Protokoll-Nr. 19/140

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Wortprotokoll
der 140. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 17. Mai 2021, 15:00 Uhr
10557 Berlin
Konrad-Adenauer-Str. 1
Paul-Löbe-Haus, Raum 4 900

Vorsitz: Andrea Lindholz, MdB

Tagesordnung - Öffentliche Anhörung

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät

BT-Drucksache 19/28169

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss Digitale Agenda
Haushaltsausschuss (mb und § 96 GO)

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Josef Oster [CDU/CSU]
Abg. Helge Lindh [SPD]
Abg. Dr. Christian Wirth [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Ulla Jelpke [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

Protokoll-Nr. 19/140

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Inhaltsverzeichnis

Mitglieder des Ausschusses

	Ordentliche Mitglieder	**Stellvertretende Mitglieder**
CDU/CSU	Lindholz, Andrea Müller, Axel Oster, Josef	
SPD	Lindh, Helge	
AfD	Schulz, Uwe	
FDP	Höferlin, Manuel	
DIE LINKE.	Pau, Petra	
BÜNDNIS 90/DIE GRÜNEN	Notz, Dr. Konstantin von	
Fraktionslos		

Protokoll-Nr. 19/140

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 17. Mai 2021, 15.00 bis 17.00 Uhr
„eID-Gesetz“

Simon Japs
Deutscher Städtetag, Bundesvereinigung der kommunalen Spitzenverbände

Prof. Ulrich Kelber
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn

Prof. Dr. Marian Margraf
Freie Universität, Berlin

Linus Neumann
Chaos Computer Club, Berlin

Prof. Dr. Isabell Peters
Kommunale Hochschule für Verwaltung in Niedersachsen, Hannover

Rainer Rehak
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V., Berlin

Rudolf Schleyer
Vorstandsvorsitzender - Anstalt für Kommunale Datenverarbeitung in Bayern, München

Einziger Tagesordnungspunkt

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät

BT-Drucksache 19/28169

Vors. **Andrea Lindholz** (CDU/CSU): Ich darf ich alle ganz herzlich zur 140. Sitzung unseres Ausschusses begrüßen. Die Anhörung ist mit einem Zeitfenster von bis zu zwei Stunden vorgesehen, zwischen 15:00 und 17:00 Uhr. Es geht um den elektronischen Identitätsnachweis und wir gehen wie folgt vor: Die Anhörung wird wie üblich im Livestream übertragen und später dann auch in der Mediathek allen zum Abruf bereitgestellt. Die Bundesregierung ist durch Herrn Ministerialdirektor Ernst Bürger vertreten. Ich möchte mich bei allen Sachverständigen ganz herzlich für Ihre Teilnahme und Ihre Bereitschaft, uns mit Ihrer Expertise zur Verfügung zu stehen, bedanken, ebenfalls für die bereits eingegangenen Stellungnahmen. Diese Stellungnahmen werden zusammen mit dem Protokoll, das wir von der Sitzung anfertigen, als Gesamtdrucksache der Öffentlichkeit zur Verfügung gestellt. Sie erhalten das Protokoll vorab, können es dann noch einmal durchsehen und eventuelle Korrekturwünsche anbringen. Das nähere Verfahren wird Ihnen mit der Übersendung mitgeteilt. Wir fertigen von der heutigen Anhörung ein Wortprotokoll an.

Wir werden zunächst jeden Sachverständigen in alphabetischer Reihenfolge bitten, ein kurzes, wenn möglich maximal fünfminütiges Eingangsstatement abzugeben. Danach werden die Fraktionen ihre Fragen in der ersten Runde stellen. Nach Beendigung der Fragerunde erhalten Sie die Möglichkeit, allen gesammelt zu antworten. Für den Fragemodus gilt, dass es zunächst möglich ist, zwei Fragen an einen Sachverständigen zu stellen oder an jeweils zwei Sachverständige eine gleiche Frage oder zwei unterschiedliche Fragen an einen Sachverständigen. Je nachdem, wie viel Zeit wir dann noch für eine zweite Runde haben, sehen wir dann, wie wir mit dem Fragemodus hinkommen. Die Mikrofone der zugeschalteten Gäste sind bitte ausgeschaltet, wenn Sie nicht selbst sprechen. Wir beginnen mit Herrn Japs, bitte schön.

SV **Simon Japs** (BVkom, Berlin): Sehr gern. Sehr geehrte Frau Vorsitzende, sehr geehrte Abgeordnete, sehr geehrte Damen und Herren. Vielen Dank für die Einladung, die Position der Kommunen vortragen zu dürfen. Wir hatten bereits zum Referentenentwurf im Januar Stellung genommen – leider sind nur wenige unserer Anregungen aufgenommen worden, deswegen sind viele unserer Punkte unverändert.

Grundsätzlich begrüßen wir das Vorhaben, eine einheitliche elektronische Identität einzuführen. Das setzt allerdings den nachhaltigen und zügigen Aufbau beziehungsweise die Erweiterung digitaler Angebote voraus. Flankiert von einer gezielten Informationskampagne zur Nutzbarkeit der eID-Funktionen sehen wir die Möglichkeit, die Nutzung des elektronischen Identitätsnachweises bei den Bürgerinnen und Bürgern deutlich zu steigern. Dies ist vor allem im Hinblick auf die Digitalisierung von Verwaltungsleistungen mehr als notwendig. Von zentraler Bedeutung für eine durchdringende Nutzung der eID in der Breite sind die Einfachheit der Anwendung und die Gewährleistung von Sicherheit und Datenschutz, um das Vertrauen der Bürger in das Verfahren zu erlangen. Wesentlich ist aus unserer Sicht, dass die Nutzerzentriertheit im Zentrum der technischen Umsetzung steht, denn nur eine einfache und transparente Handhabung kann zu einer Erhöhung der Nutzerzahlen führen.

Bei der Einführung neuer digitaler Systeme und erleichterter Zugangsmöglichkeiten wird das Themenfeld „Support“ oft unterschätzt. Nutzende erwarten aber in diesem Zusammenhang insbesondere bei den öffentlichen Stellen, dass Prozesse reibungslos funktionieren, Fehler zeitnah analysiert und behoben werden. Dies erfordert hohen Kommunikations- und Arbeitsaufwand mit Nutzern, Verfahrensanbietern, Zahlungsdienstleistern und Portalbetreibern.

Darüber hinaus ergeben sich zu dem Gesetzentwurf unter anderem folgende Fragen: Was passiert bei der Änderung von dem auf dem Ausweis gespeicherten Daten? Sind die Bürgerinnen und Bürger hier selbst für die Aktualisierung der Daten zuständig? Werden die Daten im Hintergrund mit dem Ausweisregister der Ausweisbehörde abgeglichen? Wenn ja, wie wird mit Diskrepanzen im Datenbestand umgegangen? Was passiert, wenn das Mobilgerät verloren geht, ist dann ein neuer Personalausweis auszustellen? Wie kann die

Funktion bei Verlust des Mobilgerätes gesperrt werden? Viele weitere Fragen waren in unserer Stellungnahme zusätzlich genannt. Wir weisen darauf hin, dass bislang leider keine Gesamtstrategie für die Nutzung elektronischer Identitäten auf Bundesebene zu erkennen ist. Vielmehr ist die Eilbedürftigkeit deswegen nicht nachvollziehbar und für uns nur unter dem Eindruck der ablaufenden Legislaturperiode und der Umsetzungsfrist des Onlinezugangsgesetzes zu erklären.

Dennoch haben wir uns heute hier alle unerwartet versammelt, um das Gesetz noch schneller auf den Weg zu bringen. Umstritten ist dabei eine Regelung, die den Ländern ermöglichen soll, ein zusätzliches zentrales Lichtbild- und Unterschriftenregister aufzubauen. Begründung ist, dass Kommunen es nicht allein schaffen werden oder zumindest erst viel zu spät. Dies erschließt sich uns als Kommunen nicht. Denn wenn es einen auf XÖV basierenden Abruf- und Austauschstandard gibt, wird dieser auch in den Kommunen über Fachverfahren umgesetzt. Das wird möglicherweise in den kleineren Gemeinden mit Personalausweisbehörde nicht einfach, aber doch möglich. Große Städte, wo wohl die allermeisten Anfragen landen werden, haben damit unserer Einschätzung nach keine Probleme. Im Änderungsantrag wird zudem immer noch von der Nichterreichbarkeit der Personalausweisbehörden gesprochen. Das widerspricht jedoch der Verpflichtung zu effizienter und digitaler Verwaltung. Die Sicherheitsbehörden machen auch heute oft schon Besuche in unseren Behörden. Von Eilbedürftigkeit Ihrer Anliegen, schon gar von 24/7, ist dabei wenig zu erkennen. Wenn also nun die Kommunen für die Schaffung von Landesregistern herhalten sollen, müsste diese Begründung belastbar unterlegt sein. Ebenso wie das Erfordernis für extrem wenig eilbedürftige Anfragen von Sicherheitsbehörden, neue Landesregister aufzubauen.

So komme ich zum Schluss: Wir Kommunen unterstützen die Einführung einer einheitlichen elektronischen Identität ausdrücklich. Die Einführung von Landesregistern erschließt sich uns allerdings bislang nicht. Insbesondere die Eilbedürftigkeit dieser Einführung ohne eine ausreichende Beratung sehen wir mit Sorge, weil sie das Vertrauen der Bürgerinnen und Bürger in die so wichtige digitale Identität gefährden könnte. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Herr Kelber, bitte.

SV **Prof. Ulrich Kelber** (BfDI, Bonn): Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren Abgeordnete, herzlichen Dank für die Einladung und der damit verbundenen Möglichkeit zur Stellungnahme. Das mit dem Gesetzentwurf verfolgte Ziel stellt einen weiteren Schritt dar, hin zu einer ganz praktisch erfahrbaren, digitalen Wirklichkeit. Viele Bürgerinnen und Bürger erwarten solche Fortschritte, weil sie ihnen den Alltag im Umgang mit gesetzlichen Auflagen und behördlichen Abläufen eindeutig erleichtern können. Diese Entwicklung sowie auch die einzelnen Elemente einer solchen digitalen Transformation sind auch nicht per sé datenschutzkritisch, sondern im Gegenteil sehr gut datenschutzfreundlich umsetzbar. Diese Umsetzung bedarf dann allerdings des aufmerksamen Hinschauens, wenn im Bestreben nach kurzfristigen Erleichterungen für Bürgerinnen und Bürger, wie auch für Staat und Verwaltung, Lösungswege beschritten werden, die sich auf den zweiten Blick möglicherweise als gravierend nachteilig für den Einzelnen und sein Recht auf informationelle Selbstbestimmung herausstellen können. Ich würde mir wünschen, dass die Umsetzung dieser Ziele ohne „Tunnelblick“ erfolgt, also Datenschutz und Datensicherheit uneingeschränkt von Anfang an mitbedacht werden und man diese auf dem Lösungsweg auch integriert.

Mit einer ersten Stellungnahme habe ich mich am 22. März an den Ausschuss gewandt und konkreten Änderungs- und Ergänzungsbedarf aufgezeigt: Das eine ist die Geltungsdauer des Identifikationsnachweises über mobile Endgeräte, die zumindest gesetzlich deutlich zu lang bemessen ist. Hier sollte kürzer gefasst werden und in Bezug auf gesetzlich [Tonaussetzer] Identifizierung dienenden Daten verändert haben und das mobile Endgerät sich nicht mehr in der Verfügungsgewalt der darüber zu identifizierenden Person befindet. Diese Verbesserungsvorschläge halte ich weiterhin für datenschutzrechtlich notwendig.

Der Gesetzentwurf hat darüber hinaus durch einen durch die Koalitionsfraktionen eingebrachten Antrag eine Erweiterung erfahren, die in Teilen erhebliche datenschutzrechtliche Bedenken auslöst. Die eingebrachten Änderungen sehen unter anderem die Einräumung einer Befugnis zugunsten

der Länder vor, die für gesetzlich zulässige automatisierte Abrufe von Lichtbild und Unterschrift benötigten Daten der Pass- und Personalausweisbehörden zusätzlich zentral zu speichern und zu diesem Zweck auch dauerhaft vorzuhalten. Die dafür angeführte Begründung erscheint auf den ersten Blick nachvollziehbar, greift aus meiner Sicht aber zu kurz. Diese Regelungsbefugnis öffnet den Ländern auf der Grundlage eigenen Rechts die Errichtung eines zentralen Datenbestandes zur Durchführung des Abrufverfahrens und damit eine gedoppelte Datenhaltung zu den ja schon existierenden Registern der kommunalen Pass- und Personalausweisbehörden. Damit steigen die Anzahl der Angriffsflächen und die potenzielle Gefahr eines Missbrauchs oder einer zweckfremden Verwendung am Ende bei einem Datenbestand sämtlicher Bürgerinnen und Bürger eines Bundeslandes. Auch werden die technischen Möglichkeiten für weit über heutige gesetzliche Befugnisse hinausgehende Auswertungen der Daten geschaffen. Gemessen an den Grundsätzen zur Einhaltung der Datenminimierung und –erforderlichkeit müssten schon unabweisbare Gründe vorgebracht werden, um einen solchen zusätzlichen Datenbestand zu legitimieren.

Hinzu kommt, dass es sich bei den Lichtbildern in den Registern der Pass- und Personalausweisbehörden um biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person und damit um Daten im Sinne des Artikels 9 der Datenschutzgrundverordnung handelt. Das heißt, diese Daten unterliegen einem besonderen Schutz und für ihre zulässige Verarbeitung sind erhöhte Anforderungen zu stellen. Dieser strenge Maßstab muss auch schon dann angelegt werden, wenn mit dem Gesetz zunächst lediglich eine entsprechende Ermächtigung, also eine Öffnungsklausel für den daraufhin tätig werdenden Landesgesetzgeber geschaffen wird, denn die Entscheidung, es bestehe ein erhebliches öffentliches Interesse an der Errichtung zentraler Abrufregister für Lichtbild und Unterschrift auf Landesebene, die trifft dann bereits der Bundesgesetzgeber. Und die Schaffung der gesetzlichen Grundlage mit dem Motiv der Sicherstellung eines möglichst reibungslosen und effizienten Verfahrens liegt sicherlich im öffentlichen Interesse, aber umfasst dies eine dauerhafte Verarbeitung biometrischer Daten, bedarf es der Feststellung eines gesteigerten und qualifizierten öffentlichen Interesses, um dem besonderen Schutzbedarf Rechnung zu tragen. Konkrete Anhaltspunkte für die Annahme eines solchen Interesses sind dem Gesetzentwurf nicht zu entnehmen. Eine funktional gleiche, datenschutzfreundliche Alternative ist vorhanden. Vielen Dank für die Aufmerksamkeit.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank Herr Professor Kelber. Herr Professor Margraf, bitte.

SV **Prof. Dr. Marian Margraf** (Freie Universität Berlin): Auch noch einmal von meiner Seite vielen Dank für die Einladung und dass ich die Möglichkeit habe, hier Stellung zu nehmen. Dazu möchte ich gleich sagen, ich nehme nur Stellung zum geplanten Vorhaben, den elektronischen Identitätsnachweis auf ein mobiles Endgerät umzusetzen und nicht zu den anderen Änderungsvorschlägen. Ganz kurz noch einmal: Die Onlineausweisfunktion wurde ja 2010 eingeführt und setzt sehr sicher und sehr datenschutzfreundlich die Authentisierung von Bürgerinnen und Bürgern gegenüber Dienstanbietern um – jetzt mittlerweile seit elf Jahren. Kernidee ist eben eine Zwei-Faktor-Authentisierung, die auf Besitz, nämlich einer Ausweiskarte und dem Wissen einer sechsstelligen PIN beruhen und dass Bürgerinnen und Bürger eben jederzeit wissen, wem gegenüber sie sich authentisieren und dass Dienstanbieter auch nur die personenbezogenen Daten erhalten, die sie für ihren Dienst tatsächlich auch nutzen – das alles wird ja über Berechtigungszertifikate, die vom Bundesverwaltungsamt ausgestellt werden, geregelt. Meine Erfahrung ist, dass das wirklich eine sehr sichere und sehr datenschutzfreundliche Umsetzung ist und dem Gesetzentwurf ist zu entnehmen, dass diese Technik eben eins zu eins auf ein mobiles Endgerät übertragen werden soll, was ich sehr gut finde.

Die Sicherheit der geplanten Lösung hängt natürlich von der konkreten Ausgestaltung ab, die ja naturgemäß solch einem Gesetz nicht zu entnehmen ist. Ich weiß aber, dass das Bundesamt für Sicherheit in der Informationstechnik hier schon erhebliche Vorarbeiten geleistet hat und schon Richtlinien und Vorgaben erarbeitet hat, wie man so eine Lösung sicher umsetzen kann. Wichtig dafür ist, dass ein sogenanntes Sicherheitselement auf einem mobilen Endgerät genutzt wird, was insbesondere einen sicheren Schlüsselspeicher umsetzt, aber eben auch ermöglicht, kryptografische Protokolle sicher umzusetzen. Das

schränkt am Anfang natürlich die Nutzungsbreite deutlich ein, also nicht alle Geräte verfügen über solch ein Sicherheitselement beziehungsweise kommt man da ran und kann dann da irgendetwas umsetzen, das heißt also am Anfang werden wir eingeschränkte Bandbreite haben. Das wird sich aber meines Erachtens in Zukunft ändern.

Was jetzt die Sicherheit betrifft im Gegensatz zu so einer Ausweiskarte, die im Wesentlichen aus einem Sicherheitschip besteht, besteht ja so ein Mobiltelefon aus deutlich mehr Software und das bedeutet letztendlich, dass es da potenziell auch deutlich mehr Sicherheitslücken geben kann, die dann im Endeffekt auch den elektronischen Identitätsnachweis betreffen können. Deswegen wäre mein Vorschlag, ein Schwachstellenmanagement aufzubauen, was es eben dem Betreiber, also der Bundesdruckerei im Auftrag der Bundesregierung, ermöglicht, Schwachstellen zu erkennen, zu bewerten und entsprechende Gegenmaßnahmen einzuleiten – im schlimmsten Falle eben Geräte von der Nutzung des elektronischen Identitätsnachweises auszuschließen, wenn es zu erheblichen Sicherheitslücken kommt.

