Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)54

29.06.2022

öA Digitale Identitäten

Fragenkatalog Anhörung Digitale Identitäten – Digitalausschuss 04. Juli 2022

Einleitung

Die Diskussion im Bereich der digitalen Identitäten ist irritierend. Es scheint, dass der nPA, als er 2010 veröffentlicht wurde, seiner Zeit so sehr voraus war, dass das Potential nicht erkannt und verstanden werden konnte. Beigetragen dazu haben sicherlich auch vergangene Bundesregierungen, welche die Mittel für Öffentlichkeitsarbeit, um das Potential des nPA zu kommunizieren, mindestens zweimal ersatzlos gestrichen haben.

Aufgrund der sich beschleunigenden Digitalisierung und durch den vorhandenen Innovationsdruck ist viel Forschung finanziert worden, um Probleme mit "Buzzwordtechnologien" (SSI, Blockchain, DLT, Wallets) auf technisch schlechtere Weise zu lösen, als der nPA (eID) bereits heute, ohne jegliche weitere Forschung, ermöglicht.

Ich bin fest davon überzeugt, das über 90% der legitimen und wichtigen Nutzungsszenarien und Anwendungsfälle, die im Bereich der SSI-Debatte, im Bereich der Diskussion über eventuelle Wallet-Lösungen, und im Zusammenhang mit Blockchains, erwähnt werden, durch Verwendung heute vorhandener Funktionen des nPA (eID) auf technisch sicherere und datensparsamere Weise, ohne weitere Forschung, konkret umgesetzt werden könnten.

Der neue Personalausweis (eID) ist aus meiner Sicht eine deutsche Ingenieursleistung der besonderen Art. Obwohl technisch sehr viel möglich wäre, hapert es primär an der Unterstützung der Bundesregierung und der zuständigen Ministerien, um sowohl die Digitalisierung der Verwaltung, als auch die gesamtgesellschaftliche Nutzung von digitalen Identitäten zu ermöglichen. Ein Bruchteil der Gelder, die bisher für Forschungsvorhaben im Bereich von SSI, Blockchain, Wallets, DLT, usw. usf. aufgewendet wurden, hätte vollständig ausgereicht, um das technische Potential des nPA allen an Digitalisierung interessierten Akteuren (Wirtschaft, Verwaltung, Bevölkerung) zu kommunizieren.

Nationale Ebene

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

- Technologisch ist die deutsche eID weiterhin federführend und hat internationale Standards gesetzt (z.B. PACE). Sowohl die NFC-Schnittstelle, als auch die anderen zahlreichen Funktionen des nPA waren schon 2010 seiner Zeit voraus - und sind immer noch hochaktuelle Technologien.
- Die größte Hürde ist in Bezug auf die eID nicht die Technologie, sondern primär die deutsche Verwaltung und die Verwaltungsprozesse. Aus meiner Sicht haben die zuständigen Bundesregierungen hier die Anpassung und Aktualisierung der Verwaltungsprozesse nicht durchgeführt, so dass das vorhandene technologische Potential bisher verpufft ist.

- Auch die Kommunikation des technologischen Potentials gegenüber der Gesellschaft und der Wirtschaft ist nicht erfolgt, so dass auch innovative Unternehmen, die Interesse an einer Nutzung der Möglichkeiten gehabt hätten, nicht so adressiert worden sind, dass sie den Technologiestack “eID” wirklich hätten verwenden können.
- Der Staat steht sich weiterhin selbst im Weg - die Website www.persoapp.de wurde ursprünglich von der TU Darmstadt im Auftrag des BMI entwickelt - das Projekt und seine Finanzierung endete jedoch im Jahr 2015 - seitdem ist diese Website nicht mehr verfügbar und die aus staatlichen Mitteln bezahlte Software “PersoApp” für den Bürger nicht mehr erreichbar. (http://web.archive.org/web/20160903000051/http://www.persoapp.de/impressum/)

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?

- Die eID ist ein datenschutzrechtlicher Fortschritt und technologisch auch heute noch Ihrer Zeit voraus. Die selektive Offenlegung einzelner Daten, bei Wahrung vollständiger Transparenz für alle Beteiligten ist ein technischer Vorteil, den auch andere Technologien, wie z.B. Zertifikatsbasierte Authentifizierung oder “SSI” so nicht bieten können.
- Die Lösung eID konnte ihr Potential bisher nicht realisieren, weil zwar die Technologie geschaffen wurde, alle anderen Aspekte, wie z.B. die Öffentlichkeitsarbeit, die Förderung des Einsatzes in Behörden oder die Schaffung von Anwenderprogrammen vernachlässigt oder sogar unterlassen wurden.
- Damit die eID ihr technologisches Potential wirklich auf die Straße bringen kann, ist es notwendig, dass alle Behörden jegliche Authentifizierungs- und Validierungsprozesse auf Basis der eID umsetzen und dafür entsprechende Applikationen für die Anwender und Bürger geschaffen werden.
- Die 2010 noch geplanten Werbemaßnahmen, um die Mitarbeiter der kommunalen Pass- und Ausweisbehörden zu schulen, und mit einem Werbe-LKW sowohl die Mitarbeiter der Behörden, als auch interessierte Bürger zu informieren, wurde durch Umwidmung des Budgets im Bundeskanzleramt verhindert.
- Eine weitere Kampagne zur Bewerbung der Einführung der eID wurde vom damaligen Wirtschaftsminister Phillipp Rösler verhindert - das so freigewordene Budget wurde angeblich in die Sportförderung gesteckt.

