20. Wahlperiode

Deutscher Bundestag
Ausschuss für Digitales

Wortprotokoll
der 13. Sitzung

Ausschuss für Digitales
Berlin, den 4. Juli 2022, 14:00 Uhr
10117 Berlin, Adele-Schreiber-Krieger-Str. 1
Sitzungssaal: MELH 3.101

Vorsitz: Tabea Rößner, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt 1 **Seite 04**

a) Digitale Identitäten

b) **Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität**

KOM(2021)281 endg.; Ratsdok.-Nr. 9471/21

Federführend:
Ausschuss für Digitales

Mitberatend:
Ausschuss für Inneres und Heimat
Rechtsausschuss
Wirtschaftsausschuss
Ausschuss für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz
Ausschuss für die Angelegenheiten der Europäischen Union

c) **Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS)**

KOM(2021)290 endg.; Ratsdok.-Nr. 9492/21

Federführend:
Ausschuss für Digitales

Mitberatend:
Ausschuss für Inneres und Heimat
Rechtsausschuss
Wirtschaftsausschuss
Ausschuss für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz

Mitglieder des Ausschusses

	Ordentliche Mitglieder	Stellvertretende Mitglieder
SPD	Becker, Dr. Holger	Diedenhofen, Martin
	Kassautzki, Anna	Esken, Saskia
	Marvi, Parsa	Hakverdi, Metin
	Mesarosch, Robin	Kaiser, Elisabeth
	Mieves, Matthias David	Klüssendorf, Tim
	Mohrs, Falko	Leiser, Kevin
	Schätzl, Johannes	Müller (Chemnitz), Detlef
	Wagner, Dr. Carolin	Papendieck, Mathias
	Zimmermann, Dr. Jens	Peick, Jens
	Zorn, Armand	Schneider, Daniel
CDU/CSU	Biadacz, Marc	Bär, Dorothee
	Brandl, Dr. Reinhard	Hahn, Florian
	Durz, Hansjörg	Hauer, Matthias
	Hoppermann, Franziska	Heilmann, Thomas
	Jarzombek, Thomas	Henrichmann, Marc
	Kemmer, Ronja	Metzler, Jan
	Reichel, Dr. Markus	Müller, Florian
	Santos-Wintz, Catarina dos	Schön, Nadine
	Zippelius, Nicolas	Steiniger, Johannes
BÜNDNIS 90/DIE GRÜNEN	Außendorf, Maik	Bär, Karl
	Bacherle, Tobias	Christmann, Dr. Anna
	Gelbhaar, Stefan	Grützmacher, Sabine
	Khan, Misbah	Klein-Schmeink, Maria
	Rößner, Tabea	Notz, Dr. Konstantin von
FDP	Funke-Kaiser, Maximilian	Brandenburg (Südpfalz), Mario
	Mordhorst, Maximilian	Höferlin, Manuel
	Redder, Dr. Volker	Konrad, Carina
	Schäffler, Frank	Kruse, Michael
AfD	Cotar, Joana	Höchst, Nicole
	Lenk, Barbara	König, Jörn
	Schmidt, Eugen	Naujok, Edgar
	Storch, Beatrix von	Wiehle, Wolfgang
DIE LINKE.	Domscheit-Berg, Anke	Pau, Petra
	Sitte, Dr. Petra	Reichinnek, Heidi

Tagesordnungspunkt 1

a) Digitale Identitäten

b) Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität

KOM(2021)281 endg.; Ratsdok.-Nr. 9471/21

c) Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS)

KOM(2021)290 endg.; Ratsdok.-Nr. 9492/21

Die **Vorsitzende**: Ich weise auf das Angebot des Vereins Bürgerservice.org hin, im Anschluss an die Anhörung Hilfestellung dabei zu geben, die Online-Ausweisfunktion aller zu aktivieren.

Ich begrüße alle Ausschussmitglieder im Saal und die Vertreter/-innen der Bundesregierung. Der Parlamentarische Staatssekretär Johann Saathoff vom Bundesministerium des Innern und für Heimat ist nur kurzzeitig anwesend und wird dann von Herrn Ernst Bürger, Abteilungsleiter Digitale Verwaltung, Steuerung OZG, hier im Saal vertreten. Herr Staatssekretär Markus Richter kann aus terminlichen Gründen nicht teilnehmen, auch den wird Herr Bürger kompetent vertreten. Ich weiß aus Erfahrung, dass Sie sich mit voller Leidenschaft für die fortschreitende Verwaltungsdigitalisierung stark machen. Die Fachebene des Bundesministeriums für Digitales und Verkehr verfolgt die Anhörung im Livestream. Ich begrüße die Öffentlichkeit und alle Interessierten hier im Saal. Als Sachverständige haben wir eingeladen:

Dr. Silke Bargstädt-Franke, Abteilungsleiterin Cybersicherheit in der Digitalisierung und für elektronische Identitäten beim Bundesamt für Sicherheit in der Informationstechnik. Sie ist uns virtuell zugeschaltet.
Dann begrüße ich Flüpke vom Chaos Computer Club in Präsenz.
Herrn Christian Kahlo, Experte für Digitale Identitäten (aus der Zivilgesellschaft), auch in Präsenz.
Zugeschaltet ist uns Prof. Ulrich Kelber, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.
Dann haben wir eingeladen Herrn Prof. Dr. Marian Margraf, Abteilungsleiter für Secure-Systems Engineering vom Fraunhofer AISEC.
Dann Dr. Kim Nguyen, Senior Vice President der Bundesdruckerei GmbH und Geschäftsführer der D-Trust GmbH, auch in Präsenz.
Prof. Dr. Peter Parycek, Leiter des Kompetenzzentrums Öffentliche IT am Fraunhofer FOKUS.
Dann ist uns noch zugeschaltet Isabel Skierka, Program Leader an der European School of Management and Technology, herzlich willkommen.
Und last but not least Rebekka Weiß, Leiterin der Abteilung für Vertrauen und Sicherheit im Bitkom e.V., herzlich willkommen.

Zum Ablauf der Sitzung: Die Sachverständigen sind gebeten, zu Beginn ein circa fünfminütiges Eingangsstatement abzugeben. Dann erhält jede Fraktion ein Zeitfenster von 5 Minuten für Fragen und Antworten. Sie brauchen also nicht zu warten, bis ich Ihnen das Wort erteile. Die Reihenfolge bestimmt sich nach Stärke der Fraktionen. Bei jeder weiteren Fragerunde bestimmt die Vorsitzende die Reihenfolge entsprechend den Vorgaben von § 28 Absatz 1 GO-BT. Die Redezeit pro Runde wird bei Bedarf verkürzt. Ein gemeinsamer Fragenkatalog der Fraktionen liegt vor und wurde als Ausschussdrucksache SB 20(23)4 verteilt. Die schriftlichen Stellungnahmen der Sachverständigen liegen den Ausschussmitgliedern vor und wurden auf der Internetseite des Ausschusses veröffentlicht. Es wird ein Wortprotokoll angefertigt werden. Die Anhörung wird live im Internet auf Kanal 3 des Parlamentsfernsehens gestreamt und ist anschließend über die Mediathek des Bundestages abrufbar. Einige Hinweise zum technischen Verfahren: Die Sitzung wird als hybride Webex-Sitzung durchgeführt. Ausschussmitglieder und eingeladene Gäste, die sich über die Videoschaltung beteiligen, weise ich darauf hin, wenn möglich Headsets zu nutzen und nach den Redebeiträgen die Mikrofone auszuschalten. Letztgenanntes gilt auch im Saal. Nutzen Sie die Chatfunktion, wenn Sie einen Wortbeitrag anmelden wollen.

Das Thema der heutigen Sachverständigenanhörung lautet Digitale Identitäten. Die Identität einer Person ist einmalig und unverwechselbar. In der realen Welt sind es körperliche Merkmale wie ein Fingerabdruck oder ein Gesichtsbild, die uns – in Verbindung mit hoheitlichen Dokumenten – helfen nachzuweisen, wer wir sind. Bei Vorgängen in der virtuellen Welt ist das nicht immer ganz so einfach. Es gibt viele verschiedene Verfahren, um Personen online zu identifizieren. Und was Verlässlichkeit und vor allem Sicherheit angeht, gibt es durchaus sehr unterschiedliche Anforderungen. Ziel der Digitalpolitik muss es sein, einerseits immer mehr digitalisierte Verfahren zum Beispiel bei Verwaltungsdienstleistungen zu ermöglichen und gleichzeitig digitale Identitäten, die dafür notwendig sind, bestmöglich zu schützen und Missbrauch von sensiblen Daten zu verhindern. Dazu bedarf es einerseits eines Rechtsrahmens, der elektronische Transaktionen – auch grenzüberschreitend – vertrauenswürdig nutzbar macht, und andererseits hochsicherer Technologien. Die Änderung der eIDAS-Verordnung trägt daher den technischen Entwicklungen Rechnung und hilft, Identifizierungsprozesse zwischen Mitgliedstaaten effizienter zu gestalten. Mit der heutigen Anhörung holt der Ausschuss für Digitales nun externen Sachverstand ein. Wir beleuchten, welche Technologien geeignet sind - auch im Hinblick auf den europäischen Binnenmarkt. Im Mittelpunkt dessen steht immer die Selbstbestimmung der Menschen. Und ich freue mich, dass Sie uns bei der Suche nach europäischen Lösungen helfen, die Potenziale und Risiken abzuwägen. Der Ausschuss freut sich auf Ihre Beiträge und wir beginnen nun mit den fünfminütigen Eingangsstatements. Zuerst darf ich Dr. Silke Bargstädt-Franke um ihr Statement bitten, Sie haben das Wort.

SVe **Dr. Silke Bargstädt-Franke** (BSI): Sehr geehrte Frau Rößner, sehr geehrte Damen und Herren Abgeordnete des Deutschen Bundestages, meine Damen und Herren, ich bedanke mich ganz herzlich auch im Namen von Herrn Schönbohm und des erkrankten Dr. Schabhüser für die Einladung zu dieser Anhörung. Uns ist allen bewusst: Je weiter die Digitalisierung in der Lebenswelt, aber auch in der Arbeitswelt voranschreitet, nicht zuletzt auch beschleunigt durch die Corona-Pandemie, desto größer wird die Bedeutung sicherer digitaler Identitäten. IT-Sicherheit ist - und hierfür steht das BSI - die Voraussetzung für eine erfolgreiche, sichere Digitalisierung. Meine Damen und Herren, es ist eine staatliche Kernaufgabe, Bürgerinnen und Bürgern sichere Identifikationsmittel zur Verfügung zu stellen. Mit dem Online-Ausweis existiert bereits heute eine solche digitale und sichere Technologie. Nur wenn die angebotenen Produkte einfach zu verwenden sind und gleichzeitig auch notwendigen Anforderungen an Datenschutz und IT-Sicherheit Genüge tragen, werden sie auf eine breite Akzeptanz stoßen. Nutzbarkeit und IT-Sicherheit müssen Hand in Hand gehen. Darüber hinaus – wir haben es eben schon gehört – müssen die Lösungen auch im europäischen Rahmen skalieren können. Wie Ihnen bekannt ist, läuft aktuell die Überarbeitung der eIDAS-Verordnung derzeit im Rat, ist aber noch nicht abgeschlossen. Der erste Entwurf beinhaltet hier als wesentliche Änderung die Einführung eines Identitäten-Ökosystems mit einer EUDI-Wallet als Kern. Deutschland ist hier in den sogenannten Large Scale Pilots beteiligt und als BSI begleiten wir eng diese zukünftigen Lösungen und halten diese europäische Ebene für den Erfolg des Roll-outs für ganz entscheidend. Sehr verehrte Abgeordnete, die Ausgestaltung der Sicherheitselemente digitaler Identifizierungssysteme obliegt den Herstellern bzw. Diensteanbietern. Ich appelliere daran, beim für die jeweilige Anwendung benötigten Sicherheits- und Vertrauensniveau Augenmaß zu wahren. Ich möchte die Gelegenheit heute auch nutzen, um mich im Namen des BSI nochmals bei Ihnen für den sehr gelungenen Koalitionsvertrag zu bedanken. Der Relevanz und der Notwendigkeit der Stärkung von IT-Sicherheit wird Rechnung getragen. Hierfür ist es notwendig, dass das BSI bei großen Digitalisierungsprojekten des Bundes von Beginn an einbezogen wird. Die Entwicklung und Implementierung der Corona-Warn-App ist hierzu ein positives Beispiel, wie sichere und anwenderfreundliche Digitalprojekte in Deutschland zügig realisiert werden können. Wir müssen aber alle stets den Endanwender und die Endanwenderin im Blick haben. Das BSI leistet bereits heute im digitalen Verbraucherschutz einen wichtigen Beitrag zur Stärkung und Akzeptanz des Vertrauens in

digitale Dienstleistungen und Technologien. Unter der Überschrift „Tipps zum Schutz vor digitalem Identitätsdiebstahl“ finden Verbraucher /-innen auf der BSI-Webseite hilfreiche Informationen und Hinweise. Das BSI veröffentlicht jährlich einen Bericht zum digitalen Verbraucherschutz. Dieser zeigt, mit welchen Risiken und aktuellen Bedrohungen der private digitale Alltag konfrontiert wird. In der kommenden Ausgabe wird hier das Thema digitale Identitäten einen Schwerpunkt bilden. Denn, meine Damen und Herren, digitale Souveränität beginnt beim Einzelnen. Meine Damen und Herren Abgeordnete, beim wichtigen Thema sichere digitale Identitäten muss der Staat in letzter Konsequenz Grundrechte gewährleisten. Den Schutz des Eigentums, der Privatsphäre und der Vertraulichkeit der Kommunikation im digitalen Raum. Daher nochmals an dieser Stelle mein Apell, IT-Sicherheit bei der Weiterentwicklung digitaler Identitätssysteme direkt und von Anfang an mitzudenken gemäß der BSI-Prämisse „security by design, security by default“. Denn sonst drohen im Nachhinein teure und zeitaufwendige Redesigns. Last but not least erlaube Sie mir, verehrte Abgeordnete, an dieser Stelle noch einmal auf die Umsetzbarkeit hinzuweisen. Um ein digitales Ökosystem in Deutschland und auf europäischer Ebene richtig auszurollen, müssen Haushaltsstellen und Finanzmittel bereitgestellt werden. Lassen Sie uns gemeinsam in dieser Legislaturperiode die entscheidenden Schritte bei der Entwicklung unserer digitalen Identitäten gehen. Hierbei steht das BSI jederzeit mit seiner Expertise zur Verfügung. Herzlichen Dank für Ihre Aufmerksamkeit und ich freue mich auf Ihre Fragen.

Die **Vorsitzende**: Vielen Dank für Ihr Statement, Frau Dr. Bargstädt-Franke für das BSI. Als nächstes hat das Wort Flüpke vom Chaos Computer Club.

