verfahren in die eIDAS-VO dem Prinzip der Technologieneutralität widersprechen und das im übrigen Verordnungstext eingehaltene angemessene Abstraktionsniveau verletzen. In der eIDAS-VO sollten stattdessen technische Anforderungen für die gewünschten Funktionalitäten definiert und keine konkreten Umsetzungsmöglichkeiten festgeschrieben werden.

Ergänzend weist das BSI darauf hin, dass die Nutzung von ZKP in den meisten Fällen nicht dazu dienen soll, sich ohne Preisgabe von Daten auszuweisen, sondern lediglich die Preisgabe für den jeweiligen Zweck nicht erforderlicher Daten verhindern soll (z. B. Alters-/Wohnortverifikation). Viele dieser Funktionalitäten, bei denen lediglich die jeweils erforderlichen Daten übermittelt werden oder eine Prüfung bekannter Daten möglich ist, sind in der eID-Funktion bereits seit über zehn Jahren umgesetzt, ohne dass dafür ZKP erforderlich wären.

23. Welche Rolle spielen aus Ihrer Sicht gemeinsame internationale Standards im Hinblick auf die Interoperabilität von eID-Lösungen?

Die Festlegung von Standards oder einheitlichen Spezifikationen ist für eine funktionierende Interoperabilität von eID-Lösungen notwendig. Im Kontext der aktuellen eIDAS-VO gibt es bereits das eIDAS Netzwerk, das basierend auf festgelegten Spezifikationen die gegenseitige Anerkennung und Nutzung von eID Systemen ermöglicht. Aufgrund der bestehenden rechtlichen Vorgaben hat dies aber hauptsächlich im öffentlichen Sektor Anwendung gefunden.

Welche Standards/Spezifikationen für die EU-DI-Wallet zugrunde gelegt werden, wird derzeit in der eIDAS Expert Group diskutiert, die eben diese Festlegungen treffen soll. Hierbei werden aktuelle Standards miteinbezogen und geprüft, inwieweit sie für die Zwecke der EU-DI-Wallet, wie sie in der eIDAS-VO festgelegt sind, geeignet sind. Dieser Prozess ist nicht abgeschlossen.

24. Ein Kritikpunkt, ist die Verpflichtung der Unternehmen oder relying Parties, die EUid-Wallets als Identifizierungsmittel zu akzeptieren. Dies sei eine größere Herausforderung, da sie bisher keine hoheitlichen Identifizierungsprozesse innerhalb ihrer Services vorsehen. Wie schätzen Sie diesen Punkt ein? Ist die Kritik berechtigt? Welche Folgen hat diese Regelung und wie könnte eine Alternative aussehen?

Nach aktuellem Stand soll es einheitliche Schnittstellen geben, über die Relying Parties mit einer EU-DI-Wallet kommunizieren und diese nutzen können. Über diese Schnittstellen sollen dann sowohl Identifizierungsdaten als auch andere Attribute übermittelt werden können. Inwiefern die Relying Parties hier unterschiedliche Schnittstellen in Bezug auf hoheitliche Attribute oder andere Attribute anbinden müssen, oder es eine gemeinsame Schnittstelle gibt, ist noch nicht final festgelegt. Inwiefern mit der Anbindung der noch zu definierenden Schnittstellen andere Anforderungen verbunden sind als mit der Anbindung an bestehende Systeme ist noch nicht objektiv zu beurteilen.

Im aktuellen Entwurf ist unserem Verständnis nach keine Anbindungspflicht für alle Unternehmen/Relying Parties vorgesehen. Es sind hier nach unserem Verständnis beilspeisweise Unternehmen aus dem Geldwäschegesetz Kontext betroffen, für die aber auch heute schon starke Anforderungen gelten. Wichtig zu beachten ist in diesem Kontext, dass eine solche Regelung eine breite Einsetzbarkeit der zukünftigen Lösung schafft.

Ob die EU-DI-Wallets selbst eID-Mittel sind, nur Container eines solchen oder als eID-Mittel in Verbindung mit einem notifizierten eID-Mittel fungieren, ist aktuell noch nicht abschließend geklärt und Gegenstand der Verhandlungen.

25. Die Novellierte eIDAS-Verordnung sieht vor, dass qualifizierte Webseitenauthentifizierungszertifikate automatisch von Webbrowsern anerkannt und der Vertrauensstatus visualisiert dargestellt werden muss. Die Kritik ist, dass die Unabhängigkeit von Webbrowsern und die von Unternehmen entwickelten Sicherheitsvorkehrungen durch diese Regelungen beeinträchtigt werden. Aus diesem Grund soll Artikel 45 eIDAS-VO gestrichen werden. Teilen Sie die Kritik und was wären die Folgen einer automatischen Anerkennung?

