Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)53

29.06.2022

Stellungnahme zur Anhörung Digitale Identitäten – Digitalausschuss 4. Juli 2022

Autor: Flüpke (Carl Fabian Lüpke)

Zusammenfassung

Deutschland verfügt seit 12 Jahren über ein System für die digitale Identität: Den *neuen Personalausweis*.

Während anfangs noch Bedenken bezüglich des Datenschutzes und der Auslesbarkeit aus der Ferne der NFC-Schnittstelle bestanden, so hat sich diese Entscheidung als sehr vorausschauend herausgestellt. NFC ist omnipräsent hat sich bei der kontaktlosen Bezahlung im Alltag fest etabliert.

Anstatt die breite Verfügbarkeit dieses eID-Systems praktisch nutzbar zu machen, was kurzfristig möglich wäre, evaluiert die Bundesregierung eine neuartige Technologie, die so genannte „Self Sovereign Identity“ (SSI).

Hier hat die Bundesregierung, unter anderem im „Schaufenster sichere digitale Identitäten“ und der ID Wallet App viel Zeit und Geld investiert, ohne dass dabei belastbare Prototypen entstanden. So ist die ID Wallet App binnen weniger Tagen nach ihrer Vorstellung wegen struktureller Sicherheitsschwachstellen depubliziert worden. Zudem zeigte sich davon unabhängig eine mangelhafte Leistungsfähigkeit.

Diese bei der SSI-Technologie aufdeckten Risiken wurden durch geeignete Designentscheidungen und Sicherheitsanforderungen beim neuen Personalausweis vermieden.

Aus Datenschutz- und IT-Sicherheitsperspektive ist der neue Personalausweis einer smartphonebasierten Wallet App zu bevorzugen, denn solange in einem unvertrauenswürdigen Smartphone Daten im Klartext verarbeitet werden, können diese abfließen.

Die Bundesregierung kann durch minimales Eingreifen kurzfristig die Voraussetzungen für eine breite Adoption der Onlineausweisfunktion in der Wirtschaft schaffen. Hierzu sollten die Preise für so genannte Berechtigungszertifikate reguliert werden und Referenzimplementierungen als Open Source Software bereitgestellt werden.

Auch auf europäischer Ebene sollte sich Deutschland konsequent für hohe Standards im Datenschutz und in der IT-Sicherheit einsetzen. Diese sind nicht mit einer ID Wallet erreichbar, weil die ihr zugrundeliegende Technologie strukturelle Schwachstellen aufweist.

Die Förderung dieser Technologie sollte aus zeitlichen und finanziellen Gründen zugunsten eines besseren, bereits vorhanden Lösung eingestellt werden.

Nationale Ebene

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

Deutschland verfügt seit 12 Jahren über ein System für die digitale Identität: Den neuen Personalausweis[1].

Während anfangs noch Bedenken bezüglich des Datenschutzes und der Auslesbarkeit aus der Ferne der NFC (Near Field Communication) Schnittstelle bestanden, so hat sich diese Entscheidung als sehr vorausschauend herausgestellt: NFC ist heute in nahezu jedem Smartphone verbaut und bei der kontaktlosen Bezahlung im Alltag fest etabliert.

Anstatt die breite Verfügbarkeit dieses System praktisch nutzbar zu machen, was kurzfristig möglich wäre, evaluiert die Bundesregierung eine neuartige Technologie, die so genannte „Self Sovereign Identity".

Hier hat die Bundesregierung, unter anderem im „Schaufenster sichere digitale Identitäten" und der ID Wallet App viel Zeit und Geld investiert, ohne dass dabei belastbare Prototypen entstanden. So ist die ID Wallet App binnen weniger Tagen nach ihrer Vorstellung wegen struktureller Sicherheitsschwachstellen depubliziert worden. Zudem zeigte sich davon unabhängig eine mangelhafte Leistungsfähigkeit.