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

- Zuallererst benötigen wir eine Rückbesinnung auf den ursprünglichen Projektplan und eine solide Finanzierung für die seit 2010 eingesparten Maßnahmen. Diese Maßnahmen müssen konsequent durchgeführt werden. Nachdem diese Maßnahmen Wirkung gezeigt haben, kann es unter bestimmten Umständen sinnvoll sein, die Etablierung der notwendigen Technologien in den Ministerien koordinierend zu begleiten - allerdings habe ich große Zweifel ob ein “Laborformat” für die Etablierung einer Technologie der richtige Weg ist - sinnvoller erscheint es mir, durch konkrete Projekte und deren Finanzierung endlich Nägel mit Köpfen zu machen.

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?

- Weitere Umsetzung des eGovG in allen Geschäftsbereichen von Bund und Ländern https://www.bmi.bund.de/DE/themen/moderne-verwaltung/e-government/e-government-gesetz/e-government-gesetz-node.html Das heißt überall dort, wo im ersten Schritt nur ein Antrag, aber kein Vertrag, notwendig ist, die eID zur Feststellung der Person verwenden und auf unnötige Signaturen oder Unterschriften verzichten. Siehe auch § 126 BGB "Schriftformerfordernis".
- Experimentierklausel nutzen, um Zugangshürden zu senken und Alltagsszenarien zu fördern, z.B. zentral vom Bund bereitgestellte Online-Altersverifikation, Anwendungen für Privatpersonen, kleine NGOs auf Basis der Pseudonymfunktion, z.B. auch siehe BSI FIDELIO. https://dserver.bundestag.de/btd/19/261/1926176.pdf
- Der deutsche Ausweis basiert auf der auch vom frz. ANSSI mitgetragenen eIDAS-Token Spezifikation, diese erlaubt die flexible Erweiterung um beliebige Datengruppen, so dass alle Ausweise, vom Angelschein bis zum Funksprechzeugnis, von der Gesundheitskarte bis zum Führerschein digital auf der (Smart-) eID gespeichert werden könnten, sofern dies politisch gewünscht ist. Die Funktionalität für sog. pseudonyme Signaturen, sowie lokale und globale "Generic Attributes" sind bereits vorhanden und müssten nur ausdefiniert und benutzt werden. Gerade die Smart eID eröffnet hierbei große Chancen.
- Auch die juristisch äußerst fragwürdige Auslegung der gesetzlichen Grundlage für VideoIdent, die von Anbietern wie z.B. IDNow oder PostIdent genutzt wird für Prüfungen nach §6 GWG kann durch die Bereitstellung einer entsprechenden Smartphone Applikation beendet werden. Es ist aus meiner Sicht mehr als fragwürdig, ob eine Inaugenscheinnahme eines Ausweisdokuments per Videokonferenz die Pflichten des §6 GWG erfüllen kann, wenn in der für IT-Sicherheit zuständigen Behörde ein Prototyp existiert, wie diese VideoIdent Lösung umgangen werden kann.

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?

- Durch die bisher fehlende Umsetzung des Projekts eID jenseits des technischen Rahmens sind im Markt diverse Anbieter entstanden, die digitale Identifizierungslösungen anbieten, weil sich die eID bisher nicht ausreichend durchgesetzt hat. Diese Anbieter haben ein großes Interesse daran, dass sich das technische Potential der eID nicht realisiert, weil es ihr Geschäftsmodell, nämlich den Betrieb einer Brückentechnologie, gefährdet.
- Das Ausschreibungsdesign und die Forschungsförderung im Bereich der eID ist ursächlich für ein Übermaß an Schaufensterprojekten und einen Mangel an konkreter Umsetzung. Nach 12 Jahren ist es aus meiner Sicht nicht mehr notwendig Grundlagenforschung durchzuführen, wenn die Ziele der Forschungsprojekte durch vorhandene und noch nicht ausgeschöpfte Technologie erreicht werden können.

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?

- Diese Frage betrifft vorrangig das BSI und kann dort am Besten beantwortet werden.
- Es ist jederzeit auch eine Reinstallation basierend auf dem Originalausweis möglich, dieser ist unabhängig gültig. Bei Verlust einer Smart eID kann die jeweilige Smart eID einzeln gesperrt werden, alle Anderen (Smart) eID behalten Ihre Gültigkeit weil im Besitz der Bürger.

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)?

- Die Bürger entscheiden immer wem (relying party authentication) sie welche ihrer Daten offenlegen oder nicht, auch wird heute schon der Zweck und der DSB-Kontakt durch den eID-Client (AusweisApp2) verpflichtend angezeigt und somit kund getan.
- Der Gesetzgeber schafft die Grundlage in Form des PAuswG und der PAuswV, das Bundesverwaltungsamt vergibt nicht-technische Berechtigungszertifikate, die von einer Berechtigungs-CA in technischen Zertifikaten repräsentiert werden. Der Ausweis prüft das technische Zertifikat und stellt sicher, dass niemals mehr Daten als a) grundsätzlich erlaubt und b) von den Nutzern auch zugestimmt übertragen werden.
- Auch heute schon entscheidet das Bundesverwaltungsamt mit Vorlage eines eindeutigen Geschäftszwecks, eines Handelsregisterauszugs, einer Datenschutzerklärung, einer Dienstbeschreibung und eines Datenverwendungsnachweises ob und wer ein Berechtigungszertifikat erhält oder nicht.