SV **Carl Fabian Lüpke (Flüpke)**: Sehr geehrte Damen und Herren, seit über zwölf Jahren verfügt Deutschland über ein System für die digitale Identität, den neuen Personalausweis. Die Entscheidung, sich auf eine NFC-Schnittstelle festzulegen, hat sich als sehr vorausschauend herausgestellt. NFC ist omnipräsent. Sie alle haben bestimmt schon einmal im Supermarkt kontaktlos bezahlt. Anstatt die breite Verfügbarkeit des elektronischen Personalausweises praktisch nutzbarer zu machen, was kurzfristig möglich wäre, evaluiert die Bundesregierung eine neuartige Technologie, die sogenannte Self Sovereign Identity – kurz SSI. Zur Forschung an dieser noch nicht abschließend standardisierten SSI-Technologie hat die vorherige Bundesregierung unter anderem im Schaufenster sichere digitale Identitäten und der ID-Wallet-App viel Zeit und Geld investiert, 100 Millionen Euro, ohne dass dabei belastbare Prototypen entstanden. So ist die ID-Wallet-App binnen weniger Tage nach ihrer Vorstellung wegen struktureller Sicherheitsschwachstellen panisch offline genommen worden. Zudem zeigte sich davon unabhängig eine mangelhafte Leistungsfähigkeit. Hierbei ist darauf hinzuweisen, dass die Schwachstellen nicht nur die ID-Wallet-App betreffen, sondern alle SSI-Wallets. Aufgrund der Schwachstelle war für einen Benutzenden nicht zweifelsfrei abklärbar, wem eine staatlich beglaubigte Ausweiskopie übermittelt wird. Eine selbstsouveräne Preisgabe der Daten ist so nicht möglich. Nun muss ein großes Konsortium diese Spezifikation mit hohem Zeitaufwand anpassen, um diese seit langem bekannten Angriffsmöglichkeiten zu beheben. Einen diesbezüglichen frühzeitigen Hinweis des Bundesamtes für Sicherheit in der Informationstechnik ignorierte man bei der ID-Wallet einfach. Scheinbar war IT-Sicherheit kein Designkriterium und eine Fertigstellung zur Bundestagswahl wichtiger. Sie, liebe Vertreterinnen und Vertreter der neuen Bundesregierung, sollten hier aufräumen und - drastisch formuliert - die Reißleine ziehen. Denn jede Lösung, welche sich auf die Sicherheit von Smartphones verlässt, und das tun Wallet-Apps zur Speicherung der Ausweisdaten, wird prinzipbedingt angreifbar sein. Insbesondere alte Modelle verfügen selten über aktuelle Sicherheitsfeatures und Updates. Secure Elements – also speziell abgesicherte Hardwaremodule – können hier eine Abhilfe schaffen, sind aber nur in den wenigsten Modellen verfügbar. Zudem darf die Sicherheit der eigenen elektronischen Identität keine Geldfrage sein. Ein weiterer Kritikpunkt an der SSI-Technologie ist die Empfangsdatenspeicherung. Beim Empfänger der Daten fallen staatlich signierte Ausweisdaten an,

eine beglaubigte Ausweiskopie. Die kann jederzeit, also auch später bei einem etwaigen Datendiebstahl von einer Internetplattform als echt geprüft werden. Durch die staatliche Signatur macht man diese ohnehin schon wertvollen Daten noch wertvoller und schafft monetäre Anreize, sie zu sammeln und für Angreifer sie zu stehlen. Je nach SSI-Technologie sind damit zudem ein Tracking und eine Profilbildung über Geräte und Plattformen hinweg zu Lasten der Privatsphäre im Internet möglich. Beim Personalausweis hat man vor zwölf Jahren bereits die heute bei der SSI-Technologie neu eingeführten Risiken durch geeignete Designentscheidungen und Sicherheitsanforderungen effektiv vermieden. Für dieses existierende, etablierte und deutlich sicherere Verfahren sind günstige und auch alte Smartphones geeignet. Denn auch diese verfügen in der Regel über eine NFC-Schnittstelle zum Auslesen des Ausweises. Im interministeriellen Laborformat sollte evaluiert werden, wie mit weiteren konkreten Anwendungsszenarien die 62 Millionen elektronischen Personalausweise eingesetzt werden können. Die Technologie dafür ist da und im Gegensatz zur noch diffusen SSI-Technologie, bei der es diverse Umsetzungsszenarien gibt, klar spezifiziert – seit zwölf Jahren. Von der Forschung an Buzzword-Technologien sollte jedenfalls abgesehen werden. Zudem kann die Bundesregierung durch minimales Eingreifen kurzfristig die Voraussetzung für eine breite Adoption der Onlineausweisfunktion in der Wirtschaft schaffen. Hierzu sollten die Preise für sogenannte Berechtigungszertifikate reguliert werden und Referenzimplementierung als Open-Source-Software frei zur Verfügung gestellt werden. Um es zusammenzufassen: Sparen Sie sich viel Zeit und Geld, setzen Sie auf eine vorhandene, solide Technologie – den Personalausweis – und stellen Sie die Forschungsvorhaben hinsichtlich der schlechteren SSI-Technologie Ihrer Vorgängerregierung ein. Und zu allerletzt: Es darf keine Ausweispflicht im Internet geben. Das Vorzeigen des Ausweises muss auch weiterhin die Ausnahme bleiben und zwar nur dort, wo es aufgrund bestehender Gesetze notwendig ist.

Die **Vorsitzende**: Vielen Dank, das war Flüpke, der die Sicht des Chaos Computer Club deutlich gemacht hat. Als nächstes hat das Wort Christian Kahlo, er ist langjähriger Experte für digitale Identitäten. Sie haben das Wort.

SV **Christian Kahlo**: Vielen Dank für Ihre Einladung zu dieser öffentlichen Anhörung. Mein Name ist Christian Kahlo. Ich habe die technischen Richtlinien der eID persönlich mitgestaltet. Seit dreizehn Jahren wirke ich dafür in den Arbeitsgruppen des BSI mit. Heute sitze ich nicht als Vertreter für einen Verband oder ein Unternehmen hier, sondern für die netzpolitische Zivilgesellschaft. Im Sinne der Transparenz möchte ich anmerken, dass meine Entwicklungstätigkeiten am neuen Ausweis im Rahmen meines Anstellungsverhältnisses unter anderem bei der adesso SE erfolgten. Ich bin inzwischen davon überzeugt, dass der nPA, als er 2010 veröffentlicht wurde, seiner Zeit so sehr voraus war, dass das Potenzial nicht erkannt und verstanden werden konnte. Das möchte ich heute ändern, denn wir brauchen hier ein allgemeines Umdenken. Aufgrund der sich beschleunigten Digitalisierung und des vermeintlichen Informationsdrucks ist viel Forschung finanziert worden. Diese Forschung versucht, Probleme mit Buzzword-Technologien wie SSI, Blockchain und DLT-Wallets zu lösen, die technisch aus meiner Sicht bereits abschließend gelöst sind. Der nPA mit seiner eID-Funktion ermöglicht bereits heute, alle mir bekannten Anwendungsszenarien der Unternehmen, der Zivilgesellschaft und der staatlichen Verwaltung sicher und datenschutzfreundlich zu realisieren. Damit auch die Bürgerinnen und Bürger ohne das technische Wissen diese Funktion nutzen können, benötigen sie eine App. Ich führte die Entwicklung der ersten App, mit der man den Ausweis auf einem Mobiltelefon nutzen konnte. Dies mündete in das BMI-Projekt Perso-App, das bis circa 2015 verfügbar war. Nach der Ablösung des früheren Bürger-Clients hat das BMI die Applikation AusweisApp 2 geschaffen. Obwohl viele der Entwickler fähig und kompetent sind, wurden hier relevante Designentscheidungen der Applikation nicht von Software-Entwicklern, sondern von Juristen gefällt. Dies hat offensichtlich negative Auswirkungen auf die User Experience. Sowohl beim Projekt Perso-App als auch bei BSI fidelio und nun auch bei der AusweisApp 2 zieht sich ein roter Faden durch. Die zuständigen Ministerien versäumten, die Anwendung am Bedarf zu orientieren. Schlimmer ist jedoch, dass die Kommunikation

vernachlässigt wurde. Die Einführung eines digitalen Identitätssystems in einem Land hat große Parallelen mit der Einführung eines neuen Zugangssystems in einem Unternehmen. Jeder, der einen solchen Wandel mitgemacht hat, weiß, dass dafür ein Change-Prozess notwendig ist, der über eine reine Technologieentwicklung hinausgeht. Eine geeignete technische Lösung existiert. Wer das Heilsversprechen glaubt, dass eine neue technologische Basis ohne Änderung der Prozesse genutzt werden kann, wurde getäuscht oder ist naiv. Wenn Sie Ihr Auto von einem Verbrenner zu einem Elektroauto wechseln, brauchen Sie nicht nur eine elektrische Ladesäule an der Tankstelle, sondern auch eine Lademöglichkeit zu Hause und in Ihrem Büro. Das Elektroauto haben wir, aber Lademöglichkeiten zuhause – also Integration in die Lebenswelt der Bürgerinnen und Bürger –wurde zu wenig nachgedacht. Wenn ich in diesem Kontext von einem Change-Prozess spreche, dann meine ich, dass wir auch bis in die Lebensrealität der Bürger, bis in die Prozesse und Abläufe der Behörden und bis zum konkreten Nutzen für die Unternehmen denken müssen. An diesen drei Stellen müssen wir Dialog ermöglichen, Veränderungen bewirken, Prozesse entwickeln und Menschen mitnehmen. Hierzu ist ein intensiver Austausch mit Bürgerinnen und Bürgern, Zivilgesellschaft, Wirtschaft und Behörden notwendig. Hierbei ist es im gesamtgesellschaftlichen Interesse, digitale Identitäten als öffentliche, digitale Infrastruktur mit entsprechenden Geschäftsmodellen zu gestalten. Die Nutzung muss wie das Vorzeigen eines Ausweises für die Nutzerinnen und Nutzer kostenfrei bleiben. Auch von staatlicher Seite ist dringend darauf zu achten, dass die Kosten eines entsprechenden Betriebs sich nicht nach der erwünschten Nutzung der Bürgerinnen und Bürger richten, sondern externalisiert wird. Auch eine Verwertung von Betriebs- und Nutzungsdaten sollte in einem Open Data-Modell erfolgen. Ich habe die Hoffnung, dass die Debatte um digitale Identitäten sich zusehends versachlicht. Nach Gutachten des BSI, des Pentagon und Stellungnahmen der US-Zivilgesellschaft an den US-amerikanischen Kongress zeigt sich, dass modische Ansätze wie Blockchain, Distributed Ledger oder Wallets eine Technologie mit schwerwiegenden gesellschaftlichen Implikationen zweckentfremden. Schrauben ziehen Sie sicherlich auch nicht mit einem Hammer an. Glücklicherweise ist der richtige Nagel bereits erfunden. Mir scheint, dass das zentrale Problem hier nicht die Technologie ist, denn die funktioniert. Auch die Innovationsleistung der beteiligten Unternehmen ist nicht das Problem. Wie im Bereich der Digitalisierung häufig der Fall, müssen hier keine neuen Technologien entwickelt werden, sondern bestehende technische Verfahren adaptiert werden. Richtig ist der Schritt weg von alten Zertifikaten für ID-Verfahren wie bei einigen unserer europäischen Nachbarn, da diese weder selektive Offenlegung, Funktionen wie anonyme Altersverifikation, Krypto-Agilität oder andere moderne Funktionen leisten können. Als sehr problematisch sehe ich aber, dass in den zuständigen Ministerien weder die Leistungsfähigkeit der entwickelten Komponenten verstanden wird, noch die Notwendigkeit der Kommunikation mit Zivilgesellschaft, Wirtschaft und Behörden gesehen wird. Meine Hoffnung ist, dass eine Versachlichung der Debatte eine zeitgemäße, rasche europäische Lösung für eIDs mit den bestehenden Normen, Standards und Technologien ermöglicht. Vielen Dank.

Die **Vorsitzende**: Vielen Dank, Sie hätten noch ein wenig Zeit gehabt. Das war Christian Kahlo, langjähriger Experte für digitale Identitäten und Vertreter der Zivilgesellschaft. Als nächstes hat das Wort Prof. Ulrich Kelber, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Sie haben das Wort.

SV **Prof. Ulrich Kelber** (BfDI): Vielen Dank, Frau Vorsitzende, meine sehr geehrten Damen und Herren Abgeordnete. Vielen Dank für die Gelegenheit zur Teilnahme an der Anhörung. Der Bedarf für sichere Identifizierung und Authentifizierung ist weiter gewachsen. Viele Bürgerinnen und Bürger fordern dies ein - und die dazugehörigen digitalen staatlichen Angebote ebenfalls. Aus unserer Sicht sind Datenschutz und digitale Identitäten sehr wohl vereinbar. Sie sind sogar analogen oder hybrid analog-digitalen Lösungen vorzuziehen, wenn sie gut gemacht sind. Angesichts der teilweise sehr technischen Einzeldebatten um digitale Identitäten lohnt sich eine grundsätzliche Vergewisserung. Das Recht auf informationelle Selbstbestimmung steht in einem Spannungsfeld zu staatlicher und privater

Identifizierung. Es gibt grundsätzlich erhebliche Risiken bei solchen Identifizierungen, die in Tracking bestehen, in der Erstellung von Verhaltens- und Bewegungsprofilen, sodass das Recht auf informationelle Selbstbestimmung betroffen sein kann. Dem ist von vornherein mit den richtigen Weichenstellungen zu begegnen. Faktische Anonymitäten sind ein wichtiger Bestandteil einer freiheitlich-demokratischen Gesellschaft. Es ist deswegen für Viele mit europäischen Werten nicht vereinbar, zum Beispiel in öffentlichen Räumen durch staatliche oder private Identifizierung erfasst zu werden. Gerichtlich ist geklärt, dass es keinen Klarnamenzwang zum Beispiel bei der Nutzung von Plattformen wie Facebook geben darf. Und natürlich hat die doch große Vielfalt von Internetangeboten, die Vielfalt auch von selbstgeschaffenen Identitäten deutlich abgestufte Anforderungen an Identifizierung und Authentifizierung je nach Schutzbedarf das bisher ermöglicht. Und diese rechtliche und technische Ausgestaltung digitaler Identitäten mit solchen weniger eingriffsintensiven Identifizierungskonzepten sollte unbedingt gewahrt bleiben. Die Bedenken angesichts App-gestützter, mobiler ID-Wallet-Lösungen sind nachvollziehbar. EID-Lösungen, erst recht ID-Wallets, als Anhäufung verschiedenster Attribute, bergen je nach Ausgestaltung in mindestens drei Punkten gravierende Datenschutzrisiken: Verhaltens- und Standorttracking durch die Aussteller der in der Wallet vorhandenen Attribute. Anstelle eines Endes des Onlinetrackings, wie es ja leider im Digital Services Act vergeblich gefordert wurde, entsteht ein neues Einfallstor für Online-Profilbilder. Es kann eine Überidentifizierung geben, wenn leicht die Möglichkeiten genutzt werden, im Rahmen von vertraglichen Anforderungen darüber hinausgehend durch private Nutzerinnen und Nutzer das Ganze zu machen, also pseudonyme Nutzungen, anonyme Nutzungen zu reduzieren. Und drittens haben wir natürlich Sicherheitsrisiken und ganz neue Dimensionen des Identitätsdiebstahls, wenn das gebotene hohe Schutzniveau für eine auf Smartphones laufende App-Lösung nicht erreicht wird. Deswegen war in der Tat das Vorgehen bei der missglückten Einführung der ID-Wallet der letzten Bundesregierung etwas, was auch Vertrauen gekostet hat. In der Summe geht es also um erhebliche Risiken digitaler Identitäten. Diese können durch eine entsprechende datenschutzfreundliche Ausgestaltung bewältigt werden, die aber von Anfang an zum Einsatz kommen muss. Wir haben in der Tat, das wurde erwähnt, mit dem digitalen Personalausweis bereits eine sehr gute Lösung, die in einer ganz anderen Form zum Einsatz kommen muss, und natürlich auch bei allen staatlichen Angeboten genutzt werden kann. Auch das erleben wir heute, dass oft nicht auf diese Technologie zurückgegriffen wird. Das heißt, für die Verhandlungen über die eIDAS-Verordnung gilt für uns natürlich, dass die Wallets für das Identity Matching nicht mit einem einheitlichen Personenkennzeichen verknüpft werden sollten. Das wäre eine Position, die unbedingt gehalten werden sollte. Sie wird natürlich aus einer kulturellen Situation in anderen Ländern anders diskutiert. Aber wir haben eben alternative Möglichkeiten, mit denen es bei der Bedienung und Qualität der Datenverknüpfung keinerlei Einschränkungen geben würde und dieses Problem eben nicht entstehen lassen würden. Deswegen vielleicht zwei grundsätzliche Bemerkungen: Auch wir als Beauftragte und Beratungsinstitution für Regierung und Parlament sind offen für neue Technologien, die Datenschutz und Datensicherheit fördern – also Privacy Enhancing Technologies. Aber sie müssen natürlich immer dem jeweiligen Gewährleistungsziel dann auch logisch entsprechen. Wir beraten gerne in dem weiteren Prozess auch die Bundesregierung - und da schließe ich mich dem BSI an: Diese Beratung muss aber natürlich frühzeitig erfolgen, sodass die Empfehlungen auch noch aufgenommen werden können und nicht nur als Widerspruch zur gewählten Lösung dann auf dem Markt bestehen bleiben. Vielen Dank für die Aufmerksamkeit.