Die aufgedeckten Schwachstellen[2,3] sind struktureller Natur und betreffen alle Wallet-Anwendungen, welche die schwache und für Machine-in-the-Middle-Angriffe[4] (MitM) anfällige SSI-Spezifikation (DIDComm) implementieren.

Nun muss ein großes Konsortium diese Spezifikation mit hohem Zeitaufwand anpassen, um diese bereits bekannten Angriffsmöglichkeiten zu mitigieren. Einen diesbezüglichen frühzeitigen Hinweis[5] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ignorierte der Hersteller der ID Wallet App.

Die Fixierung auf die SSI-Technologie seitens der Bundesregierung stellt eine Hürde bei der Adoption sicherer zuverlässiger Identitätslösungen dar.

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?

Beim neuen Personalausweis besteht keine MitM-Angriffsmöglichkeit. Auch andere bei der SSI-Technologie einhergehende Risiken wurden durch geeignete Designentscheidungen und Sicherheitsanforderungen beim neuen Personalausweis vermieden.

Dass sich die Onlineausweisfunktion bisher nicht durchsetzte liegt vor allem in fehlenden Anwendungsszenarien begründet. Zudem sind kostspielige Berechtigungszertifikate notwendig. Hier kann der Gesetzgeber durch minimales Eingreifen kurzfristig die Voraussetzungen für eine breitere Adoption in der Wirtschaft schaffen: Wenn der Einsatz der Onlineausweisfunktion günstiger wird als kostspielige Videoidentverfahren, werden ökonomisch agierende Unternehmen diese auch anbieten.

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

Es braucht kein „Labor" zur zeitaufwändigen Forschung an neuen Verfahren in der eID. Zumal bei einem interministeriellen Format eine Verantwortungsdiffusion droht. Eine vergleichbare Herangehensweise gipfelte bei der ID Wallet App in der öffentlichen Äußerung Andi Scheuers, er sei „stocksauer", denn sein Ministerium habe einmal alles richtig gemacht. Solche Aussagen schaden dem Vertrauen und Ansehen einer staatlichen Identitätslösung.

Das BSI sollte diesem interministeriellen Laborformat verbindliche Vorschriften für die IT-Sicherheitsanforderungen machen dürfen. Es dürfen nicht erneut eindringliche Warnungen[5] und Apelle des BSI ignoriert werden.

Das Laborformat könnte dazu genutzt werden, gut dokumentierte Open Source Software für die Verwendung des bereits existierenden Personalausweises zu schaffen und diesen damit zugänglicher zu machen.

Zudem könnten die Ministerien mit minimalen Abstimmungsaufwand Anwendungsszenarien für die Onlineausweifunktion schaffen. Die hierfür umzusetzenden Spezifikationen stehen bereits seit Jahren fest und es sind kurzfristig keine Änderungen (z. B. zur Mitigation von Sicherheitsrisiken) absehbar.

Über 62 Millionen Deutsche haben bereits den Personalausweis mit dem Chip und damit den Online-Ausweis[6]. Auf derartige Nutzerzahlen kommt nicht einmal die Corona-Warn-App[7]. Hier sollte das interministerielle Laborformat auf Basis vorhandener, klar spezifizierter Technologie anknüpfen.

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 folgenden Maßnahmen sollten ergriffen werden:

1. Einstellen der Förderung von – insbesondere aber nicht ausschließlich blockchainbasierten – SSI-Lösungen.

   Hier kann viel Zeit und Geld eingespart werden. In Anbetracht des ID Wallet Desasters und des Umgangs damit sollte die Reißleine gezogen werden.