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 stellt technisch einen Rückschritt dar und kommt aus einem Umfeld in dem es keine breiten Erfahrungen mit sicheren elektronischen Identitäten gibt (USA). Einige Ideen von SSI sind konzeptionell grundsätzlich gut und werden von der eID bereits technisch ermöglicht.
- Das zentrale technische Problem ist hier, ähnlich wie bei Zertifikaten, dass validierte, echte Personendaten signiert, d.h. mit „Echtheitsgarantie“ bei der kontrollierenden Stelle landen. Dieser Datensatz, kann vollständig und ohne Kenntnis des Bürgers weiterverwendet werden. Es wäre hier möglich, dass ein Unternehmen, gegenüber dem ich mich mittels SSI ausweise, diese Daten mit Echtheitsgarantie weitergibt. (siehe Identitätsdiebstahl, Adresssammler, Datenhandel)

- Dies ist bei der eID so nicht der Fall - denn für jede einzelne Nutzung wird ein sicherer, vertrauenswürdiger Kanal aufgebaut und die jeweiligen Daten darin übertragen. Ähnlich einem Geldschein, der durch Sicherheitsmerkmale als "echt" erkennbar ist und die Zahlen "10", "20", "50", "100" tragen kann wird hierbei der Identitätsträger (z.B. Ausweiskarte) auf Echtheit geprüft und damit sichergestellt, dass die übertragenen Werte ebenso vertrauenswürdig sind - so wie die Wertangabe des Geldscheins. Damit ist einerseits möglich auch nur eine reduzierte Auswahl aller Attribute zu übertragen und es fällt keine Signatur über diese Attribute an.
- Eine vollständige Vermeidung der Empfangsspeicherung ist technisch unmöglich, deshalb versucht die SSI-Gemeinschaft mit Verfahren wie Zero-Knowledge-Proof eine zusätzliche Indirektion zu erschaffen. ZK-Proofs sind aber bestenfalls als "sehr junge und zweckendfremdete Technologie" anzusehen im Kontext Identitäten. Auch der Mehrwert zu sagen "ich heiße Hans Muster will aber die Signatur unter meinen Daten nicht verraten" ist eher widersinnig bis obsolet.
- Selbst eine reine Software-Implementierung der eID, wie bereits seit 2014 prototypisch gezeigt, löst alle bisher aufgeworfenen rechtlichen und technischen Fragestellungen schneller, präziser und einfacher als SSI.

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?

- "Secure Enclave" ist ein Begriff des Unternehmens Apple und beschreibt das "Trusted Execution Environment" (TEE) auf der normalen App-CPU. Diese "Secure Enclave" ist NICHT mit einem "Secure Element" gleichsetzbar und anfällig für alle Angriffe wie Row-Hammer, Spectre, etc. sowie weitere Angriffe dieser Art, die auch ARM CPUs betreffen. Das TEE/Apple Secure Enclave ist kein dedizierter Chip und läuft nur in einem getrennten Modus der Haupt-CPU und ist dadurch wesentlich schlechter geschützt. Das beginnt zum Beispiel schon bei fehlenden geeigneten Evaluierungen und Zertifizierungen z.B. nach Common Criteria (ISO 15408) EAL 4+.
- Secure Elements existierten schon länger, z.B. ab dem Galaxy S7 und verbreiten sich immer mehr, durch die "Android SE Ready Alliance" wird in neueren Geräten eine stärkere Verbreitung über alle Varianten und Ausstattungsversionen hinweg zu erwarten sein.
- Wichtig ist die gedankliche Evolution weg von der reinen "Ausweiskarte" zum generischen "Identitätsträger". Die Ausweiskarte ist nur ein Identitätsträger von vielen, genauso wie das embedded Secure Element im Telefon. Identitätsträger können aber auch eSIMs und normale SIM-Karten sein, genauso wie Wearables in Form von Ringen, Armbändern, Schlüsselanhängern, Smartwatches, Multifunktionstokens ("personal secure element") die mehrere Dinge (Bezahlung, Nahverkehr, Türschlüssel, Zwei-Faktor-Authentisierung, PGP, eID, usw.) heutzutage spielend vereinen können. Die Technologie hat massive Fortschritte gemacht die in den Köpfen der Politik, Verwaltung, diverser Gremien und der Bürger noch gar nicht angekommen sind. Viele Vorbehalte entbehren hierbei auch einer naturwissenschaftlichen Grundlage. Wearables funktionieren mit

vielen Geräten unterschiedlichen Alters und Preisklasse über die existierende NFC-Schnittstelle und können bei Defekt oder Verlust des Gerätes einfach mit dem nächsten Gerät weiterverwendet werden.

- Eine sozialverträgliche - und durch jahrelange Nachnutzung - Umweltfreundliche und Geräteübergreifende Lösung könnte die Ergänzung durch die SIM-Karte sein, so wie in Estland in der Vergangenheit schon geschehen.
- Die Performanzunterschiede sind im tagtäglichen Einsatz nahezu vollständig unerheblich, der Unterschied ist, wenn überhaupt vorhanden, marginal, wesentlich entscheidender ist die Sicherheit der Daten der Bürger*innen.