Die **Vorsitzende**: Vielen Dank, Prof. Kelber. Als nächstes Prof. Dr. Marian Margraf, Abteilungsleiter am Fraunhofer Institut AISEC.

SV **Prof. Dr. Marian Margraf**: Vielen Dank für die Einladung. Meines Erachtens sind digitale Identitäten eine wesentliche Voraussetzung für die Verlagerung von Geschäftsprozessen in die digitale Welt und werden heute auch schon vielfältig genutzt, zum Beispiel Verfahren wie

Benutzername/Passwort oder Login via Facebook, Google oder Apple. Allerdings erfüllen die natürlich nicht die sicherheitstechnischen Voraussetzungen für sichere Anwendungen, wie zum Beispiel einer Kontoeröffnung oder der Antragstellung in einer Behörde. Mit der Onlineausweisfunktion existiert bereits seit zwölf Jahren eine sichere Lösung. Dass diese von den Nutzerinnen und Nutzern nicht so angenommen wird, wie wir uns das am Anfang erhofft haben, liegt zum einen an den fehlenden Angeboten. Nutzer/-innen können eben mit ihrer Onlineausweisfunktion - selbst wenn sie wollen und wenn die eingeschaltet ist - nicht viel anfangen. Ich war damals an der Entwicklung der Onlineausweisfunktion noch vonseiten BSI beteiligt - das zur Transparenz. Unter anderem deswegen finde ich die auch toll. Ich denke aber, dass mit dem Onlinezugangsgesetz ein wichtiger Schritt in die richtige Richtung getan wird. Unsere Usability-Untersuchungen in diesem Bereich zeigen auch, dass Nutzer/-innen das verwenden wollen. Sie werden diese Onlineausweisfunktion verwenden, wenn sich für sie Prozesse vereinfachen, also zum Beispiel ein Gang zur Behörde entfällt. Das ist mein wesentlicher Punkt dazu. Ich möchte auch kurz auf das Thema SSI eingehen, weil das auch einen großen Teil im Fragenkatalog eingenommen hat. Grundsätzlich finde ich die Prinzipien, die SSI vorschreibt, offene Teilnahme, Barrierefreiheit, Sicherheit, Datenschutz und minimale Offenlegung sehr wünschenswert. Allerdings sehen wir, dass die aktuell umgesetzten SSI-Lösungen viele Kritikpunkte haben. Für mich ist fundamental unter anderem, dass in diesem SSI-Kontext kein Unterschied zwischen digitalen Identitäten und sogenannten Beglaubigungen gemacht wird. Eine Beglaubigung ist für mich zum Beispiel ein Zeugnis. Die müssen ganz anders betrachtet und sicherheitstechnisch umgesetzt werden. Mit einem Diplomzeugnis beweise ich, dass eine gewisse Person ein Diplom in Mathematik hat. Ich beweise nicht, dass die vorlegende Person diese Person ist. Mit einer digitalen Identität beweise ich, wer ich bin. Wenn man sich anguckt, wie man das sicherheitstechnisch umsetzen will, dann sind das verschiedene Voraussetzungen. Eine Beglaubigung könnte ich von einem Gerät auf das andere kopieren. Ich muss mir das nicht neu ausstellen lassen von der Hochschule. Eine elektronische Identität sollte ich nicht von einem Gerät auf das andere kopieren können. Sonst könnte sie weitergegeben werden und irgendjemand könnte behaupten, er sei ich. Neben diesem Kritikpunkt gibt es noch weitere, die schon genannt wurden oder in meiner Stellungnahme zu finden sind. Deswegen wäre meine Lösung eine zweigeteilte Betrachtung. Das Projekt Smart eID des BMI kann dafür genutzt werden, elektronische Identitäten – auch auf dem Smartphone – abzubilden. Das andere kann per SSI-Technologie verfolgt werden. Zur Beteiligung von Bürgerinnen und Bürgern bei solchen Lösungen: Wir haben in der Vergangenheit gesehen, dass große Teile der Zivilgesellschaft großen IT-Projekten der öffentlichen Hand sehr kritisch gegenüberstehen – typisches Beispiel war 2010 die Onlineausweisfunktion. Da gab es großen Widerstand. Mittlerweile hat sich das gelöst. Befürchtet wird nach unseren Untersuchungen, dass dem Staat keine IT-Kompetenz zugetraut wird. Deswegen finde ich, dass die Zivilgesellschaft schon in der Konzeptionsphase in das Projekt integriert werden sollte, um zu diskutieren und einen Austausch herzustellen, etwa warum man bestimmte Verbesserungsvorschläge nicht aufgenommen hat.

Die **Vorsitzende**: Ganz herzlichen Dank, Prof. Margraf vom Fraunhofer Institut. Als nächstes Dr. Kim Nguyen, Senior Vice President der Bundesdruckerei GmbH und Geschäftsführer der D-Trust GmbH. Sie haben das Wort.

SV **Dr. Kim Nguyen**: Vielen Dank, sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren Abgeordnete, sehr geehrte Kolleginnen und Kollegen. Ich bedanke mich herzlich für die Möglichkeit, hier einige Punkte in die Diskussion um das Thema digitale Identitäten einbringen zu können. Für die Bundesdruckerei sind – trotz des Namens – digitale Identitäten schon seit vielen Jahren ein Kernthema, nicht erst seit Einführung des nPA. Aufseiten der Bundesdruckerei durfte ich bei der Einführung des Personalausweises teilnehmen. Wir freuen uns, dass das Thema in letzter Zeit an politischer Aufmerksamkeit gewonnen hat und dass die Bedeutung von digitalen Identitäten als Voraussetzung der erfolgreichen Digitalisierung der Verwaltung, aber auch der Wirtschaft und der Gesellschaft, insgesamt auf breiter Basis gesehen wird. Die

vergangenen Jahre der Pandemie haben uns eindeutig gezeigt, dass das Thema Digitalisierung in allen diesen Bereichen ein ganz wesentliches ist. Dementsprechend begrüßen wir die verschiedenen Aktivitäten und Projekte auf nationaler Ebene, mit denen das Thema vorangetrieben wird und auch den Vorschlag der Kommission zur eIDAS-Novellierung aus dem letzten Jahr. National wurden zahlreiche Projekte aufgesetzt, darunter auch etliche mit Beteiligung der Bundesdruckerei, die wichtige Grundlagen für die weitere Entwicklung, aber auch für die EU-weite Weiterentwicklung gelegt haben. Einige möchte ich kurz nennen. Das Projekt ONCE, das ein Förderprojekt des BMWK ist zur Anwendung von sicheren digitalen Identitäten. Das Projekt IDunion, auch ein BMWK-Förderprojekt zur Schaffung eines Ökosystems für dezentrale, selbstbestimmte Identitäten. Nicht zuletzt das Projekt Smart-eID, das die Realisierung der Onlineausweisfunktion auf dem Smartphone darstellt. Zugleich möchte ich noch einmal hervorheben, dass wir in Deutschland bereits eine digitale Identität ausgerollt haben. Wir haben bereits eine gut etablierte und mittlerweile deutlich einfacher nutzbarere eID-Funktion des Personalausweises. Ende des letzten Jahres war bei circa 46 Millionen Ausweisen, das sind fast 75 Prozent von insgesamt 61 Millionen Ausweisen, die digitale Identitätsfunktion bereits freigeschaltet. Von daher ist die Frage: Wie kann es hier weitergehen und wie bringen wir die Entwicklung auf nationaler und auf EU-Ebene zusammen? Aus unserer Sicht erscheint es wichtig, einerseits national Geschwindigkeit aufzunehmen und die begonnene Entwicklung schnell und sicher voranzutreiben und andererseits die EU-Aktivitäten voll zu unterstützen, um beide Entwicklungen zu verzahnen. Dabei sollte unserer Meinung nach die bestehende Basis in Deutschland genutzt werden und die Entwicklung in Richtung eines nationalen Ökosystems für digitale Identitäten vorangetrieben werden. Die Nutzung der eID-Funktion sollte für Verwaltung und Wirtschaft über neue Anwendungsfälle gefördert und die Nutzerfreundlichkeit, insbesondere über die Nutzung der Smart-eID im mobilen Kontext, weiter verbessert werden. Wir sind der Meinung, dass es hier nicht kurzfristig eine einheitliche EU-Lösung geben wird und daher auch die Fertigstellung der Large Scale Pilots keine Option im Sinne des Abwartens darstellt, da hier zu viel Zeit verloren gehen würde. Zugleich müssen wir natürlich die europäische Dimension im Blick haben. Der Bund sollte - wie als Möglichkeit im Kommissionsvorschlag vorgesehen - eine nationale hoheitliche Rolle mit der Smart-eID als Kernidentität, aber mit offenen Schnittstellen als nutzbare Referenzimplementierung zur Verfügung stellen. So kann ein Höchstmaß an Datenschutz und Sicherheit sowie Vertrauen gewährleistet werden und gleichzeitig ein Wettbewerb entstehen. Die Systeme zur Herausgabe beziehungsweise zur Ableitung hoheitlicher Identitäten und Nachweise sollten durch eine Vertrauensstelle des Staates geleistet werden, ebenso die Koordination des Betriebs, des Service und der Weiterentwicklung. Diese Grundversorgung sollte aus unserer Sicht nicht kommerziell erfolgen und auch nicht durch privatwirtschaftliche Konzerne wie Apple oder Google bereitgestellt werden. Die Herausgabe von privatwirtschaftlichen Nachweisen sowie die Entwicklung von entsprechenden kompatiblen Wallets oder Apps sollten aber darüber hinaus allen Marktteilnehmern offen stehen. Schließlich möchte ich noch auf die europäische Dimension eingehen. Um parallel abgestimmte Entwicklungen zu gewährleisten, ist es hier wichtig, an den richtigen Schnittstellen der EU mitzuarbeiten. Das kann auch die Bundesdruckerei mit unterstützen. Das ist zum einen die Beteiligung an der nationalen Toolbox-Gruppe, die sozusagen ein Spiegelgremium der entsprechenden Gruppe in Brüssel darstellt, und zum anderen die Beteiligung an den Large Scale Pilots. Hier wird es um die grenzüberschreitende Pilotierung von Anwendungsfällen zur Erprobung der neuen Digital Identity Wallet nach der eIDAS-Verordnung gehen. Hier wird in den Jahren 2023/2024 eine entsprechende Pilotphase erwartet. An dem Projekt, an dem Deutschland sich beteiligt, sind derzeit circa 15 Mitgliedstaaten beteiligt. Ich glaube, dass wir in Deutschland bereits eine sehr gute, auskömmliche Basis an digitalen Identitäten gelegt haben und diese nun mit großer Energie und Kraft auch im nationalen und europäischen Kontext weiterentwickeln können, und darauf freue ich mich. Vielen Dank.

Die **Vorsitzende**: Ganz herzlichen Dank, Herr Dr. Nguyen. Als nächstes Prof. Praycek, Leiter des

Kompetenzzentrums Öffentliche IT am Fraunhofer FOKUS.