2. Regulierung der Preise der Berechtigungszertifikate für den neuen Personalausweis der Bundesdruckerei.

   Die Berechtigungszertifikate erlauben Anbietern von Onlinediensten den selektiven Zugriff auf einzelne Datenfelder des Personalausweises mit selbstbestimmter Zustimmung des Benutzenden. Hierbei ist durch das Berechtigungszertifikat sichergestellt, dass ein Diensteanbieter nur Felder abfragen kann, für die er ein berechtigtes Interesse demonstrieren konnte, beispielsweise gesetzliche Anforderungen. So kann Datensparsamkeit auf technischer und regulatorischer Ebene forciert werden.

   Die Bundesdruckerei ist der einzige Anbieter von derlei Zertifikaten. Preise werden nur nach Abschluss eines Non-Disclosure-Agreements (NDA) genannt. Vermutlich fallen diese aufgrund der Monopolstellung außergewöhnlich hoch aus. Dies muss die Politik regulieren.

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?

Eine staatliche Identität bereitzustellen ist eine Aufgabe des Staates und nicht der Wirtschaft. Die Wirtschaft sollte auf diese unter Berücksichtigung hoher Datenschutz- und IT-Sicherheitsanforderungen zugreifen können.

Das Schaffen eines profitorientierten Marktes für Wallet Apps und Identitäten birgt das Risiko, dass Gewinnerzielungsabsichten über den Datenschutz und die IT-Sicherheit gestellt werden.

Anbieter von SSI basierten Lösungen werben damit, dass bei der SSI-Technologie ein stabiles Identifizierungsmerkmal anfällt[8]. Dadurch können Onlinediensteanbieter Identitätsdaten geräte- und plattformübergreifend sammeln und zur Profilbildung zusammenführen.

Für die Datensammlung und Profilbildung ist es sicherlich von Vorteil, dass nicht nur Identitätsdaten, sondern auch Gesundheitsdaten, Zeugnisse und weitere Dokumente in den Wallet Apps gespeichert werden sollen. Entsprechend hoch ist das Risiko für die Privatsphäre der Betroffenen.

Durch ein einfaches Drohszenario kann die „selbstsouveräne" Zustimmung zur Freigabe sämtlicher Daten eingeholt werden: Entweder werden die Daten freigegeben oder ein bestimmter Onlineservice darf nicht genutzt werden.

Es ist nach derzeitigem Stand keine Regulierung vorgesehen, wer welche Daten aus den SSI-Wallets abrufen darf.

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?

Beim Personalausweis gibt es für die Wiederherstellung der persönlichen Identifikationsnummer (PIN) – die so genannte *PIN-Recovery* – ein Verfahren[9].

Bei der ID Wallet App wird bei der Einrichtung explizit davor gewarnt, dass eine solche PIN-Recovery nicht möglich ist.

Tatsächlich offenbart sich hier aber ein weiteres Risiko: Die nur mit einer numerischen PIN mit fester Länge geschützten und im Speicher des Telefons hinterlegten Daten können trivial durch einen so genannten *Brute-Force-Angriff*, dem einfachen Ausprobieren aller möglichen PINs, ausgelesen werden, was im Endeffekt einen Identitätsdiebstahl ermöglicht.

Dies ist nicht nur möglich, wenn das Mobiltelefon verloren oder gestohlen wird, sondern auch wenn über Schadsoftware auf dem Gerät oder Lücken in darauf installierten Applikationen wie beispielweise Webbrowsern auf diese gespeicherten Daten zugegriffen werden kann. Die Haftungsfragen sind hier völlig unklar.

Ein solcher Brute-Force-Angriff wird beim Personalausweis ähnlich wie bei SIM-Karten durch Prüfung der PIN auf einem Hardwaremodul („Secure Element") effektiv unterbunden.

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)?

Staatlich beglaubigte elektronische Personendaten sollten im Interesse des Datenschutzes und des Grundsatzes der Datensparsamkeit nur dort eingesetzt werden dürfen, wo der Gesetzgeber dies auch verlangt. Beispielsweise bei Behördengängen, Beauftragung von Telekommunikationsdienstleistungen, bestimmten Bankgeschäften. Bei anderen Diensten sollte diese nicht eingesetzt werden dürfen, weil sich insbesondere bei der SSI-Technologie das Risiko des Trackings, wie es bereits von Cookies bekannt ist, ergibt: Es fallen bei unterschiedlichen Anbietern identische Identifizierungsmerkmale an, die zur Profilbildung genutzt werden können.

