Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)61

4.07.2022

Ausschuss für Digitales
z.Hd. Frau Anne Vallée
Sekretariat PA 23

Deutscher Bundestag
Platz der Republik 1
11011 Berlin

Isabel Skierka
Digital Society Institute
ESMT Berlin

Schloßplatz 1
10178 Berlin

E-Mail: isabel.skierka@esmt.org

Per Email an: adi@bundestag.de

Sachverständigenstellungnahme von Isabel Skierka, Leiterin Technologiepolitik beim Digital Society Institute der European School of Management and Technology (ESMT) Berlin für die Sitzung des Bundestagsausschusses für Digitales am 04.07.2022 zum Thema „Digitale Identitäten“

I. Übergreifendes Statement

Für jede digitale Transaktion benötigt eine Person, Organisation oder ein Objekt eine digitale Identität – ob eine verifizierte Identität wie die des Personalausweises oder eine bloße pseudonyme Kennung – oder einen digitalen Nachweis über bestimmte Attribute. Digitale Identitäten sind daher der Schlüssel für den Zugang zur digitalen Welt.

Die Diskussion um digitale Identitäten in Deutschland dreht sich aktuell vor allem um **Technologien** – ob es um den Personalausweis, die mobil abgeleitete Smart eID, Wallet-Technologien, SSI-Protokolle, oder Blockchain geht. Die **Probleme**, welche wir lösen wollen, vor allem die **Bedürfnisse** der Nutzer:innen und die **Verbreitung** bei Anwendungspartnern, kommen dabei zu kurz.

Umfrageergebnisse von PwC[1], Bitkom Research[2] und dem eco Verband der Internetwirtschaft[3] sowie das Marktgeschehen zeigen: Nutzer:innen wünschen sich **vertrauenswürdige**, leicht und mobil zu **bedienende** und **breit anwendbare** Lösungen zur digitalen Identifizierung und Authentifizierung und zur Verwaltung ihrer digitalen Identitätsdaten und **Nachweise** wie den Impfpass, den Führerschein, Bahntickets, oder andere Zugangsberechtigungen.

Mit der **eID** des Personalausweises verfügt Deutschland über eine der weltweit technologisch **sichersten** und ausgereiftesten Identitätslösungen und -infrastrukturen, aber **weder** war die

[1] https://www.pwc.de/de/finanzdienstleistungen/der-online-ausweis-auf-dem-smartphone-und-die-digitale-brieftasche.html
[2] https://www.bitkom-research.de/de/pressemitteilung/sechs-von-zehn-deutschen-wollen-sich-digital-ausweisen Die Umfrage von Bitkom Research bezieht sich auf den Einsatz von elektronischen Brieftaschen bzw. Wallets
[3] https://www.eco.de/presse/eco-umfrage-deutsche-wollen-digitale-identitaeten-staerker-nutzen/

eID bisher besonders **einfach nutzbar, noch war sie breit anwendbar**. Deutschland verfügt aktuell über kein Ökosystem für digitale Identitäten, das die aktuellen Bedürfnisse der Nutzer:innen und Anwendungsanbieter abdeckt.

Bisher ist eine **Strategie der Bundesregierung** für digitale Identitäten noch nicht klar erkennbar oder transparent. Es ist wichtig, dass die Bundesregierung verschiedene Projekte für digitale Identitäten einheitlich und sektorübergreifend koordiniert: PA, Smart eID, Beitrag der Schaufenster-Projekte auf kommunaler und regionaler Ebene, ELSTER, Gesundheits-Telematik-Infrastruktur, Bürgerkonten. Dazu gehört eine Bündelung der Verantwortlichkeiten und ein Verfolgen gemeinsamer Ziele, interoperable Standards und transparente Sicherheitsniveaus, sowie ein konsequenter Einsatz für europäische Lösungen und deren Mitgestaltung.

Ich möchte in dem Eingangsstatement auf folgende Punkte eingehen, die ich für wichtig halte und als Ergänzung zur Position der anderen Sachverständigen vorbringen möchte.