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?

- Von dieser Lösung ist abzuraten. Diesen Weg zu gehen würde nicht dem Stand der Technik und Wissenschaft entsprechen, unvorhersehbare Risiken provozieren und die Absicherung des Zugriffes auf den Hauptspeicher im Prinzip auf den Hersteller des Smartphones externalisieren. Dieser Weg wurde vom gescheiterten Projekt “IDWallet” versucht und ist gescheitert.
- Ein Performanzunterschied wäre aus meiner Sicht vernachlässigbar gering.

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?

- Staatenbünde wie die EU sollten meiner Meinung nach hier gesetzlich auf die MNOs einwirken, um den Zugang zu eSIMs und SIMs für ID-Verfahren zum Zwecke der sinnvollen Digitalisierung der Gesellschaft zu ermöglichen. Die 2007 in Estland eingeführte mobile ID konnte im Wesentlichen nur deshalb nicht fortgesetzt weil die eingekaufte Menge durch die prinzipbedingt sehr kleine Zahl von Nutzern (~200.000) für die MNOs wirtschaftlich uninteressant war. Die EU hat hier a) wesentlich größere zu erwartende Nutzerzahlen und b) ganz andere Hebel diese Marktmacht in Schranken zu weisen.
- Zum Digital Markets Act im Detail kann ich selbst nichts sagen, ob dieses Gesetzespaket der richtige Ort wäre für eine solche Gesetzgebung - allgemein halte ich europäische Vorgaben in diesem Kontext allerdings für notwendig.

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?

- Es besteht eine wesentliche und dauerhafte Gefahr. Smartphones sind so gut wie immer in Betrieb, und dabei auch so gut wie immer online. Auf Smartphones läuft Programmcode verschiedenster Hersteller - deren Codequalität und damit IT-Sicherheit stark variiert und damit insgesamt fraglich ist. Auch wird es immer Apps geben, die z.B. aufgrund der legitimen Funktion ein Backup des Smartphones durchzuführen, vom User

die Genehmigung bekommen auf alle Speicherbereiche des Smartphones zugreifen zu dürfen.

- Bei der Prüfung der IT-Sicherheit solcher Systeme ist es immer von zentraler Bedeutung, nicht einfach anzunehmen, das das Gerät selbst, also das Betriebssystem und die Gesamtmenge des die Hardware verwendenden Code, sicher ist, und nur das Konzept und der Code der App geprüft werden müsste.
- Je weniger Code auf der Hardware läuft, desto eher ist es möglich, wirklich jede Zeile davon aufwendig zu prüfen, um Identifikationsdiebstähle sicher ausschließen zu können. Vor diesem Hintergrund möchte ich nicht nur auf den nPA, sondern auch auf SIM-Karten hinweisen. Diese sind oft hochsichere Hardware, die teilweise EAL6+ genügen.
- Diese dedizierten Chips (embedded Secure Elements, eSIMs, SIMs, Wearables) haben harte Evaluierungskriterien und überprüfbare Zertifizierungen nach gemeinsamen Standards (ISO 15408) und können ggf. vom Nutzer auch entfernt und in anderen Geräten genutzt werden, ohne das Daten irgendwie entschlüsselt und/oder über Netzwerke übertragen werden müssen
- Diese Vorteile hat eine eSIM/eSE natürlich nicht.
- Damit die Gefahr von Identitätsdiebstählen von Daten aus Wallets technisch reduziert wird, müssten Mobiltelefone, deren Betriebssystem und die Apps ähnlich hart evaluiert und zertifiziert werden damit das Sicherheitsniveau auch nur in die Nähe der technischen Güte der anderen Lösungen kommt. Das ist wirtschaftlich wie technisch aber völlig unrealistisch.

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?

- Nach eingehender, auch öffentlicher, Diskussion hat sich der Einsatz von Blockchain-Technologie im Bereich Identity als unsinnig erwiesen. Die Blockchain löst kein Problem - schon gar nicht besser - dass es ohne sie nicht gäbe. Blockchains basieren auf Mathematik aus den 1950er Jahren, die mit der Entwicklung von Public-Key-Kryptographie Mitte der 1970er für die meisten Anwendungsfälle, insbesondere jedwede Art von Identität, obsolet wurde.
- Blockchains (“ewige Logfiles“) eignen sich u.a. für die Führung von Kassenbüchern, Eingangsvermerke (Archivsysteme), Transaktionshistorien oder nachweispflichtigen Herkunftslisten (z.B. Flugzeugteile) und in begrenzten Szenarien möglicherweise auch im Bereich von Reparatur- und Wartungsdokumentation oder im Bereich der Logistik.
- Blockchains eignen sich nicht für Identitätsmanagement, dafür haben wir seit den 70er Jahren bessere technische Lösungen.
- Prinzipbedingt schließt eine Blockchain systematisch das Aufräumen oder Löschen nicht mehr benötigter Daten technisch aus. Die gespeicherte und damit zu schützende Datenmenge, wächst also ewig an und erreicht über die Zeit sehr unhandliche Größen.
- Selbst wenn nur Meta- oder Schema-Daten auf der Blockchain landen, lässt sich auch dieses Problem einfacher lösen weil es dafür bereits abschließende und hinreichend genaue Protokollspezifikationen gibt.