Mein weiterer Vorschlag ist, in den gesamten Entwicklungsprozess die Zivilgesellschaft stark einzubinden. Also wir wissen, dass eben Teile der Gesellschaft großen Digitalisierungsprojekten des Bundes sehr skeptisch gegenüberstehen, was natürlich damit zu tun hat, dass der Staat unterschiedliche Interessen verfolgt. So wurde zum Beispiel ja die Einführung der Onlineausweisfunktion im Jahr 2010 sehr negativ begleitet von einigen Teilen. Und um die Akzeptanz der geplanten Lösung einfach zu steigern, wäre es eben wichtig, ähnlich wie bei einem Open-Source-Projekt, alle Konzepte, die darum herum geschrieben werden, mit der Öffentlichkeit frühzeitig zu diskutieren, diese zu veröffentlichen, die Software, die erstellt werden soll, das bedeutet eben die Software auf dem Smartphone, aber auch auf dem Sicherheitselement als Open Source zur Verfügung zu stellen und mit der Community gemeinsam diese Geschichten zu entwickeln. Das ist mein Vorschlag.

Fazit ist: Ich begrüße die Initiative sehr. Die Onlineausweisfunktion oder jetzt eben den elektronischen Identitätsnachweis auf Smartphones oder Tablets zu bringen, das wird die Nutzerakzeptanz deutlich steigern, auch die Reichweite. Es ist wichtig für eine sichere Umsetzung der Digitalisierung unserer Gesellschaft, aber eben genauso wichtig ist die Sicherheit eben konkret auszugestalten, ein transparentes Handeln und die Zivilgesellschaft eben frühzeitig mit einzubeziehen. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank. Herr Neumann, bitte.

SV **Linus Neumann** (CCC, Berlin): Vielen Dank Frau Vorsitzende, vielen Dank an die Mitglieder des Ausschusses. Der CCC hat bei diesem Thema gemeinsam mit dem „Forum der InformatikerInnen für Frieden und gesellschaftliche Verantwortung“ (FIfF) eine Stellungnahme formuliert. Ich konzentriere mich daher jetzt erst einmal nur auf den Änderungsantrag der Fraktionen der CDU/CSU und der SPD bezüglich der zentralisierten Speicherung biometrischer Daten: Grundsätzlich ist zu sagen, eine eID ist durchaus möglich. Und man kann das auch sicher und derart gestalten, dass die Nutzer*innen dem System nicht nur vertrauen, sondern auch vertrauen können. 2005 bei der Einführung der Biometrie in Pässe und Ausweise haben wir als Chaos Computer Club gewarnt, ich zitiere aus der damaligen Sachverständigenauskunft: „…denn biometrische Verfahren und die eingesetzten Funkchips bieten mannigfaltige Möglichkeiten zur Überwachung von Menschen.“ Und dass einmal installierte Technologien zur Identifizierung und Überwachung die Begehrlichkeiten von Geheimdiensten, Ermittlungsbehörden, aber auch kommerziellen Unternehmen wecken werden, ist kein neues Phänomen. Eine biometrische Datenbank, eine zentrale Speicherung, so wurde es damals noch hoch und heilig versprochen, käme überhaupt nicht in Frage. Erst recht nicht ein automatisierter Abruf. 2017 haben Sie dann mit dem Gesetz zur Förderung des elektronischen Identitätsnachweises diesen Zugriff auf die biometrischen Daten stark vereinfacht und den zentralen Zugang ermöglicht. Man fragt sich tatsächlich, wie denn eine solche Maßnahme die Nutzung des elektronischen Identitätsnachweises fördern soll, der ja tatsächlich trotz einiger seiner Vorteile in keiner Form irgendwo Anwendung findet und nun wollen Sie 2021 das Vorhaben der biometrischen Erfassung und Zugänglichkeit der biometrischen Daten quasi als Trojaner zur mobilen eID noch schnell mit in das Gesetzesvorhaben hineinschleusen. Sie wollen

Biometrie-Datenbanken in jedem Bundesland – das sogenannte zentrale Lichtbild- und Unterschriftenregister. Für diese neuen Datenbanken erkenne ich keine nennenswerten Sicherheitsvorgaben. Und das alles geschieht hier in einer Zeit, in der wir in unserer Gesellschaft seit mehreren Jahren das Terrorphänomen des selbsternannten sogenannten NSU 2.0 haben und dieser Fall zeugt ja durchaus von der Qualität der Absicherung der Daten, die Sie den Behörden zugänglich machen. Es hält sich sogar der Verdacht, so entnehme ich den Nachrichten, der Täter hätte sich die Daten einfach telefonisch erfragt. Und einer Sicherheits- und Sensibilitätskultur wollen Sie nun die biometrischen Daten der Bevölkerung anvertrauen? Ich schließe mich der Perspektive von Herrn Kelber an, der sagt: Hier vervielfältigen sich die Angriffsfläche und auch die Missbrauchspotentiale. Ich glaube, ich brauche Ihnen nicht- - aber ich werde es trotzdem machen: Ich erkläre Ihnen noch einmal, welche Bedeutung die Biometrie als Authentifizierungsmerkmal hat beispielsweise für den Zugriff auf Mobiltelefone, für den Zugriff auf Rechner – als Authentifizierungsmerkmal also ein sehr wichtiges Merkmal, was der Chaos Computer Club mit dem Fingerabdruck des damaligen Innenministers Herrn Dr. Schäuble demonstriert hat.

Biometrie ist aber gleichermaßen ein sehr geeignetes Überwachungsinstrument und hat für die Massenüberwachung erhebliche Bedeutung. Da nehmen wir als Beispiel das Projekt der Videoerfassung am Bahnhof Südkreuz, wo die eigentlich datentechnisch zunächst unüberblickbare Datenmenge eines Videos zu einer säuberlichen, zeitgenauen Datenbank wird, die zeigt, wer wann an diesem Bahnhof war. Und genau diese Reduktion der Daten ist es, was dann eine Massenüberwachung ermöglicht, die im öffentlichen Raum so eigentlich nicht möglich ist, die wir sonst nur aus dem Internet kennen. Die Themen der Fehleranfälligkeit lasse ich einmal im Rahmen der Zeit außen vor.

Fazit: Ich habe teilweise den Eindruck, dass Sie das auch wissen und nicht nur trotzdem, sondern genau deshalb machen wollen. Aber wenn Sie sich schon um die Akzeptanz von Ihrer eID Sorgen machen und das inzwischen seit 16 Jahren, dann sollten Sie vielleicht die spannenden Möglichkeiten, die diese Technologie gerade im Privacy-Bereich bietet, mehr in den Vordergrund stellen. Wir stellen ja fest, Anwendungsmöglichkeiten meiner eID sind nach wie vor schlichtweg nicht vorhanden und das ändert sich wahrscheinlich auch nicht, wenn ich sie jetzt auf dem Telefon habe, aber wenn Sie diese Verfahren jeweils mit derartigen Risiken und Überwachungsambitionen verbinden, dann nähren Sie doch den Eindruck, dass hier Technologien gegen die Bürger*innen statt für die Bürger*innen gebaut werden. Das Beispiel eID ist nur eines, die Biometrie- Datenbank, die hintendran kam, ein weiteres und ich möchte gar nicht wieder das alte Lied von der „De-Mail“ singen. Allgemein schließe ich mich auch der Einschätzung an, dass das notwendige technische Schutzniveau nicht einheitlich auf allen Geräten sinnvoll erreichbar ist und verweise ansonsten auf die Einlassung und die Stellungnahme von Herrn Rainer Rehak. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Frau Professor Peters, bitte.

SV **Prof. Dr. Isabell Peters** (HSVN, Hannover): Danke sehr. Sehr geehrte Vorsitzende, sehr geehrte Damen und Herren, sehr geehrte Abgeordnete, vielen Dank für die Gelegenheit, zur heutigen Anhörung Stellung zu nehmen. Ich möchte meine Ausführungen vor allem auf die Zielsetzung des Gesetzentwurfs fokussieren und zwar beabsichtigt die Bundesregierung mit dem Gesetzentwurf in erster Linie, die Verbreitung und Akzeptanz einer Identifizierung per mobilem Endgerät zu ermöglichen. Ich halte diese Maßnahme für sehr sinnvoll. Allerdings glaube ich, man könnte sie insofern zielgerichteter ausgestalten, indem man folgende drei weitere Maßnahmen anstrebt: Erstens. Eine Lösung für Wirtschaft und Staat entwickeln. Zweitens. Mindestens eine einheitliche Lösung für hoheitliche Anwendungsbereiche schaffen. Drittens. Die Lösung um eine elektronische Signatur erweitern.

Zu erstens: Momentan gibt es am Markt unterschiedliche Identifizierungsmöglichkeiten, wir kennen das alle als Konsumenten mindestens aus dem Bereich des Onlinebanking. Die Folge dieser vielen Lösungen ist, dass es nutzerseitig und angebotsseitig Nachteile gibt und von diesen Nachteilen sind wir alle betroffen. Wenn wir rein auf den Teil der Identifizierungsvorgänge schauen, die die öffentliche Verwaltung ausmacht, dann betrifft diese nur einen Bruchteil aller Identifizierungsvorgänge – es sind unter zehn Prozent. Der

größte Anteil an Identifizierungslösungen entfällt auf Nutzungen in der Finanzbranche. Insofern sollte der Staat eine einheitliche Lösung schaffen und nach Möglichkeit die Finanzbranche dafür mit ins Boot holen. Und das kann er tun, indem er entweder die vorhandene Lösung ausbaut und die Finanzbranche einlädt, daran mitzuwirken, oder aber indem er selbst in Identifizierungslösungen einsteigt, die private Anbieter für den Konsumentenbereich bereits entwickelt haben.

Zu zweitens: Der Staat sollte mindestens eine einheitliche E-Government-Identifizierungslösung entwickeln und nicht verschiedene Lösungen nutzen, wie zum Beispiel im ELSTER-Steuerverfahren (EKONA) und bei der nationalen Patientenakte eine dritte Identifizierungsvariante. Das wäre wichtig für eine stärkere Marktdurchdringung und Akzeptanz.

Und drittens sollte die Lösung um eine elektronische Signatur erweitert werden. Elektronische Signaturen haben vor allem im Bereich E-Government eine ganz maßgebliche Funktion, da sie das Schriftformerfordernis ablösen. Also genau das, was wir momentan als Bürger in Onlineverfahren erleben: Wir füllen einen Onlineantrag aus, drucken ihn aus, unterschreiben ihn und schicken ihn dann postalisch zur Verwaltung. Das könnte man mit der Verknüpfung um eine elektronische Signatur, die kostenlos mit der eID zur Verfügung gestellt werden sollte, deutlich verbessern. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank. Dann Herr Rehak.

SV **Rainer Rehak** (FIfF, Berlin): Vielen Dank liebe Frau Vorsitzende und liebe Abgeordnete und alle Zuschauenden für die Möglichkeit, hier sprechen zu dürfen. Auch wir unterstützen das Ziel, was gesteckt wird, ausdrücklich und ich sehe unsere Aufgabe hier, so bestimmte architektonische Richtungen und technische Grundstrukturen in einen gesellschaftlichen Kontext zu setzen – was wir als Forum der InformatikerInnen für Frieden und gesellschaftliche Verantwortung da auch besonders tun können.

Es scheint hier so ein bestimmtes Vorurteil zu herrschen, dass in der Digitalisierung so Einzelsachen schnell geändert werden können und schnell implementiert werden können und wenn man dann große neue Anwendungszwecke hat, dann kann man die einfach so integrieren und zusammenfließen lassen. Das ist aber nicht so. Man kann sagen: Digitalisierung ist Verwaltung mit anderen Mitteln. Und da ist gar nichts schnell und einfach zusammenzufließen und vor allem nicht ohne Plan. Was es dafür braucht und es wurde gerade schon von diversen sachverständigen Auskunftspersonen hier gesagt, ist eine ganzheitlich gedachte Grundarchitektur. Hier fehlt so etwas wie ein öffentliches System für Signaturauthentifizierung und Kommunikation für Bürger*innen, Ämter, aber auch juristische Personen, wie eben angesprochen worden ist. Es ist aber hier keine offene Struktur angedacht, es wird eine geschlossen proprietäre Monopolinfrastruktur wie damals „De-Mail“, das wurde von Linus Neumann gerade schon genannt. Aber das ist der Punkt: Man kann natürlich erst einmal fragen, warum Dinge nicht funktioniert haben, um sie danach anders zu machen. Diese fehlende Vision und das fehlende Verständnis sieht man auch ganz konkret an den fehlenden Umsetzungsaufwänden im Gesetz, da ist also nichts vorgesehen, was die Umsetzaufwände von den TSM oder App-Anbietern selbst wäre. Das heißt zum Beispiel ganz konkret: So etwas wie Unterschriftensammlung muss ja digital gehen, aber dafür muss eben eine NGO selbst auch als Anbieterin auftreten. Das ist hier überhaupt nicht vorgesehen, weil das System so, wie es angedacht ist, den analogen Vorgang digital kopiert und eben nicht – wie sagt man so schön – „die Potentiale der Digitalisierung“ hebt. Wir können jetzt deswegen viele Details kritisieren, aber die Ursache vieler Punkte liegt genau im Fehlen dieser größeren Strategie mit vielen Insellösungen. Und diese nötige, ganzheitlich gedachte offene Grundarchitektur wäre dann eine gesellschaftlich-öffentliche Infrastruktur, so etwas wie Internet oder Eisenbahn auf einer ein bisschen abstrakteren Ebene. Und da kann auch keiner sagen, es hätte keiner vorher gewarnt oder diese Kritik geäußert, es wurde die Möglichkeit des Open-Government-Partnership-Programms nicht benutzt, bei der Verbändeanhö-rung gab es einen Verband. Und auch in anderen Situationen haben wir schon einmal darauf hingewiesen, dass es eigentlich diese Grundarchitektur bräuchte.

Und auch die zentrale Biometrie-Datenbank, dieses Vorhaben, dieser Zugriff war auch schon damals abzulehnen. Ich möchte aber jetzt hier ein Augenmerk darauf werfen, dass das auch wieder ein Symptom für diesen verfehlten Plan darstellt, für

diese verfehlte Digitalpolitik. Lesen Sie sich die Begründungen für diese Datenbestände durch. Da steht was von „Fax-“ und „Bildqualität“ – das ist natürlich ein Riesenproblem. Also ich möchte noch einmal eindringlich warnen: Lesen Sie jetzt unsere Stellungnahmen mit Zeit und wenn noch Möglichkeiten da sind oder Sie sind eben später gezwungen, sich mit diesem Chaos auseinanderzusetzen, was da entstanden und wildgewachsen ist, mit den Kommunen, die dann selbst eigene Lösungen bauen und draufsetzen müssen. Dann wird es nämlich sehr, sehr viel schwieriger. Und darauf haben wir auch schon bei der Digitalisierung von Familienleistungen hingewiesen.

Eine kurze Bemerkung inhaltlich zu der zentralisierten Speicherung von Lichtbildern und Unterschriften: Keine Erforderlichkeit und keine Verhältnismäßigkeit ist dabei gegeben. Es ist ganz wichtig darauf hinzuweisen, noch einmal das wurde auch schon gesagt, aber man kann es nicht genug unterstreichen: Es ist ein eigener Datenbestand, der begründet werden muss. Zentralisierung ist kein Bequemlichkeitsfeature, sondern im Gegenteil: Dezentralisierung ist ein demokratietheoretisches Sicherheitsfeature, was sich auch technisch abbilden muss. Da kann man jetzt nicht sagen: „Ah, das können die eh schon, jetzt sammeln wir das alles einmal zentral“. Das heißt, was hier vorgeschlagen wird, ist ein gefährlicher Workaround.

Aber zurück zum Punkt: Die IT-Sicherheit aktueller Smartphones ist sehr schlecht. Aktuell ist auch für den hier angesprochenen Newscase nur ein einziges zugelassen. Und besonders günstige Geräte sind sowieso notorisch unsicher. Aber was sollen denn viele Menschen dann machen? Auch hier verläuft die Digitalisierung wieder entlang der sowieso schon vorhandenen gesellschaftlichen sozioökonomischen Ungleichheiten und Ungerechtigkeiten. Denn auch später werden eher teurere Geräte diese Funktion haben – das ist natürlich nicht gerecht. Und das ist leider wieder eine Quittung für eine insgesamt schlechte IT-Sicherheit in Endgeräten, das ist ein generelles Problem. Trotz diverser Sicherheitsgesetze gibt es bezüglich Smartphones keine Mindeststandards, keine Verantwortlichkeiten oder vielleicht sogar auch Angebot aus der öffentlichen Hand.

Es gibt schon ein paar Stimmen, die vom „Lex Samsung“ reden, weil das einzige Gerät, was das aktuell kann, ist das Gerät im „Optimus-Projekt“, das „ Galaxy S20“. Das ist jetzt gehackt worden, wie es ein Vortrag ankündigt in der renommierten Hackerkonferenz „Blackhead“ – Sie mögen sich dazu anlesen. Das heißt, selbst das einzige Gerät, was das kann, hat sich leider in der Hinsicht damit erledigt. Das ist allerdings alles vermeidbar und keine Naturgewalt. Hinter nahezu jedem Hackerangriff steht immer individuelles oder meistens systemisches Versäumnis. Dazu nur so viel. Sie können später dazu noch Fragen stellen.

Noch zwei kleine Punkte: Bei Personenkontrollen werden wir später aufpassen müssen, dass, wenn ich mich über mein Smartphone identifizieren kann – und dazu muss ich es entsperren – dass da problematische Effekte entstehen, wenn die Polizei eine Identifizierung verlangt, die dann eventuell nur mit dem Smartphone passiert und nur durch ein Entsperren. Da muss man viel darüber nachdenken, wie man das verhindern kann. Genauso die Metadaten, die bei der Benutzung dieser Systeme anfallen, da muss man noch viel Detailarbeit leisten.