1. Deutschland muss bei digitalen Identitäten **über den deutschen Tellerrand hinausblicken**
    a. Dazu gehört neben dem europäische eIDAS-Gesetzgebungsprozess eine Auseinandersetzung mit den **Global Playern** und deren schnell voranschreitenden ID-Angeboten. Über ihre marktbeherrschende Stellung bei Mobilgeräten und Betriebssystemen werden globale Technologieplattformen eine Vielzahl von Nutzer:innen erreichen und nicht nur Eintrittskarten und Flugtickets integrieren, sondern auch Bezahldaten und bald verifizierte Identitäten wie den Führerschein und vielleicht auch hoheitliche Identitäten – Stichwort Apple Wallet.
    b. Die EUID steht im Wettbewerb mit diesen Angeboten, ist aber gleichzeitig auf die Nutzung von deren Technologie angewiesen. Wie ist eine Kooperation zu erreichen?
    c. Falls Deutschland und die EU mit ihren Projekten nicht erfolgreich sind, könnte es in der EU möglicherweise Identitätslösungen ähnlich wie in den USA geben: Staatliche Register stellen den Plattformen Identitäts-Daten und -Attribute zur Verfügung, die dann von diesen als Dienstleistung an die Relying Parties (Diensteanbieter) vermarktet bzw. weitergegeben werden.
    d. Als Voraussetzungen für einen Erfolg der ID-Lösungen in Deutschland und in der EU
        i. Müssen diese Lösungen selbst wettbewerbsfähig, insbesondere auch hinsichtlich Nutzerfreundlichkeit und Anwendungsbreite sein
        ii. Muss die Nutzung entscheidender technischer Komponenten der mobilen Plattformen wie z.B. das SE über geeignete technische Standards und geeignete regulatorische Rahmenbedingungen möglich sein. Beispiel: über den DMA und die eIDAS-VO könnte die EU die Mitbenutzung von SE/eSIM-Technologien für europäische Identitätslösungen möglich machen und entsprechende Standards bei ENISA/GSMA entwickeln.
2. Der Personalausweis hat **weniger ein Technologie- als ein Anwendungs- und Vermarktungsdefizit**

a. Das bestehende Vermarktungsdefizit kann man nicht durch Technologie-Tausch beseitigen. Der **PA muss sich natürlich dem technologischen Wandel** stellen, was er mit der kontaktlosen Schnittstelle, der Nutzung mobiler Endgeräte über die NFC-Schnittstelle, der Vorbereitung der Smart-eID, der frühen eIDAS-Notifizierung und der Beteiligung an den eIDAS-Pilotprojekten bereits getan hat bzw. jetzt tun muss.
b. Noch wichtiger ist die Schaffung von **Voraussetzungen für eine breite Marktakzeptanz und breite Einbindung der Lösungen bei Diensteanbietern** (Vergleich nordische Staaten, Belgien, Niederlande) sowie ein **einheitliches rechtliches Rahmenwerk.**
c. Um Marktbarrieren abzubauen und die Anwendungen zu fördern, sollte eine **Integration in Anwendungen leichter und vor allem kostengünstiger für Diensteanbieter werden** (Stichpunkt hoher finanzieller und zeitlicher Aufwand für Diensteanbieter für die Anbindung an eID-Infrastruktur über Berechtigungs-Zertifikate oder eID-as-a-service-Anbieter).
d. Man sollte jetzt wichtige und von Bürger:innen **viel genutzte Anwendungsfälle vorantreiben**, z.B. haben andere Länder über die Kombination des digitalen Nachweises der Covid-Impfung mit einem digitalen Ausweisdokument die Verbreitung ihrer digitalen Ausweislösung gestärkt (s. ID Austria Österreich)
e. Außerdem sollte die BReg die **Vereinheitlichung des bisher sehr fragmentierten regulatorischen Rahmenwerks** für digitale Identitäten voranbringen und rechtliche Hürden z.B. mithilfe von **Reallaboren** mindern.