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 eID-System verstehe ich in diesem Zusammenhang als die existierende technische Infrastruktur im nPA - welche eIDAS kompatibel ist.
- Eine "Wallet"-Architektur ist in der aktuellen technischen Umsetzung des nPA nicht vorgesehen. Nichtsdestotrotz könnte der nPA in einer noch zu konzeptionierenden Wallet-Infrastruktur auf vielfältigste und äußerst flexible Weise genutzt werden.
- Ob ein zentraler Cloud-Anbieter überhaupt nötig ist, hängt im Zusammenhang mit einem "Wallet" vom Systemdesign ab.
- Die hier scheinbar implizierte Befürchtung des Fragestellers, dass durch Nutzung eines Wallets, personenbezogene Daten Anbieterübergreifend verknüpft werden könnten, kann leider nicht entkräftet werden. Würde man jedoch kein Wallet, sondern heute vorhandene Funktionen des nPA verwenden, so könnte diese Befürchtung effektiv entkräftet werden.
- Bereits jetzt generiert der nPA eine pseudonyme Identität für jeden neuen Anfragenden, die ohne Mitwirkung des Personalausweisinhabers nicht zusammen- oder rückgeführt werden können. Natürlich gilt dies nur dann, wenn keine personenbezogenen Daten dem Anfragenden übertragen werden - dies kann aber auch nicht ohne Mitwirkung des Personalausweisinhabers geschehen.

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

- Hier möchte ich auf die Differenzierung im oberen Teil der Antwort auf Frage 14 hinweisen und getrennt zu der vorhandenen eID, also dem nPA und einem potentiellen zukünftigen Wallet antworten.
- Der nPA (eID), Secure Elements Lösungen, Wearables mit technischen Funktionen nach DIN CEN/TS 15480 sind bereits jetzt immer offline verfügbar. Lediglich der Anbieter, der die Ausweiskontrolle durchführt benötigt in manchen, aber nicht allen Szenarien einen Internetzugriff (z.B. im Bereich Straße & Grenze die Sperrlistenprüfung).
- Eine Walletlösung müsste, je nach Systemdesign, sehr wahrscheinlich immer online sein, um einen Nutzen zu bieten. Eine vollständige offline-Verfügbarkeit, wie dies die eID bereits heute bietet, wäre wahrscheinlich nicht möglich.

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.

- Eine Unterscheidung in technische und regulatorische Ansätze ist immer von vornherein unsinnig, da beide Teile (technische Umsetzung und regulatorische Festlegung und Kontrolle) immer sauber aufeinander abgestimmt ineinander greifen müssen. Sonst ist das ganze Prozedere wertlos. Es gibt kein "entweder-oder". Eine regulatorische

Festlegung muss technisch vollständig bis zur letzten Stelle durchsetzbar sein, sonst ist sie angreifbar und zahnlos.

- Relying party authentication ist ein immer zwingendes “MUST HAVE”-Kriterium, sonst ist jedweder Form von Online-Betrug Tür und Tor geöffnet, da es für die Bürger unmöglich wird zuverlässig zu überprüfen wem sie Ihre Daten anvertrauen und auch Over-Identification kein Riegel mehr vorgeschoben werden kann.
- Es steht jedem und jederzeit frei zu sagen “das möchte ich nicht” und ohne oder mit einer niedrigeren Berechtigung oder Validierung fortzufahren, oder das Vertragsverhältnis dann nicht einzugehen.
- Absolut verhindern zu wollen sich auch in Online-Shops und Social Media z.B. via Pseudonymfunktion sicher einzuloggen ergibt meines Erachtens keinen Sinn. Oder für den Versand höherwertiger Waren auf Rechnung eine valide Rechnungsanschrift (“ladungsfähig“) abzufragen. Sowie bei der Online-Gewährung einer Ratenzahlung für Weißgeräte - z.B. Mutter von 5 Kindern hatte Blitzschlag und Waschmaschine, Trockner, Kühlschrank, Herd sind kaputt und müssen ersetzt werden. Es sollte lediglich verhindert werden, dass beliebiger und ungeprüfter Einsatz und somit auch Missbrauch stattfindet.
- Berechtigungszertifikate stellt immer eine Berechtigungs-CA aus, das Modell ist marktoffen, jedoch ist derzeit die Bundesdruckerei GmbH die letzte verbliebene produktiv tätig Instanz (T-Systems und Post sind vom Markt).
- Berechtigungs-CA müssen bereits Mindestanforderungen erfüllen, deren Umsetzung überprüft und dokumentiert und bei Erfolg bestätigt wird (Zertifizierung), prozedural das bisher sicherste Prinzip.
- Berechtigungszertifikate verhindern effektiv Over-Identification indem ein Geschäftszweck, eine Datenschutzerklärung, eine Dienstbeschreibung und ein Datenverwendungsnachweis vorgelegt werden muss.
- Der Staat ist hierbei in der Pflicht seine Bürger zu beschützen, so dass eben nicht z.B. 40 tracking cookies mit der ID des Ausweises verknüpft werden können oder dürfen.