Weitere Punkte sind in der Stellungnahme zu finden, die gemeinsam mit dem Chaos Computer Club angefertigt ist und die Ihnen auch allen vorliegt. Abschließend ceterum censeo: Wenige Werktage waren für uns nur da, um den Gesetzentwurf zu analysieren und eine Stellungnahme abzugeben. Das machen wir immer sehr gern, aber solch absurd kurze Fristen sind leider nicht zu machen, insbesondere für die Zivilgesellschaft, die das alles ehrenamtlich macht. Wir kommen immer gern, aber überdenken Sie bitte Ihre Partizipationsvorstellungen. Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Rehak, vielen Dank. Herr Schleyer noch.

SV **Rudolf Schleyer** (AKDB, München): Sehr geehrte Frau Vorsitzende, meine sehr geehrten Damen und Herren, vielen Dank für die Gelegenheit, zu dem Gesetzentwurf aus der Sicht der kommunalen IT-Dienstleister Stellung zu nehmen. Ich möchte zunächst hervorheben, dass es außerordentlich begrüßenswert ist, dass der Staat seine Funktion als Identitätsgewährleister auch im digitalen Zeitalter beibehält. Wir erleben, dass gerade die Frage der Authentifikation und Identifikation zunehmend auch durch Dienstleister übernommen wird, und ich glaube, dass es ganz

wichtig ist, dass der Staat seiner Funktion auch im digitalen Zeitalter in dieser Hinsicht gerecht wird. Und hier leistet der Gesetzentwurf einen wichtigen Beitrag. Die Idee, die eID-Funktion auf Endgeräte zu übertragen, kommt dem geänderten Nutzerverhalten sehr entgegen. Wenn wir nur daran denken, dass mittlerweile doch in der Breite selbst Bezahlfunktionen auf das Smartphone übertragen werden, so handelt es sich hier um eine gelebte Praxis und um das tagtägliche Erleben der Nutzerinnen und Nutzer.

Dagegen ist die schon länger realisierte Funktion von Smartphones als Lesegerät für die ID-Funktion zum einen nicht in der Breite bekannt, zum anderen aber auch durchaus mit technischen Hürden verbunden und dies schränkt ganz offensichtlich die Nutzung doch in nicht unerheblichem Maße ein. Diese Situation wird durch die Übertragung der eID verbessert, wenngleich man nicht verkennen sollte, dass zumindest bei der Einrichtung diese einmalige Hürde der aktivierten eID sowie der erfolgten Änderung der Transport-PIN schon gelöst sein muss. Im Anschluss ist dann aber natürlich schon mit einem deutlich breiteren Einsatz zu rechnen, auch über die Einsatzzwecke der Verwaltung hinaus. Insbesondere die Ablöse der von mir schon erwähnten alternativen Authentifizierungsmethoden sollte dann angestrebt werden. Ich halte zum Beispiel die Videostreaming-Authentifizierung für außerordentlich problematisch und würde es sehr begrüßen, wenn hier durch diese Funktionalität auch eine Ablösung erfolgen könnte.

Ich glaube auch, dass eine erhöhte Akzeptanz dieser eID-Funktion dann Netzwerkeffekte für eine breitflächigere Nutzung entfalten kann. Dafür ist es allerdings durchaus notwendig, das Vertrauensniveau, wie die ID-Funktion auf den Ausweiskarten, sei es dem Identitätsnachweis, beziehungsweise dem Personalausweis, auch auf das Niveau hoch anzustreben. Auch hier darf nicht verkannt werden, dass das möglicherweise zu hohen technischen Hürden führen kann, was die Nutzbarkeit wieder einschränken könnte. Darauf wäre dann allerdings im Notifizierungsverfahren sehr sorgfältig zu achten.

Auch halte ich eine Begrenzung der Gültigkeitsdauer durchaus für notwendig, um auch dem wachsenden technischen Fortschritt nachzukommen und auch um sicherzustellen, dass jeweils auch die Handys mit den neuesten Betriebssystemen ausgestattet sind, die dann dafür genutzt werden, und man also auch gezwungen ist, auch tatsächlich die jeweils dann aktuellen Hürden zu überspringen, wenn man eine solche Übertragung der eID-Funktion auf das Handy vornimmt.

Ich möchte noch kurz zum Änderungsantrag der Fraktionen CDU/CSU und SPD eingehen, der es den Ländern ermöglichen soll, eigene zentrale Passregister einzurichten, aus denen dann im automatisierten Verfahren Lichtbild und Unterschrift extrahiert werden können: Ich darf daran erinnern, dass bereits seit dem Jahr 2017 diese Befugnis existiert, allerdings auf der Ebene der lokalen Pass- und Ausweisregister. Die technische Umsetzung hat bis heute nicht stattgefunden. Und deshalb glaube ich, dass die Möglichkeit, dies mit zentralen Landesregistern zu lösen, zu begrüßen ist. Ich darf dabei auf die durchaus positiven Erfahrungen mit den Landesmelderegistern verweisen, die zu einer sehr hohen Verfügbarkeit der entsprechenden Melderegisterdaten geführt haben. Wir können auch darauf verweisen, dass in den Ländern, in denen es diese zentralen Melderegister gibt, tatsächlich auch die Auskunftsqualität der Anfragen deutlich höher ist. Ich glaube auch, dass neben der sehr hohen Verfügbarkeit der Register die IT-Sicherheit tatsächlich zunimmt, weil wir eine zentrale Benutzer- und Rechtesteuerung bei einer Stelle erreichen können. Wir können die vorhandenen Infrastrukturen in einer analogen Anwendung der Struktur der Landesmelderegister nutzen und wir haben auch die Situation, dass wir nur eine einmalige Investition für die Schaffung solcher Register pro Bundesland benötigen – im Gegensatz zu jeweils lokal notwendigen Investitionen, sowohl in Infrastruktur als auch vor allem in die IT-Sicherheit.

Wir können außerdem sicherstellen, dass die lokalen Register weiterhin gegen den Zugriff von außen abgeschottet bleiben, weil sie diesen Zugriff nicht ermöglichen müssen, während wir bei den zentralen Registern entsprechende technische Vorkehrungen treffen können, die wir auch heute schon bei den Melderegistern kennen oder auch zum Beispiel bei den zentralen Personenstandsregistern.

Wenn ich nur daran erinnere, dass wir vor der Mammutaufgabe stehen, bis zum 19. Januar 2033 beispielsweise rund 40 Millionen Fahrerlaubnisse

umzutauschen, dann werden diese Register eine besondere Bedeutung auch im E-Government erlangen, denn durch eine solche Verfügbarkeit von Bild und Unterschrift können wir einen vollständig digitalisierten Prozess des Führerscheinumtausches dann auch realisieren und müssen dann nur noch den allerletzten Schritt, nämlich den des tatsächlichen Eintausches des alten Führerscheines gegen den Kartenführerschein über eine Lösung mit beispielsweise der Post realisieren, was heute nicht möglich ist, weil tatsächlich Bild und Unterschrift nicht für solche Prozesse verfügbar sind.

Zusammenfassend glaube ich, dass wir auch mit diesem Änderungsantrag einen deutlichen Gewinn erreichen könnten für verschiedene Anwendungen im E-Government. Und insgesamt glaube ich, dass der Gesetzentwurf einen wichtigen Beitrag zur Förderung der Nutzung der elektronischen Identität mit sich bringen könnte. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Schleyer, vielen Dank. Wir kommen jetzt zur Fragerunde und beginnen mit Herrn Oster.

BE Abg. **Josef Oster** (CDU/CSU): Frau Vorsitzende, meine sehr verehrten Damen und Herren, ich möchte mich zunächst einmal bei den Gutachtern herzlich bedanken für die kurzfristige Bereitschaft, hier für uns als Experten zur Verfügung zu stehen – das ist tatsächlich sportlich gewesen und deshalb mein herzliches Dankeschön, dass Sie dennoch dieser Aufgabe nachgekommen sind. Das hat natürlich seine Begründung: Unser Ziel ist und bleibt, diesen Gesetzentwurf auch zügig zu verabschieden, weil er eben ein wichtiger Baustein in unseren Digitalisierungsbemühungen ist. Und das klare Ziel ist, diesen Gesetzentwurf auf jeden Fall in dieser Wahlperiode zu verabschieden und die Stichworte „Sicherheit“ und „Vertrauen in die Technologie“ spielen dabei natürlich eine ganz besonders wichtige Rolle. Deshalb hatten wir ja vor wenigen Tagen ein erweitertes Berichterstattergespräch und haben jetzt heute auch diese Anhörung. Und ich glaube, auch nach den Äußerungen von heute sind wir da auf einem guten und sinnvollen Weg.

Ich habe eine Frage an Professor Margraf und eine Frage an Herrn Schleyer. An Herrn Professor Margraf die Frage: Sie haben das kurz angerissen, aber unser Ziel ist es ja, mit diesem Baustein der Digitalisierung, mit der eID, die Akzeptanz dieser Angebote möglichst rasch auch zu befördern, sowohl die öffentlichen Angebote, als auch die Angebote der Privatwirtschaft. Vielleicht können Sie noch einmal etwas dazu sagen, ob die gewählte Technologie, die wir hier jetzt ins Auge gefasst haben, dazu geeignet ist, möglichst in einem überschaubaren Zeitraum auch eine breite Marktabdeckung für diese Angebote zu erreichen. Das ist die Frage an Herrn Professor Margraf.

Und die Frage an Herrn Schleyer: Wir diskutieren ja, das ist ja hier auch angeklungen, insbesondere, wenn es um die Lichtbilddatei geht, um die Frage der Datensicherheit. Das ist natürlich eine sehr relevante und wichtige Frage. Jetzt war ich selbst über viele Jahre hinweg Bürgermeister einer relativ kleinen Kommune und weiß, mit welchen Herausforderungen gerade die kleineren Kommunen konfrontiert sind, die Datensicherheit, die immer steigenden Anforderungen auch zu gewährleisten. Deshalb können Sie das vielleicht noch einmal etwas intensiver ausführen, wie Sie das aus dem Blickwinkel der Kommunen bewerten: Ist es tatsächlich sicherer, wenn 5.500 einzelne Kommunen den Datenschutz zu gewährleisten haben? Oder ist die Variante mit 16 Datenbanken auf Bundesländerebene dann nicht doch wesentlich sicherer? Vielleicht können Sie das noch einmal etwas erläutern. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Oster, vielen Dank. Dann käme jetzt Herr Schulz.

Abg. **Uwe Schulz** (AfD): Da die Bundesregierung heute nicht befragt wird, sondern Sachverständige, würde ich meine ersten Fragen gern an Herrn Rehak richten, weil ich glaube, der kann sie beantworten. Herr Rehak, um die eID-Lösung nutzen zu können, benötigt ein Smartphone ja eine eingebettete Sicherheitsarchitektur, die bis zum Niveau substanziell der eIDAS-Verordnung (electronic IDentification, Authentication and trust Services-Verordnung) reichen muss. Welche konkreten Kenntnisse konnten nach Ihrem Wissen in Bezug auf diese Sicherheitsanforderungen gewonnen werden? Und haben Sie Kenntnis, wie viele und welche Endgeräte, also Smartphones und Tablets, die hohen Anforderungen des BSI an Systeme zu elektronischen Identifizierung heute erfüllen? Und gibt es eine Art Gerätekompass?

Und meine zweite Frage geht auch an Sie. Ich weiß nicht, ob Sie da etwas mitbekommen haben, also

mir ist da nichts bekannt, aber ist Ihnen bekannt, welcher Handy-Hersteller in dem Prozess zur Schaffung des elektronischen Identitätsnachweises eingebunden war oder ob überhaupt einer eingebunden war. Das waren meine ersten beiden Fragen. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann Herr Lindh.

BE Abg. **Helge Lindh** (SPD): Vielen Dank Frau Vorsitzende. Auch ich schließe mich dem Dank an die Sachverständigen an und zum Zauber einer Anhörung gehört ja auch, wenn man nicht einfach nur bestätigt wissen will, was man schon weiß, sondern dass man auch Resonanz gibt auf das, was gesagt wurde. Deshalb meine ersten drei Vorbemerkungen, bevor ich zu meinen Fragen an Frau Peters komme.

Es ist ja auch berücksichtigenswert, dass Herr Rehak darauf hinwies, dass nicht genügend Zeit für Sachverständige da gewesen wäre – zur Wahrheit der gesamten Geschichte gehört aber auch, dass sehr kurzfristig diese Anhörung erst in Gang gekommen ist und die Gesetzgebung ja auch noch vor Ende der Legislatur erfolgen soll, sodass eine Intentionalität der Kurzfristigkeit, jedenfalls seitens der Regierungsfraktion, nicht unterstellt werden kann. Und der Vollständigkeit halber: Sie hatten auf „Ceterum censeo“ hingewiesen, Cato der Ältere, aber es folgt dann noch etwas: „Carthaginem esse delendam“. Wir wollen aber nicht zerstören, wir wollen ja etwas errichten, also „Carthagiem esse construendam“. Insofern regen wir uns gegenseitig geistig auch an.

Zum Zweiten ist hier auch darauf hingewiesen worden, dass wir den Aspekt der Dezentralisierung als Gewährleistung von Sicherheit und auch Demokratie sehen sollen. Gleichzeitig wurde aber auch deutlich gemacht, dass es eine Überforderung von Kommunen sei. Das heißt, wir müssten klar machen, in welchem Sinne wir Dezentralisierung bewerten, teilweise wurde das auch in derselben Ausführung genannt.

Als Drittes und damit auch schon überleitend auf Frau Dr. Peters, wenn es auch heute nicht so eine Rolle spielt, ist es der kompletten Darlegung des Sachverhaltes dienlich, wenn wir auch sagen, dass in dem Änderungsantrag auch noch ein zweiter Punkt enthalten ist, nämlich die Stärkung der Auskunftsrechte der Ausweisinhaber – auch das sollte man der Vollständigkeit halber, glaube ich, erwähnen.

Nun meine Fragen an Frau Professor Peters: Sie haben sich sehr deutlich auf die Frage des Zieles und der Akzeptanz konzentriert und dabei hervorgestellt, dass dieser Einstieg in die Nutzbarkeit der mobilen Endgeräte ein sinnvoller Auftakt wäre, der aber eines ganzheitlichen Wurfes bedarf. Könnten Sie vielleicht noch einmal präziser deutlich machen, wie Sie sich die folgenden Schritte vorstellen, wie diese erfolgen könnten und aus Ihrer Sicht sollten.

Und zum Zweiten findet sich in Ihrer schriftlichen Stellungnahme der klare Hinweis, dass Sie eine Begrenzung der Gültigkeit auf zwei Jahre befürworten. Im Gesetzentwurf sind ja maximal fünf Jahre benannt, aber im Entschließungsantrag und Verordnung sollen zwei Jahre festgeschrieben werden. Könnten Sie bitte noch einmal präzisieren, warum Sie diese Begrenzung und für wie lange womöglich Sie diese Begrenzung auf zwei Jahre für sinnvoll erachten. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Lindh, vielen Dank. Für die FDP Herr Höferlin, bitte.

BE Abg. **Manuel Höferlin** (FDP): Danke Frau Vorsitzende. Auch von mir herzlichen Dank an die Damen und Herren Sachverständigen für die kurzfristigen Stellungnahmen. Ja, das war kurzfristig, aber der Änderungsantrag kam ja auch „auf den letzten Drücker“ und der hat letztlich diese Anhörung ausgelöst, muss man auch ehrlicherweise sagen. Also jetzt zu sagen, die Opposition hätte kurzfristig eine Anhörung beantragt, dann muss man natürlich sagen, das ist die Reaktion auf den Änderungsantrag, weil eigentlich wissen viele, den Schritt der Evolution der eID- Funktion im Personalausweis sehen wir als Freie Demokraten extrem positiv – das haben wir ja selbst mit unserem Smart-Perso-Antrag einmal gefordert. Insofern freuen wir uns natürlich immer, wenn die Bundesregierung unsere guten Vorschläge aufnimmt und fortführt. Die Wallet-Funktion ist absolut zeitgemäß. Wir könnten uns da noch viel mehr drin vorstellen, weil ich glaube, dass es auch noch viele andere wichtige Dokumente gibt, die man vielleicht zukünftig auf seinem, dann aber sicheren Smartphone mit sich herumtragen kann. Ich konzentriere mich einmal auf den Änderungsantrag, weil das der Auslöser und auch der Punkt

dieser Anhörung für uns war, ansonsten hätten wir dem Gesetz eigentlich zustimmen können – auch, wenn wir uns mehr hätten vorstellen können.

Ich möchte gern an Herrn Professor Kelber zwei Fragen richten: Meiner Ansicht nach hinkt der Vergleich mit den Strukturen zum automatisierten Abruf von Daten aus den Melderegistern schon deshalb, weil es sich bei den biometrischen Fotos, Sie haben es selbst gesagt, um besonders sensible Daten handelt. Außerdem wurden die Protokollierungspflichten für die Zugriffe im automatisierten Verfahren im Meldewesen gerade erst in einem zweiten Meldewesengesetzänderungsgesetz aus dem Januar angepasst. In den automatisierten Verfahren im Meldewesen muss jetzt zum Beispiel zusätzlich protokolliert werden, was der Anlass des Abrufes eines bestimmten Datensatzes war. Deswegen meine Frage an Sie, Sie haben es am Ende Ihres Statements gesagt, da müssten Sicherungsmaßnahmen sein – welche Sicherungsmaßnahmen müssten denn Ihrer Ansicht nach in das Gesetz aufgenommen werden, damit automatisierte Verfahren nicht nur an Meldeabfragen angepasst sind, sondern besonders den schutzbedürftigen Passdaten angepasst werden?

Und die zweite Frage, da haben Sie auch am Ende gesagt: „Es gibt ja Alternativen“. Da meine Nachfrage: Ist die Alternative der Status Quo und dort die Digitalisierung der dezentralen Datenhaltungen oder haben Sie andere Ideen, wie man automatisieren Abruf denn sonst sinnvoll, sicher und datenschutzfreundlich gestalten kann?