SV **Prof. Dr. Peter Parycek:** Vielen Dank für die Einladung. Der neue Personalausweis, wie er mal hieß, - so neu kann er nicht mehr sein, jetzt ist es doch schon zwölf Jahre im Feld. Der hat nach dem eGovernment MONITOR 2021 eine Verbreitung von circa neun Prozent in Deutschland. An dieser Stelle ein kurzer Disclaimer: Auch Fraunhofer FOKUS war an der Entwicklung mitbeteiligt, nicht in meiner Person, aber als Institution. Wenn man die Angaben über das Nutzungsverhalten vergleicht mit denen anderer führender Länder wie jener in Skandinavien, dann liegt Deutschland weit dahinter zurück. In Dänemark ist die Verbreitung, also die Nutzung über 90 Prozent innerhalb der Gesellschaft, und selbst in Österreich, das nicht zu den führenden Ländern in dem Bereich zählt, nutzen inzwischen über ein Drittel das Pendant und kommen auf eine Transaktionsmenge pro Monat von circa vier Millionen. Im Vergleich dazu wurden in Deutschland von Januar bis Mai absolut 1,8 Millionen Transaktionen durchgeführt. Es gibt also einen wesentlichen Abstand zu den führenden Ländern in Europa. Weil bisher sehr viel gelobt worden ist, muss man an der Stelle kurz aufzeigen, dass es noch Luft nach oben gibt, was die Nutzung insgesamt betrifft. Warum ist das so? Wenn wir die anderen Ökosysteme vergleichen, dann ist dort das entstanden, was jetzt angesprochen worden ist, nämlich der Aufbau eines florierenden Ökosystems mit einer hohen Verbreitung innerhalb der Gesellschaft und auch zahlreichen Anbietern von Internetservices, die das auch einbauen als Registrierung, als Login. Das ist leider nicht ganz so gelungen beim Personalausweis. Wie stark nutzt das die Wirtschaft? Es sind nach den öffentlich zugänglichen Angaben 175 Anwendungen. Das heißt, das Ökosystem ist schwach ausgeprägt. Warum ist das so? Das ist nicht hundertprozentig kausal nachweisbar. Aber es ist durchaus die angesprochene Benutzerfreundlichkeit. Da ist Luft nach oben. Das Kartenlesegerät in den ersten Jahren war nicht unbedingt ein treibender Faktor. Der aktuelle Prozess vor allem in der Kopplung zwischen PC, Laptop und Smartphone, den man gleichzeitig durchführen muss, ist auch nicht auf dem aktuellen Stand der typischen Internetprozesse in der Anwendung. Das dritte Element ist die SmartID, die wieder in die Richtung geht, eine Technologie zu forcieren, wie seinerzeit den Personalausweis, die noch nicht weit verbreitet ist innerhalb der Gesellschaft. Eine Plattform braucht immer zwei Seiten. Es braucht auch die Diensteanbieter und auf deren Seite gibt es die Hürde der Registrierung. Die kann man niedriger gestalten. Es gibt die technischen Hürden. Die sind in den letzten Jahren nachgebessert worden, aber waren in den ersten Jahren doch sehr hoch, und auch die finanzielle Planbarkeit ist zwar nachvollziehbar, jedoch nicht unproblematisch für Unternehmer ohne zu wissen, wie viele diesen Dienst zukünftig abfragen werden. Wir haben auf Seiten der Bürger und der Anbieter relativ hohe Hürden und eine relativ geringe Motivation, diese zu überwinden. Das ist das Kernproblem der mangelnden Nutzung. Wenn man jetzt nach vorne schaut, was wären die Maßnahmen? Höhere Benutzerfreundlichkeit bei den Bürgerinnen und Bürgern, Mobile First-Ansatz, das kann man auch kombinieren. Smartphones alleine? Ja, aber es gibt Prozesse, mit denen man es gut absichern kann. Bei den Secure Elements, die nutzen, die vorhanden sind - und sie sind breit vorhanden in den aktuellen Plattformen. Das angesprochene Smart eID: Wenn wir es durchrechnen bis zur weiten Verbreitung des Secure Elements, muss man mindestens mit zwei bis drei Jahren rechnen. Zusätzlich ist die große Frage, ob Apple dieses Element je einführen wird, und zusätzlich dauert es durchschnittlich drei Jahre, bis ich tatsächlich eine hohe Verbreitung in der Gesamtgesellschaft habe. Das heißt, hochgerechnet kommt man auf fünf bis sechs Jahre, bis man die breite Gesellschaft erreichen kann. Wenn man auf die Perspektive der Diensteanbieter schaut, dann wäre es dort eine teilautomatisierte Registrierung, die man vielleicht für einfache Logins durchführen könnte, die teilweise mit Pseudonymisierung arbeiten könnte. Als technische Standards kann man die Industriestandards verwenden, die vorhanden sind. OpenID Connect, OAuth, unterschiedliche Sammelkombinationen. Und von der politischen Perspektive eine Kostenübernahme für die freie Nutzung der Dienste für den öffentlichen Sektor, für Gesundheit und auch für die Wirtschaft. Das wäre ein Element, um das Zertifikat niedrigschwelliger zur Verfügung zu stellen. Wir haben wenig davon, wenn wir ein hochsicheres

Element haben, das nicht genutzt wird, weil wir am Ende damit eine unsichere Gesellschaft schaffen, die sich eben nicht elektronisch ausweisen kann. Insofern gilt es jetzt daran zu arbeiten, eine Balance zwischen technischer Sicherheit und Benutzerfreundlichkeit herzustellen. Aber durchaus auf Basis der vorhandenen Architektur, bei der man an der einen oder anderen Stelle drehen muss.

Die **Vorsitzende**: Vielen Dank für Ihr Statement. Nun hat das Wort Isabel Skierka, Program Leader am ESMT, sie ist uns virtuell zugeschaltet.

SVe **Isabel Skierka:** Vielen Dank, sehr geehrte Mitglieder des Ausschusses für Digitales, für die Gelegenheit, in dieser Anhörung heute meine Einschätzungen zum Thema digitale Identitäten einzubringen. Mein Name ist Isabell Skierka, ich bin Forscherin am Digital Society Institute der ESMT Berlin. Wir arbeiten dort an verschiedenen Projekten zu digitaler Sicherheit, aber eben auch unter anderem zu digitalen Identitäten. Aktuell ist unser Institut ebenfalls Teil der Begleitforschung des vom BMWK geförderten Schaufensters sichere digitale Identitäten. Ich spreche hier in meiner unabhängigen Forscherrolle. Wir alle wissen, welche Schlüsselrolle digitale Identitäten in Gesellschaft und Wirtschaft einnehmen. Wir werden viel über den Personalausweis sprechen und haben das auch schon getan. Wir haben mit dem Personalausweis und der eID eine der sichersten digitalen Identitätslösungen - sogar weltweit. Aber sie wird - wie bereits gesagt - sehr wenig genutzt und ist auch nur für sehr wenige Anwendungspartner verfügbar. Momentan sind wir in einem Umbruch. Wir sehen das auf EU-Ebene und an den Bedürfnissen der Nutzer/-innen. Viele wünschen sich Möglichkeiten, sich vertrauenswürdig, aber auch intuitiv und einfach nutzbar bei vielen Anwendungen zu authentifizieren und auch digitale Nachweise wie zum Beispiel Führerschein, Impfpass oder Bibliotheksausweis zu verwalten. Jetzt gilt es erst einmal, auf nationaler Ebene verschiedene Projekte der Bundesregierung zu bündeln. Dazu gehören der Personalausweis, die Smart eID, die Schaufensterprojekte, aber auch solche Lösungen wie Elster oder Gesundheitslösungen, die mit der Telematik-Infrastruktur zusammenhängen, und Bürgerkonten. Da passiert zurzeit auch schon sehr viel. Ich möchte noch drei Punkte ansprechen. Zum einen sollte Deutschland ganz klar über den eigenen Tellerrand hinausblicken. Dazu gehört nicht nur der eIDAS-Gesetzgebungsprozess, sondern auch eine Auseinandersetzung mit den Global Playern, also großen Technologieplattformen, die eine marktbeherrschende Stellung bei Mobilgeräten und Betriebssystemen haben und die mit ihren sehr schnell voranschreitenden Angeboten für digitale Identitäten auch eine Vielzahl von Nutzer/-innen erreichen werden. Diese globalen Plattformen sind jetzt auch dabei, in ihre Wallets zum Beispiel hoheitliche Identitäten zu integrieren. Es beginnt mit dem Führerschein in den USA und anderen Dokumenten, die man zum Reisen vorweisen kann. Das heißt also, die EU und deutsche Lösungen stehen im Wettbewerb, sind aber auch auf eine Kooperation mit diesen Herstellern angewiesen. Eine Voraussetzung für einen Erfolg in diesem Kontext ist, dass die Lösungen aus Europa und Deutschland erst einmal wettbewerbsfähig sind. Das gilt insbesondere für die Nutzerfreundlichkeit und Anwendungsbreite – natürlich auf den Datenschutz- und IT-Sicherheitsgrundlagen. Außerdem muss die Nutzung entscheidender technischer Komponenten auch möglich sein. Da gibt es über die sich im Entwurfsstadium befindliche eIDAS-Verordnung und einen Verweis auf den Digital Markets Act auch entsprechende Möglichkeiten, eine Kooperation zu erzwingen. Den Personalausweis betreffend, sehe ich insgesamt sehr stark das Anwendungsdefizit. Es ist sehr schwierig, den Personalausweis bei vielen Anwendungen einzusetzen. Die Diensteanbieter selbst müssen mit finanziellen und zeitlichen Hürden kämpfen, um den Personalausweis bei sich einzubinden oder einen Service Provider beauftragen. Das heißt, es gibt sehr klare Marktbarrieren und es gibt auch eine sehr starke Fragmentierung des regulatorischen Rahmenwerks für digitale Identitäten. Zuletzt möchte ich dafür werben, dass man auch auf Grundlage der eID-Infrastruktur und darüber hinaus durchaus den Rahmen setzen kann, auch als Staat ein Ökosystem für digitale Identitäten und Vertrauensdienste zu fördern. Dazu gehören Grundlagen für transparente Sicherheitslevel und verschiedene technologische Lösungen. Ich plädiere dafür, dass die Prozesse sowohl auf gesetzgeberischer Ebene als auch auf technischer

Standardisierungsebene sehr viel transparenter gestaltet sein sollten und auch Experten aus Zivilgesellschaft und Wissenschaft besser eingebunden sein sollten. Das gilt auch für die EU-Ebene und den Toolbox-Prozess in diesem Bereich. Vielen Dank.

Die **Vorsitzende**: Vielen Dank. Jetzt kommen wir zur Sachverständigen Rebekka Weiß vom Bitkom e.V. Sie ist im Saal.

SVe **Rebekka Weiß**: Herzlichen Dank, sehr geehrte Frau Vorsitzende, sehr geehrte Abgeordnete, werte Damen und Herren, Kolleginnen und Kollegen. Ich möchte mich im Namen unserer 2.000 Mitglieder für die Einladung bedanken, nicht nur in meiner Person als Sachverständige, sondern auch dafür, dass diese Anhörung heute in dieser Form zu diesem großen Thema überhaupt stattfindet. Denn digitale Identitäten sind für uns im Bitkom definitiv ein zentrales Thema. Ein erfolgreiches Identitätenökosystem, sei es mittels ID-Wallets, Perso auf dem Smartphone oder auch einer zukünftigen Technologie, ist der notwendige und nächste große Schritt für die Gesamtdigitalisierung unseres Landes. Die Bedeutung des Themas kommt hier und heute durch die Anhörung zum Tragen und bringt endlich alle Initiativen, Expertenmeinungen und Anwenderdimensionen zusammen. Denn genau das ist es, was im vergangenen Jahrzehnt gefehlt hat. Bei allen notwendigen Detaildiskussionen rund um zu wählende Technologie, Sicherheitsanforderungen, Standards, die es schon gibt oder die noch zu entwickeln sind: Der holistische Ansatz ist genau das, was wir brauchen. Wir haben uns im vergangenen Jahrzehnt tatsächlich verfranzt und auch aufgerieben in zu vielen nicht koordinierten Einzelprojekten und haben angesichts der unüberschaubaren Zuständigkeiten zu schnell auch zu viele neue Initiativen und Projekte gesehen, ohne dass es je eine kohärente eID-Strategie – national oder auf EU-Ebene – gab. Genau die muss jetzt schnellstmöglich entwickelt werden. Und zwar nicht auf einem leeren Blatt Papier, sondern entlang der bisherigen Projekte, der bisherigen Anwendungsfälle im Markt und natürlich auf Basis der bereits geleisteten Arbeit. Denn die bisherige Arbeit hat sehr viel Gutes gezeigt. Die eID selber, insbesondere aus dem Personalausweis, ist nichts Neues. Gerade der Personalausweis und die daraus ableitbare eID sind in Deutschland seit über einem Jahrzehnt bereits vorhanden, eIDAS-notifiziert und damit als Lösung für die digitale Identität bereits im Markt. Die noch nicht vollständige Marktdurchdringung und die nicht flächendeckende Verwendung durch Bürgerinnen und Bürger haben jedoch dazu geführt, dass Deutschland mittlerweile von den anderen EU-Mitgliedstaaten, obwohl wir eigentlich die beste Technologie haben, überholt wurde. Es liegt zum Teil an dem mangelhaften Rollout-Prozess. Wer damals den nPA beantragt hat, wird sich vielleicht noch an die Ausführungen in den jeweiligen Bürgerämtern erinnern, wo teilweise sogar davon abgeraten wurde, die Funktionen zu aktivieren. Das hatte auch etwas mit mangelndem Marketing zu tun, aber in jedem Fall wirkt genau das bis heute nach. Das als Henne-Ei bekannt gewordene Phänomen kann daher weder durch eine einzelne gesetzgeberische Handlung, wie es jetzt mit dem Smart eID-Gesetz bezweckt ist, noch mit der zukünftigen Wallet allein gelöst werden. Denn die größte Hürde besteht nach wie vor in dem Fehlen eines holistischen Ansatzes, der alle verschiedenen Ebenen zusammenführt und in ein kohärentes Gesamtwerk gießt. So gut der Personalausweis ist, er ist kein Führerschein, keine Gesundheitskarte, ist keine Kundenkarte, kein Bibliotheksausweis. Wir müssen all diese Ebenen zusammenbringen. Gerade dort liegt sicherlich auch das große Potenzial der zukünftigen Wallet, was aber nicht heißt, dass wir die gute Basis, die wir hier in Deutschland haben mit der eID aus dem Personalausweis, nicht ganz dringend ausbauen müssten. Positiv ist zu bewerten, und das sehen wir im Bitkom verstärkt in den vergangenen zwei, drei Jahren, dass das Bedürfnis nach digitaler Identität vor allem auch in der Bevölkerung angekommen ist. Wir sehen, dass immerhin sechs von zehn Deutschen mittlerweile gerne eine digitale Identität hätten. Sie kann nur noch nicht ausgerollt werden und das ist genau die große Aufgabe in dieser Legislatur, dieses Bundestages und definitiv auch die Leitlinie für die Arbeit der Ressorts. Denn die Mehrheit der Deutschen sagt ganz klar, sie würde gerne aufs Portmonee verzichten, sie würde gerne ihre digitalen Identitäten über das Smartphone, über andere Wege ausschöpfen, sie möchte ihre

Karten zu Hause lassen und so besser an der Digitalisierung partizipieren. Andere Länder sind deutlich weiter als wir. Gerade die Beispiele aus Dänemark zeigen, dass es durchaus geht. Ein guter und richtiger Schritt ist daher das angedachte ressortübergreifende Laborformat, weil auch dort die Initiativen zusammengebracht werden. Wir seitens der Wirtschaft erhoffen uns, dass die Expertise, die jahrzehntelang existierenden Anwendungsfälle, die wir in der Praxis durchgespielt haben, eingebunden werden und aus den bisherigen Projekten das Beste behalten wird, um den Bürger/-innen schneller als in fünf oder zehn Jahren mit der digitalen Identität zu dienen. Wir stehen dafür selbstverständlich wie immer sehr gerne auch als Experten bereit. Vielen Dank.

Die **Vorsitzende**: Ganz herzlichen Dank. Wir beginnen nun die Frage-Antwort-Runde. Es ist gut geübte Praxis, dass die Abgeordneten sehr präzise fragen und sagen, an wen sich die Frage richtet. Bitte dann direkt antworten. Zunächst für die Fraktion der SPD der Abgeordnete Robin Mesarosch.

Abg. **Robin Mesarosch** (SPD): Vielen Dank an alle Sachverständigen für die Beantwortung der Fragen. Herr Prof. Margraf, wie können wir zu mehr Anwendungsfällen bei der eID kommen? Das ist ja ein ganz grundsätzliches Problem und inwiefern kann das OZG ein Hebel sein? Was müssen wir tun, damit es ein möglichst guter Hebel dafür ist, mehr Anwendungsfälle zu schaffen?