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

- Die in Deutschland im Zuge der eID entstandene Software ist nach wie vor leider nicht wirklich benutzerfreundlich. Häufige (teils kommentarlose) Abstürze, viele durchzuführende Clicks, umständliche und altbackende UIs, unnötig große Apps und langsame Frameworks (Qt), welche hohe Anforderungen an die Systemleistung stellen, machen die User Experience zur Hölle.
- Die vorgenannten Probleme führten dazu, dass mehrere Marktteilnehmer eigene Lösungen gebaut haben. Hier muss dringend vom Bund ordentlich neu gedacht und nachgebessert werden. Die furchtbare UX ist einer der Hauptgründe für die Ablehnung der eID, nicht jedoch die technischen Möglichkeiten des nPA selbst.
- Dabei müssen das eID-System selbst und die offizielle App als lediglich einer von drei oder mehr eID-Clients (andere “AusweisApps”) gedanklich voneinander getrennt werden. Das System selbst lässt sich problemlos effizient, klein, schnell und auch nutzerfreundlicher implementieren, wie u.a. in mehreren Prototypen von BMI PersoApp und BSI FIDELIO auch gezeigt wurde. Meines Erachtens muss an dieser Stelle angesetzt werden, z.B. über die Experimentierklausel aus Antwort 4.

- Unsere Chancen stehen dabei sehr gut mit geringem Aufwand deutliche Erfolge zu erzielen. Ich möchte dabei anregen auf die Expertise von professionellen App-Entwicklern, dem technisch versierten netzpolitischen Umfeld aus CCC e.V., c-base e.V. und deren Universum sowie kreativen Köpfen z.B. aus der SPRIN-D zuzugehen. Es böten sich hier auch Hackathon Formate an bei denen ein Know-How Transfer von der tief-technischen und kryptographischen Ebene hin zum App-Entwickler-Level stattfindet und anschließend verschiedene Wege und Problemlösungsstrategien verfolgt und die besten produktiv weiter umgesetzt werden.

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 eIDAS VO ist sehr zerfasert, langatmig und besitzt wenig klare Ansagen
- Templates für die Anwendung der eIDAS VO im eigenen Land über ID Issuance, ID Management, ID use-cases/verification oder kurz ID Life-Cycles könnten Ländern helfen von Ihren eigenen Konzepten (alte X.509 Zertifikate, unsichere Apps) abweichende Prinzipien und deren Mehrwerte zu verstehen
- Deutschland hatte seit den späten 90ern Signaturkarten mit denen man rechtskräftig unterschreiben und sich somit auch identifizieren konnte, das ist der technologische Stand auf dem sich viele EU-Nachbarn, so auch das hochgelobte Estland, bewegen. Da waren wir schon und haben uns bereits vor 12-13 Jahren weiterentwickelt. Eine Rückkehr zu alten und vor allem unflexibleren Technologien erscheint wenig sinnvoll und sollte vermieden werden.
- Die Verordnung ist aktuell ein Text der sagt “ich bin jetzt da” und nicht “warum bin ich da”, “was mache ich in Zukunft für euch alle besser” das macht es schwierig für Aussenstehende zu verstehen dass es dabei um ein EU-weites interoperables ID-System geht

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 beides geben dürfen. Einerseits ein “Template” wie die eIDAS Token Spezifikation als Modell einer modernen, datenschutzfreundlichen ID-Architektur, die sowohl Ausweiskarten aber auch andere Identitätsträger mit einem erweiterbaren Datenmodell unterstützt
- aber auch die Möglichkeit bei Einhaltung entsprechender Standards (CEN 15480, ICAO 9303, FIDO2, OIDC, …) das eigene ID-System einzukoppeln sollte ermöglicht werden
- eine mögliche Antwort versucht das Projekt https://id4me.org/ zu geben bei dem sowohl Privatpersonen, privatwirtschaftliche Unternehmen, NGOs, staatlich akkreditierte Betreiber oder Staaten selbst Ihre ID-Systeme einkoppeln können. ID4Me versucht die Frage zu lösen wie man zu einem einheitlichen Routing (“wer will sich wo, wie mit welchen Mitteln identifizieren oder authentifizieren”) und einer einheitlichen Rückantwort die wiederum Alle verstehen (wissen wie und auf welchem Level ich der ID vertrauen kann) können zu lösen. Selbst wenn es nicht global funktionieren sollte, wäre das ein möglicher offener, effizienter Ansatz für einzelne Staaten und die EU die

unterschiedlichen Systeme unter einen Hut zu bringen. Die dringend notwendige ganz klare Definition von gegebenem Input ("Bürger*in") und klar definiertem Output ("Identitätsdatum") fehlt(e) bisher bei allen Konzept. Das war Wildwuchs mit Faustrecht.