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank, Herr Höferlin. Im Zweifel ist natürlich immer die Opposition schuld. Oder Verursacher, sagen wir es einmal so. Frau Pau, bitte.

Abg. **Petra Pau** (DIE LINKE.): Meine Fragen richten sich an Herrn Rehak. Aber vornweg auch ein Dankeschön an alle Sachverständigen, dass Sie sich dieser Aufgabe und Debatte hier gestellt haben. Ich habe Ihre Grundkritik verstanden, die Planlosigkeit und darauf heraufsetzend könnte man eigentlich sagen: „Erst einmal den Plan auf den Tisch. Und dann schauen, mit welchen sinnvollen Dingen setzen wir das Ganze um.“ Das ist offensichtlich von der Mehrheit nicht gewollt, Herr Kollege Oster hat es eben schon gesagt: „Das muss noch in dieser Legislatur sein.“ Ich weiß nicht, ob wir uns nicht dann in sehr schneller Zeit wieder damit beschäftigen müssen, um hier entsprechend zu reparieren. Deswegen möchte ich Ihnen, Herr Rehak, die Möglichkeit geben, uns noch ein paar praktische Hinweise, die in Ihrer Stellungnahme schon angelegt waren, mit auf den Weg zu geben. Es war hier schon die Rede davon, dass es im Moment ein Smartphone geben soll, welches die Anforderungen erfüllt und obendrein, ich las das auch, gerade gehackt wurde. Können Sie uns etwas dazu sagen? Sind nach Ihrer Einschätzung überhaupt Smartphones nach derzeitigem Stand von Recht und Technik überhaupt dauerhaft sicher genug, dass wir also auf diese Lösung an dieser Stelle setzen?

Zweitens haben Sie ja vorhin schon über Anwendungsmöglichkeiten gesprochen und einige angedeutet, die über das, was einem sonst so einfällt, wie Anbahnung eines Geschäftes oder Abschluss eines Vertrages hinausgehen, zum Beispiel die Personenkontrolle: Sie haben Ihren Personalausweis nicht dabei und wollen sich dann über die elektronische Identität entsprechend identifizieren. Sie hatten vorhin schon angedeutet, dass Sie dazu ausführlicher noch darstellen könnten, welche Risiken Sie hier für die Nutzerinnen und Nutzer sehen – auch mit Blick auf die zukünftige Erweiterung der Funktionalität.

Und ich hänge da gleich noch das Stichwort „Metadaten“ dran. Es ist zwar vorgesehen, dass eben diese nicht in der Smartphone-ID enthalten sein sollen. Aber ich sehe das Risiko und frage Sie: „Sehen Sie es auch?“, dass andere auf dem Gerät installierte Apps während dieses Identifizierungsvorganges auf genau diese sensiblen Daten zugreifen? Und sehen Sie überhaupt nach derzeitigem Stand, sowohl was unsere Aufgabe als Gesetzgeber betrifft, was den Regelungsbedarf betrifft, aber natürlich auch technisch, da eine Möglichkeit, die Risiken mindestens zu minimieren – ausschließen würde ich das nach unseren Erfahrungen, die wir alle haben, sowieso nicht.

Vors. **Andrea Lindholz** (CDU/CSU): Dann haben wir noch Herrn von Notz.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Frau Vorsitzende, erst einmal bin ich dem Kollegen Lindh ganz herzlich dankbar, dass er deutlich macht, dass wir es der Opposition zu verdanken haben, dass es eine Anhörung im Deutschen Bundestag gibt, wenn die Große Koalition vorhat, eine zentrale biometrische

Datenbank zu eröffnen. Das stimmt, die GroKo will so etwas ohne Anhörung machen – ich sage einmal geschichtlich und unter allen Gesichtspunkten ziemlich verrückt. Gut, dass wir darüber reden und uns hier treffen auf so einen Nachmittag und einfach einmal darüber sprechen.

Vors. **Andrea Lindholz** (CDU/CSU): Wenn ich mich erinnere, haben alle der Anhörung zugestimmt, das sollte man bei den Ausführungen der Vollständigkeit halber noch mit erwähnen.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Frau Vorsitzende, vielen Dank, dass Sie mich unterbrechen. Aber ich habe mich ausdrücklich auf den Kollegen Lindh bezogen und Sie haben dann noch einmal unterstrichen, dass am Ende immer die Opposition Schuld ist und ich habe Sie bestätigt, Frau Vorsitzende, dass in diesem Fall die Opposition Schuld ist. So ist es. Deswegen sitzen wir hier und wir haben ja viele interessante Sachen gehört, die sonst der Deutsche Bundestag nicht gehört hätte, die hier nicht zu Protokoll gegangen wären – bei einem solchen Hack, wenn ich das einmal sagen darf.

Man könnte unheimlich viel dazu sagen. Aus eigener Anschauung der letzten zwölf Jahre: Alles, was die Bundesregierung im Bereich der IT-Großprojekte angefasst hat, zerfällt zu Staub. Angefangen bei ELENA, da schreckt der Herr Bürger richtig zusammen. Gerade das BMI ist da häufig beteiligt. Und irgendwie lernt man nicht so richtig, was da nicht so gut läuft. „Warum nutzen diese dummen Bürgerinnen und Bürger nicht den ePerso?“ Das versteht man gar nicht. Und ich kann Ihnen sagen, das liegt daran, dass man mit solchen Anhörungen so ignorant umgeht. Deswegen, ich bin wirklich sehr gespannt, wirklich sehr gespannt, was Sie aus dieser Anhörung mitnehmen in die Gesetzesvorlage, um das hier umzusetzen. Denn sonst ist es genau so, wie die Kollegin Pau sagt: Das Ding landet auf jeden Fall vor dem Bundesverfassungsgericht, aber auf jeden Fall wird es überarbeitungsbedürftig werden. Und das Problem, was man hat ist, gerade weil es so ein wichtiges Projekt ist: Wenn es nicht „schwimmt“, fällt Deutschland weiter zurück in der Digitalisierung und das ist schlecht. Deswegen frage ich die Sachverständigen Neumann und Kelber, einfach in zwei Minuten kurz zu sagen, wie man es denn gut machen könnte. Was sind sozusagen die drei Grundvoraussetzungen, die man erfüllen müsste, um hier ein gutes Gesetz zu machen für dieses wichtige Anliegen, was hinter dem Gesetz steht?

Vors. **Andrea Lindholz** (CDU/CSU): Ich hätte noch eine Frage an Herrn Professor Margraf. Ein Punkt, der jetzt zum Schluss auch noch einmal angesprochen wurde, ist die Frage der mobilen Endgeräte, die in der Lage sind, die Vorgaben zu erfüllen. Es wird auch vom „Lex Samsung“ gesprochen. Was glauben Sie, wie schnell sind andere Anbieter in der Lage, entsprechende Geräte anzubieten? Und glauben Sie, dass am Markt auch günstige Endgeräte vorhanden sein werden, die diesen Zweck ebenfalls erfüllen?

Dann kommen wir jetzt zur Antwortrunde, fangen im Alphabet von vorne wieder an und beginnen mit Herrn Professor Kelber.

SV **Prof. Ulrich Kelber** (BfDI, Bonn): Vielen Dank Frau Vorsitzende. Ich hatte zwei Fragen bekommen, von Herrn Höferlin und von Herrn von Notz. Ja, es gibt aus meiner Sicht natürlich erst einmal naheliegend den Vergleich mit der entsprechenden Entwicklung im Meldewesen. Allerdings der entscheidende Unterschied ist tatsächlich schon die Qualität der Daten, es geht insbesondere bei den Lichtbilddaten auch um biometrische Daten. Diese haben einen besonderen Schutzbedarf und müssen dementsprechend gerade auch natürlich bei einer öffentlichen Verwendung auch entsprechende Schutz- oder Sicherungsmaßnahmen bekommen. Da bin ich ja gefragt worden, wie diese Sicherungsmaßnahmen denn aussehen würden, wenn man nicht ohnehin auf die ja eigentlich datenschutzrechtlich notwendigen Verzicht abzielt, keinen doppelten Datenbestand herzustellen. Dort sind natürlich Maßnahmen, wie zum Beispiel eine Protokollierung nötig, die eine entsprechende Nachvollziehbarkeit – wer hat wann was aus welchen Gründen gemacht? – ermöglicht. Man könnte mit automatischen Prüfungen vorgehen – war das ein berechtigter Zugriff? Man könnte die Rollen- und Rechtekonzepte entsprechend bewerkstelligen. Alles das wären zusätzliche Sicherungsmaßnahmen gegen unbefugten Zugriff aus der Behörde selbst oder von inneren Täterstellen. Das sind natürlich noch keine Sicherungsmaßnahmen gegen Angriffe von außen und auch nicht gegen spätere, dann durch diese technischen Vorkehrungen ja leichteren, Erweiterungen der Möglichkeiten. Die Alternative, die ich tatsächlich angeboten hatte, war nicht einfach nur den Status

Quo, sondern den Status Quo-digital gestärkt. Die Kommunen, die ja ohnehin Zugriffsmöglichkeiten auf die Lichtbilder für viele Zwecke anbieten, dass diese Kommunen auch diejenigen sind, die dann mit einer durchaus auch zentral entwickelten Lösung – es wäre auch gut, wenn nicht jeder „selbst strickt“ – natürlich dann diese entsprechenden Angebote machen kann.

Zur zweiten Frage, zur eID selbst, also jetzt nicht zu dieser Erweiterung des Abrufes. Wir hatten Ihnen vorgeschlagen, bereits im Gesetz die kürzere Frist hineinzunehmen und für den Fall, dass es sich als positiv herausstellt, später die gesetzliche Frist dann zu erweitern. Wir brauchen die Regelungen, wenn Daten falsch sind, wenn Geräte nicht mehr in der Verfügungsgewalt sind. Und es wäre natürlich gut, wenn in dem Gesetz auch festgelegt wird, wie hoch die Vertraulichkeitsstufe nach eIDAS zu machen ist. Ein bisschen Angst hat man als Datenschützer, dass später mit der Bequemlichkeit auch ein Absenken der Vertraulichkeitsstufe erfolgen würde – das wäre ein großer Verlust für die Sicherheit und damit für die dauerhafte Akzeptanz der eID.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Kelber, vielen Dank. Herr Professor Margraf.

SV **Prof. Dr. Marian Margraf** (Freie Universität Berlin): Ich habe zwei Fragen bekommen. Die erste Frage bezog sich darauf, ob die jetzt geplante umzusetzende Technik tatsächlich zu einer breiten Marktabdeckung führt. Ich denke, da gibt es eben immer so zwei Sachen, die man beachten muss: Auf der einen Seite muss es natürlich auch Angebote geben für sichere elektronische Identitäten. Und ich denke, dass das im Rahmen des Onlinezugangsgesetzes, in dem ja geplant ist, insbesondere die Verwaltung stark zu digitalisieren und dabei auf jeden Fall sichere Authentifizierungsmechanismen dringend benötigt werden, damit Bürgerinnen und Bürger sich eben ausweisen können und sagen können: „Ich bin beispielsweise Marian Margraf.“ Das ist das eine – das wird kommen. Und natürlich folgt die Idee, jetzt das Mobiltelefon zu nutzen für eine sichere Authentifizierung, ja dem Trend, Karten, also auch Sicherheitskarten, auf das Smartphone zu bringen, wie zum Beispiel Kreditkarten oder EC-Karten über ApplePay oder GooglePay, was ja schon passiert. Also das ist etwas, was sich, glaube ich, Bürgerinnen und Bürger wünschen, womit sie sich dann auch zukünftig authentisieren können und die Zeit, sage ich einmal, auch bei aller Kritik an der Onlineausweisfunktion, die ja vor elf Jahren eingeführt wurde, war wahrscheinlich noch gar nicht reif – es gab noch nicht genügend Angebote, wo man die nutzen konnte, aber das wird sich eben mit dem Onlinezugangsgesetz ändern. Und ich denke, dass eben das Aufbringen auf das Mobiltelefon die einzige Chance ist, da auch tatsächlich eine breite Marktabdeckung zu erreichen.

Die zweite Frage war bezüglich mobiler Endgeräte die Sicherheit. Ich stecke in dem Markt der mobilen Endgeräte nicht so richtig drin, weiß aber auch, dass in dem schon angesprochenen Projekt „Optimos“ zumindest ein Samsung-Telefon benutzt wurde, um eine sichere Umsetzung zu erreichen. Ich kenne jetzt den aktuellen Angriff nicht, freue mich, dass ich gleich mehr Informationen dazu bekomme. Wesentlich ist eben die Nutzung eines Secure Elements oder eines Sicherheitselements, in dem eben kryptografische Schlüssel sicher gespeichert werden können. Das Gesetz sagt ja, dass das BSI da beurteilen soll, welche Sicherheitselemente für dieses Ding zumindest als sicher gelten, beispielsweise über Zertifizierungen. Da arbeitet das BSI gerade dran, das besser einschätzen zu können. Deswegen gehe ich davon aus, dass es zukünftig eben mehr Geräte geben wird, wo das verbaute Sicherheitselement als sicher eingestuft wird. Nicht alle Geräte, das war ja auch Ihre Frage, haben ein Sicherheitselement, gerade nicht im unteren Preissegment – die können dann eben dafür nicht genutzt werden. Klar ist das dann immer eine Diskussion, dass man dann eben nur einigermaßen teure Geräte nutzen kann, aber man will die Lösung ja auch sicher umsetzen. Und es gibt ja immer noch die Möglichkeit, den elektronischen Identitätsnachweis über eine Karte, zum Beispiel den Personalausweis zu nutzen, den sowieso die meisten Bürgerinnen und Bürger haben.

Aber eben nicht nur die Sicherheit des Secure Elements muss umgesetzt sein, sondern auch das Betriebssystem des Smartphones muss eben sicher sein, weil sich Sicherheitslücken, die sich da ergeben, auch auf den elektronischen Identitätsnachweis auswirken können. Keine Lösung kann zu einhundert Prozent sicher sein, es kann eben immer zu Sicherheitslücken kommen. Aber um das Sicherheitsrisiko zu minimieren, sollte man ein

Schwachstellenmanagement aufbauen, worüber man frühzeitig Informationen bekommt, welche Geräte weiterhin sicher sind, beziehungsweise unsicher werden und kann dann abschätzen, was das für Auswirkungen hat, um dann entsprechende Gegenmaßnahmen einleiten zu können. Das ist das übliche Vorgehen, was man ja heute für IT-Infrastrukturen sowieso machen sollte. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Herr Neumann.

SV **Linus Neumann** (CCC, Berlin): Ich beantworte die Frage von Herrn von Notz: „Wie macht man es besser?“ Ich denke, die bezieht sich nicht auf die Biometrie-Datenbanken, denn das ist relativ einfach: Die lässt man einfach weg. Bei der eID muss man sehen, es handelt sich ja ohnehin hier um einen deutschen Alleingang. Und Identifizierung ist oft gar nicht unbedingt das, was man eigentlich braucht. Was wir in einer digitalen Zukunft viel häufiger benutzen möchten, wäre zum Beispiel eine Signaturfunktion, wäre zum Beispiel eine Verschlüsselungsfunktion und nicht notwendigerweise nur der Nachweis einer Identität, sondern der Nachweis von spezifischen Befähigungen. Also beispielsweise, dass Sie eine Fahrerlaubnis haben, ohne gleichzeitig noch Ihre Adresse und Ihr Geburtsdatum verraten zu müssen. Auf die Idee eines Impfnachweises will ich Sie ausdrücklich gar nicht erst bringen, aber es sollte Ihnen einleuchten, dass sich sehr viel mehr mit den Methoden der Signatur, mit den Methoden der Verschlüsselung und der Methode, spezifische Erlaubnisse nachzuweisen, in eine spannende digitale Zukunft entwickeln könnte, wo auch sehr viel mehr ermöglicht wird. Dann wäre eben die Kreditkarte potenziell auch nur noch eine weitere Funktion eines Secure Elements, wie sie auch heute schon zur Anwendung kommt und auch da verrate ich ja nicht meine Adresse bei der Bezahlung. All das muss natürlich verständlich sein für die Bürgerinnen und Bürger und deswegen ist es so wichtig, damit zu beginnen, dass man sich erst einmal überlegt: Was brauchen wir eigentlich? Und das ist eben nicht irgendwas mit Handy, sondern das sind konkrete Anwendungsfälle im digitalen Leben der Bürgerinnen und Bürger. Das wäre möglich – man braucht dafür natürlich eine einheitliche, sichere Infrastruktur mittels Secure Element, das ist aber am Ende auch nur eine eingebaute smart card ins Telefon, um das Schlüsselmaterial gegen Diebstahl zu schützen. Damit ist aber das Bedrohungsszenario noch lange nicht erledigt, weil sich natürlich sehr viele Möglichkeiten bieten durch Schwachstellen auf dem Telefon, zum Beispiel an die PINs zu kommen. Da kann ich auch an eine Demonstration des CCC erinnern bei der Einführung der ersten eID, bei der eben mit einfachen Keylogger-Methoden dann die PIN für die eID extrahiert wurde. Und das ist dann quasi etwas, was bei der reinen Betrachtung einer secure empalte häufig so ein bisschen out of scope gesehen wird. Jetzt irgendetwas zu erfinden, was sich an der technischen Realität da draußen vorbei orientiert, sehe ich da tatsächlich nicht zielführend.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Frau Peters, bitte.

SV **Prof. Dr. Isabell Peters** (HSVN, Hannover): Danke. Ich habe zwei Fragen bekommen. Die eine Frage richtet sich nach dem ganzheitlichen Entwurf, sofern es den geben kann. Meine Empfehlung wäre dafür, entweder auf die vorhandene eID zu setzen und zu schauen, kann ich Partner aus der Wirtschaft gewinnen, an diesem Vorhaben mitzuwirken und diese ins Boot zu holen. Die zweite Alternative wäre, mittelfristig eine ganz andere Lösung zu suchen und von der eID sukzessive abzurücken. Die Bundesregierung hat dazu den Innovationswettbewerb „Sichere nationale Identitäten“ ausgerufen. Das wäre eine Möglichkeit, eine Lösung, die unter Federführung des Bundeswirtschaftsministeriums erarbeitet wird und die darauf abzielt, Akteure aus der Wirtschaft einzubinden, um eine Identifizierungslösung zu erarbeiten, die von Verwaltung und Wirtschaft genutzt wird.