Das Offenbarungsverbot im Transsexuellengesetz verbietet die Offenlegung vorheriger Vornamen eines Antragsstellers:

> Ist die Entscheidung, durch welche die Vornamen des Antragstellers geändert werden, rechtskräftig, so dürfen die zur Zeit der Entscheidung geführten Vornamen ohne Zustimmung des Antragstellers nicht offenbart oder ausgeforscht werden, es sei denn, daß[sic!] besondere Gründe des öffentlichen Interesses dies erfordern oder ein rechtliches Interesse glaubhaft gemacht wird.

Um das Offenbarungsverbot einhalten zu können, ist wichtig, dass keine staatlich beglaubigten Daten anfallen, die auch nachträglich noch validiert werden können. Das ist bei SSI nach derzeitigem Stand aber der Fall: So können zwei Ausweisdokumente nach einer Geschlechtsänderung zusammengeführt werden. Durch die Signatur kann nachvollzogen werden, dass es sich um garantiert echte Dokumente handelt. Die Signatur kann zurückgezogen werden. Dann ist das Dokument zwar nicht mehr gültig, aber es trägt immer noch eine staatliche Signatur.

Dass bei der SSI-Technologie diese Daten unbegrenzt beglaubigt werden und eben nicht nur im Rahmen der Übertragung, steigert den Wert dieser Daten und damit das ökonomische Interesse diese zu sammeln massiv. Dies läuft Datenschutzinteressen zuwider. Statt einer langlebigen Beglaubigung der personenbezogenen Daten reicht es, wenn diese im Kontext der Übertragung überprüfbar sind.

In der eIDAS 2.0 Verordnung sollte festgelegt werden, dass das Geschlecht, sofern ein solcher Eintrag überhaupt notwendig ist, als UTF-8 enkodierter Freitext mit einer sinnvollen Längenbegrenzung (mindestens 32 Zeichen) gespeichert wird.

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?

„Self Sovereign Identity“ bezeichnet ein Verfahren, bei dem der Staat oder anderen Organisationen den Bürgern digitale Ausweise, Führerscheine oder andere Dokumente ausstellen. Diese werden in einer sogenannten Wallet App auf einem Smartphone gespeichert und verwaltet. Verlangt ein Onlinedienst nach einem solchen Dokument, kann es über diese Wallet App mit Zustimmung des Benutzenden freigegeben werden. Häufig wird dazu ein 2D (QR) Code gescannt.

Die von der Bundesregierung kurz vor der Wahl publizierte ID Wallet App basiert auf dieser SSI-Technologie.

Anhand dieser App deckten Sicherheitsforscher strukturelle Schwachstellen in dem zur SSI-Technologie gehörenden DIDcomm-Protokoll auf[2]. Diese Schwachstelle betrifft alle SSI Wallet Apps, welche das DIDcomm-Protokoll implementieren (z. B. auch die Wallet App „Lissi“) und nicht ausschließlich die ID Wallet App.

Ein Lösungsansatz sieht vor, das Risiko von MitM-Angriffen mit TLS-Zertifikaten zu mitigieren.

Die Verwendung von SSL/TLS[10] ist seit langem Industriestandard und sichert bei HTTPS-Verbindungen zu Webseiten ab. Es ist verwunderlich, dass der Einsatz dieser Basistechnologie erst nach Warnungen des BSIs und der Recherche aus Kreisen des Chaos Computer Clubs in Betracht gezogen wird.