SV **Prof. Dr. Marian Margraf**: Jede Bürgerin und jeder Bürger hat durchschnittlich 1,6 Behördenkontakte im Jahr. Davon ist einer die Steuererklärung. Dafür gibt es eine ausreichend sichere Lösung, bleiben also 0,6 übrig. Man kann sich fragen, ob attraktivere staatliche Dienste zu mehr Verwendung der Online-Ausweisfunktion führen. Wenn ich heute beispielsweise einen Bauantrag stelle, bekomme ich nach ein paar Monaten vielleicht eine Antwort. Bürgerinnen und Bürger sind es heute aber gewöhnt, bei anderen Prozessen wie Online-Einkauf sofort zu sehen, wie der Stand der Bestellung ist und wann das Paket ankommt. Das heißt, wenn man versucht, Verwaltungsdienstleistungen zu digitalisieren, darf man nicht die heutige Praxis abbilden, sondern man muss die Digitalisierung als Schnittstelle zur Kommunikation mit der Behörde sehen und gleichzeitig die behördeninternen Vorgänge digitalisieren, sodass ich zum Beispiel regelmäßig schauen kann, wie der Stand meines Bauantrages ist. Mir ist klar, dass das nicht einfach ist.

Abg. **Robin Mesarosch** (SPD): Vielen Dank. Frau Skierka, Sie haben über Benutzerfreundlichkeit gesprochen. Dazu gehört im weiteren Sinne auch, dass Lösungen für digitale Identitäten jedem zugänglich sind. Wenn es um Secure Elements geht, finden wir die vor allem auf teuren Smartphones. Das heißt, es wäre Leuten nicht zugänglich, die kein solches Smartphone haben. Wie sehen Sie das, sollten wir überhaupt auf Secure Elements setzen? Ist das ein Problem, wenn ein Teil der Bevölkerung diverse Geräte nicht hat und welche Alternativen gäbe es?

SVe **Isabel Skierka**: Vielen Dank. Natürlich ist es ein Problem, wenn wir eine Lösung implementieren, die nicht für alle zugänglich ist. Sie hatten auch die NFC-Schnittstelle erwähnt, auch in der schriftlichen Frage, und über eine solche verfügen sehr viele Smartphones. Das heißt, die Nutzung der eID über diese Schnittstelle ist möglich. Das Secure Element benötigen wir, um eine digitale Identitätslösung mobil auf hochsicherem Niveau, also eIDAS-hoch, zu verankern und um ein äquivalentes Sicherheitsniveau wie das einer Smartcard auch mobil gewährleisten zu können. Nun ist es aber auch so, dass wir nur wenige Smartphone-Modelle haben, die momentan über ein solches Secure Element verfügen. Das heißt, in den nächsten Jahren gibt es einen Anreiz, dass sich das Secure Element weiter verbreitet. Aber das wäre eher mittel- bis langfristig eine Option, dass wir wirklich in die Breite kommen damit. Gleichzeitig stehen diese sicheren Elemente unter der Kontrolle der Hersteller von Hardware und Betriebssystemen. Das heißt, hier müsste man durchaus auch mit den Herstellern kooperieren und regulatorisch bis zu einem gewissen Grad eine Kooperation erzwingen. Über die eIDAS-Verordnung mit Verweis auf den Artikel 6 im DMA. Es wäre aber auch eine Möglichkeit, alternative Hardware-Anker zu verwenden. Es gibt auch noch andere Sachverständige, die dazu bestimmt Vorschläge haben. Die andere angesprochene Möglichkeit ist, dass man eine

Software-Lösung nutzt, auch für die Smart eID. Ich selbst kann zu dieser Lösung nicht viel sagen, was die Smart eID angeht. Es gibt allerdings Software-Varianten in anderen Ländern zum Beispiel die Smart ID in Estland, Lettland und Litauen. Allerdings erfüllen diese Varianten eben nicht das eIDAS-Sicherheitsniveau „hoch“, sondern wenn, dann eher substanziell. Das heißt zusammenfassend: Ja, das ist keine sehr gute Lösung aktuell. Ich denke, wir müssen an diesem Strang Secure Element weiterarbeiten. Und gleichzeitig über Software-Varianten nachdenken, die aber dann auf jeden Fall nicht für wirklich hochsensible Anwendungsfälle verwendet werden dürften und parallel dazu auch noch nach alternativen Hardware-Ankern suchen, die man verwenden kann.

Die **Vorsitzende**: Nun für die Fraktion der CDU/CSU der Abgeordnete
Dr. Markus Reichel.

Abg. **Dr. Markus Reichel** (CDU/CSU): Für die Möglichkeit, heute Fragen zu stellen, möchte ich mich herzlich bedanken. Frau Weiß, ist SSI ohne Blockchain realisierbar? Ist es aus Ihrer Sicht wichtig, dass man sich technologisch in irgendeiner Form festlegt oder ist Technologieoffenheit gefragt?

SVe **Rebekka Weiß**: Vielen Dank. Die Frage nach der Technologiewahl wird sicherlich ganz entscheidend sein, auch um die digitalen Identitäten in die Breite zu bekommen. In der Tat heißt SSI nicht automatisch Blockchain. In den konkreten Anwendungsfällen, die wir bisher gesehen haben, die zum Teil auch erprobt werden, auch viel besprochen wurden in den vergangenen zwei Jahren, sind es häufig DLT-Anwendungen, die zum Tragen kommen. Dort sind noch nicht alle Standards geschrieben, die wahrscheinlich notwendig sind, um solche Systeme zu Ende zu bauen. Auch darüber wurde eine ganze Menge bereits publiziert. Es ist in der Tat so, dass auch wir von der Anwenderperspektive hier sehen, dass noch einige Schritte zu tun sind, bis man wirklich sagen kann, SSI ist definitiv die Technologie, die wir zwingend brauchen, um digitale Identitäten entweder in der Wallet oder in anderen Anwendungsszenarien in die Breite zu bekommen. Es gibt Alternativen und daher ist eine Festlegung in dieser Phase nicht zwingend. Und die Erfahrungen der bisherigen Digitalregulierung als Ganzes zeigen eigentlich, dass Technologieneutralität und -offenheit wahrscheinlich das Wichtigere ist. Was aber nicht heißt, und das muss ganz klar gesagt werden, dass wir diese Technologien nicht weiter erproben sollten. Die bisherigen Projekte zeigen durchaus, dass es Anwendungsfelder gibt, die funktionieren. Vielleicht sind es nicht immer die Anwendungsfelder, wo wir später den Personalausweis reinlegen. Es gibt verschiedene Ebenen zu dieser Thematik. Es ist hochkomplex. Ich denke, das merken wir immer wieder. Die Anwendungsszenarien sind komplex. Wallet-ID und staatliche Identität ist nicht gleich einer kleinen Wallet-SSI-Anbindung oder Anwendung für ein anderes Szenario. Diese Möglichkeiten sollten exploriert werden, einfach auch um die Technologie zu erforschen. Ob sie dann am Ende in der Wallet zum Einsatz kommt, steht auf einem anderen Blatt.

Abg. **Dr. Markus Reichel** (CDU/CSU): Vielen Dank. Es gibt im Rahmen von eIDAS die Diskussion, ob jetzt die Wallet ein Container sein soll oder ob sie letztlich eine eID in sich sein sollte. Es gibt die These, wenn sie nur ein Container ist, haben wir keinen Fortschritt gegenüber dem Status quo. Stimmen Sie dieser These zu?

SVe **Rebekka Weiß**: Es kommt drauf an. Beides ist möglich. Das kann man ganz klar sagen. Nach meiner Einschätzung hat sich die EU in ihren Vorhaben richtigerweise noch nicht festgelegt. Wenn wir immer wieder schauen, dass wir jegliche Wallet und digitale Identität für den Nutzer bauen, kann es Sinn ergeben, eine Wallet als Container zu entwickeln. Allein aus dieser Nutzerperspektive gedacht. Das ist das, was die Nutzer häufig schon kennen, nämlich aus den Wallets, die sie bisher benutzen, aus den Wallets die wir in unseren Smartphones haben, wo wir unsere Bordkarten reinlegen oder auch andere Dinge. Das ist ein bekannter Vorgang. Was wir auch häufig feststellen, generell in der Digitalisierung aber gerade wenn es um digitale Identitäten geht, ist, dass Vertrauen ein ganz wichtiger Bestandteil des Ökosystems ist. Vertrauen bildet sich häufig entweder, weil ich einem Anbieter vertraue oder eben auch, weil ich Vorgänge oder Maßnahmen, Authentifizierungswege, wiedererkenne, die ich

aus anderen Kontexten kenne. Deswegen kann die Containerlösung durchaus Sinn ergeben. Das heißt aber nicht, dass ein anderweitiges Aufsetzen der Wallet per se falsch wäre. Dann müsste aber im Zweifel ein bisschen mehr Überzeugungsarbeit und auch wieder Marketing betrieben werden, um die Mehrwerte, die daraus entstehen, nämlich die Wallet selber, zu einem Identifikator zu entwickeln und an den Bürger heranzutragen.

Abg. **Dr. Markus Reichel** (CDU/CSU): Sie sprechen sich für mehrere Wallets aus, was ist der Grund dafür?

SVe **Rebekka Weiß**: Einerseits die Überzeugung, dass Wettbewerb beflügelt und Innovation fördert. Also dort, wo es verschiedene Lösungsansätze gibt, kann etwas Besseres entstehen, als wenn es monopolartige Technologien gibt. Ein anderer Faktor ist sicherlich auch der, dass wir seitens der Wirtschaft ein Stück weit überzeugt davon sind, dass wir ganz gut darin sind, UX zu entwickeln, anders als teilweise bei staatlichen Lösungen. Auch das kann dann den Wettbewerb untereinander beflügeln. Man lernt ja voneinander. Ein dritter und ganz wichtiger Punkt ist, die eine Wallet kann und muss es nicht geben. Es kann Wallets geben, die ganz besondere Mehrwertdienste haben für eine ganz besondere Branche. Nehmen Sie einen hochregulierten Bereich wie die Gesundheitswirtschaft. Dann habe ich bestimmte Punkte, die ich nur in dieser Wallet fixieren kann, und eine andere Wallet, mit der ich meinen Personalausweis ansteuere.

Die **Vorsitzende**: Nun für die Fraktion Bündnis 90/Die Grünen die Abgeordnete Misbah Khan.

Abg. **Misbah Khan** (Bündnis 90/Die Grünen): Vielen Dank, ich habe eine Frage an Herrn Kahlo. Wir haben vom Potenzial der eID im nPA an unterschiedlichen Stellen gehört und auch Sie sagen, das Problem sei die Umsetzung. Mich interessiert, welche konkreten Instrumente der Bund jetzt priorisieren sollte, abseits von einer konsequenten Bereitstellung in der Verwaltung. Wo sehen Sie es als möglich und nötig an, mit externen Stakeholdern etwa aus der Gesellschaft zusammenzuarbeiten?

SV **Christian Kahlo**: Zum Thema Umsetzung, was sollten wir zuerst tun: Es ist sicherlich ganz wichtig zu kommunizieren, dass der Ausweis eine Lösung ist, die tatsächlich funktioniert. Die ist da, die können wir einsetzen. Was ich bereits in der Stellungnahme geäußert habe, ist die Anregung, auf die Zivilgesellschaft zuzugehen, sprich auf den CCC, auf das Universum, was da herum ist, um dort zum Beispiel auch im Bereich Apps und Wallet-Entwicklung Prototypen zu bauen. Also ein Hackathon-Format zum Beispiel, ganz einfach das Wissen, was jetzt bei uns in dieser Expertenrunde existiert, einfach mal in die Breite zu tragen. Wie binde ich den Ausweis an, wie funktioniert das im Detail? Welches Bit wird wie gesetzt? Dann kann man daraus eine UX entwickeln, die von den Leuten selber kommt, die nicht aus Gesetztestexten abgeleitet wird und dann ein Formular ist, was in irgendeine App gegossen wird. Und dann sitzt der Nutzer davor und weiß nicht, was er machen soll. Das heißt also, hier können wir tatsächlich Einiges tun. Das geht sogar relativ schnell, kostet uns wenig Geld und sorgt dafür, dass wir die Leute einbinden. Daraus können wir bessere Strategien ableiten. Das ist das, was wir zuerst machen sollten, denn genau diese Experimentierklausel, die wurde sehr reichlich in den Bereichen Blockchain und SSI angewendet. Aber die Ausweis-Technologie, die wir die ganze Zeit haben, gar nicht. Ich denke, das können wir sehr einfach ändern.

Abg. **Misbah Khan** (Bündnis 90/Die Grünen): Vielen Dank. Es geht nun um Large Scale Projects. In der Öffentlichkeitsarbeit der EU und auch in den Regierungen der Mitgliedstaaten ist das eine wichtige Komponente, gerade auch in der Weiterentwicklung der europäischen Identität. Sie kritisieren die Sinnhaftigkeit des Ansatzes im Ganzen, aber auch die konkrete Umsetzung im Speziellen. Welche Rolle sollte Deutschland nun bei der konkreten Umsetzung spielen und wie können externe Akteure besser eingebunden werden?

SV **Christian Kahlo**: Der Punkt bei den Large Scale Projects ist, dass versucht wird von den einzelnen größeren Treibern innerhalb der Europäischen Union, diese Projekte an das eigene System möglichst nah heranzuführen. Interessanter ist bei der ganzen Lösung allerdings, wie ich es hinbekomme, generell über die gesamte Europäische Union, die Anrainerstaaten und andere eine Lösung zu haben, mit der ich ein ID-System aufbauen kann, wo es am Ende des Tages

eigentlich egal sein sollte, welches Land mit welcher Wallet oder mit welcher ID-Lösung kommt. Ob das jetzt ein deutscher Ausweis ist oder ob das eine Signaturkarte in Estland ist oder eine SSI-Wallet aus Frankreich, das sollte keine Rolle spielen dürfen. Dafür gibt es tatsächlich Lösungen. Wir haben im Umfeld der SPRIND auch ein Projekt, was das versucht zu adressieren, nämlich genau zuzuordnen: Ich habe eine Mail-Adresse, ein ganz einfaches Datum @bundestag.de. Dann muss ich in der Lage sein festzustellen: Da kommt jemand vom Bundestag. Ich möchte mich jetzt also mit einem Bundesdienstausweis zum Beispiel anmelden. Oder ich komme als Privatbürger von ausweisident.de, ein Dienst von der Bundesdruckerei. Dann wird dieser Dienst verwendet, um mich zu identifizieren. Wichtig ist aber, dass wir am Ende bei einer Antwort herauskommen, die alle gleichermaßen verstehen. Das heißt, dass wir uns auf ein Minimum Data Set verständigen, was es auch schon gibt, aber noch bei allen ankommen muss. Denn in den anderen EU-Staaten ist das noch nicht ganz präsent, dass es ganz andere Anforderungen gibt oder kulturell eine andere Einstellung zum Datenschutz. Gerade in den Ländern, die Sie angesprochen haben, also Estland, Dänemark etc. sieht man das ein wenig differenzierter. Dort hat man kein Problem mit offenen Datenbanken. Das ist das, wo wir hinmüssen, ein globaler Ansatz. Wir müssen in der Lage sein, quer durch alle Länder sagen zu können: Das ist das ID-System, mit dem du dich identifizieren möchtest, und dort kommt eine Antwort heraus. Diese wird überall verstanden, und das Vertrauensniveau ebenso. Dann kann ich damit überall arbeiten, kann Cross Border-Dienste sowohl von der Verwaltung als auch im privatwirtschaftlichen Sektor nutzen.