Die zweite Frage richtete sich auf diesen Zeitraum der Begrenzung der Gültigkeitsdauer. In dem einen Entwurf wird von über fünf Jahren gesprochen, in dem anderen wird auf zwei Jahre abgestellt. Ich halte diese zwei Jahre insofern für einen geeigneten Zeitraum, als dass das der Mindestzeitraum ist, wo marktübliche Smartphone-Hersteller Patches gewährleisten und ich würde mich da eher am Minimum und nicht am Maximum orientieren, um nicht Gefahr zu laufen, dass Identitätsnachweise auf dem Smartphone gespeichert sind und der Hersteller diese Patches nicht mehr gewährleistet und entsprechend der Nutzer keine Updates mehr

fahren kann, um nicht Gefahr zu laufen, dass Identifizierungsnachweise außerhalb der vom Hersteller garantierten Laufzeit, in der Updates vorgenommen werden, auf dem Smartphone gespeichert werden.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank, Frau Peters. Herr Rehak.

SV **Rainer Rehak** (FIfF, Berlin): Vielen Dank für die Fragen. Es freut mich sehr, dass wir so tief in die Materie auch einsteigen können. Erstens die Frage zum Gerätkompass. Also die Frage war ja mit dem „substanziell, ist das überhaupt möglich“ oder so. Aber das electronic Secure Element, dieser eSE-Chip, der ist nach Common Criteria mit ERL5+ zertifiziert. Damit ist es substanziell möglich. Das war jetzt eine sehr detaillierte Antwort, aber das heißt im Endeffekt: Ja, das kann funktionieren, das kann es geben. Und Gerätekompass? Naja, aktuell gibt es einen Handyhersteller, das habe ich ja vorhin so ein bisschen angerissen, das sind die Handys der Modellreihe „Galaxy S20“, die aber auch nicht allein auf die Idee gekommen sind, das irgendwie umzusetzen, sondern das ist im Rahmen dieses „Optimus 2.0“-Projektes des Wirtschaftsministeriums entstanden. Es gibt auch andere Hersteller, auch große, die da Interesse zeigen würden, aber, wie ich schon angerissen habe, das sind eher die hochpreisigen Geräte, die das eventuell dann später haben könnten. Und dann gibt es wahrscheinlich auch so etwas wie einen Gerätekompass.

Der Angriff, der hier die Runde machte, der heißt übrigens Chip-Chop. Wer da jetzt ein bisschen mehr recherchieren möchte – soviel dazu.

Dann war die Frage nach den praktischen Hinweisen, sind denn Smartphones dauerhaft sicher genug? Man darf hier nicht den Fehler machen zu sagen, weil die Aufgabe so groß ist, fangen wir lieber gar nicht erst an. Dann landen wir nämlich in der Ecke, in der wir bei vielen Innovationen schon sind, in der wir gar nicht sein wollen. Wir sind ja auch, gerade hier die kritische „Technikriege“, wir wollen ja nicht keine Technik, sondern wir wollen es ja gut und richtig machen. Und man kann ja auch parallel die Vorhaben, die jetzt hier in aller politischen Realität und zeitlichen Dringlichkeit gemacht werden müssen, verfolgen und gleichzeitig aber schon einmal Projektgruppen aufsetzen, die das nachverfolgen und perspektivisch aufziehen und dann gucken, wie können die aktuellen Projekte da noch mit reinpassen. Man kann das Eine tun, ohne das andere zu lassen. Man muss immer sehen: So eine IT-Landschaft ist natürlich ein Tanker und wenn man da am Rad dreht, sieht man zwei oder drei Jahre später erst, dass sich etwas bewegt. Aber wir müssen ja woanders hin, als wir gerade sind. Das heißt, wir brauchen eben eine langfristige Strategie und das heißt eben, nicht wieder T-Systems und SAP zu fragen, was die denn machen würden. Obwohl man sagen muss, bei der Corona-Warn-App haben sie jetzt nicht alles falsch gemacht, also Ehre wem Ehre gebührt. Aber der erste Schritte wäre, welche offenen Standards gibt es denn, um das, was unsere Strategie irgendwie befeuern und unterstützen kann, um die zusammenzusammeln und damit zu hantieren. Dass nicht wieder so etwas wie das „beA-Destaster“ entsteht, wo da für 36 Millionen EUR selbst etwas gebaut wird, obwohl es offene Standards gäbe, die genau das gekonnt hätten. Und dann die Frage zu stellen: „Wie ist das interoperabel mit anderen Projekten?“ und so weiter, „wie kann das mit freier Software sein?“, damit dann diese Infrastruktur auch als öffentliches Gut und nicht als geschlossenes System behandelt werden kann. Das könnte man praktisch schon auf den Weg bringen, in die Richtung zu blicken. Das kann man machen Schritt für Schritt. Und ich glaube, die Expertise ist ja auch da, also es ist ja nicht so, dass wir das irgendwie als Gesellschaft nicht könnten.

Die nächste Frage ging in Richtung Personenkontrolle, was ist da die Gefahr? Ich möchte ein realistisches Szenario kurz umschreiben: Natürlich wird die Identifikation mit dem Smartphone freiwillig sein und das werden natürlich auch alle weiter betonen. Aber wir kennen, glaube ich, also zumindest aus den Medien- - also ich kenne das aus eigener Erfahrung nicht, weil ich ein teutonisch aussehender Deutscher bin, aber viele Menschen auf die das nicht zutrifft haben die Erfahrung, dass man da kurz in eine Personenkontrolle kommt und wenn man gerade den Ausweis eben nicht mithat, dann kann man natürlich mit auf die Wache kommen. Oder man kann das eben auch ganz schnell regeln, dann entsperrt man kurz das Telefon und der Kartenleser ist halt leider im Polizeiauto, deswegen muss man kurz das Telefon aus der Hand geben und dann merkt man, wie die Freiwilligkeit halt dahin ist mit dieser einfach

praktischen Situation. Und solche Sachen muss man eben mitdenken und die dann aber auch rechtlich ganz klar ausschließen, explizit, dass da auch niemand Kreatives im Dienst auf die Idee kommt, da irgend so etwas zu formulieren. Solche Sachen kann man da auch mitdenken. Ich will das jetzt nicht weiter ausführen, aber dieses Szenario wird es viel geben und das wird marginalisierte Gruppen betreffen.

Dann zu den Metadaten und wer wird auf diese sensiblen Daten zugreifen? Naja, das ist natürlich eine Frage der IT-Sicherheit, aber es ist auch eine Frage des Datenschutzes. Das heißt, für all diese Projekte müssen auch Datenschutzfolgenabschätzungen erstellt werden, die die Betroffenenfragen und so weiter betrachten, die auch das gesamte System in den Blick nehmen. Und dann muss man eben auch sehen, dass auch die Smartphone-Betriebssysteme, wie es bei der Antwort vorher auch benannt worden ist, die müssen auch mit in den Blick genommen werden. Das heißt manchmal eben auch, wenn man das sicher machen will, das Geschäftsgeheimnis dahinter zurückzustellen, dass wir so eine Art von sicherer Infrastruktur haben wollen. Nur als Beispiel: Bei der Corona-Warn-App hat man Apple und Google vertraut, dass die ihre Arbeit schon richtig machen. Jetzt kam vor ein paar Wochen raus, die Betriebssysteme selbst, also das Google-Betriebssystem und das Apple-Betriebssystem, die schreiben bestimmte dieser IDs in die Log-Dateien raus. Und das wurde nicht erkannt, weil man gesagt hat, wir vertrauen einfach den Anbietern, diesen beiden in dem Falle, die werden das schon richtig machen. Haben die aber nicht. Das heißt, man kann das schon sicher machen, dann muss man aber auch konsequent sagen, was die Priorität ist. Ist unsere Priorität, das gut zu machen? Oder ist unsere Priorität, Unternehmen zu vertrauen, die ein eigenes Interesse haben? Das ist auch okay. Aber deswegen sind Sie ja auch hier in der Politik da, die Interessen abzuwägen. Und ich weiß, welche Abwägung ich als Bürger, der so ein System haben möchte, treffen würde.

Ganz zum Abschluss noch eine Frage, die nicht mir gestellt worden ist, aber dezentral versus zentral: IT-Sicherheit ist nie absolut. IT-Sicherheit ist immer eine Frage der Relation, das heißt Aufwand und Nutzen. Wenn man jetzt sagt, na ist es nicht viel besser, das ganze zentral zu sichern, dann kann man es sehr gut absichern? Ja, dann erhöht sich aber eben auch der Nutzen und damit auch die Verlockung. Das heißt, aus Datenschutzsicht ist natürlich sozusagen eine Dezentralisierung auch eine Verringerung der Angriffsfläche. Das heißt, Angriffe skalieren auch nicht mehr, das ist auch ein IT-Sicherheitsplus an der Stelle und ein Datenschutzplus auch. Nur hinsichtlich Erforderlichkeit und Verhältnismäßigkeit muss man eben abwägen. Vielen Dank für Ihre vielleicht etwas strapazierte Aufmerksamkeit.

Vors. **Andrea Lindholz** (CDU/CSU): Wir liegen ja gut in der Zeit, so passt ja alles. Herr Schleyer noch.

SV **Rudolf Schleyer** (AKDB, München): Danke schön. Ich habe eine Frage gestellt bekommen zur IT-Sicherheit bei insbesondere kleineren Kommunen. Ich möchte vorweg schicken, die Frage, ob der Zugriff von Sicherheitsbehörden oder durch andere autorisierte Stellen oder auch im Rahmen von Onlinediensten durch die Bürger selbst auf diese gespeicherten Bilder und Unterschriften erfolgt, diese Frage stellt sich ja nicht, weil sie bereits heute durch geltendes Recht im § 22a des Passgesetzes beziehungsweise § 25 des Personalausweisgesetzes normiert ist. Wir gehen also von einem geltenden Rechtszustand aus und die Frage, die sich jetzt stellt, ist ja im Rahmen dieses Änderungsantrages: Macht es Sinn, diesen Zugriff weiterhin auf die dezentralen Datenbestände zuzulassen oder zu ermöglichen, oder ist es besser, hier die Möglichkeit zu schaffen, einen zentralen Zugriff zu ermöglichen? Die Situation ist nun so: Ich kann, glaube ich, die Situation in Bayern sehr gut beurteilen, aber auch im restlichen Bundesgebiet. Bayern ist insofern ein gewisser Sonderfall, gemeinsam mit Baden-Württemberg, als dass wir hier sehr viele, sehr kleine Kommunen haben, allein in Bayern hätten wir circa 1.380 Personalausweis- und Passbehörden, die hier entsprechend sich ausrüsten müssten. Wenn wir den Zustand betrachten, dann ist es ja schon ein Unterschied, ob diese Kommune den Zugriff auf ihre Bestände ermöglichen muss und entsprechend absichern muss, auch die entsprechenden Zugriffsprotokollierungen durchführen muss, die Rollen- und Rechtekonzepte pflegen muss oder ob die Kommunen tatsächlich an eine dezidierte Stelle diese Daten liefern und an dieser Stelle dann diese IT-Sicherheitsvorkehrungen wahrgenommen

werden müssen. Ich gebe Herrn Rehak Recht, das ist letztendlich eine Abwägung von verschiedenen Bedrohungsszenarien beziehungsweise auch der zu erwartenden Störwirkbreite. Natürlich ist es richtig, dass es weniger Schaden anrichtet, wenn beispielsweise der Zugriff auf ein Pass- oder Ausweisregister einer Kommune mit 5.000 Einwohnern erfolgt, als wenn tatsächlich ein erfolgreicher Angriff auf ein zentrales Landesregister erfolgen sollte. Dennoch ist es so, dass natürlich auch da die Größe durchaus unterschiedlich sein kann und die Aufwände, um das zu gewährleisten, in der Fläche natürlich entsprechend hoch skalieren, heißt mit anderen Worten: Wenn wir die gesamten 5.500 Personalausweis- und Passbehörden in Deutschland betrachten und von ihnen erwarten, dass das selbe Schutzniveau erreicht wird, haben wir natürlich deutlich höhere Kosten, als wenn wir eine zentrale Speicherung jeweils pro Land entsprechend absichern wollten. Natürlich federn die IT-Dienstleister in den Ländern dies teilweise ab, wir haben nicht die Situation, dass alle Kommunen sich vollständig selbst auf eigene IT-Systeme verlassen, aber auch wieder der Blick nach Bayern: Von den 1.380 Personalausweis- und Passbehörden sind nur knapp die Hälfte mit ihrer IT in einem Rechenzentrum. Die andere Hälfte bewerkstelligt dies nach wie vor autonom vor Ort, ich könnte jetzt sagen, „im Keller des Rathauses“. Und die entsprechenden Vorkehrungen zu treffen, ist für diese Kommunen heute schon eine erhebliche Herausforderung. Und je sensibler die Daten werden, und da sind wir uns ja nun alle einig, dass es sich bei den biometrischen Daten um hochsensible handelt, umso schwieriger wird das dann auch durch diese Kommunen zu leisten.

Bei den Melderegistern, um diese Parallele dann doch herzustellen, handelt es sich natürlich schon um weniger sensible Daten, aber auch hier haben wir beispielsweise in den zentralen Registern Sperrvermerke zu berücksichtigen, wir haben Bedrohungen von Leib und Leben zu berücksichtigen – all das sind hochsensible Daten in den zentralen Melderegistern, die hier abgesichert werden. Wir haben beispielsweise auch die Verpflichtung zur logischen Trennung der Datenbestände nach Meldebehörden, die wir entsprechend durchführen und derartige Vorschriften wären dann auch selbstverständlich im Rahmen der Gesetzgebungsverfahren für die zentralen Landesregister an die jeweiligen Landesgesetzgeber als Forderung zu erheben. Ich glaube, dass wir mit den Systematiken der Protokollierung der Zugriffe und der entsprechenden Zugriffs- und Rollenkonzepte tatsächlich die Expertise bei den Betreibern der heutigen zentralen Meldedatenbestände haben, um das auch sicher für die entsprechenden Register für die biometrischen Daten und die Unterschriften sicherzustellen.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank, damit ist die erste Fragerunde abgeschlossen. Wir haben noch 35 Minuten, das heißt, wir kommen noch zu einer weiteren Fragerunde im üblichen Modus. Ich habe zwei Fragen an Herrn Professor Margraf: Einmal diese Gültigkeitsdauer von zwei oder fünf Jahren – wie bewerten Sie das? Denn zwei Jahre scheinen ja durchaus sinnvoll zu sein aus meiner Sicht.

Und eine Verständnisfrage zu dem, was Herr Rehak gesagt hat: Egal, wie man jetzt so einen elektronischen Identitätsnachweis ausgestaltet, in dem Moment, wo sich das auf meinem Smartphone befindet – ich komme jetzt in eine Personenkontrolle und mich kontrolliert die Person XYZ und will wissen, wer ich bin und ich zeige meinen elektronischen Identitätsnachweis, egal, wie der ausgestaltet worden ist. In dem Moment, wo er sich auf meinem Endgerät befindet, ist es immer nur möglich, wenn dann das gesamte Gerät entsperrt wird – einfach einmal technisch gefragt – oder könnte man das grundsätzlich auch so ausgestalten, wie etwa bei meiner Kamera-App, die ich benutzen kann, ohne das komplette Gerät zu entsperren. Das kann ich ja mit dem Smartphone auch machen, ohne gleich das ganze Gerät zu entsperren. Oder funktioniert das mit der eID immer nur, egal wie man es ausgestaltet, dass das Gerät entsperrt werden muss? Wenn das so ist, dann ist das ein Dauerproblem, dann käme ich aber nur zu dem Ergebnis: Ich werde nie einen elektronischen Identitätsnachweis auf meinem Gerät, egal in welcher Form, so hinbringen, dass ich nicht mein Gerät entsperren muss. Das heißt, ich muss meinem Gegenüber dann vertrauen, falls ich ihm das Gerät in die Hand drücke, dass er nicht weiter auf meinem Handy nachschaut, weil das dürfte er nicht. Oder könnte man es rein theoretisch auch so programmieren, technisch so ausgestalten, dass man so etwas tatsächlich vermeiden könnte? Das ist einfach einmal eine Frage, die mich jetzt interessiert.

Dann kommen wir jetzt zu Herrn Oster.

BE Abg. **Josef Oster** (CDU/CSU): Ich will vielleicht noch einmal einen Hinweis geben, da wir jetzt viel über Datenbanken auf Bundesländerebene gesprochen haben. Da ist es mir doch noch einmal wichtig zu verdeutlichen: Das ist ja keine Initiative oder kein Gedanke, den sich irgendein Ministerialbeamter ausgedacht hat, sondern das war ja der ausdrückliche Wunsch gleich mehrerer Bundesländer, diese Möglichkeit jetzt zu schaffen. Also diese Initiative kommt ja gar nicht aus Berlin, sondern sie kommt aus den Bundesländern heraus – das sollte nicht ganz vergessen werden.

Ich habe noch eine Frage an Herrn Professor Margraf: Jetzt sind wir ja zugegebenermaßen nicht die Ersten, die mit elektronischen Identifikationslösungen an den Markt gehen. Wie bewerten Sie unsere Lösung, die wir jetzt hier vorhaben, was Nutzerfreundlichkeit und Datenschutz anbelangt, im Vergleich zu anderen Ländern, die solche Lösungen schon haben? Vielleicht können Sie dazu noch etwas sagen.