- eindeutig klar gemacht werden sollte dass alte Zertifikats- und SSI-basierte Lösungen auf Grund ihrer prinzipbedingten Funktionsweise aktuellen Datenschutzansprüchen und dem Zeitgeist nicht (mehr) entsprechen können und nicht mehr sinnvoll weiterverfolgt werden können

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

- Die deutsche eID ist unabhängig von neuen Identitätsträgern (z.B. Smart eID) ausgereift und auf einem modernen Level, das den Ist-Stand vieler EU-Länder übertrifft. Als Beispiel für andere Länder wie man es auch solide machen kann (offene Spezifikation, Erweiterbarkeit, Datenschutzfreundlichkeit, moderne Technologiewahl) ist sie durchaus dienlich.
- Es fehlt die Verdeutlichung und das Verständnis bei anderen EU-Staaten, dass kulturell signierte Personendaten aller Einwohner eines Landes in einer offenen Datenbank, über die man bisweilen auch mal komplett die Kontrolle verliert, schlichtweg ein großes, klares NO-GO für andere EU-Staaten sind und das dort auch nicht ohne harte Konsequenzen bliebe. Hier lässt sich Deutschland mit seiner eID-Strategie sehr leicht politisch Kleinreden weil Fehler in Prozessen, aber nicht in der Technologiewahl an sich gemacht wurden. Mehr Selbstbewusstsein und Unterstützung würde schlussendlich allen EU-Bürgern gut tun. Und die Phrase eines neues deutschen "Exportschlagers" sollte man dabei tunlichst vermeiden. Entweder wir tun das gemeinsam für uns Alle im Miteinander und dann ist es eine "europäische Lösung" oder es wird eine "deutsche Lösung", die allen Europäern übergestülpt wird und trifft dann ganz natürlich auf reichlich Ablehnung. Die Haltung der Politik ist an dieser Stelle sehr entscheidend, ich hoffe dass die Ampel weiser reagiert.
- Die eID ist seit knapp 12 Jahren im Feld und hat damit einen hinreichend hohen Reifegrad zu jeder Zeit zu einer Weiterentwicklung der eIDAS-Verordnung beizutragen.

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?

- Momentan ist die Zielsetzung, gerade in Bezug auf den Test konkreter Forderungen wie Datenschutz und IT-Sicherheit, noch sehr vage.
- Grundsätzlich würde die textuelle und in Schaubildern Aufbereitung bekannter Systeme und Szenarien für das gemeinsame Verständnis ausreichen. Die Large Scale Pilots verbrennen Zeit und Geld und Sinnhaftigkeit, ob dabei ein gemeinsames Verständnis über die Auswahl an Optionen erreicht werden kann erscheint mir fragwürdig. Diese Zielsetzungen müssten klarer formuliert und auch die Testgruppen, z.B. offene Bürgertests für die Beteiligung der Zivilgesellschaft, klarer angesagt und eingeplant werden. Inklusive Feedback Möglichkeit und der Option innerhalb des Pilots nachzusteuern.

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?

- Das Vorhaben ist in sich widersinnig. Es gibt bereits heute mit dem nPA Varianten, sich rechtssicher auszuweisen. Dabei gilt es nicht nur, der anfragenden Stelle nachzuweisen, dass der Nachweis echt ist, sondern auch der Personalausweisinhaber muss rechtssicher erfahren, wem gegenüber (ladungsfähige Anschrift) er sich ausweisen soll - und dann eine Entscheidung fällen können. Dies ist mit ZKP so nicht möglich. Es gibt aus meiner Sicht einen einzigen denkbaren Anwendungsfall, dieser ist die anonyme Überprüfung des Alters oder der Gemeindekennzahl. Das sind genau nur 2 Attribute oder Funktionen von zwei Dutzend, die die eID mitbringt und auch bereits erfüllt.
- ZKP-Verfahren existieren nur als Krücke, um noch nicht ausgereiften Ansätzen wie SSI mit Blockchain über Umwege Sicherheitsfunktionen mitzugeben, die man nicht bräuchte wenn man SSI mit Blockchain nicht hätte.
- Die eIDAS Token Spezifikation enthält bereits Funktionen wie die anonyme Altersverifikation, die anonyme Gemeindekennzahlverifikation, die Pseudonymfunktion und Erweiterungen wie pseudonyme Signaturen über Attributen und Nachrichten um die datensparsame Übermittelung und Überprüfung einzelner Attribute zu ermöglichen.
- Es ist schlichtweg nicht zielführend seinen (zwangsläufig echten) Klartext Namen zu sagen danach nicht die Stellen seines Ausweises zeigen zu wollen. ZKP verhindert nicht dass Personen trotzdem identifizierbar bleiben. Es ist eine esoterische akademische Idee einer Lösung für ein Problem, dass es sonst ganz einfach nicht gibt.

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

- Etablierte, teils sogar globale (UN-weit gültige und ratifizierte), internationale Standards wie ISO 7816, ISO 14443, ISO 24727, CEN 15480, ICAO 9303, OIDC, FIDO sind essentiell für die Interoperabilität von eID-Lösungen.
- Ohne diese Standards setzt in der EU sehr schnell wieder “it works for me”-Mentalität ein und das führt zu Basteleien einzelner Marktteilnehmer und schlechter User Experience und nur teils funktionierenden (Insel-)Lösungen. Ähnliche Versuche wurden in der Vergangenheit schon mit dem bekannten (und von vornherein erwartbarem) Ausgang gemacht, sonst gäbe es diesen aktuellen Anlauf nicht.

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?

- Wenn die EUid-Wallet statt auf eigenwilligen Neuentwicklungen auf Industriestandards aufsetzt wie z.B. OIDC und FIDO dann ist es ein Leichtes zu sagen anstatt “Login with Facebook”, “Login with Google” nun auch “Login with EUid”. Wenn man auf die Unternehmen zugeht und sinnvolle Standards implementiert, werden die Unternehmen dies dankbar annehmen. Bisher wurde oft versucht Individuallösungen durchzusetzen und das müssen Alle für sich erstmal neu implementieren. Das kostet Zeit, Geld, Nerven.