Abg. **Misbah Khan** (Bündnis 90/Die Grünen): Sie beschreiben in Ihrer Stellungnahme das Potenzial verschiedener Identitätsträger: Sim-Karten, Wearables etc. Können Sie ausführen, was die Potenziale für so ein Ökosystem staatlicher Identitäten sind, wie Sie die sehen? Gerade auch in der Frage der Architektur?

SV **Christian Kahlo**: In welchem Kontext? Ganz kurz vielleicht eine Präzisierung. Architektur für das Ökosystem im Kontext Wearables als Alternative?

Abg. **Misbah Khan** (Bündnis 90/Die Grünen): Ich formuliere die Frage noch mal: Sie beschreiben das Potenzial eines Ökosystems in Ihrer Stellungnahme und ich wüsste gerne einfach, ob Sie das noch mal deutlicher ausführen können. Welches Potenzial besteht durch dieses Ökosystem?

SV **Christian Kahlo**: Ich glaube, ich habe verstanden, um was es geht. Momentan ist es so, dass wir einfach einen Fokus haben auf zwei große Technologien. Das eine ist der Ausweis, das andere ist, was mit SSI und Blockchain gemacht worden ist. Wir haben wesentlich mehr Möglichkeiten. Ein Weg ist natürlich, einfach von der Ausweiskarte wegzukommen in Richtung des Identitätsträgers. Die Ausweiskarte ist ein Identitätsträger. Das hier ist auch ein Identitätsträger. Das ist mein Ring, mit dem ich vorhin Kaffee gekauft habe. Da ist aber auch eine Spielzeug-eID drauf. Das kann auch jeder andere Bürger haben. Das heißt, man muss nicht unbedingt auf das vorhandene oder nicht vorhandene Secure Element im Smartphone festgelegt sein, sondern man kann diese sicheren Chips in vielen, vielen anderen Formfaktoren haben. Man kann auch auf SIM-Karten ausweichen, hat auch Estland vorgemacht. Das sind Dinge, wo wir wesentlich breiter denken können, auch nachhaltiger, und für sozial Schwächere eine Teilhabe erzeugen. Eine SIM-Karte kann ich schnell mal tauschen. Die kann ich langlebig weiterverwenden, da muss ich nicht ständig ein neues Smartphone kaufen. Das heißt hier würde sich anbieten, mehr Offenheit in der Denkweise an den Tag zu legen. Da haben wir viele Möglichkeiten.

Die **Vorsitzende**: Dankeschön. Für die Fraktion der FDP der Abgeordnete Dr. Volker Redder.

Abg. **Dr. Volker Redder** (FDP): Vielen Dank, dass Sie als Experten hier sind. Das freut mich sehr. Ich habe eine Frage an Herrn Nguyen. Ich habe nicht nur eine Frage, ich habe mehr, aber eine an Sie. Die öffentliche Hand ist der größte Auftraggeber in Deutschland, was IT-Projekte angeht. Beim OZG sehen wir, wie schwierig das ist, die öffentliche Hand zu digitalisieren. Wir reden hier von informationeller Selbstbestimmung, was die Bürger und Bürgerinnen angeht. Aber die Wirtschaft braucht ja auch diese digitalen Signaturen und

elektronischen IDs und so weiter, seit zwölf Jahren. Wir haben natürlich Plattformen, wo man Ausschreibungen machen kann. Was meinen Sie denn, woran es liegt, dass wir nicht richtig vorangekommen sind?

SV **Dr. Kim Nguyen**: Vielen Dank für die vielschichtige Frage. Ich glaube, einer der Aspekte ist, dass wir digitale Identitäten und die damit verbundenen Dienste als eine Infrastruktur begreifen müssen. Und die Infrastruktur muss natürlich gestellt werden. Und ich glaube, dass das einer der Aspekte ist, der die Anwenderfreundlichkeit erhöht. Wenn der einzelne Bürger im Bedarfsfall immer erst wieder in komplizierte einzelne individuelle Beschaffungsprozesse geht, dann ist es tatsächlich schwierig. Deswegen glaube ich persönlich, dass der Staat mit dem eID-System eine Identität geschaffen hat, die jetzt zur Verfügung steht, und man jetzt größer denken muss. Es hat sich durch die einzelnen Antworten der Experten gezogen: das magische Wort Ökosystem. Das heißt nicht nur, dass man über eine spezifische Technologie nachdenkt, man muss ein gesamtes System denken, das Ende zu Ende für den Bürger verfügbar ist und im besten Fall mobil und mit hoher Anwenderfreundlichkeit. Ich glaube, das wäre ein ganz wesentlicher Faktor, um eine höhere Akzeptanz und Durchsetzung zu erzeugen.

Abg. **Dr. Volker Redder** (FDP): Vielen Dank. Eine Frage an Frau Skierka. Sie sprachen vorhin von den regulatorischen Rahmenbedingungen, die vielleicht zu aufwendig sind, vielleicht überregulierend sind. Das interpretiere ich jetzt rein. Ich habe Erfahrungen gemacht mit Anwendungen im Privatbereich, zum Beispiel ein Clubbetreiber, der checken wollte, ob die Leute, die kommen, über 18 sind, denn nur über 18-jährige durften rein. Seine Idee war, den Personalausweis auslesen, was ihm von der Landesdatenschutzbeauftragten untersagt wurde. Also eine typisch gute Anwendung eigentlich. Woran liegt es, dass solche Anwendungen nicht in den Markt kommen?

SVe **Isabel Skierka:** Also zunächst einmal: Was ich mit dem fragmentierten regulatorischen Rahmenwerk meinte, ist, dass es je nach Sektor wirklich ganz unterschiedliche regulatorische Anforderungen gibt. Und da können wir jetzt in den Finanzsektor gehen oder in den Gesundheitssektor, in den Telekommunikationssektor oder zu Vertrauensdiensten. In all diesen unterschiedlichen Sektoren gelten verschiedene Regelungen, was die Erhebung und die Wiederverwendung von Identitätsdaten und Nachweisen angeht, oder Verfahren für die Identifizierung und entsprechende Aufsichtsbehörden. Und das macht es natürlich extrem schwierig für Identitätsanbieter oder auch Lösungen von Vertrauensdiensten wie der qualifizierten elektronischen Signatur, hier einheitliche Lösungen zu schaffen. Das macht es auch sehr schwierig, dann wiederum, Identitätslösungen einheitlich nutzbar zu machen für Anwender. Das würde ich jetzt erst mal so stehenlassen, noch mit dem Hinweis, der gerade noch mal kam, dass man durchaus auch die Möglichkeit hat, Reallabore auf Grundlage von Experimentierklauseln einzurichten. Dass man zeitlich und räumlich begrenzte rechtliche Räume oder Experimentierklauseln einrichtet, mit denen man zum Beispiel in Bereichen, wo aktuell noch das Schriftformerfordernis oder die persönliche Vorstellung gilt, zum Beispiel im Bereich Standesamt, dass man solche Prozesse dann auch digitalisieren kann, und hier auch erst mal, wenn man noch nicht ganz sicher ist, ausprobieren kann, wie das mit verschiedenen Technologien funktionieren könnte. Und das ist auch ein ganz wichtiger Weg vorwärts.

Abg. **Dr. Volker Redder** (FDP): Danke. Herr Parycek, dann frage ich Sie. Mein persönlicher Eindruck ist, ich bin lange genug dabei glaube ich, dass sozusagen die Usability und die User Experience einfach mangelhaft sind. Und vor allem das fehlende Angebot. Das haben wir jetzt aber schon hundertmal gehört. Wie können wir das denn beschleunigen? Wir haben wirklich so viele Möglichkeiten. Sie wissen selber, dass wir im OZG von 575 Fachverfahren reden. Wir wollen als Booster über 500 killen, damit überhaupt irgendetwas fertig wird. Das kann nicht die Lösung sein. Haben Sie eine Idee, wie wir das beschleunigen können, wie wir einen Datenmodell-Standard, eine Datenstandardisierung machen können, eine verbesserte Interoperabilität zwischen den eIDs und dem Rest? Denn das eID ist die Grundlage von allem. Kurze Antwort bitte.

SV **Prof. Dr. Peter Parycek:** Es liegen Konzepte auf dem Tisch, jetzt muss man in die Umsetzung gehen. Zum einen mit dem Personalausweis, mit der NCF-Schnittstelle hat man den zweiten Faktor und kann damit auch softwarebasiert Lösungen bauen. Die brauchen nicht viel Kommunikation, denn wenn es gut und leicht funktioniert, dann wird es weitergegeben. Ich glaube, es ist der entscheidende Moment, Entscheidungen zu treffen, die zu Services führen, die wir aus dem Rest der Internetdienste kennen. Und es ist wahrscheinlich jetzt auch notwendig, weil bei den OZG-Dienstleistungen heißt es noch lange nicht, dass die Länder auch den neuen Personalausweis einsetzen. Ich glaube es ist ein sehr kritischer Zeitpunkt, dass man jetzt dieses kleine Fenster, das man noch hat, effektiv nutzt. Smart-ID ist etwas für die Zukunft, die nächsten sechs Jahre. Wallet ist für die Zukunft, die nächsten sechs Jahre. Deshalb habe ich mich in meiner Stellungnahme darauf fokussiert, dass man dieses kleine Zeitfenster jetzt nutzt und ein paar Zöpfe abschneidet in der aktuellen Architektur und dann innerhalb von einem halben Jahr auch etwas haben kann, was man schnell in die Breite bringt.

Die **Vorsitzende**: Für die Fraktion der AfD die Abgeordnete Barbara Lenk.

Abg. **Barbara Lenk** (AfD): Vielen Dank an die Sachverständigen für die Expertise. Ich habe eine Frage an Herrn Prof. Margraf. Sie hatten in Ihrem Statement schon das Thema Bürgerbeteiligung angesprochen. Wie stellen Sie sich das Vorhaben konkret vor und könnte da Open Source eine wichtige Rolle spielen?

SV **Prof. Dr. Marian Margraf**: Die erste Vorstellung, die ich da habe: Natürlich sollte man, wenn der Staat eine Lösung entwickelt, daraus von Anfang an ein Open Source-Projekt machen. Also nicht erst, wenn die Software fertig ist, diese als Open Source-Software bereitstellen, sondern tatsächlich von Anfang an ein Open Source-Projekt machen. Das heißt für mich, zu Beginn schon mit der Community diskutieren, die Sicherheitskonzepte, die Datenschutzkonzepte, Architekturkonzepte, alles, was dazugehört, daraus ein Projekt machen. Eingaben - Eingaben nennt man das vielleicht nicht -, aber Verbesserungsvorschläge aus der Community aufnehmen, bewerten, auch zurückspielen, was mit diesem Verbesserungsvorschläge gemacht wurde. Das ist wichtig, nicht nur als schwarzes Loch, sondern das auch zurück zu spielen.

Abg. **Barbara Lenk** (AfD): Vielen Dank. Zur Thematik Open Source auch noch mal die Frage an Flüpke. Wie ist das aus Ihrer Sicht einzuschätzen und zu bewerten?

SV **Flüpke:** Ja, also, da stimme ich meinem Vorredner schon zu, dass solche Lösung wünschenswert sind. Und die können auch dazu beitragen, dass sich Verfahren etablieren. Also für Anwendende ist es natürlich einfacher, wenn die Referenzimplementierung unter einer freien Lizenz vorliegt, diese Verfahren entsprechend dann zu implementieren. Das könnte man beim neuen Personalausweis machen.

Abg. **Barbara Lenk** (AfD): Vielen Dank. Und noch eine Frage an Herrn Prof. Kelber. Es gab schon den Punkt „Vertrauen in die digitale Identität“. Gibt es in Ihrem Haus schon Maßnahmen, wie dies konkret verbessert werden könnte?

SV **Prof. Ulrich Kelber** (BfDI): Sehr geehrte Frau Abgeordnete, es geht natürlich darum, von vornherein die Fragen der Datensicherheit und des Datenschutzes in den Projekten so zu verankern, dass eine hohe Vertrauensquote sowohl bei staatlichen als auch bei privatwirtschaftlichen Identifizierungen stattfinden kann. Das sollte von vornherein Bestandteil jeglicher Projekte sein. Es sollte Bestandteil der regulatorischen Regelungen sein. Deswegen empfehlen wir, keine Scheuklappen-Digitalisierung zu betreiben. Nach dem Motto: Da ist mein Ziel, da will ich jetzt auf kurzmöglichem Weg hin. Sondern das Ziel fest im Auge zu behalten. Aber den Weg dorthin grundrechtsfreundlich auszugestalten, um damit das Vertrauen zu erhöhen.

Abg. **Barbara Lenk** (AfD): Vielen Dank. Und noch eine Frage an Frau Weiß. Sie hatten schon angesprochen, dass gerade in der Bevölkerung ein großer Wunsch nach digitaler Identität oder nach der Nutzung von Services vorhanden ist. Sind aus Ihrer Sicht ein besseres Marketing oder bessere Möglichkeiten sinnvoll, um eine Marktdurchdringung zu erreichen?

SVe **Rebekka Weiß**: Vielen Dank für die Frage. Es ist in der Tat auch hier so, dass verschiedene Ebenen ineinander greifen müssen, denn was wir

wegen des fehlenden Marketings beim Rollout des nPA natürlich gesehen haben: Dass jedem Bürger definitiv der unmittelbare Mehrwert vermittelt werden muss von jeder neuen Anwendung, die er nutzt. Ich glaube, jeder kennt das auch von sich selbst. Man nutzt gerne Dinge, die man kennt. Und alles, was man neu aktualisieren oder auf das Handy oder auf sonstige Geräte bringen muss, macht man nur, wenn sich der unmittelbare Mehrwert erschließt. Ein sehr gelungenes Beispiel für gelungenes Marketing, für Bürgernähe einer neuen Anwendung war die Corona-Warn-App. Das muss man ganz klar sagen. Da gab es ganz umfangreiche und über alle Kanäle gespielte - ich nenn es mal - Werbung. Dem Bürger wurde ganz klar gesagt: Liebe Bürgerin, lieber Bürger, wenn du das installierst, hast du unmittelbaren Mehrwert, weil 1, 2, 3. Das könnte man hier auch machen. Und zwar bei der Frage: Wie kann ich dem Bürger näherbringen, dass er über die Ausweis-App ganz wunderbar schon seinen Personalausweis „auf das Handy bringen“ kann. Das ist möglich, um über neue Anwendungsfälle zu informieren. Gerade auch die Verwaltung kann hier einen ganz relevanten Schritt tun, indem sie die Bürgerinnen und Bürger in ihrem jeweiligen Einzugsgebiet darüber informiert, wenn es neue Maßnahmen gibt, und so können wir die Bürgernähe und dann auch die entsprechende Durchdringung in der Bevölkerung erreichen. Es ist auch hier wieder eine Vielzahl von Maßnahmen notwendig.