3. **Ökosystem-Ansatz** stärken
   a. Die eID Infrastruktur muss weiterentwickelt werden, aber auch **in ID-Ökosystemen von Partnern aus Wirtschaft und Staat zugänglich** sein
   b. Die Ökosysteme müssen Lösungen einbinden, die Erbringung **digitaler Nachweise** ermöglichen, also auch Vertrauensdienste
   c. Staat kann ein Ökosystem nicht allein steuern, kann aber in Kooperation mit privaten Anbietern Impulse setzen, rechtlichen Rahmen schaffen und durch Standardisierung Interoperabilität fördern, insb. auf EU-Ebene
   d. **Verschiedene Sicherheitslevel** sind erforderlich, die eine hohe Transparenz über Sicherheit gewährleisten
   e. **Wallets, Credentials und zugängliche Register** sollten Kern der Strategie sein. Zudem sollte die Strategie auf **mehrere Wallets im Wettbewerb** setzen, und technologieoffen sein.
4. **SSI**
   a. SSI ist zunächst einmal eine Philosophie und keine Technologie. Neue Standards, die SSI umsetzen sollen, befinden sich noch in der Entwicklung.
   b. Mit Bezug auf den PA: Zunächst hat der PA seit 2010 bereits SSI-Eigenschaften auf der Grundlage klassischer Technologie. Die Forderung nach absoluter „Self-Sovereignity“ hat ihre Grenzen bei hoheitlichen Identitäten darin, dass nach wie vor jeweils der Staat die Richtigkeit von hoheitlichen Personenidentitäten gewährleisten muss.
   c. Wenn SSI/DL/BC Technologien für digitale Identitäten eingesetzt werden sollen, muss geprüft werden, ob sie diese Voraussetzungen auch erfüllen. Dazu

gehören auch einschlägige Sicherheits- und Datenschutzeigenschaften. Hier ist offensichtlich noch einiges zu tun (siehe BfDI und BSI – Bewertungen dazu) und es besteht ggf. auch noch Forschungsbedarf. SSI muss nicht mittels Blockchain umgesetzt werden.

5. Insgesamt sollten **Prozesse** – sowohl auf gesetzgeberischer Ebene als auch auf technischer / Standardisierungsebene **transparenter gestaltet sein und Expert:innen aus Zivilgesellschaft und Wissenschaft besser einbinden**

    a. Sowohl auf nationaler Ebene (eine „lessons learned“ aus dem ID-Wallet Launch)
    b. Is auch EU-Ebene (s. Toolbox-Prozess, der nur für Vertreter:innen von MS zugänglich ist)

II. Beantwortung ausgewählter Fragen des Fragenkatalogs

Fragen 1, 2 und 4: Zu den Herausforderungen der eID

Deutschland verfügt mit der eID des PA über eine der weltweit sichersten Identitätslösungen – doch sie wird kaum, von ca. 9 % der Bevölkerung, genutzt, wie Erhebungen bspw. vom E-Government Monitor regelmäßig zeigen.[4] Nutzer:innen können die eID bisher auch für nur sehr wenige Anwendungen nutzen.

Neben der eID des Staates existieren zahlreiche andere Identitätslösungen, von denen jedoch keine eine kritische Größe erreichen konnte.[5]

Die Folge: ein **Flickenteppich** von Lösungen, der bedingt ist durch:
Fragmentierte regulatorische Anforderungen an digitale Identitäten: Je nach Sektor unterschiedliche regulatorische Anforderungen. Dazu gehören neben der öV Identifizierungen und Authentifizierungen im Finanzsektor (vgl. § 12 Abs. 1 und § 13 Abs. 1 GWG und Art. 97 PSD2-RL), im Gesundheitssektor (vgl. § 291 a SGB V), Telekommunikationssektor (vgl. § 172 TKG) oder Identifizierungen im Rahmen von qualifizierten elektronischen Vertrauensdiensten (vgl. Art. 24 (1) eIDAS-VO). Die sektorspezifischen Regelungen des OZG, GWG, TKG, SGB V unterscheiden sich jedoch bezüglich der Erhebung von Identitätsdaten, der Anforderungen an Identitätsfeststellung und der Nachweise, die abgesehen von Ausweisdokumenten zugelassen sind – das GWG erlaubt beispielsweise eine qualifizierte elektronische Signatur für die Identitätsprüfung, das TKG nicht. Auch die Verfügungen und Technischen Richtlinien der zuständigen Aufsichtsbehörden – die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) für den Finanzsektor, die Bundesnetzagentur für den Telekommunikationssektor und Vertrauensdienste, das BSI für die öV – unterscheiden sich. Diese stellen wiederum unterschiedliche Anforderungen an Identifizierungsverfahren. Beispielsweise ist das VideoIdent-Verfahren laut BaFin (Rundschreiben 03/2017) für den Bankensektor und für