Und noch eine Frage an Herrn Schleyer: Herr Schleyer, das Ganze ist ja ein elementarer Baustein auch im Zusammenhang mit dem OZG (Onlinezugangsgesetz). Und unser Ziel ist es ja, mit dieser eID nicht nur das OZG in die Breite zu tragen, sondern möglichst auch private Anbieter mit zu gewinnen – nur dann kann es ein Erfolg werden, ich glaube, da sind wir uns alle einig. Auch da hätte ich gern eine Einschätzung von Ihnen gehört, wie Sie das von den Chancen her einordnen, dass dieses Ziel, sowohl in Bezug auf OZG als auch auf die Privatwirtschaft gelingen kann.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann wäre jetzt Herr Schulz an der Reihe. Hat die AfD noch Fragen?

Abg. **Uwe Schulz** (AfD): Nein, keine Fragen mehr, vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Danach Herr Lindh.

BE Abg. **Helge Lindh** (SPD): Vielen Dank. Erst einmal muss ich ja doch dem Ausdruck verleihen, dass ich immer die geistige Frische des Kollegen von Notz sehr schätze, wir aber offensichtlich etwas abweichende Akzentsetzungen in Bezug auf parlamentarische Demokratie vornehmen: Nach meinem Verständnis ist das nicht eine besondere Leistung, sondern gerade Aufgabe der Opposition, zu opponieren und infrage zu stellen, weswegen wir ja auch bei Anhörungen nur ein Quorum von 25 Prozent der Mitglieder des federführenden Ausschusses haben. Insofern wird man nur der Aufgabe gerecht als Opposition, wenn man nachfragt.

Neben diesem Aperçu vielleicht zwei Punkte zur Legendenklärung: Kollege Oster hat das so zurückhaltend genannt und wir waren jetzt sehr stark auf Bayern bezogen. Und wir als SPD-Fraktion haben auch keinen Grund, das BMI unkritisch zu betrachten, sondern machen das ja durchaus immer kritisch – ich möchte nur darauf hinweisen, dass unter anderem eine Stellungnahme des Landes Thüringen vorliegt, im Rahmen des Verfahrens der Beteiligung der Länder in Bezug auf die Verordnung. Und dort ist explizit darauf verwiesen, ich zitiere: „…ein Aufbau zentraler Strukturen ist den Ländern auch in Ermangelung einer Regelung nach § 55 Absatz 2 und 8 Bundesmeldegesetz damit rechtlich nicht möglich…“ – Einschätzung von Thüringen. Und dann wird die Forderung erhoben einer „…seitens der bundeseinheitlichen Umsetzung der PPDAV in den Ländern sicherzustellen und einen länderübergreifenden Datenabruf in der Praxis zu gewährleisen…“ und dann wird im Folgenden sogar auch noch die Forderung erhoben einer Sicherstellung, dass ein Abruf auch bezüglich der Lichtbilder früherer und zwischenzeitlich ungültiger Pässe und Personalausweise möglich sein sollte. Also es gibt durchaus auch diverse Länder, die diese Forderungen erhoben haben, es ist nicht allein Bayern. Das fand ich wichtig, auf dieses Detail hinzuweisen.

Meine Fragen wären jetzt zum einen an Herrn Schleyer noch einmal: Es wurde einerseits in den Stellungnahmen deutlich gemacht, dass es scheinbar kaum Bedarfsfälle gäbe, also relativ wenige automatisierte Abrufe stattfänden. Können Sie das präzisieren, beziehungsweise mögliche Gründe dafür nennen? Weil wir da ja so changieren zwischen mangelndem Interesse, aber auch vielleicht mangelnder technischer Möglichkeit – da bräuchten wir vielleicht noch etwas Erhellung.

Und zum Zweiten ein Punkt, der bisher noch gar nicht zum Tragen kam, an Frau Professor Peters: Sie erwähnen in Ihrer schriftlichen Stellungnahme, dass Sie, bezugnehmend auf die Evaluierung, das Ziel für zu wenig ehrgeizig halten und eine

Steigerung der Identifizierungsvorgänge nicht um 50 Prozent, sondern um 200 Prozent für notwendig halten würden innerhalb von fünf Jahren unter besserer Nutzung von Skalen und Verbundeffekten. Könnten Sie Hinweise geben, wie das umsetzbar und erreichbar wäre?

Vors. **Andrea Lindholz** (CDU/CSU): Herr Lindh vielen Dank. Dann Herr Höferlin.

BE Abg. **Manuel Höferlin** (FDP): Frau Vorsitzende vielen Dank. Vielleicht können die Kollegen Lindh und von Notz im Nachgang zu dieser Sitzung einen Klassenbeitrag zum Thema „Parlamentarische Pflichten und Rechte aus Sicht von Opposition und Koalition“ schreiben – ich wäre bereit, ein kurzes Vorwort zu liefern.

Ich habe zwei Fragen noch einmal an Herrn Professor Kelber: Vielleicht noch einmal einen Schritt zurück zu den Grundlagen und zu den Fragen am Anfang. Wir haben jetzt einiges dazu gehört, dass im Prinzip derzeit das einzige eID-fähige Gerät, mit dem so etwas verbaut werden kann, gerade gehackt wurde. Für zentrale Datenbestände mit biometrischen Daten ergeben sich dann ja noch einmal potenzierte Sicherheitsrisiken, wenn man das nachher auf vielen Geräten bereithält. Welche grundsätzlichen Gefahren ergäben sich denn aus dem Aufbau von den Spiegelpassregistern auf Landesebene? Und welche Begründung bräuchte es für den Aufbau und die Notwendigkeit solcher zentraler Landesstrukturen aus Ihrer Sicht – wenn die sich überhaupt begründen lassen oder wenn es Alternativen gäbe.

Und die zweite Frage. Zum Sicherheitsniveau der eID und der mobilen Endgeräte haben wir jetzt ja einiges gehört und auch zu der Tatsache, dass das eID-Gesetz nichts dazu vorsieht. Welches Vertrauensniveau nach der eIDAS-Verordnung sprechen Sie sich für die eID auf den mobilen Endgeräten aus, beziehungsweise welches Vertrauensniveau wäre denn den bisher getroffenen Sicherheitsvorkehrungen im vorliegenden Gesetzentwurf überhaupt möglich? Herzlichen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Höferlin, vielen Dank. Jetzt kommt dann Frau Pau.

Abg. **Petra Pau** (DIE LINKE.): Wie so oft hat Herr Höferlin meine Fragen mehr oder weniger schon gestellt. Deshalb nur noch einmal eine Nachfrage an Herrn Rehak zum Änderungsantrag: Also ich habe Sie so verstanden, dass Sie, genauso wie ich, eigentlich der Auffassung sind, dass der verzichtbar ist. Aber vielleicht können Sie die Gefahren, die von den dort vorgesehenen Regelungen ausgehen, noch einmal komprimiert aus Ihrer Sicht darstellen.

Vors. **Andrea Lindholz** (CDU/CSU): Und Herr von Notz.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Ich habe nur noch einmal eine Frage zur Biometrie-Datenbank an Herrn Neumann: Biometrie-Datenbank klingt ja irgendwie immer freundlich, sogar „Bio“ irgendwie. Deswegen die Frage: Was bedeutet das eigentlich konkret, eine Biometrie-Datenbank, eine zentrale? Was für Daten gehen da rein? Gab es in dem Bereich in den letzten Jahren Hacks? Was kann man mit Biometrie-Daten so alles machen und vor allen Dingen: Wo liegt der Unterschied zu Passwörtern und ähnlichem – also was ist das besondere Problem bei Biometrie-Daten? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann geht es jetzt im Alphabet rückwärts und wir beginnen mit Herrn Schleyer.

SV **Rudolf Schleyer** (AKDB, München): Die Frage, die mir gestellt wurde, ist, ob wir durch die Möglichkeit, die eID auf das Handy zu bekommen, auch eine gesteigerte Nutzung in den Verwaltungsverfahren oder auch durch private Anbieter zu erwarten hätten. Ich glaube, dass tatsächlich die Frage der Authentifizierung nach wie vor eine Hürde darstellt, die nicht zu unterschätzen ist. Und wenn man diese Hürde kleiner macht und beispielsweise durch die Nutzung des Smartphones dann auch diese Hürde abbaut, dass man dann auch eine verstärkte Inanspruchnahme bekommen wird. Ich kann Ihnen dazu eine Erfahrung mitteilen, die wir im Rahmen der internetbasierten Kfz-Zulassung gemacht haben: Es ist so, dass diese Funktionalität der internetbasierten Kfz-Zulassung nach wie vor bis zum Ausbruch der Pandemie sehr, sehr zurückhaltend in Anspruch genommen wurde. Ein wesentlicher Punkt ist ganz offensichtlich, dass für alle substanziellen Vorgänge, die im Rahmen der i-Kfz-Thematik vorgenommen werden mussten, die Nutzung des Personalausweises obligatorisch ist. Es hat sich auch gezeigt, als die Kfz-Zulassungsstellen dann flächendeckend geschlossen waren, dass sich die Nutzung nicht wesentlich erhöht hat.

Dann kam es zu einer Freigabe an die KfZ-Zulassungsstellen, diese eID-Funktion rauszunehmen und durch Benutzername und Passwort zu ersetzen und eine Kopie des Personalausweises nachzureichen als Authentifizierung. Und tatsächlich von einer Woche auf die andere ist die Nutzung dieses Dienstes um das beinahe Zwanzigfache gestiegen. Das heißt also, die Hürde, sich mit dem neuen Personalausweis mit der eID-Funktion dort auszuweisen, war tatsächlich so hoch, dass selbst bei dem Druck der geschlossenen Kfz-Zulassungsstellen zunächst keine höhere Inanspruchnahme des Onlinedienstes erfolgt ist. Wenn man es also schafft, diese Hürde geringer zu machen, ohne die Sicherheitsanforderungen der Authentifizierung aufzugeben – und das verspricht der Gesetzentwurf durch die Übertragung auf das Smartphone – dann glaube ich sehr wohl, dass auch eine erhöhte Nutzung der Dienste erfolgen wird, die heute noch eine Authentifizierung mit dem neuen Personalausweis erfordern.

Was die privaten Anbieter betrifft, da teile ich allerdings die heute schon mehrfach geäußerte Einschätzung, dass es dazu noch einer erheblichen Kampagne bedarf, beziehungsweise sanften Druckes auch auf insbesondere die Kreditwirtschaft, die von Anfang an seit Einführung der eID-Funktion des neuen Personalausweises sich hier in äußerster Zurückhaltung geübt hat und lieber auf die eigenen Systeme der Authentifizierung gesetzt hat. Und ich glaube schon, dass es ein Angebot wäre insbesondere für die Kreditwirtschaft, nicht mehr auf diese doch etwas teilweise antiquiert anmutenden Authentifizierungssysteme zu setzen, wie zur Postfiliale gehen zu müssen oder irgendwelche fremde Menschen ins Wohnzimmer blicken zu lassen, um sich zu authentifizieren. Insofern: Die Chance besteht hier allemal nach meiner Meinung.

Warum werden die Abrufmöglichkeiten, die heute schon kodifiziert sind, so wenig genutzt? Ganz einfach: Weil es diese nicht gibt. Diese Speicherung, die Zugriffe auf die Pass- und Ausweisbilder sind schlichtweg nicht möglich. Die entsprechenden technischen Voraussetzungen wurden nie normiert, man hat sich darauf nicht einigen können, das heißt, das findet de facto nicht statt und dazu kommt noch eines: Man muss sich vor Augen halten, dass die einschlägigen Vorschriften des Passgesetzes und des Personalausweisgesetzes den automatisierten Abruf durch die Sicherheitsbehörden unter einen ganz wesentlichen Vorbehalt stellen, nämlich dass zum Zeitpunkt des Zugriffs auf das Bild die Pass- und Ausweisbehörden auf andere Weise nicht erreichbar sind. Das heißt also, hier ist schon die Zugriffshürde sehr hoch gelegt, was nicht heißt, dass kein Bedarf bestünde, sondern tatsächlich ist die Frage, welche Voraussetzungen überhaupt zu erfüllen sind, dass dann ein solcher Abruf erfolgen kann. Heute kann der Abruf de facto nicht erfolgen, denn die Pass- und Ausweisbehörden sind dazu gar nicht in der Lage.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Schleyer, vielen Dank. Dann Herr Rehak.

SV **Rainer Rehak** (FIfF, Berlin): Herzlichen Dank. Es ging ja bei der ersten Frage um die Ausgestaltung der eID auf dem Smartphone insgesamt, es ging dabei um diese Personenkontrolle und Entsperrung, das war der Hintergrund der Frage. Diese Kamera ist ein gutes Beispiel, wo man quasi so einen Teilzugriff auf ein Smartphone geben kann – die eID kann man schon auch so bauen. Aber das ist natürlich so eine Frage: Es gibt genug IT-Sicherheitsangriffe, die auch bei gesperrten, eingeschalteten Geräten funktionieren. Dafür verbindet man ein USB-Gerät und dieses sagt, „ich würde dich gern auslesen“, indem es sich als Tastatur ausgibt oder so. Da gibt es also ziemlich viele Angriffsvektoren, die trotz dem, dass das Gerät gesperrt ist, als Angreifer funktionieren, die im Moment aber wenig Rolle spielen, weil keine hoheitlichen Aufgaben damit verbunden sind und ein Angriff deswegen weniger interessant ist. Ich würde aber denken, an dieser Stelle gibt es auch keinen technischen Fix, dass man jetzt einfach sagt, wir wollen mehr IT-Sicherheit und dann geht das schon. Eher würde man so etwas, wenn man so etwas möchte, organisatorisch oder organisational sicherstellen. Das heißt, die Lesegeräte müssen dann halt mobil sein und der Prozess muss ausschließlich durchgeführt werden, ohne dass die Betroffenen ihr Gerät aus der Hand geben müssen. Das ist die einzige Möglichkeit, ansonsten kann das eben nicht gemacht werden. Und das muss dann eben auch organisational in den entsprechenden Behörden auch so kommuniziert werden, dass die gar nicht erst auf die Idee kommen, das selbst zu machen oder dass die sich strafbar machen, wenn sie es selbst machen. Und das ist ja auch nicht neu. Der nPA (neuer elektronischer Personalausweis),

den wir haben, den darf man auch nicht aus der Hand geben, das ist rechtlich so geregelt. Also immer, wenn irgendeine Garderobe sagt, „wir würden den gern als Pfand nehmen“, ist das illegal. Da kann man dann eben sagen: „Ich berufe mich auf das Ausweisgesetz, ich darf den gar nicht aus der Hand geben.“ Und so müsste man das bei der eID auch machen, also in die Richtung müsste man da denken. Wenn man das will.

Der Punkt zwei war: Die Gefahren der zentralisierten Biometrie-Datenbank. Da hat Linus Neumann in seinem Eingangsstatement schon viele Sachen aufgezählt, das wird ja zum Glück hier auch gestreamt und recorded, da lohnt es sich auf alle Fälle noch einmal reinzuhören. Ich will das jetzt nicht so an Beispielen aufziehen, sondern auch einen ein bisschen größeren Hintergrund mit hineinziehen und zwar: Zentralisierung ist natürlich immer Informationsmacht. Und gerade in staatlichen Händen ist das eine Informationsmacht, der auch eine reale Macht folgen kann. Insgesamt ist Datenschutz immer eine Frage von Machtasymmetrien, so wie bei freiheitlichen Staatsüberlegungen immer. Es hat ja einen Grund, warum die Verkehrspolizei keine schwere Bewaffnung hat, einfach, weil wir immer minimale Rechte geben, um die Erfüllung der Aufgaben sicherzustellen. Und nicht mehr. Das heißt, ich muss da jetzt so als „Grundrechtspatriot“ auch einfach einmal in die Offensive gehen und sagen: „Ich muss doch nicht begründen, worin die Gefahr dieser biometrischen Daten besteht, sondern die, die diese Datenbanken aufbauen, sollen mir doch einmal begründen, wofür das zunutze ist.“ Das heißt, das Verhältnis muss sich umdrehen an der Stelle. Und da kann ich dann auch leider nicht mit Herrn Schleyer mitgehen, dass das primäre Argument ein finanzielles sein kann – Demokratie ist halt teuer. Das, was wir hier machen, kostet auch. Wir würden ja auch nicht auf die Idee kommen zu sagen, dass unser erstes Sparziel heißt, die Ausschüsse müssen weniger werden. Also quasi auch wenn das teurer ist, wenn das dem Zwecke dient, eine sichere Infrastruktur aufzubauen, dann soll man das machen. Aber im Falle wie mit der Biometrie: Es bleiben zu lassen, ist die beste Möglichkeit. Man kann jetzt auch nicht sagen: „Naja, die Begründung für diese Zusammenführung jetzt ist ja das Gesetz von 2017 und 2017 begründet man den Zugriff damit, dass die Daten ja da sind, damals von 2006.“ Wir müssen uns erinnern: Die Begründung damals für die Biometrie war die Fälschungssicherheit, wobei auf eine Kleine Anfrage die Bundesregierung gesagt hat, dass von 2001 bis 2006 insgesamt sechs Fälle aufgetaucht sind. Da frage ich mich dann doch- - anfangs war eine Lüge als Begründung oder eine kleine Ungenauigkeit und die wurde festgeschrieben und jetzt baut man auf dieser Sache so lange wieder Systeme auf, bis keiner mehr weiß, was eigentlich die ursprüngliche Voraussetzung war, warum man das gemacht hat. Und das müssen wir aber tun, NSU 2.0 ist ein Beispiel. Und so weiter. Menschen können ihr Gesicht nicht wechseln und das ist das Problem bei Biometrie. Und deswegen muss man immer die Frage stellen, warum. Und diese Frage wurde hier, zumindest mir bekannt, noch nicht beantwortet, warum das überhaupt sinnvoll ist, um dieses Risiko für Bürgerinnen und Bürger einzugehen. Dankeschön.

BE Abg. **Josef Oster** (CDU/CSU): Ich muss einmal ganz kurz, wenn ich darf, Frau Vorsitzende, eine Zwischenfrage stellen, weil jetzt mehrfach ein Sachverhalt genannt wurde, der so meines Erachtens nicht richtig ist. Also meines Wissens ist zum Beispiel die Polizeikontrolle überhaupt keine Funktion der eID. Das wird gar keine Funktion sein, die die eID hat – dafür werde ich weiterhin meinen physischen Personalausweis brauchen. Also nur, weil das jetzt hier mit „Handy aus der Hand geben“ und so weiter aufkam, das wird keine Funktion dieser eID sein. Und deshalb wird das auch nicht ein Problem sein, was Sie da jetzt mehrfach geschildert haben.