Nach derzeitigem Stand fallen mit der SSI-Technologie beim Onlinedienst staatlich signierte, also garantiert echte, personenbezogene Daten an, welche auch im Nachhinein digital auf ihre Echtheit geprüft werden können.

Das ist vor dem Hintergrund diverser Datenabflüsse bei Onlinediensten in den vergangenen Jahren ein erhebliches Risiko, weil es die Daten sehr viel wertvoller macht, schließlich sind sie garantiert echt.

Für das Problem der Empfängerdatenspeicherung gibt es ebenfalls Lösungsansätze, die so genannten *Zero-Knowledge-Proofs* (ZKP). Die ID Wallet App hat dieses Verfahren nicht implementiert.

Während Hersteller gerne mit ZKPs werben, gibt es nur wenige Wallets, die diese Funktionalität tatsächlich unterstützen.

Eine Interoperabilität ist hier derzeit nicht gewährleistet.

Das Problem der Empfangsdatenspeicherung existiert bei der Onlineausweisfunktion nicht, weil keine signierten Personendaten anfallen. Ein Empfänger von Ausweisdaten kann sich nur aufgrund des Kontextes der Übertragung der Echtheit der Daten vergewissern, aber nicht darüber hinaus.

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?

Smartphones verfügen über moderne, komplexe Betriebssysteme, die eine große Angriffsfläche für Schadsoftware und Cyberkriminelle bieten. Zudem erhalten viele ältere und günstige Android Modelle keine Sicherheitsupdates mehr. Ein Smartphone kann daher keinen Vertrauensanker in einer eID-Lösung darstellen, stattdessen muss es als unvertrauenswürdig und unsicher betrachtet werden.

Genau einen solchen Ansatz verfolgt der Personalausweis, bei dem ein dezentraler eID Server eine abgesicherte Verbindung über das Smartphone in das Ausweisdokument aufbaut. Dem Smartphone muss hierbei nicht vertraut werden, es muss lediglich eine NFC-Schnittstelle bereitstellen.

Die Aussage, nur neue, teure Smartphones würden über eine NFC-Schnittstelle verfügen, ist falsch. Milliarden Smartphones, auch Günstige, verfügen über eine solche NFC-Antenne.[11]

Die Sicherheitsrisiken eines Smartphones können auch durch ein eingebautes „Secure Element“ möglicherweise mitigiert werden. Dabei handelt es sich um besonders abgesichertes Hardwaremodul, in welches kryptographische Berechnungen ausgelagert werden.

Um ein Secure Element in Wallet Apps einsetzen zu können, bräuchte es aber Absprachen der Smartphonehersteller und eine gründliche Überprüfung jedes eingesetzten Moduls. Diese sind eher in höherpreisigen, neuen Modellen verbaut.

Einfacher und sozialverträglicher ist das bisherige Verfahren, ein einheitliches, gut auditiertes Secure Element, den Personalausweis, per NFC mit dem Smartphone zu koppeln. Damit wird auch alten oder unsicheren Modellen die sichere Verwendung der eID ermöglicht.

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?

Eine verschlüsselte Speicherung reicht nicht aus, um die Ausweisdaten hinreichend zu schützen.

In einer Wallet App fallen die Daten trotz verschlüsselter Speicherung bei Benutzung im Klartext ein und sind somit im Kontext der unsicheren Ausführungsumgebung „Smartphone“ angreifbar.

Diese Daten sind für Angreifer äußerst lukrativ, weil sie einen Identitätsdiebstahl begehen können.

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?

Auch bei einer Speicherung auf einer eSIM werden die Ausweisdaten bei einer SSI-Applikation im Klartext durch eine Wallet App verarbeitet. Beim neuen Personalausweis fallen diese Klartextdaten nicht an, ein Datendiebstahl vom Smartphone wird effektiv unterbunden.

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?

Smartphones kann, sollte und muss für eine digitale Identität nicht vertraut werden. Der neue Personalausweis demonstriert die Machbarkeit einer Lösung, die dem nicht vertrauenswürdigen Smartphone alle sensiblen Daten vorenthält.