[4] https://initiatived21.de/app/uploads/2021/10/egovernmentmonitor2021.pdf#page=12
[5] Payment and Banking (2020). “Digital Identity in Deutschland – Übersicht“, https://paymentandbanking.com/digital-identity-uebersicht-deutschland/

Vertrauensdienste im Rahmen der Modulbestätigung alternativer Identifizierungsmethoden nach Art. 24 eIDAS Abs. 1 erlaubt. Für die öV erlaubt das BSI diese nicht.
Diese Fragmentierung der regulatorischen Anforderungen erschwert die sektorübergreifende Einbindung von Identitätslösungen und von Vertrauensdiensten wie der QeS und auch ihr Angebot extrem.
Mangelnde Anwendungen (Stand 2020 banden 131 Anwendungen die Onlineausweisfunktion des nPA ein, wovon 86 Dienste einzelner Kommunen oder Länder sind, welche nur wenigen Bürger:innen zugänglich sind. Insgesamt sind daher nur 45 Dienste mit dem nPA bundesweit nutzbar, davon sind nur 28 Dienste privatwirtschaftlicher Anbieter.[6])
Marktbarrieren für Diensteanbieter
Kosten und Zeitaufwand für Einbindung in die eID Infrastruktur sind für viele Diensteanbieter zu hoch (Berechtigungszertifikat, Compliance, Beauftragung „eID-as-a-service"-Anbieter, damit verbundene Transaktionsbasierte Abrechnung)
Die genauen finanziellen und zeitlichen Kosten konnten wir bisher nicht ermitteln (nicht öffentlich oder für Forscher:innen zugänglich). Daten, die wir in Expert:innengesprächen erhoben haben, zeigen, dass die Kosten für Berechtigungs-CA für kleinere oder mittelgroße Firmen finanziell nicht oder kaum tragbar sind und der Zeitaufwand für die Ausstellung des Berechtigungs-CA (einschl. Beantragung, Auditierung, weitere Überprüfungen, Ausstellung) ebenfalls hoch ist.
Wenn diese Kosten nicht übernommen / subventioniert werden, werden kleinere Firmen sich eine Anbindung an die eID-Infrastruktur nicht leisten können und auf kostengünstigere Lösungen umsteigen bzw. keine eID-Lösung anbieten, die entsprechende hohe technologische Standards wie der PA einhält
Mangelnde Nutzerfreundlichkeit der eID Funktion und der damit verbundenen Apps[7], wobei der Zugang zur eID über mobile Endgeräte, bereits per NFC-Schnittstelle, die Nutzung erleichtert hat. Doch auch die User Experience und die intuitive Bedienbarkeit sollten weiter optimiert werden.
Mangelhafte Kommunikation und Vermarktung der eID: Inbesondere der Launches der Smart eID sollte unbedingt mit einer aussagekräftigen und leicht verständlichen Kommunikations- und Vermarktungskampagne einhergehen
Während der Bedarf an Anwendungen für die Erbringung **digitaler Nachweise** steigt, ob Berufsqualifikation, Impfausweis, Führerschein, ist diese mit der eID und damit verbundenen Angeboten bisher ebenfalls nicht / nur schwer möglich. Es ist wichtig, Lösungen für digitale Nachweise auf Grundlage hoher IT-Sicherheits- und Datenschutzstandards weiterzuentwickeln.

8. **Wie definieren und bewerten Sie das Self-Sovereign Identity (SSI)-Konzept? Eine Kritik an SSI ist, dass beglaubigte Daten bei den Empfängern gespeichert**

[6] Boston Consulting Group und Nortal (2020). "Zehn Jahre elektronischer Personalausweis: Wie Deutschland ein erfolgreiches eID-Ökosystem aufbauen kann", https://web-assets.bcg.com/43/c6/6101a4034a958228b6cce70229e8/bcg-zehn-jahre-elektronischer-personalausweis.pdf, auf Grundlage von https://www.personalausweisportal.de/SharedDocs/artikel/Webs/PA/DE/informationsmaterial/erteilte-berechtigungszertifikate/erteilte_Berechtigungszertifikate.html
[7] Akzeptanz und Nutzerfreundlichkeit der AusweisApp: Eine qualitative Untersuchung, https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/6296/file/tbhpi69.pdf

würden. Wie bewerten Sie die Datensicherheit des SSI-Konzepts? Gibt es aus Ihrer Sicht technische Wege, wie diese Empfangsspeicherung durch SSI vermieden werden kann?