Vors. **Andrea Lindholz** (CDU/CSU): Ich glaube, das war vorher so, dass wir gesagt haben, ich habe den Personalausweis gerade nicht dabei, so habe ich das verstanden, und versuche mich dann anders zu legitimieren.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Um nicht zur Identitätsfeststellung mit auf die Wache kommen zu müssen.

Vors. **Andrea Lindholz** (CDU/CSU): Ja, genau.

BE Abg. **Josef Oster** (CDU/CSU): Ich glaube, die Polizei kann das gar nicht auslesen.

Vors. **Andrea Lindholz** (CDU/CSU): Es ging ja darum, es aufzumachen und zu zeigen. So hatte ich das jetzt verstanden.

SV **Rainer Rehak** (FIfF, Berlin): Genau, man kann das auch nicht. Aber wir wissen ja, die Realität ist

meistens sehr viel schmutziger als die Regeln, das formale und das informale.

Vors. **Andrea Lindholz** (CDU/CSU): Der Fall war ja klar: Ich stehe irgendwo, ich habe meinen Ausweis nicht dabei, ich versuche, mich anderweitig auszuweisen. Das war die Überlegung, die ich jetzt nicht von der Hand weisen kann, dass man einmal auf die Idee kommt, dass so ein Fall eintreten kann und deswegen wollte ich ja wissen, kann man sowas jetzt generell schützen? Absolute Sicherheit gibt es nie, aber dieser konstruierte, aber aus meiner Sicht nicht völlig fernliegende Fall, dass jemand so versucht, sich der Sache zu entledigen, sollte bedacht werden.

SV **Rainer Rehak** (FIfF, Berlin): Und vielleicht einen Satz dazu: Wenn wir uns da alle einig sind, finde ich, dann kann man genau das ja auch rechtlich so explizieren, dass das auch wirklich so bleibt.

Vors. **Andrea Lindholz** (CDU/CSU): Aber schön wäre es trotzdem, wenn man es gar nicht erst entsperren müsste. Frau Peters ist dran.

SV **Prof. Dr. Isabell Peters** (HSVN, Hannover): Danke sehr. Ja, ich möchte auf die Frage von Herrn Abgeordneten Lindh Bezug nehmen zu dem Evaluationsziel und zwar heißt es im Gesetzentwurf, man möchte anhand von einer 50 prozentigen Steigerung in einem Fünfjahreszeitraum den Erfolg dieser Gesetzesänderung erheben. Und ich halte diese 50 Prozent für ein doch relativ wenig ambitioniertes Ziel, da wir von einem niedrigen Plateau im Status Quo ausgehen. Das Onlinezugangsgesetz mit den maßgeblichen über 575 Leistungen tritt erst Ende nächstes Jahr in Kraft und dann haben wir erst ein nennenswertes Angebot von Onlineverwaltungsleistungen. Darüber hinaus geht es darum: Wir haben es hier mit einem „Henne-Ei-Problem“ zu tun, anbieterseitig gibt es wenige Angebote, sodass es in der Folge auch nur wenige Nutzer gibt. Die aus wenigen Angeboten resultierenden niedrigen Nutzerzahlen führen gleichermaßen dazu, dass auch die Anzahl der Angebote nicht steigt. Insofern plädiere ich dafür, erst einmal mehr Angebote zu schaffen und das können wir maßgeblich nur mit privaten Partnern, um auf diese Weise eine höhere Durchdringungsbreite des Marktes und höhere Nutzungszahlen zu erzielen. Danke.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Herr Neumann.

SV **Linus Neumann** (CCC, Berlin): Ich beantworte die Frage von Herrn von Notz nach der Bedeutung und dem Wesen der Biometrie. Sie wissen, Biometrie – das sind eindeutige Merkmale des Körpers, die mit hoher Wahrscheinlichkeit zwischen zwei Menschen so unterschiedlich sind, dass man davon ausgeht, dass sie für jeden Menschen einzigartig sind. Und was diese biometrischen Systeme machen: Die arbeiten mit einer mathematisch-geometrischen Repräsentation der biometrischen Merkmale. Das könnten Fingerabdrücke sein, in diesem Falle eben Gesichter. Wir wenden die Biometrie zu zwei Zwecken gerade an. Das ist einmal der Zweck der Authentifizierung und andererseits der Zweck der Identifizierung. Das sind zwei fundamental unterschiedliche Anwendungsgebiete: Bei der Authentifizierung verwenden wir die Biometrie im Interesse der Person, zum Beispiel zum Entsperren ihres Smartphones, wobei man da schon sieht, dass die Biometrie eigentlich nur als zweiter Faktor geeignet wäre und das ist auch das, was sich an diesem System so eignet: Sinnvoll wäre, wenn man sie mit einem Passwort kombinieren könnte. Wenn man also sagt, „okay, du musst mein Gesicht haben und mein Passwort kennen“ – also eine starke Zwei-Faktor-Authentifizierung. Der zweite Anwendungsbereich ist eben die Identifizierung von Personen und das geht nun einmal leider auch gegen die Interessen der Person und ohne ihr Wissen, was gerade bei der Gesichtsbiometrie das große Risikofeld ist. Und das Problem ist, dass wir gerade beides haben. Also wir gewöhnen uns einerseits daran, mit Fingerabdrücken und Gesichtern in alle möglichen kritischen, technischen Systeme hineinzukommen und rollen gleichzeitig diese Datenbanken aus, in denen diese Infrastruktur quasi diese als Identifizierungs- und Authentifizierungsmerkmal genutzten Merkmale genutzten biometrischen Daten sammelt.

Was ist das Problem bei der Authentifizierung? Sie kennen das Beispiel von den Passwörtern, auch wenn Sie es im Zweifelsfall zu 60-70% unter Ihnen nicht umgesetzt haben, das größte Risiko ist die Wiederverwendung. Weil wenn Sie dann ein Passwort verlieren, dann verlieren Sie direkt den Zugang zu mehreren Accounts. Bei der Biometrie ist es leider so, die wird man nicht los und die kann man auch nicht ändern, beziehungsweise es

wäre teuer. Das ist auch die Erfahrung, die der ehemalige Innenminister Wolfgang Schäuble schon gemacht hat, als wir seinen Fingerabdruck veröffentlicht haben. Man versucht das noch mit anderen Merkmalen, als den Gesichtern, wie den Mustern in der Hand, also teilweise Merkmale, die nicht ganz so offensichtlich getragen werden, die aber trotzdem einfach klonbar sind, weil quasi ihre Repräsentation auch gleichzeitig zeigt, was man dem Sensor vorgaukeln muss. Wir beim Chaos Computer Club machen das als Hobby. Jan Christer, bekannt als Starbuck, ist eines unserer Mitglieder, der sehr viel in diesem Bereich macht, also die Sensoren austricksen mit einfachen Attrappen. Inzwischen gibt es auch eine ganze Reihe an privatwirtschaftlichen Horrorszenarien: Clearview AI und PimEyes, also Systeme, die biometrische Massenerkennungen in Fotos, teilweise sogar schon in Videos anbieten. Stellen Sie sich die Folgen vor für Demonstrationen unter Vermummungsverbot in Deutschland nach Ende der Pandemie, für Stalking, für Massenüberwachungstechniken. Und diese Systeme werden ja immer weiter zentralisiert. Die kommen ja niemals hier irgendwie an und sagen, wir haben hier was und haben uns überlegt, wir dezentralisieren das, um es ein bisschen sicherer zu machen. Die kommen immer nur an und wollen alles auf einen Haufen werfen und einfacher zugreifbar machen. Also werden natürlich auch solche „Südkreuz-Systeme“ zusammengeschlossen und dann ist der Bahnhof Südkreuz irgendwann überall und die Datenbank, die die Bebilderung feststellt und zentral speichert, das ist dann auch eine und nicht überall eine andere. Und diese Mischung aus Authentifizierungs- und Identifikationsmerkmal und dass genau dem keine Rechnung getragen wird, das macht die Missbrauchsszenarien nur umso schlimmer. Weil beispielsweise es bei insbesondere schlechten Face-Sensoren relativ einfach ist, mit einem biometrischen Foto einen Klon zu bauen und ein Gerät zu entsperren und umgekehrt. Deswegen engagieren wir uns als Chaos Computer Club im Bündnis „Reclaim Your Face“ für eine europäische Bürger*innen-Initiative, um insbesondere die biometrische Massenüberwachung in ihre Grenzen zu weisen.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann Herr Professor Margraf.

SV **Prof. Dr. Marian Margraf** (Freie Universität Berlin): Ja, ich habe drei Fragen bekommen. Zwei zur Gültigkeitsdauer von Ihnen, Frau Lindholz, die ich zuerst beantworte. Die Idee dahinter, von fünf auf zwei Jahre herunter zu gehen, ist, dass man nicht annimmt, dass die Smartphones fünf Jahre lang sicher sind, um den Identitätsnachweis sicher umsetzen zu können. Das kann allerdings auch schon nach eineinhalb Jahren passieren, deswegen gebe ich noch einmal meinen Punkt mit dem Schwachstellenmanagement ein. Man muss eben frühzeitig erkennen, welche Geräte Schwachstellen haben, die dann eben auch die Sicherheit des elektronischen Identitätsnachweises beeinflussen und muss die dann auch ausschalten. Also eine feste Zeit, aber ich kann auch sagen, ich plädiere dafür von fünf auf zwei Jahre runter zu gehen. Nichts desto trotz braucht man immer noch das Schwachstellenmanagement.

Zu Ihrer zweiten Frage mit der Personenkontrolle: Ich glaube, das hat sich in der zwischenzeitlichen Diskussion schon so ein bisschen erledigt. Ich würde dazu trotzdem noch zwei Sachen sagen: Dem Gesetzentwurf ist nicht zu entnehmen, dass die Polizeien diesen elektronischen Identitätsnachweis auch nutzen – sie können das auch technisch gar nicht, weil sie kein Berechtigungszertifikat bekommen, wenn das so gesetzlich nicht vorgeschrieben oder erlaubt ist, deswegen geht das gar nicht. Und das Ding als „Sichtausweis“ zu machen, ergibt ja gar keinen Sinn. Also einfach sozusagen nur ein Foto vom Personalausweis zu zeigen, das bringt, glaube ich, nicht viel. Nichts desto trotz kann man sich natürlich zukünftig überlegen, ob man Smartphones nicht auch für solche Einsatzzwecke nutzt. Da gibt es durchaus auch Möglichkeiten, das so zu machen, dass das Smartphone vom Nutzer gar nicht mit einer PIN oder irgend so etwas freigeschaltet werden muss, sondern zum Beispiel über die NFC-Schnittstelle, das wäre dann eben nur eine Ein-Faktor-Authentisierung, aber über die NFC-Schnittstelle zumindest die Daten ausgelesen werden können, wenn ein entsprechendes Berechtigungszertifikat für so ein Szenario da ist. Also technisch wäre das möglich.

Und dann zur Frage von Herrn Oster zur Bewertung der Lösung hinsichtlich Benutzbarkeit und Datenschutz. Also für die Benutzbarkeit, auch gerade im Vergleich zu anderen europäischen Lösungen, ist meines Erachtens natürlich ein wesentlicher Faktor, dass man das Smartphone zur Authentifizierung nutzen kann. Auch da wieder

hängt die Benutzbarkeit von der konkreten Ausgestaltung ab. Da sollte man entsprechend Usability-Experten frühzeitig einbeziehen. Zum Datenschutz lobe ich ja die eID-Funktion des Personalausweises immer wieder, also dass eben über Berechtigungszertifikate gesteuert wird, welche Daten überhaupt ausgelesen werden dürfen. Nämlich nur die, die der Dienst auch tatsächlich braucht – Nutzerinnen und Nutzer können das abwählen und nur eine eingeschränkte Auswahl zur Verfügung stellen. Ich glaube, wir sind uns alle einig, dass die Lösung datenschutzmäßig wirklich sehr vorbildlich ist. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank. Zum Schluss noch Herr Professor Kelber.

SV **Prof. Ulrich Kelber** (BfDI, Bonn): Vielen Dank Frau Vorsitzende. Ich hatte zwei Fragen von Herrn Abgeordneten Höferlin. Einmal zu den grundsätzlichen Gefahren: Ich bin nicht ganz sicher, ob Sie beide Verfahren angesprochen hatten, bei eID ist es ja teilweise auch schon genannt worden. Natürlich sind bei den jetzt nicht mehr kartenbasierten Onlineverfahren weitere Sicherheitselemente mit einbezogen. Diese können natürlich angegriffen werden. Und umso länger die Gültigkeitsdauer ist- - und wir erleben ja leider einen nicht sehr nachhaltigen Markt der Endgeräte, wo sowohl bei den Sicherheitselementen als auch beim grundsätzlichen Betriebssystem die Sicherheitsupdates nach einer Zeit nicht mehr geliefert werden oder lange hinterher hinken. Und da sind natürlich verschiedene Angriffe möglich. Bei der zentralen Datenhaltung ist es natürlich so, dass wenn eine gute Lösung wird, Angriffe von außen erst einmal schwieriger sind, als bei einer einzelnen Kommune, die diese Lösung nicht implementiert hat. Wobei natürlich auch die Kommunen, die ja auf diesen Datenbeständen sitzen, natürlich entsprechende Sicherungsmethoden entwickeln müssen, weil Sie sonst trotzdem eine zweite Stelle haben, wo Angriffe durchgeführt werden können. Der „Honeypot-Effekt“ ist natürlich wesentlich größer, wenn dort nicht mehr nur von vielleicht 1.000 oder 2.000, also die Daten einer kleinen Kommune liegen, sondern mit Bayern dann vom 13 Millionen, mit Nordrhein-Westfalen von 18 Millionen Bürgerinnen und Bürgern die entsprechenden Personalausweisdaten angreifbar sind. Vor allem aber auch die Nutzung von innen heraus, also Missbrauch aus Behörden von Zugangsberechtigten für andere Zwecke. Und da kennen wir ja nicht nur die besonders pathologischen Fälle, sondern wir wissen einfach, dass in solchen Datenbanken nach Konzerten von berühmten Sängern, nach bestimmten Interviews die Abfragedaten nach oben schnellen und natürlich, wie gesagt, wenn ein solches Datenvolumen erst einmal da ist, ist die Möglichkeit der Ausweitung der daraus stattfinden Auswertungen natürlich groß. Und das ist natürlich durchaus etwas, was die letzten 20 bis 25 Jahre geprägt hat, dass Daten, die einmal eingeführt wurden, immer wieder Interesse an zusätzlichem politischen Nutzen haben: Mautdaten, Steuer-ID, ähnliches – das ist ja keine Verschwörungstheorie, sondern wirklich passiert.

Was das Vertrauensniveau nach eIDAS angeht, würden wir uns natürlich wünschen, möglichst das Vertrauensniveau „hoch“ zu erreichen. Wobei für die meisten der angedachten Anwendungsszenarien auch „substanziell“, so wie es auch vom BSI in der entsprechenden technischen Richtlinie schon entwickelt wurde, ausreichend ist.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank. Das ist eine echte Punktlandung, wir sind jetzt gleich bei 17:00 Uhr. Ich bedanke mich noch einmal bei allen für die Teilnahme heute und für die gute Anhörung und wünsche allen noch eine gute restliche Woche und schließe damit die Sitzung.

Schluss der Sitzung: 16:59 Uhr

Andrea Lindholz, MdB
Vorsitzende

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)845 A

AKDB | Postfach 150 140 | 80042 München

An den

Innenausschuss des Deutschen Bundestages

Anstalt des öffentlichen Rechts
Hansastraße 12-16
80686 München

Vorstand
vorstand@akdb.de
Telefon 089 5903 1547

14. Mai 2021

Stellungnahme für die Sachverständigen-Anhörung

zum

Gesetz zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät (Drucksache 19/28169)

sowie zum

Änderungsantrag der Fraktionen der CDU/CSU und der SPD

im Innenausschuss des Deutschen Bundestages

Management Summary

Der Gesetzentwurf ist zu begrüßen, da er potenziell die Anwenderbasis des neuen Personalausweises (nPA) bzw. des elektronischen Aufenthaltstitels (eAT) und der elektronischen Identität (eID) erhöht. Soweit der Änderungsantrag der Fraktionen der CDU/CSU und der SPD berücksichtigt wird, ergibt sich zudem eine für die (kommunale) Verwaltungsdigitalisierung sinnvolle und notwendige Erleichterung bei der Abfrage von Lichtbild und Unterschrift, soweit die Länder von der Regelungsbefugnis Gebrauch machen.

Bedeutung einer sicheren und nutzerfreundlichen Identifizierungslösung für die OZG-Umsetzung

Eine wesentliche Herausforderung für eine gelungene Verwaltungsdigitalisierung, also auch für die Umsetzung des OZG, ist die breitflächige Nutzung und Akzeptanz der Angebote durch Bürgerinnen, Bürger und Unternehmen. Hierfür unerlässlich ist das Vertrauen durch sichere Identitäten. Die Übertragung des nPA/eAT auf das Smartphone entspricht der Lebenswirklichkeit im Privaten wie in der Wirtschaft und ist deshalb uneingeschränkt zu begrüßen.

Anwendungen außerhalb der Verwaltung

Jede praxis- und bürgernahe Form einer elektronischen Identität hilft der Verwaltung wie der Privatwirtschaft, sichere und personenbezogene Angebote umzusetzen. Eine Lösung wie der nPA/eAT auf dem Smartphone kann durch eine erhöhte Akzeptanz die notwendigen Netzwerkeffekte für eine breitflächige Nutzung entfalten. Wichtig wäre allerdings, dass eine Ausgewogenheit zwischen eIDAS-Vertrauensniveau (möglichst Stufe "hoch" auch für den nPA/eAT auf dem Smartphone) und dem Verzicht auf überschießende Sicherheitsanforderungen (Hardware Secure Element) gewahrt wird. Eine softwareseitige Absicherung, in Abstimmung mit den Betriebssystem-Herstellern der Smartphones, wäre nach unserer Einschätzung zielführend.