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?

Blockchain-Technologie wird bei der ID Wallet App dazu eingesetzt, öffentliches Schlüsselmaterial und Schemadefinitionen zu speichern. Eine Schemadefinition besagt, welche Datenfelder ein bestimmtes Dokument enthält (z. B. Geburtsdatum, Wohnort, etc.). Das öffentliche Schlüsselmaterial dient der späteren Validierung der ausgestellten Dokumente. Es gibt keine Notwendigkeit bei der SSI-Technologie

eine Blockchain einzusetzen. Ein herkömmliches (dezentrales) Datenbankmanagementsystem (DBMS) ist besser geeignet, weil es sich hierbei um deutlich weniger komplexe und besser auditierte Standardsoftware handelt.

Durch den Einsatz der Blockchaintechnologie ergeben sich bei der ID Wallet vordergründig keine Datenschutzbedenken, da hier keinerlei personenbezogene Daten gespeichert werden. Ein Nutzen ist aber auch nicht erkennbar.

Tatsächlich kann auf eine verteilte Datenbank ohne Nachteile auch gänzlich verzichtet werden: Die Schemadefinitionen können in einer Spezifikation initial festgelegt werden und für die Verteilung des Schlüsselmaterials kann auf traditionelle Public Key Infrastructure gesetzt werden. Dies hat keine negativen Auswirkungen auf die Dezentralität des Systems.

Eine Schemadefinition wird anhand einer kryptischen Adresse in der Blockchain referenziert, im Falle der ID Wallet lautete diese für den Personalausweis `XmfRzF36ViQg8W8pHot1FQ:3:CL:5614:<Base-ID>`.

Hier ergeben sich praktische Fragen:

1. Wie soll sichergestellt werden, dass ausstellende und verifizierende Instanz die gleiche Adresse kennen?
2. Wie soll sichergestellt werden, dass ausgerechnet diese Adresse ein gültiges staatliches Dokument referenziert?
3. Wer darf solche Schemadefinitionen publizieren?

Durch die Komplexität dieses Systems können sich jedoch, wie auch das BSI warnt[12], Sicherheitsrisiken ergeben, die wiederum Auswirkungen auf den Datenschutz haben können, ohne dass sich irgendein Nutzen durch den Einsatz dieser Technologie ergibt.

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?

Eine eID-Lösung muss im Betrieb dezentral funktionieren, sodass an keiner zentralen Stelle Daten anfallen, um hohe Datenschutz- und Verfügbarkeitsanforderungen einhalten zu können. Dazu zählen auch Metadaten. Die ID Wallet App verfügt über zentrale Komponenten, die bereits bei geringen Benutzerzahlen überlastet waren. Beim SSI-Verfahren kann nicht verhindert werden, dass eine bösartige Wallet App mit zentralen Systemen kommuniziert. Zumal sich eine bösartige Wallet App ohnehin völlig einer staatlichen und damit demokratischen Kontrolle entzieht. Eine solche bösartige Wallet App könnte vom Betreiber benutzt werden, um Daten missbräuchlich auszuleiten und sie für wirtschaftliche Zwecke zu verwenden.

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

Da der neue Personalausweis offline funktioniert, sollte eine eID-Wallet um konkurrenzfähig zu sein, ebenfalls eine solche Funktion bieten.

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.

Berechtigungszertifikate dienen dazu den Zugriff auf Ausweisdokumente zu regulieren. Ein Onlinedienst muss ein begründetes Interesse (z. B. gesetzliche Anforderung) vorweisen können, um beim Benutzenden Zugriff auf einzelne Datenfelder des Ausweises erbitten zu dürfen.

Dadurch wird Over-Identification, also das anlasslose Abrufen hoheitlicher Ausweisdaten, effektiv ausgeschlossen, entsprechend sind Berechtigungszertifikate zu befürworten.