(s.o.:) SSI bezieht sich zunächst auf eine Philosophie der selbstbestimmten Identitäten und ist daher keine Technologie an sich. Neue Standards, die SSI umsetzen sollen, befinden sich zurzeit noch in der Entwicklung.

Wenn SSI/DL/BC Technologien für digitale Identitäten eingesetzt werden sollen, muss geprüft werden, ob sie die damit verbundenen Voraussetzungen der Selbstbestimmtheit auch erfüllen. Dazu gehören auch einschlägige Sicherheits- und Datenschutzeigenschaften. Hier ist offensichtlich noch einiges zu tun (siehe BfDI und BSI – Bewertungen dazu) und es besteht ggf. auch noch Forschungsbedarf. SSI muss zudem nicht mittels Blockchain-Technologien umgesetzt werden.

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?**

Über NFC-Schnittstellen verfügen sehr viele Smartphones, womit eine breite Nutzbarkeit der eID über die NFC-Schnittstelle gewährleistet sein sollte. Daher wäre zumindest die Nutzung der eID-Funktion über die Ausweis-App2 per Anhalten an die NFC-Schnittstelle möglich.

Ein hohes Sicherheitsniveau einer mobilen eID-Lösung (wie Smart eID) ist nur durch eine Verankerung der eID im Secure Element (SE) möglich sein. Das von SE gebotene Sicherheitsniveau entspricht ungefähr dem Sicherheitsniveau klassischer Smartcards.

(Hintergrund zu SE: Ein sicheres Element (SE) ist eine manipulationssichere Hardware, die in der Lage ist, Anwendungen (Applets) und deren vertrauliche und kryptografische Daten (z. B. Schlüssel) sicher zu hosten.

Es gibt verschiedene Formfaktoren von SE:

a. *eine SIM-Karte (Universal Integrated Circuit Card, UICC)*
b. *eSIM (Embedded Integrated Circuit Card (eUICC): eine auf die Hauptplatine des Smartphones gelötete erweiterte SIM-Karte, auf die SIM-Profile (als Anwendung) und Anwenderdaten geladen werden können*
c. *embedded SE (eSE): eine auf die Hauptplatine des Smartphones gelötete Smartcard*
d. *microSD: ein Smartcard-Chip im Formfaktor der microSD)*

Über Secure Elements (SE) verfügen weniger Smartphone-Modelle (einige Modelle von Samsung, Huawei, Google Pixel 3, Apple iPhones ab Serie 6 u.a.). Da sich SEs auch für den Einsatz in vielen Anwendungsfeldern eignen, z.B. beim mobilen Bezahlen oder digitalen Identitäten, haben sie Potenzial in Zukunft eine große Verbreitung am Markt zu finden und Marktakteure (Smartphonehersteller, MNOs, Service Providers) dementsprechend kooperieren werden.

Kurzfristig wird ein Zugang für eID-Lösungen zur SE-Funktion daher **nur auf bestimmten Smartphone-Modellen möglich sein**. **Mittel- bis langfrsitig** könnte sie auf sehr viel **mehr Mobilgeräten verfügbar sein, wenn die oben genannte Marktentwicklung eintritt.**

DE und die EU sollten jedoch weitere Maßnahmen treffen, um den Zugang zum SE führender Smartphone-Hersteller zu öffnen. **Die eIDAS-VO könnte zum Beispiel über einen Verweis auf den DMA den Zugang zum SE erzwingen.**

Darüber hinaus soll es für die Smart eID z.B. auch eine **Software-Variante** geben, die Hardware-unabhängig implementiert werden kann. Der baltische Vertrauensdienst SK ID Solutions betreibt bspw. sehr erfolgreich eine Software-Variante für die Smart-ID, welche in Estland, Lettland und Litauen verbreitet ist. Solche Software-Varianten erfüllen jedoch in der Regel nicht das hohe Vertrauensniveau, welches ein SE bietet. Damit böten diese Lösungen **höchstens ein Vertrauensniveau entsprechend eIDAS „substanziell", was aber für viele Anwendungsfälle ausreichen könnte.**

Im Sinne der Resilienz und Diversifizierung von Angeboten sollten zudem **alternative Hardware-Anker** zur sicheren Verwahrung krypotgrafischer Daten und der zugehörigen Applets geprüft werden.