Das BSI bewertet den bestehenden Artikel 45 als positiv und teilt die Kritik daher nicht in dieser Form. Die Verknüpfung der Identitätsinformationen mit der Verschlüsselung im Zertifikat ist sinnvoll, um Täuschungen zu verhindern. Andere Möglichkeiten (wie Hinterlegung eines Links im DNS Record) sind grundsätzlich weniger sicher. Daher ist der Einsatz von QWACs insb. für Seiten auf denen persönliche Daten eingegeben werden, sinnvoll und wird vom BSI z.B. in der Technischen Richtlinie TR-03116-4 empfohlen. Für Nutzer von Browsern ist das jedoch effektiv nur hilfreich, wenn sie Identitätsinformationen in leicht erkennbarer Form angezeigt, was derzeit in der Praxis nicht gegeben ist. Zudem befinden nicht alle Root-Zertifikate für qualifizierte Webseitenzertifikate in den Trust Stores der Browser, z.B. weil diese CAs nicht die individuellen Kriterien der Browseranbieter erfüllen. Hierdurch war der Vorteil der QWACs in der Praxis bisher deutlich eingeschränkt, die Begründung in dem zugehörigen Recital des Verordnungsentwurfs wird geteilt. In Bezug auf die Ausgestaltung sieht §45 einen Implementing Act vor. Hier sollte Bezug auf Sicherheitsfragen auf geeignete Standards (z.B. ISO/IEC 27099) verwiesen werden.

26. Der Artikel 12b des Kommissionsentwurfs zur eIDAS-Verordnung sieht vor, neben den großen Plattformbetreibern auch zahlreiche Branchen zur Akzeptanz der EU-Wallet zu verpflichten. Wie schätzen Sie diese Verpflichtung ein? Aktuell wird auf europäischer Ebene diskutiert, ob es nur eine staatliche Wallet geben soll oder verschiedene Wallets, die zertifiziert sind. Welchen Weg bevorzugen Sie und warum?

Für die erste Frage verweisen wir hier auf die Antwort zu Frage Nr. 24. Insbesondere im Kontext großer Plattformbetreiber besteht hier die Möglichkeit die EU-DI-Wallet als Gegenentwurf zu bestehenden Lösungen zu etablieren und so auf Sicherheit, Datenschutz etc. zu setzen.

Auch mit Hinblick auf die Frage wie viele Wallets pro Mitgliedstaat möglich sein sollten verweisen wir auf die Antwort zu Frage Nr. 19. Eine Herausforderung wird sein, dass zwischen verschiedenen Lösungen keine Konkurrenzsituationen entstehen und gleichzeitig ein gleiches Niveau an Sicherheit und Datenschutz etc. erreicht wird. Das BSI setzt sich auch auf EU-Ebene dafür ein, dass entsprechende Regelungen/Vorschriften festgelegt werden.

Das BSI unterstützt wie die Bundesregierung die Bestrebung zur Verpflichtung, die EUDI-Wallet mit einer integrierten eID zu akzeptieren.

27. Gemäß Art. 6a des Kommissionsentwurfs soll die Benutzung der Europäischen Wallet für natürliche Personen kostenfrei sein. Auf welche Aspekte der Nutzung einer Wallet sollte sich diese Vorgabe beziehen?

Nach unserem Verständnis gilt dies im Wesentlichen für die Basis-Use-Cases, also Identifizierung/Authentisierung und (nach aktuellem Stand auch) qualifizierte elektronische Signaturen. Der zweite Punkt fällt eher in die Expertise der BNetzA, daher konzentrieren wir uns hier auf den ersten Punkt: Identifizierung und Authentisierung ermöglichen die Nutzung von Diensten, oder sind die Basis, auf der Dienste agieren. Unserem Verständnis nach sollte dies kostenlos sein, was aber nicht bedeuten muss, dass die verwendeten Dienste kostenlos sind.

28. Die Mitgliedsstaaten haben möglicherweise unterschiedliche Interpretationen bestimmter Attribute der eID, etwas was Geschlecht oder Heiratsstatus angeht. Wird ein von einem Mitgliedsstaat ausgegebener Wert eines Attributs immer von den anderen anerkannt werden? Wie wird das durchgesetzt werden? Falls nein, wird ein Rechtsbehelf vorgesehen? Wie sollen die Semantiken der Typen und Werte von Attributen standardisiert?

Das nationale Recht sieht für die eID nicht vor, dass Daten zum Geschlecht und zum Heiratsstatus erhoben werden. Diese werden entsprechend auch nicht übermittelt (vgl. § 5 Abs. 5, 5a PAuswG (Speicherung), § 18 Abs. 3 S. 2 PAuswG (Übermittlung).

Das BSI kann keine juristische Einschätzung zu diesem Sachverhalt geben.

Die Übermittlung von Identifizierungsattributen und die Übermittlung anderer Attribute haben allerdings eine unterschiedliche (juristische) Bedeutung. Während erstere für eine Identifizierung benötigt werden und in ihrem Umfang weitestgehend abgestimmt und festgeschrieben werden, wird es für weitere Attribute voraussichtlich weniger Vorgaben geben.

Die Formate und Sätze an Identifizierungsattributen werden voraussichtlich in einer Weise festgelegt, dass eine Anerkennung möglich ist. Bei den weiteren Attributen, die z.B. von einem Vertrauensdiensteanbieter ausgegeben werden, kann dies anders sein. Hier hat der Vertrauensdiensteanbieter viele Freiheiten, wenn es für den jeweiligen Sektor beispielsweise keine Vorgaben gibt. Dabei wird er nach Einschätzung des BSI aber auf bestehende Formate/Templates zurückgreifen oder ein neue entwickeln. Ein Diensteanbieter wiederum kann zu Beginn eines jeweiligen Prozesses festlegen welche Daten benötigt werden und nur diese anfordern. Es ist vorstellbar, dass hierbei

auch Formate/Templates vorgegeben werden. So wird sich ein gewisser Satz an verschiedenen Formatierungen durchsetzen.