Die **Vorsitzende**: Vielen Dank. Für die Fraktion DIE LINKE. nun die Abgeordnete Domscheit-Berg.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Ich hätte zuerst eine Frage an Sachverständigen Flüpke. Und zwar ist die ID-Wallet, die deutsche Variante, in allen möglichen Stellungnahmen, auch in Ihrer, sehr scharf kritisiert worden. Aber wie sieht es denn mit anderen ID-Wallets anderer Anbieter aus? Vielleicht war ja nur unsere schlecht, weil von Scheuer, haben Sie andere angeguckt. Können Sie etwas dazu sagen?

SV **Flüpke**: Es ist tatsächlich angedacht, dass es einen Marktplatz für solche Wallet-Anwendungen geben soll. Da stellt sich allerdings natürlich die Frage: Was ist überhaupt das Geschäftskonzept? Warum sollte ich Geld in die Entwicklung einer Wallet-App stecken? Und sobald es da einen Marktplatz gibt, gibt es natürlich auch böswillige Akteure, die ein Interesse daran haben, diese wirklich sehr wertvollen Daten aus dieser Anwendung zu stehlen oder zu entführen. Und ich habe mir auch andere Anwendungen angeschaut. Eigentlich sollte das gar nicht meine Aufgabe sein, das kostenfrei in meiner Freizeit mir anzuschauen und zu kritisieren. Und da ist mir auch bei anderen Anwendungen aufgefallen, dass sie zu zentralen Diensten beispielsweise kommunizieren. Es ist unklar, wie diese Wallets zertifiziert werden sollen und wie sichergestellt werden soll, dass daraus keine Daten gestohlen werden.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Die haben etwas getan, von dem man dachte, sie tun das nicht?

SV **Flüpke**: Genau. Die haben mit zentralen Diensten kommuniziert, obwohl bei diesen Anwendungen immer auf die Dezentralität hingewiesen wird.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Das ist natürlich ein Problem. Wir haben verschiedene Probleme auch im Zusammenhang mit den SSI-Varianten von verschiedenen Seiten schon gehört. Mich würde interessieren, der ePA wurde hier auch schon gelobt, auch wurde von vielen Seiten angemerkt, dass es zu wenige Anwendungsszenarien gibt. Wie kurzfristig kann man hier diskutierte Lösungen für eine breite und sichere Nutzung bereitstellen?

SV **Flüpke**: Die SSI-Technologie ist noch im Forschungsstadium. Das heißt, sie kann nicht umgehend eingesetzt werden. Stattdessen sollte man diese sehr kostspielige Forschung, die vor allem viel Zeit kostet, einstellen. Stattdessen sollte man hier und sofort auf den neuen Personalausweis setzen. Der ist da und hinreichend sicher und auch noch sicherer, als die bisher evaluierten SSI-Anwendungen. Das Geld kann man sich sparen, und stattdessen in Anwendungsszenarien stecken. Diverse Verwaltungsvorgänge könnte man digitalisieren auf Basis von diesem Personalausweis. Da wäre das Geld sehr viel sinnvoller investiert, als in eine Forschung an einer Technologie, die es schon gibt und bei der wir keine Forschung brauchen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Und eine Marketingkampagne wäre vermutlich auch nicht schlecht?

SV **Flüpke**: In der Tat.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Und ein bisschen Usability?

SV **Flüpke**: Also man könnte schlicht und ergreifend einen Bruchteil von diesen 100 Millionen Euro nehmen und in die Verbesserung der Usability stecken. Ganz wichtig: Unter Beibehaltung der bisherigen technischen Verfahren, die wie dargestellt sicher sind oder deutlich sicherer als die bisher gesehenen SSI-Lösungen, diese App mal etwas aufhübschen und Lösungen dafür zur Verfügung stellen, wie man Open Source irgendwie einbindet in diesen Personalausweis. Und ganz wichtig, was bisher auch noch eine Hürde war bei der Verwendung des neuen Personalausweises: Die Berechtigungszertifikate. Bei der SSI-Technologie kann einfach jeder, der will, versuchen, Daten abzurufen von einer Bürgerin oder einem Bürger. Beim neuen Personalausweis hingegen braucht es ein Berechtigungszertifikat. Da ist reincodiert, was die Person überhaupt mit Zustimmung des Benutzers abrufen darf. Das fehlt bei der SSI-Technologie komplett. Diese Berechtigungszertifikate werden in einer Monopolstellung von der Bundesdruckerei verkauft. Die Preise dafür gibt es leider erst, wenn man ein NDA unterschreibt. Das heißt, da könnte man regulativ eingreifen und damit diese Technologie zugänglicher machen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Okay, vielen Dank! Dann würde ich noch eine Frage an Ulrich Kelber, den Bundesbeauftragten für Datenschutz und Informationsfreiheit, stellen. Meine Nachfragen bei der Bundesregierung haben ergeben, dass Sie bei der ID-Wallet, die leider an den Baum gefahren worden ist, so gut wie gar nicht einbezogen worden sind. Sie haben mir selber gesagt: Das sollte sich nicht wiederholen. In welcher Art und Weise werden Sie bei den Large Scales Pilots einbezogen und gibt es eventuell Zuständigkeitshürden?

SV **Prof. Ulrich Kelber** (BfDI): Die Antwort ist kurz: Wir sind nicht eingebunden worden bei den Large Scales Pilots. Wir haben das angeboten. Auf dieses Angebot wurde bisher nicht zurückgegriffen.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Und das finden Sie vermutlich nicht gut?

SV **Prof. Ulrich Kelber** (BfDI): Nein. Es entspricht vor allem auch nicht dem Beratungsauftrag, den wir haben. Aus dem Beratungsauftrag folgt ja für öffentliche Stellen die Verpflichtung, sich beraten zu lassen. Es ist wie so oft: Wenn man sich am Anfang nicht von denen beraten lässt, die man finanziert, finden sich nachher immer gute Gründe, warum man etwas nachträglich nicht mit viel Aufwand wieder einbaut.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Vielen Dank. Ich hoffe, die Ampel macht es besser.

Die **Vorsitzende**: Vielen Dank. Wir kommen in eine zweite Runde. Da die erste Runde nicht ganz scharf mit den fünf Minuten geklappt hat, machen wir eine kürzere. Wir gehen mal von drei Minuten aus. Für die SPD Dr. Jens Zimmermann.

Abg. **Dr. Jens Zimmermann** (SPD): Herzlichen Dank. Meine erste Frage an den Bitkom. Der Markt hat das geregelt: Ihre Mitgliedsunternehmen haben entschieden und die letzten zwölf Jahre dem elektronischen Personalausweis den Rücken gekehrt. Was müssen wir tun, damit sich das ändert? Oder woran liegt das eigentlich? Bei mir jammern die alle unglaublich herum. Video-Ident, das ist so teuer und kompliziert, sehe ich genauso. Aber warum nutzen die nicht den elektronischen Personalausweis?

SVe **Rebekka Weiß**: Vielen Dank für die Frage. Es ist nicht so, dass die Wirtschaft dem Personalausweis oder auch der daraus ableitbaren eID den Rücken gekehrt hätte. Aber die Wirtschaft braucht mehr als den Personalausweis, denn es gibt bestimmte Informationen, die hat der Personalausweis schlicht und ergreifend nicht. Auch die sind aber durchaus für wirtschaftliche Anwendungsfälle interessant. Ein einfaches Beispiel: Die Tatsache, dass ich einen Führerschein besitze und ein bestimmtes Auto fahren darf, ist - zumindest meines Wissens nach - nicht im Personalausweis hinterlegt. Das heißt, um eine entsprechende digitale Anwendung zu benutzen…

Abg. **Dr. Jens Zimmermann** (SPD): Okay, ich habe nicht so viel Zeit. Okay, habe ich verstanden.

SVe **Rebekka Weiß**: … und um darüber Nachweis zu erbringen, mache ich das dann über andere Attribute. Nichtsdestotrotz ist es auch unser Interesse, die Anwendungen jetzt noch stärker zu

forcieren, weil insbesondere die Entwicklung rund um die Wallet gezeigt haben, dass wir immer von der Stammidentität und damit der staatlichen Identität aus dem Personalausweis ausgehen. Das Ökosystem wird sich dann darum herumbilden.

Abg. **Dr. Jens Zimmermann** (SPD): Ok, also ich fasse zusammen: Die Wirtschaft hat nur Anwendungen, die mehr brauchen als das, was auf dem Personalausweis vorhanden ist. Vielen Dank. Dann an die Bundesdruckerei: Jetzt wäre die einmalige Möglichkeit, dass Sie Werbung machen für die Berechtigungszertifikate. Was kosten die eigentlich? Sind sie wirklich so teuer? Und warum kaufen die Mitgliedsunternehmen von Bitkom die Ihnen nicht ab?

SV **Dr. Kim Nguyen**: Vielleicht kurze Erläuterung: das ist keine Monopolstellung, sondern ein marktoffenes Modell mit genau noch einem Marktteilnehmer.

Abg. **Dr. Jens Zimmermann** (SPD): Das ist dann aber kein Monopol, oder?

SV **Dr. Kim Nguyen**: Genau, das ist kein Monopol, sondern ein marktoffenes Modell mit noch einem Marktteilnehmer. Das ist erst einmal ein definitorischer Unterschied. In der Praxis ist es kein Unterschied. Die Preise sind marktüblich in Größenordnungen von…

Abg. **Dr. Jens Zimmermann** (SPD): Jetzt wäre es spannend geworden. Die Volksbank Odenwald, da bin ich Kunde, die möchte den elektronischen Personalausweis nutzen, kommt zu Ihnen, was müssen die dann auf den Tisch legen?

SV **Dr. Kim Nguyen**: Da gibt es eine initiale Gebühr. Die liegt in der Höhe von ein paar Tausend Euro, und dann gibt es eine laufende jährliche Gebühr, die liegt auch in der Größenordnung von 1.000 bis 2.000 Euro.

Abg. **Dr. Jens Zimmermann** (SPD): Und pro Transaktion?

SV **Dr. Kim Nguyen**: Nein, das ist alles pauschal.

Abg. **Dr. Jens Zimmermann** (SPD): Okay, herzlichen Dank.

Die **Vorsitzende**: Vielen Dank. Für die Fraktion der CDU/CSU Dr. Reinhard Brandl.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Meine erste Frage geht an Herrn Parycek: Wenn der Staat jetzt nicht handeln würde und von staatlicher Seite keine elektronische Identität entwickelt werden würde: Wie glauben Sie, würde sich der Markt entwickeln?

SV **Prof. Dr. Peter Parycek:** Die Aufgaben werden teilweise vielleicht noch von den Ländern übernommen werden für ihre jeweiligen Verfahren. Die Wirtschaft hat teilweise schon eigene Lösungen gefunden. Für den Bürger ist es vielfach gar nicht mehr unterscheidbar, weil ich andere Lösungen habe, wo ich meinen Personalausweis anhalten kann, der ausgelesen wird, und ich mich darüber auch identifizieren kann. Und es ist ganz interessant: Wenn Sie auf die unterschiedlichen Anwendungen schauen, wo der Personalausweis integriert ist, dann finden Sie dort auch weitere private Anbieter, die Sie genauso auswählen können. Das heißt, Sie haben jetzt schon einen regen Wettbewerb. Das sind nicht mal ausländische Anbieter, sondern das sind Anbieter, die aus Deutschland kommen. Aus meiner Sicht gibt es ein ganz kleines Zeitfenster und das schließt sich. Zwei Jahre und dann ist es vielleicht auch kein Thema mehr.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Was macht Dänemark besser als wir?

SV **Prof. Dr. Peter Parycek:** Dänemark hat von Beginn an auf eine extrem niederschwellige Technologie gesetzt, nämlich ein ausgedrucktes Code-Blatt. Das mag man belächeln, aber es hat funktioniert und zu einer extrem hohen Verbreitung geführt. Das ist eines der wesentlichen Dinge. Man muss zuerst sehen, dass man in die Breite kommt und dann kann man sukzessive die Sicherheit auch schrittweise iterativ erhöhen. Die Technologien entwickeln sich weiter. Das angesprochene Secure Element wird vielleicht in drei oder vier Jahren weit verbreitet sein, dann kann man es auch integrieren. Aber nicht vorab, weil man damit verhindert, dass es die gesamte Gesellschaft nutzt. Das war damals beim Kartenlesegerät eines der zentralen Probleme.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Meinen Sie, dass die hohen Sicherheitsanforderungen, die wir von Beginn an an den Personalausweis gestellt haben, am Ende dazu geführt haben, dass er nicht genutzt worden ist?

SV **Prof. Dr. Peter Parycek:** Es ist immer eine

Balance, es ist auch mehrfach angesprochen worden, zwischen Sicherheitsanforderungen und Usability. Hohe Sicherheitsanforderungen per se würde ich jetzt nicht ausschließen, aber die kann man unter Umständen auch anders herstellen. Es gibt andere Absicherungsmethoden, wie zum Beispiel die Umstellung auf NFC mit dem zweiten Faktor. Das ist eine sehr gut gewählte Variante. Wenn man die konsequent jetzt weiter umsetzen würde und gewisse andere Sicherheitsmerkmale ein bisschen zurückfährt, kann man wahrscheinlich sehr schnell zu einer sehr großen Verbreitung kommen und dann hat man wieder die Chance, sich jetzt gut zu etablieren.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Ich habe eine kurze Frage an Bitkom. Die großen Anbieter Google, Apple - welche Erfahrungen haben die, wie stehen die dazu, dass von staatlicher Seite so etwas entwickelt wird? Unterstützen die das oder sehen die das als Konkurrenz?

SVe **Rebekka Weiß**: Ich glaube, einerseits sind natürlich gerade von den genannten Anbietern schon eigene Wallet-Lösungen etabliert. Was wir durchaus sehen, ist, dass natürlich gerade was Architektur-Überlegungen angeht, durchaus auch ein Austausch stattfindet, weil die bisherigen Überlegungen sich natürlich auch gegebenenfalls für den staatlichen Einsatz zumindest in Teilen übertragen lassen. Ich glaube, wichtig ist auch hier wieder, dass man die Ebenen staatliche Identität und Wallet und weitere wirtschaftliche Nutzung voneinander trennt. Ich denke, wir sind uns hier in Deutschland und Europa einig, dass gerade die Ausgabe der Stammidentität, der Kernidentität, Aufgabe des Staates ist. Das soll natürlich auch in Zukunft der Staat machen. Alle Standardisierungsvorgaben, die es für eine Wallet gibt, müssen auch vorgegeben werden. Aber der Markt kann durchaus parallel noch Dinge entwickeln, die Großen wie die Kleinen.

Die **Vorsitzende**: Vielen Dank. Für Bündnis 90/Die Grünen Misbah Khan.

Abg. **Misbah Khan** (Bündnis 90/Die Grünen): Wir haben in den ersten Stellungnahmen an unterschiedlichen Stellen schon gehört, dass die Kombination von Blockchain im Bereich SSI nicht für sinnvoll gehalten wird. Jetzt ist das bei politischen Diskussionen immer noch an unterschiedlichen Stellen ein Thema. Zum Teil verwundert es, dass die Debatten immer noch nicht tot sind. Mich würde interessieren: Worauf würden Sie, Herr Kahlo, den Umstand zurückführen? Wie schätzen Sie die Zukunft der Technologie im Kontext digitaler Identitäten ein?