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?

Eine eSIM ist wie in der Antwort auf Frage 10 beschrieben ein SE. **Die Bundesregierung sollte sich für eine Nutzung des SE von Smartphoneherstellern für europäische Idenitätsdienste über die eIDAS-VO einsetzen.**

Bisher enthält die der Entwurf für eine **aktualisierte eIDAS-VO eine** solche Passage in ErwG 21. Innerhalb der Verordnung sollte Bezug **auf Art. 6 (1) (f) des DMA** genommen werden, nach dem Gatekeeper Anbietern von „ancillary services" (Nebenleistungen) Zugang zu und Interoperabilität mit dem Betriebssystem, Hardware- oder Software-Features gewähren, die auch der Gatekeeper für eigene „ancillary services" nutzt. Nebendienstleistungen umfassen laut DMA ausdrücklich Identifizierungsdienste (Art. 2 (2) (14)).

Somit sollte sich die EU durch eine Erzwingung der Öffnung der geschlossenen Systeme in eine starke Verhandlungsposition für die weitere Verhandlung über Kooperation mit den Herstellern bringen.

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

Zunächst ist es positiv zu bewerten, dass digitale Identitäten auf EU-Ebene weiterentwickelt werden sollen.

Der **unique persistent identifier** ist sehr kritisch zu sehen ((Art. 11 a) (2), eIDAS 2) und sollte in dieser Form nicht in der eIDAS-VO bleiben,

Wallet: **Profiling** sollte ausgeschlossen sein. Bisher gibt es noch eine „Hintertür" in Art. 6 a) (7) eIDAS 2, die eine Weitergabe der Daten durch ausdrückliche Zustimmung der Nutzer:in ermöglichen könnte. Das stellt ein Risiko dar, welches minimiert werden sollte.

Es ist zudem bisher noch **unklar**, wie **Wallets und technische Referenzarchitekturen technisch ausgestaltet und abgesichert würden**, einschließlich der Einbeziehung von Cloud-Lösungen. Daher sind viele Details zur technischen Ausgestaltung und Datenschutz- und -sicherheit bisher nicht klar zu beurteilen.

Der Toolbox-Prozess wird von Vertreter:innen der Mitgliedstaaten verhandelt, gewährleistet zu wenig Transparenz für Expert:innen.

Die eIDAS-VO setzt auch auf die Öffnung öffentlicher Register für die Ausstellung von Attributen über qualifizierte Vertrauensdienste. Dies ist ein wichtiger Schritt, damit Bürger:innen Daten selbst aus Registern anfragen, ableiten und weiterverwenden können.

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 einen einheitlichen Rahmen geben, der Interoperabilität zwischen Standards gewährleistet. Technologieoffenheit ist wichtig. Man sollte evolutionär auf bestehenden Standards aufbauen, aber die Entwicklung neuer Standards und Architekturen weiter vorantreiben, die evtl. in Zukunft interoperabel zum Einsatz kommen und Mehrwerte bieten können.

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?**

Der Large Scale Pilot ist eine wichtige Initiative, um vor allem Anwendungsfelder europaweit zu erschließen, geht das eingangs erwähnte Problem der Anwendungsbreite an, beispielsweise im Kontext des Piloten „Potential", an dem auch Deutschland aktiv mitwirkt,

oder das „EU Digital Identity Wallet Consortium“. Die Chancen, dass hier hohe Datenschutz- und IT-Standards gesetzt werden, schätze ich momentan als gut ein, kann dies jedoch nicht abschließend beurteilen.

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?

ZKP sind an sich ein gutes und wichtiges Konzept, welches weiter untersucht und für die Anwendung geprüft werden sollte. Aktuell scheint es jedoch noch nicht für einen sofortigen Einsatz ausgereift genug zu sein.