- Die Kritik ist insofern nur berechtigt wenn die EU plant Industriestandards zu ignorieren.
- Die Alternative ist die Regelung so wie sie ist zu behalten und dafür dann auch moderne Industriestandards zu nehmen, also keine Protokolle von vor 20 Jahren oder älter.

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?

- Ich teile diese Kritik. Denn Webseitenzertifikate mit eIDAS wären ohnehin nur eine technische Hürde geworden, die am Ende des Tages keine Wirkung entfaltet, weil die Nutzer nicht darauf trainiert sind diesen speziellen Vertrauensmodus zu erkennen. Die Kritik wurde bereits von der Mozilla Foundation geäußert, da man dort eine ähnliche Erfahrung mit Extended Validation (EV Zertifikate, grüne Adressleiste) gesammelt hat. Die meisten Nutzer wissen gar nicht was das bedeutet. Die CAs verdienen Geld für das Setzen eines Bits und Angriffe mit Phishingseiten gibt es nachwievor, weil der Nutzer erstmal wissen müsste, dass er ohne "grüne Adressleiste" nichts Vertrauenskritisches tun darf. Dazu kommt dass viele Nutzer auch außerhalb des EU-Wirkungsbereiches mit Diensten zu tun haben, die naturgemäß kein eIDAS-Zertifikat haben würden und dann funktioniert der Schutz ebenso wieder nicht.
- Die Idee ist in der Praxis nicht zielführend, da die Konditionierung der User "weiter clicken, egal was" ist und solche Dinge damit nicht den gewünschten Effekt bringen.
- Berechtigungszertifikate, die mit "normalen" TLS-Zertifikaten, der Anbieter verschränkt sind lösen das Problem der Kanal-Authentisierung bereits und sind unabhängig von der Netzwerkverschlüsselungsinfrastruktur. Man sollte die Netzwerkschicht (https://) und die Applikationsschicht (ID-Verfahren) auch gemäß dem OSI-Modell strikt voneinander getrennt halten und nicht miteinander vermengen. Am Ende führt das evtl. nur noch zum Versagen der Ziele der EUid-Wallet.

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?

- Wird, wie weiter oben schon erwähnt, ein offener Industriestandard wie OIDC verwendet gibt es keine technische Hürden oder andere valide Gründe der großen Plattformbetreiber und zahlenreicher Branchen dies nicht zu unterstützen. Denn OIDC ist ohnehin überall dort bereits vorhanden und eingebaut. Eine Verpflichtung wäre also eher begrüßenswert, um Inseldenken und proprietären Entwicklungen von vornherein klar zu begegnen.
- Eine einzige EU-Wallet birgt das Risiko zu lange Release-Zyklen und Testphasen zu haben wegen der Anzahl der Sprachen und Sprachbarrieren in der Prozesskommunikation während der Softwareentwicklung. Daher sollte es zwar eine von der EU herausgegebene Wallet geben, aber gleichzeitig auch die Möglichkeit existieren landesspezifische Wallets, die 100% kompatibel sein müssen, zu erlauben. Dies würde es auch massiv vereinfachen landesspezifische ID-Verfahren, die auf lokalen Mechanismen wie FIDO2

in der tschechischen mojeID, die verschiedenen NFC-Signaturkarten und den eIDAS-Token zu implementieren, ohne alle diese Technologien von vornherein in der einen EUid-Wallet einbauen zu müssen. Weiterhin ist es dann kein großer Schaden, wenn ein Land mal scheitert oder nicht weiterkommt, sei es wegen personellem Engpass, Uneinigkeiten in den lokalen Gremien, usw. - dann können die anderen Länder weiter machen und ggf. die zurückliegenden Länder später wieder aufgleisen.

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?

- Der Zugang zu Identitäten muss kostenfrei sein, es darf kein Geschäftsmodell basierend auf Identitätsvorgängen für den Nutzer geben. Dies fordern schon allein die Gleichbehandlungsgrundsätze eine digitale Teilhabe für Alle und somit auch für sozialschwache Mitbürger zu gewährleisten. Jede Abweichung von dieser Maßgabe öffnet Tür und Tor für profitorientierte Providerdienste, die die EU Bürger dann für jeden Vorgang einzeln zur Kasse bitten. Dies sollte ohne Ausnahme jedwede Nutzung der Wallet durch den User betreffen.

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?

- Im Rahmen von eIDAS wurde u.a. das EU Minimum-Dataset (MDS) definiert. (http://mapping.semic.eu/vdm/id/cv/eb004434a93bbeaa2ba5968d26af06be)
- Die eIDAS Token Spezifikation adressiert diese Notwendigkeit bereits ganz bewusst mit unterschiedlichen aber überall bekannten und einheitlichen Datengruppen, um eine einheitliche Nomenklatur und Nummernkreise zu schaffen.
- Die EU sollte die existierenden Grundlagen aufgreifen und zu einem EU-weiten einheitlichen Standard machen, gezielt pflegen und um die erkennbaren Deltas erweitern - dann kann man diesen Anforderungen sauber begegnen.
- Wie und ob die Werte bei korrekter, einheitlich verständlicher Kodierung, anerkannt werden obliegt der jeweiligen (außen-)politischen Ebene, nicht der gemeinsamen fachlich-technischen.