SV **Christian Kahlo**: Wieder eine sehr gute Frage. Warum sind Blockchains in der politischen Debatte noch nicht tot? Blockchains sind einfach eine Technologie, die über den ganzen Globus geht, die aus Finanzbranchen sehr stark getragen wird, die auch in den politischen Beratungen in der vergangenen Bundesregierung nachweislich sehr starken Einfluss gefunden hat. Dort ist vielfach versucht worden, Blockchain als Allheilmittel für den Digitalisierungsrückstand, den wir haben, zu verkaufen. Und damit war das Thema einfach manifest. Es ist immer noch da. Wie sehe ich den Zustand der Technologie für digitale Identitäten? Ich fand den Einwurf von Herrn Prof. Dr. Margraf vorhin sehr gut. Das erklärt es, glaube ich. Eine Beglaubigung für ein Zeugnis kann man sich sicherlich in solch einer Self-sovereign Identity, meinetwegen auch auf einer Blockchain eventuell vorstellen, aber für digitale Identitäten ergibt eine Blockchain gar keinen Sinn. Man möchte eigentlich nicht alle Identitäten in einer Blockchain verankern oder darüber verbreiten. Da haben wir wesentlich effizientere Methoden inzwischen entwickelt, da wir seit den 70er Jahren die Public-Key-Kryptographie haben und an der Stelle darüber arbeiten können. Wir brauchen keine langen Hash-Listen führen wie Kassenbücher früher. Dass es also Kassenbücher über alle Bürger gibt, muss man sich mal vorstellen. Das ist im Grundgesetz zumindest für uns auch untersagt. Das ist eigentlich ein Punkt, wo ich denke, wir können sicherlich am Rande dessen irgendwo noch eine Anwendung finden, aber im Kern dessen, was wir lösen müssen, wo wir hin müssen für Digitalisierung, werden wir keine Anwendung finden, die sinnvoll ist.

Abg. **Misbah Khan** (Bündnis 90/Die Grünen): Kann ich die gleiche Frage auch an Flüpke stellen?

SV **Flüpke:** Sehr gerne. Ich schließe mich da Herrn Kahlo an und möchte noch anmerken, dass die Blockchain in den Anwendungen, die wir bisher gesehen haben, benutzt wurde, um Schemata zu speichern. Also, wie sieht ein

Personalausweisdokument aus? Was hat es für Attribute und Felder? Das könnte man auch einfach in eine Spezifikation hineinschreiben. Dafür braucht man keine Blockchain. Und was die Verbreitung von Schlüsselmaterial angeht, gibt es Public Key Infrastruktur, auf die man zurückgreifen kann. Das Wort Blockchain hier zu droppen, dient einfach nur, Buzzwords zu bedienen und es gibt dafür absolut keine technische Notwendigkeit.

Die **Vorsitzende**: Für die Fraktion der FDP Maximilian Funke-Kaiser.

Abg. **Maximilian Funke-Kaiser** (FDP): Herzlichen Dank, Frau Vorsitzende. Auch danke an die Sachverständigen für die Ausführungen. Ich hätte eine Frage zunächst an Flüpke bezüglich der eID. Jetzt haben wir gerade von Bitkom gehört, dass für die Entstehung eines vernünftigen Ökosystems auch Informationen notwendig sind, die auf dem Personalausweis nicht enthalten sind. Deswegen die konkrete Frage: Wie schätzen Sie die Umsetzbarkeit ein, dass man so ein Ökosystem auf dem von Ihnen präferierten System der eID in die Wege geleitet bekommt?

SV **Flüpke:** Da ist die Frage: Wofür soll der Personalausweis überhaupt im Internet eingesetzt werden? Wenn ich den irgendwo vorzeige, dann muss man das gleichsetzen mit: Ich weise mich irgendwo aus. Wenn ich einkaufen gehe, dann zeig ich auch nicht meinen Personalausweis vor, bevor ich irgendwo in den Bekleidungsladen rein darf. Und das heißt, man muss da gucken, wofür soll der überhaupt eingesetzt werden? Braucht es überhaupt ein Ausweisdokument? Es gibt gesetzliche Vorgaben, wo ein Ausweisdokument erforderlich ist. Und da stehen alle notwendigen Informationen auf dem Ausweisdokument drauf, die man dafür benötigt. Man kann das Ausweisdokument übrigens auch noch um weitere Attribute ergänzen, wie zum Beispiel Fahrerlaubnisse. An den meisten Stellen braucht es gar nicht erst den Personalausweis, da reicht normaler Login-Mechanismus aus.

Abg. **Maximilian Funke-Kaiser** (FDP): Herzlichen Dank. Ich hätte eine Rückfrage bezüglich der Kosten, die entstehen, wenn man auf dem aktuellen Secure Element eine Hardware-abhängige digitale Identität umsetzt. Das ist ja auch hinlänglich bekannt, dass dort gewisse Kosten anfallen pro Transaktion. Ich hätte eine Frage an das BSI: Wie schätzen Sie es ein, dass man andere Hardware-Komponenten nutzen kann, um auch die Kostenfrage entsprechend zu klären, die auch bei dem ein oder anderen Hersteller durchaus nicht ganz kostengünstig ausfällt, sodass man, wenn man für eine Smart-eID, die personalausweisunabhängig aufgebaut ist, auf einer Hardware-Lösung entsprechend aufbauen kann.

SVe **Dr. Silke Bargstädt-Franke** (BSI): Wir sind sehr daran interessiert, eben genau bei diesem Thema Secure Element zu implementieren, dort unseren sicheren digitalen Hardware-Anker drauf zu speichern. Wir gucken uns natürlich die eigentlichen Secure Elements sehr stark an, aber haben natürlich auch sehr klare Roadmap, die schon angesprochen wurde, die in Richtung eSIM bzw. auch noch in Richtung weiterer hardware-basierter elektronischer Secure Elements auf Embedded Chips geht. Das heißt, wir sehen hier sehr klar eine Kostenroadmap, die mit Sicherheit zu einer Reduzierung der entsprechenden Kosten führt. Wenn es hierzu noch detailliertere Anfragen wirklich zu den eigentlichen Kosten der direkten Personalisierung gibt, müsste ich diese Frage leider mitnehmen, da ich heute sehr spontan eingesprungen bin und da nicht ganz aussagefähig bin.

Die **Vorsitzende**: Vielen Dank. Das nehmen wir gerne mit. Vielen Dank, dass Sie so spontan eingesprungen sind. Wir werden das nachliefern. Dann für die AfD Frau Lenk.

Abg. **Barbara Lenk** (AfD): Vielen Dank. Eine Frage an Herrn Prof. Parycek: Die EU-Kommission hält fest, dass der gegenwärtig als unzureichend empfundene Rechtsrahmen in der EU das Ergebnis uneinheitlicher nationaler Systeme sei. Sie geht weiter davon aus, dass die Überwindung dieses Problems von Bezugsnormen und technischen Spezifikationen abhängen wird. Ist es vorstellbar oder Ihnen bekannt, dass es diesbezüglich Kooperationen zwischen EU-Ländern geben wird oder dass es vielleicht eine Institution gibt, die hier federführend, normgebend oder standardsetzend wirkt?

SV **Prof. Dr. Peter Parycek:** Vielen Dank für die Frage. Die eIDAS-Verordnung ist genau in diese Richtung gegangen. Vorab war die Diskussion:

Wie stark soll man jetzt noch in die Lösungen der jeweiligen Mitgliedstaaten eingreifen? Das stand durchaus immer wieder in Diskussion und man hat sich darauf geeinigt, nicht zu stark in die jeweiligen nationalen eID-Lösungen einzugreifen und hat sich auf ein Minimum der Standardisierung zurückgezogen. Und das Minimum der Standardisierung ist das wechselseitige Anerkennen der jeweiligen Lösung. Das ist die Notifizierung, die angesprochen worden ist, die in einem Peer-Review-Verfahren läuft. Das heißt, alle Mitgliedstaaten schauen auf eine Lösung und stufen dann gemeinsam ein: Ist diese Lösung hoch anzusiedeln, substanziell oder niedrig? Das ist das aktuelle Verfahren. Und das möchten viele Staaten auch zukünftig so beibehalten. Es gibt eine offene Diskussion, ob dieses Peer-Verfahren zukünftig über eine Zertifizierung abgelöst werden beziehungsweise zumindest erleichtert werden kann. Das ist aktuell der Diskussionsstand. Das komplette Ablösen durch eine eID-Lösung seitens Europa – dafür ist es glaube ich zu spät. Das wäre vielleicht vor zehn Jahren noch eine Variante gewesen. Jetzt sind die jeweiligen Mitgliedstaats-Lösungen zu weit fortgeschritten, sodass viele wahrscheinlich nicht mehr mitmachen würden. Gerade die skandinavischen Länder, die so erfolgreich sind, müssten dann wieder das Rad zurückdrehen und dann neue Systeme einführen. Daher ist meine Prognose: Es wird wahrscheinlich bei diesem wechselseitigen Anerkennungsverfahren bleiben und vielleicht eine Vereinfachung geben, durch ein zusätzliches Zertifizierungssystem für den Wallet-Betrieb.

Abg. **Barbara Lenk** (AfD): Vielen Dank. Ich habe keine weiteren Fragen.

Die **Vorsitzende**: Vielen Dank für das Schenken der Zeit. Anke Domscheit-Berg ist die Nächste für DIE LINKE.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Es wurde immer wieder darauf hingewiesen, dass sich die Usability beim ePA verbessern müsste. Mich würden mal ein paar Sätze vom Sachverständigen Flüpke dazu interessieren: Wie es generell mit der Usability beim ePA aussieht, wo ist es schon wie, was kann man verbessern?

SV **Flüpke:** Zunächst einmal ist kein Lesegerät mehr erforderlich, wie das hier behauptet wurde. Die meisten Telefone verfügen über eine NFC-Schnittstelle. Haben Sie schon mal irgendwo offline kontaktlos bezahlt? Sehr gut. Dann haben Sie eine NFC-Schnittstelle in dem Telefon und können die benutzen. Zudem ist anzumerken, dass nur selten tatsächlich das Ausweisdokument im Internet vorgezeigt werden muss. Das ist nur notwendig bei dem Eröffnen von Bankkonten oder beim Abschließen von bestimmten Telekommunikationsdienstleistungen. Und da gibt es jetzt auch noch das Video-Ident-Verfahren, was häufig eingesetzt wird. Wenn der Einsatz des neuen Personalausweises günstiger wäre, als dieses sehr kostspieligen Video-Ident-Verfahren, dann würde die Wirtschaft natürlich auf den Personalausweis setzen und nicht auf diese teuren Video-Ident-Verfahren.

Abg. **Anke Domscheit-Berg** (DIE LINKE.): Herzlichen Dank. Ich hätte noch eine Frage an Rebekka Weiß vom Bitkom. Sie sprachen in Ihrem Anfangsstatement davon, wie wichtig es ist, klare Verantwortungen zu haben. Jetzt gibt es seit ein paar Tagen schriftlich ein paar geklärte Zuständigkeiten. Bei mir hat es aber beim Thema eID zur Verwirrung geführt. Zum einen ist für eIDAS das BMDV federführend, für das Schaufenster digitale Identitäten ist ein anderes Ministerium, nämlich das BMWK, zuständig und ein drittes Ministerium hat die Federführung bei diesem interministeriellen digitalen Identitätenlabor und das ist das BMI. Und da arbeiten BMDV, BMF, BMWK und das Kanzleramt auch noch mit. Entspricht das Ihren Vorstellungen von klaren Verantwortungen und Zuständigkeiten?

SVe **Rebekka Weiß**: Nein. Klar im Sinne von ja, diese Verteilung führt aber definitiv zu einer Dopplung an Arbeit, natürlich in den Ministerien selbst, letztlich bei uns allen anderen. Das ist auch, was wir in den vergangenen Jahren gemerkt haben, wenn auch wir als Anwender, als Experten, als Sicherheitsspezialisten und so weiter, ständig mit 20, 30, 40 verschiedenen anderen Stakeholdern Kontakt haben müssen, immer wieder auch Problemfälle aufbereiten müssen, verlieren wir dadurch massiv Zeit. Das konnte auch jetzt nicht behoben werden. Vielleicht hätte man das beheben können durch ein wirkliches Digitalministerium, haben wir nun

aber nicht und jetzt kommt es zu dieser Zuständigkeitenteilung. Deswegen sehe ich aber wirklich großes Potenzial in dieser übergreifenden Arbeitsgruppe. Ich kann mir gut vorstellen, dass das auch für die Kollegen und Kolleginnen aus der Verwaltung eine besondere und besonders schwere Aufgabe ist, ressortübergreifend zu arbeiten. Auf Bundesebene ist es sicherlich nicht ganz einfach. Es ist aber ein neuer Ansatz und genau der ist jetzt notwendig. Ich glaube, was von uns anderen Stakeholdern parallel erwartet werden kann, ist, dass wir aber auch immer wieder die uns bekannten Anwendungsfelder, Technologie-Spezifikationen, Standardisierungs-Überlegungen an die entsprechenden Gruppierungen spiegeln und so dann hoffentlich diesmal zu einer schnelleren Lösung kommen.

Die **Vorsitzende**: Vielen Dank, die Zeit ist schon wieder vorbei. Wir haben heute ausführlich darüber diskutiert und viele Fragen beantwortet bekommen. Ich hoffe, dass es auch viel Erkenntnisgewinn in den jeweiligen Fraktionen gegeben hat. Ich danke jedenfalls ganz herzlich allen Sachverständigen, die uns Rede und Antwort gestanden haben, und vielen Dank für die guten Hinweise. Ich danke den Zuhörerinnen und Zuhörern, oder Zuschauern und Zuschauerinnen im Saal und an den Endgeräten für das gezeigte Interesse. Ich danke der Technik, den zuständigen Mitarbeiterinnen und Mitarbeiter, die uns immer tatkräftig unterstützen bei öffentlichen Anhörungen. Ich danke auch dem Sekretariat, das uns hier die Vorbereitung gemacht hat und uns auch immer super unterstützt, und natürlich den Vertreterinnen, Vertretern der Ministerien, die da waren. Herrn Tauber habe ich gar nicht begrüßt. Entschuldigung, Herr Bürger, Herr Tauber, und ich hoffe, dass wir uns in diesem Rahmen vielleicht weiter austauschen werden oder bei anderen Gelegenheiten. Vielen, vielen Dank. Ein Hinweis noch auf die nächste Sitzung des Ausschusses: Mittwoch um 15 Uhr, am üblichen Ort, also in unserem Ausschuss-Saal. Wir haben jetzt einen im PLH E.600. Die Sitzung findet auch hybrid statt. Dann gebe ich noch kurz den Hinweis auf das Angebot zur Freischaltung der Online-Ausweisfunktion des Personalausweises, was hier im Anschluss möglich ist. Und Ihnen allen wünsche ich noch einen schönen Montag, einen angenehmen Abend und schließe hiermit die Sitzung. Vielen Dank.

Schluss der Sitzung: 16:04 Uhr

Tabea Rößner, MdB
Vorsitzende