Bei der SSI-Technologie fehlt ein solcher notwendiger Schutzmechanismus, stattdessen soll eine staatliche Identität alle anderen Identitäten beim Online-Shopping, auf Social Media, etc. ersetzen. Dabei ist hierfür das Vorzeigen des Personalausweises gar nicht gerechtfertigt oder notwendig. Ein herkömmlicher Login-Mechanismus, ggf. durch Zwei-Faktor-Authentifizierung abgesichert, reicht aus.

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

Die Benutzerfreundlichkeit kann gesteigert werden, in dem auf leistungsfähige Systeme und Verfahren gesetzt wird. In den wenigen Tagen Wirkbetrieb der ID Wallet wurde trotz 300.000 Downloads nur eine mittlere vierstellige Anzahl Dokumente ausgestellt, was auf eine mangelhafte Leistungsfähigkeit hindeutet.

Sich online auszuweisen, sollte auch in Zukunft die Ausnahme bleiben, weil es in den allermeisten Fällen nicht notwendig ist - analog zu Geschäftsvorgängen im analogen Leben.

Der Vorgang, den Ausweis an das Smartphone halten zu müssen ist sogar positiv zu bewerten: Er macht unmissverständlich klar, dass man sich gerade im Internet mit einem hoheitlichen Dokument ausweist.

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?

Es wird eine smartphonebasierte Lösung angestrebt, obwohl Smartphones, wie oben ausgeführt, grundsätzlich nicht vertraut werden kann. Ein solcher Ansatz ist entsprechend abzulehnen. Der Artikel 45 birgt das Risiko etablierte IT-Sicherheitsstandards zu schwächen und sollte aus den in der Antwort auf Frage 25 ausformulierten Gründen gestrichen werden.

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

Es sollte einheitliche Standards geben, um die Interoperabilität zu gewährleisten. Zu diesen Standards sollten vollständige, gut dokumentierte Referenzimplementierungen als Open Source Software bereitgestellt werden. Referenzimplementierungen helfen als Programmierbeispiel bei der Integration in konkrete Anwendungen.

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

Deutschland sollte auf europäischer Ebene auf seine seit langem existierende, erprobte eID-Lösung setzen, statt unter hohem zeitlichem Aufwand die Sicherheitsrisiken der SSI-Technologie zu mitigieren.

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?

Es wird eine smartphonebasierte Lösung angestrebt, welche aus den oben genannten Gründen abzulehnen ist. Ob eine solche European Digital Identity Wallet gängiger IT-Sicherheitspraxis entspricht wird eine kritische Begutachtung wie bei der ID Wallet App zeigen.

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?

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

Es sollte einheitliche Standards geben. Zu diesen Standards sollten Referenzimplementierungen als Open Source Software bereitgestellt werden. Zur Prüfung der Interoperabilität können entsprechende Testsuites publiziert werden.

24. Ein Kritikpunkt, ist die Verpflichtung der Unternehmen oder relying Parties, die EUidWallets 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?

Wenn Unternehmen zur Akzeptanz der EUidWallet gezwungen werden, ist es nur noch ein kleiner Schritt zur Ausweispflicht im Internet, denn damit werden die technischen Voraussetzungen geschaffen: Wird ein SSI Login-Mechanismus großflächig angeboten, droht die Gefahr, dass durch eine Gesetzesänderung andere, herkömmliche Login-Mechanismen verboten werden.

Durch eine solche Klarnamenspflicht im Internet ist das Recht auf freie Meinungsäußerung bedroht.

Entsprechend ist eine solche Verpflichtung klar abzulehnen.

Staatliche Identitäten sollten nur dort eingesetzt werden dürfen, wo gesetzliche Bestimmungen dies notwendig machen.

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?

Browserhersteller haben Verfahren zur Aufnahme von so genannten „Certificate Authorities“ (CA) etabliert. Die hierfür von einer CA einzuhaltenden technischen Anforderungen liegen deutlich über denen der eIDAS-VO.

Der Artikel 45 eIDAS-VO sollte gestrichen werden, um eine Schwächung von Sicherheitstechnologien des Internets (TLS) zu verhindern.

Zudem ergeben sich Missbrauchsrisiken durch europäische Strafverfolgungsbehörden und Geheimdienste, welche Zertifikate fälschen könnten, um in geheime Kommunikationen zu spähen.

Um diesem Missbrauchsrisiko vorzubeugen, muss die bereits existierende und von Browsern vorgeschriebene „Certificate Transparency“ eingesetzt 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?

Eine Verpflichtung ist aus den oben genannten Gründen (siehe Frage 24) abzulehnen.

Eine smartphonebasierte Wallet ist aus den oben genannten Sicherheitsrisiken abzulehnen. Ein unkontrollierter Markt für Wallet Apps, die jeweils ganz unterschiedlichen Datenschutz- und Sicherheitsniveaus entsprechen, ist umso mehr abzulehnen. Zudem stellt sich die Frage nach dem Geschäftsmodell der Wallet Anbietenden und wie dieses mit Datenschutzfragen in Einklang zu bringen ist. Eine Zertifizierung kann hilfreich sein, gewisse Standards zu forcieren. Bei Aktualisierungen einer App ist eine Re-Zertifizierung zu verlangen. Bei der Zertifizierung muss der Quelltext offenbart werden, um das Risiko des Datenabgriffs durch den Anbieter bewerten zu können. Das Risiko eines Datenabgriffs durch den Herausgeber eine Wallet App kann bei der SSI-Technologie nicht unterbunden werden.

Die EU sollte technische Standards für die Interoperabilität unter Berücksichtigung hoher Datenschutz- und IT-Sicherheitsanforderungen formulieren.

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?

Die Benutzung einer Wallet App sollte für Benutzende kostenfrei sein. Eine Finanzierung dieses Angebots durch Werbeeinblendungen oder Datenhandel (Verkauf der Benutzerdaten) sollte technisch unterbunden und rechtlich ausgeschlossen werden.

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 Geschlecht sollte, sofern ein solcher Eintrag überhaupt notwendig ist, als UTF-8 enkodierter Freitext mit einer sinnvollen Längenbegrenzung (mindestens 32 Zeichen) gespeichert werden.

Um den Interpretationsspielraum queerfeindlicher EU-Staaten zu beschränken, sollte die EU ein klares Datenformat und Enkodierung vorschreiben, die keine Möglichkeit für die Diskriminierung von Minderheiten bietet.

Twitter, Amazon, Apple und Google erlauben Menschen ein Pseudonym, beispielsweise „Flüpke“, zu nutzen. Eine staatliche Identität als Login-Mechanismus weist queeren Menschen hingegen ein möglicherweise falsches Geschlecht und Namen zu.

Referenzen

1. https://de.wikipedia.org/wiki/Personalausweis_(Deutschland)
2. https://lilithwittmann.medium.com/mit-der-id-wallet-kannst-du-alles-und-jeder-sein-au%C3%9Fer-du-musst-dich-ausweisen-829293739fa0
3. https://github.com/fluepke/ssi-poc
4. https://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff
5. https://fragdenstaat.de/dokumente/141932-bmi_idwallet/
6. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/10/10-jahre-personalausweis.html
7. https://de.statista.com/statistik/daten/studie/1125951/umfrage/downloads-der-corona-warn-app/
8. https://www.ki-note.de/fileadmin/user_upload/PDFs/EnID_netID_1906.pdf (Seite 13)
9. https://www.pin-ruecksetzbrief-bestellen.de/
10. https://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure
11. https://www.bluebite.com/nfc/nfc-usage-statistics
12. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf?__blob=publicationFile&v=2