Grundsätzlich schließen wir uns hierzu den in der Stellungnahme des Bundesbeauftragten für Datenschutz und Informationssicherheit, Prof. Ulrich Kelber, vom 12. Februar 2021 dargelegten Anpassungsvorschlägen zum eID-Gesetz an und unterstützen diese ausdrücklich.

Änderungsantrag

Der Änderungsantrag soll es den Ländern ermöglichen, eigene Passregister zu führen, aus denen dann in einem automatisierten Verfahren Lichtbild und Unterschrift (z.B. für Sicherheitsbehörden) extrahiert werden können.

Bezüglich einer zentralen Speicherung von Passbildern in zentralen Registern der Länder ist auf die positiven Erfahrungen mit den Landesmelderegistern im Rahmen der melderechtlichen Behördenauskunft zu verweisen. Diese wird in allen Flächenländern (außer Nordrhein-Westfalen) erfolgreich praktiziert. Zu den Vorteilen eines landesweiten Pass-/Ausweisregisters zählen

- die sehr hohe Verfügbarkeit solcher Register,
- die zentrale Benutzer-/Rechte-Steuerung für alle Anfragen an einer Stelle,
- die Nutzung vorhandener Infrastrukturen in analoger Anwendung der Struktur der Landesmelderegister,
- die nur einmalige Investition für die Schaffung solcher Register je Bundesland, im Gegensatz zu den andernfalls jeweils lokal notwendigen Investitionen auf Seiten der Kommunen für den Zugriff, die Infrastruktur, den Betrieb, die Sicherstellung der Verfügbarkeit sowie die Updates dezentraler Pass-/Ausweisregister.

Insgesamt ist davon auszugehen, dass eine dezentrale Ausgestaltung für die Kommunen deutliche Mehrkosten gegenüber zentraler Passregister auf Landesebene nach sich zieht. Letztere gehen zudem für die zuständigen Sicherheitsbehörden mit erleichterten Kommunikationsszenarien einher, da weniger Kommunikationspartner involviert sind. Auch die Anforderungen an die IT-Sicherheit zur Absicherung des Zugriffs auf die Register sind so deutlich einfacher umzusetzen. Dies gilt umso mehr, als eine Nutzung etwa im Rahmen des § 22a Abs. 2 Satz 6

PaßG bzw. § 25 Abs. 2 Satz 5 PAuswG mit Einwilligung der antragstellenden Person dann erheblich weniger technische Komplexität aufweist.

Mit freundlichen Grüßen

[redacted]

Rudolf Schleyer
Vorstandsvorsitzender

Seite 31 von 64

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)845 B

Freie Universität Berlin

Fachbereich Mathematik und Informatik
ID-Management

Prof. Dr. Marian Margraf
Takustraße 9
14195 Berlin

+49 30 838 75-245
marian.margraf@fu-berlin.de

Innenausschuss des
Deutschen Bundestages

nur per E-Mail

Betr.: Öffentliche Anhörung zum Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät“

Sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur öffentlichen Anhörung. Gern übersende ich Ihnen vorab meine Stellungnahme in schriftlicher Form.

Der auf dem Personalausweis, dem Aufenthaltstitel und der eID-Karte umgesetzte Identitätsnachweis (Online-Ausweisfunktion) wurde 2010 eingeführt. Bürger*innen können sich damit sicher und datenschutzfreundlich gegenüber Dienstanbietern authentisieren. Die wesentlichen Grundideen der Online-Ausweisfunktion sind:

1) Umsetzung einer Zwei-Faktor-Authentisierung, die auf Wissen (eine sechsstellige PIN) und Besitz (Ausweiskarte) basiert

2) Dienstanbieter erhalten nur diejenigen personenbezogenen Daten, die sie für ihren Dienst benötigen (umgesetzt über Berechtigungszertifikate, die vom Bundesverwaltungsamt ausgegeben werden) und

3) Bürgerinnen und Bürger wissen, wem gegenüber sie sich authentisieren (ebenfalls umgesetzt über Berechtigungszertifikate)

Dem Gesetzentwurf ist zu entnehmen, dass der geplante elektronische Identitätsnachweis mit einem mobilen Endgerät diese Technik übernimmt, d.h. sowohl eine Zwei-Faktor-Authentisierung als auch über Berechtigungszertifikate die Authentisierung datenschutzfreundlich umsetzt. Die Sicherheit hängt von der konkreten Ausgestaltung ab, die naturgemäß dem Gesetzesentwurf nicht vollständig zu entnehmen ist, sondern vielmehr, wie schon bei der kartenbasierten Lösung, über Technische Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geregelt wird. Das BSI hat hier schon Vorarbeiten geleistet und z.B. in der

Technischen Richtlinie TR-03159 Anforderungen für Identitätsnachweise auf mobilen Endgeräten formuliert, mit denen ein eIDAS-Sicherheitsniveau von subtantiell erreicht wird, welches für die meisten Anwendungsfälle ausreichend ist. Insbesondere müssen hierfür sogenannte Sicherheitselemente eingesetzt werden, die kryptographisches Schlüsselmaterial sicher speichern und es ermöglichen, kryptographische Algorithmen sicher durchführen zu können. Es kann also davon ausgegangen werden, dass die Lösung sicher umgesetzt wird.

Im Gegensatz zu der kartenbasierten Online-Ausweisfunktion, für die nur eine sehr eingeschränkte Anzahl von Sicherheitselementen (mit entsprechendem Betriebssystem und Software) genutzt wird, ist die Anzahl der verwendeten Hard- und Softwareversionen bei mobilen Endgeräten deutlich höher. Dabei ist nicht auszuschließen, dass es zukünftig zu Sicherheitslücken kommt, die auch die Sicherheit der auf den mobilen Endgeräten umgesetzten Identitätsnachweise schwächen. Dies betrifft nicht nur Sicherheitslücken des eingesetzten Sicherheitselements (inklusive der hierauf laufenden Software), sondern auch Sicherheitslücken des verwendeten Betriebssystems des mobilen Endgerätes. So könnte z.B. eine Angreifer*in bei entsprechender Sicherheitslücke eine Schadsoftware auf dem mobilen Endgerät installieren, welche es ihr ermöglicht, den Identitätsnachweis aus der Ferne wie die reguläre Nutzer*in zu verwenden. Es sollte daher ein Schwachstellenmanagement für diese Geräte aufgebaut werden, das es der Betreiberin des Gesamtsystems (Bundesdruckerei im Auftrag der Bundesregierung) ermöglicht, Sicherheitslücken zu erkennen, zu bewerten und Gegenmaßnahmen, wie z.B. in schweren Fällen einzelne Geräte von der Verwendung auszuschließen, einzuleiten.

Weiter stehen Teile der Zivilgesellschaft großen Digitalisierungsprojekten der Bundesregierung skeptisch gegenüber, auch weil der Staat divergierende Interessen verfolgt. So wurde z.B. die Einführung der Online-Ausweisfunktion im Jahr 2010 vom CCC sehr negativ begleitet. Befürchtet wurde vor allem, dass der Staat über die Online-Ausweisfunktion die Bürgerinnen und Bürger ausspähen kann und nicht in der Lage ist, die Lösung sicher und datenschutzfreundlich zu gestalten. Die kritische Begleitung solcher Projekte sollte aber als Chance begriffen werden, Bürger*innen frühzeitig zu beteiligen, die Lösung zu verbessern und so insgesamt die gesellschaftliche Akzeptanz, gerade mit Blick auf Sicherheits- und Datenschutzfragen zu steigern.

Daher sollte der gesamte Entwicklungsprozess sowie die darauffolgende Pflege und Weiterentwicklung vollständig transparent gestaltet und die Zivilgesellschaft stark eingebunden werden. D.h., alle Umsetzungskonzepte (z.B. Architektur-, Krypto-, Sicherheitskonzept sowie Richtlinien zur sicheren Softwareentwicklung) müssen schon bei der Erstellung öffentlich zugänglich sein, mit der Öffentlichkeit diskutiert, Änderungsvorschläge bewertet und vor allem eine Ablehnung von Änderungen nachvollziehbar begründet werden. Auch die Softwareentwicklung sollte als Open-

Source-Projekt unter einer geeigneten Open-Source-Lizenz gestaltet werden und auch hier die Community aufgerufen werden, daran mitzuwirken. Dies betrifft die im Projekt zu entwickelnden Softwarekomponenten, die Smartphone-Apps und die Secure-Element-Applets.

Hierfür sollte ein Internetportal bereitgestellt werden oder bestehende Services (z.B. GitHub oder GitLab) genutzt werden, auf dem alle Informationen zum Entwicklungsprozess, den Dokumenten und der Software aufgeführt sowie die Mitwirkungsmöglichkeiten dargestellt werden. Ein wesentliches Element des Portals ist die Aufbereitung von Änderungsvorschlägen an Dokumentation und Software durch die Community und deren öffentliche Bewertung durch die Projektleitung und Community (Aufnahme/Ablehnung inklusive Begründung).

Die oben beschriebenen Prozesse, sowie die Open Source Veröffentlichung im generellen, sollten den Standards und Best Practices der Open Source Community entsprechen (siehe hierfür z.B. die Veröffentlichungsstrategie der Corona-Warn App).

Fazit: Den elektronischen Identitätsnachweis für mobile Endgerät umzusetzen birgt das Potential, die Nutzungsreichweite deutlich zu erhöhen und damit die Digitalisierung sicher voranzutreiben. Vorrausetzung hierfür ist jedoch die sichere Umsetzung der Lösung, ein transparentes Handeln und die Einbindung der Zivilgesellschaft. Auch wenn Anfangs nur eine sehr eingeschränkte Auswahl von Geräten auf Grund fehlender Sicherheitsnachweise genutzt werden können, wird sich dies meines Erachtens zukünftig positiv verändern.

Mit freundlichen Grüßen

Prof. Dr. Marian Margraf

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)845 C

Chaos Computer Club

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

Gemeinsame Stellungnahme an den Ausschuss für Inneres und Heimat des Deutschen Bundestags

zum Gesetzentwurf zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät (DS 19/28169) sowie zum Änderungsantrag bezüglich der zentralisierten Speicherung biometrischer Daten (A-DS 19(4)825)

Markus Drenger, Constanze Kurz, Rainer Rehak, Lilith Wittmann

17. Mai 2021

Vorbemerkung

Digitalisierung, insbesondere wenn sie Vereinfachungen für Bürgerinnen und Verwaltung bringt, ist gut und begrüßenswert. Dies gilt aber nur unter dem Vorbehalt, dass sie auch gut gemacht ist. Im vorliegenden Gesetzentwurf sind sowohl Nutzen als auch Umsetzung fragwürdig. Der Gesetzestext sieht Änderungen im Personalausweisgesetz, im eID-Karte-Gesetz (eIDKG) sowie im Aufenthaltsgesetz vor. Es soll für natürliche Personen und Inhabende eines eID-Ausweisdokumentes die Möglichkeit geschaffen werden, Speicher- und Verarbeitungsbereiche eines „mobilen Endgerätes“ für die eID-Funktion zu nutzen.

Wir möchten darauf aufmerksam machen, dass hier eine Basistechnologie ohne ausreichende Konzeption und umfassende Planung eingeführt werden soll. Eine fundiertere Begründung für diese Mängel folgt weiter unten. Des weiteren gab es keine Bürgerbeteiligung, etwa im Rahmen des Open-Government-Partnership-Prozesses. Auch im Rahmen der Verbändeanhörung des Bundesinnenministeriums sind nur zwei öffentliche Stellungnahmen des VITAKO e. V. sowie des GDV dokumentiert. Es ist nicht öffentlich einsehbar, ob und welche weiteren Gruppen und Verbände angehört wurden.

Wir möchten auch auf folgendes hinweisen: Eine angemessene Frist für die Kommentierung des Gesetzentwurfes war auch diesmal nicht vorgesehen.[1] Im Übrigen sind wir der Meinung, dass gerade zivilgesellschaftlichen Organisationen künftig längere Kommentierungsfristen eingeräumt werden müssen.

[1] Siehe Offener Brief an die Bundesregierung: Angemessene Fristen statt Scheinbeteiligung, https://www.ccc.de/de/updates/2020/scheinbeteiligung vom 18. Dezember 2020.

Aufbau einer sicheren eGovernment-Infrastruktur nötig

Aktuell werden in den unterschiedlichsten Bereichen der Verwaltung verschiedene Authentifizierungs- und Kommunikationslösungen implementiert. Darunter sind die Bereiche Mobilität, eJustice, digitale Verwaltung sowie im Gesundheitswesen. Hinzu kommt der Kommunikationsmisserfolg „De-Mail“ und der seit Jahren ausbleibende Erfolg des elektronischen Personalausweises, obwohl seit einer Gesetzesnovelle sogar ein Zwang zur Aktivierung der elektronischen Funktionen gegeben ist. Auch der vorliegende Gesetzentwurf krankt an fehlender Weitsicht und plant leider wieder nur kleinteilig. So wird beispielsweise versäumt, Regelungen für juristische Personen vorzusehen, etwa für Signatur- und Authentifizierungsverfahren mit elektronischen Siegeln (eIDAS).

Es ist höchste Zeit, grundsätzliche und übergreifende Überlegungen zum Aufbau einer sicheren eGovernment-Infrastruktur anzustellen, bevor noch weitere lückenhafte Einzellösungen dazukommen. Der aktuelle „Überall-Inseln“-Ansatz verhindert perspektivisch eine nahtlose Integration und sichere Skalierung der jeweiligen Dienste, und auch die Einzeldienste sind aufgrund dieser limitierten Sichtweise defizitär. Für eine sichere eGovernment-Infrastruktur gibt es bereits Konzepte und Technologien, dafür muss jedoch die Authentifizierungsinfrastruktur in ihrer Gesamtheit durchdacht und endlich ganzheitlich geplant werden.

Eine ganzheitliche Architekturplanung einer Authentifizierungsinfrastruktur muss zunächst alle betroffenen Gruppen und Personen adressieren, sowohl natürliche als auch juristische Personen wie Firmen oder Verbände. Sofern der Staat das digitale Ausweiswesen nicht aufgeben möchte, sollte er selbst die dafür notwendigen Mittel bereitstellen und wo möglich Netzwerkeffekte erzeugen, um eine Adaption der Lösungen zu fördern. Es ist eben nicht damit getan, die eID-Funktion des elektronischen Ausweises nur zwangsweise zu aktivieren, wie es der Gesetzgeber in der letzten Neuregelung des eID-Gesetzes[2] nach einem Jahrzehnt von nahezu Untätigkeit vollzogen hat. Denn auch nach den seither vergangenen Jahren ist es zu keiner nennenswerten Steigerung der Nutzung der eID-Funktionen gekommen. Das ist wenig verwunderlich, da nach wie vor kaum attraktive Angebote zur Nutzung gemacht werden. Denn mit Hilfe der PIN und dem Ausweis könnten sich Bürger bei Ämtern und Online-Anbietern seit mehr als einem Jahrzehnt identifizieren, sie tun es nur nicht.

Ist die Authentifizierungsinfrastruktur erst einmal vorhanden, wäre auch die Schaffung einer Kommunikationsinfrastruktur wesentlich erleichtert. Aus unserer Sicht muss all dies nach klaren Prinzipien geschehen: Dabei sind Offenheit, Interoperabilität und Transparenz der Prozesse und des Quellcodes der Lösungen eine Voraussetzung für Vertrauen, Sicherheit und Akzeptanz, aber auch für Erweiterbarkeit und Performanz.

---

[2] Gesetz zur Förderung des elektronischen Identitätsnachweises.

Keine offene Architektur angedacht

Der Begriff des „mobilen Endgerätes“ ist unscharf und zugleich unnötig einschränkend. Einerseits kann ein stationäres Endgerät die gleichen Aufgaben erfüllen. Andererseits ist die Beschränkung auf Endgeräte ebenfalls nicht ersichtlich sinnvoll, da die Lösungen natürlich auch in andere Systeme integriert werden könnten.

Digitale Ausweisinfrastruktur ist genauso wie Ausweise in der analogen Welt eine Basisinfrastruktur. Sie sollte vom Staat so entwickelt werden, dass sie möglichst vielen Akteuren möglichst günstig bzw. kostenlos offensteht.

Momentan sieht es im Kontext der eID allerdings so aus, als ob dieselben Fehler erneut gemacht werden, die in der Konzeption und Bereitstellung der Infrastruktur, die zu einer ausbleibenden Akzeptanz von z. B. De-Mail und dem elektronischen Personalausweis (nPA) in der Wirtschaft und insbesondere auch in der Zivilgesellschaft geführt haben.

Es wird auf eine geschlossene, proprietäre Infrastruktur gesetzt, mit deren Betrieb monopolistisch einige wenige große IT-Unternehmen betraut werden. Diese haben dann durch ihr Quasi-Monopol die Möglichkeit, im Vergleich zu den eigentlichen Kosten einer Identifizierung horrende Preise dafür zu verlangen. Es ist außerdem weiterhin nicht klar, welche Kosten insbesondere im Bereich von Zertifizierungen auf die Nutzenden der eID-Infrastruktur zukommen werden.

Statt des vorgesehenen privatwirtschaftlichen Betriebs sollte die eID als Basisinfrastruktur komplett staatlich betrieben werden. Die Nutzung sollte allen kostenlos offenstehen. Durch die „Unit Economics“ von digitalen Produkten würde ein solches Vorgehen dazu führen, dass die Gesamtkosten pro Authentifizierung bei hoher Akzeptanz und einem staatlichen Betrieb der Infrastruktur bei einem Bruchteil eines Cents liegen würde.

IT-Sicherheit der mobilen Endgeräte

Aus Sicht der IT-Sicherheit ist es ein relevanter Unterschied, ob die eID-Funktion via nPA oder – wie jetzt angedacht – via Smartphone geschehen soll: Im ersten Fall des nPA liegt eine zertifizierte SmartCard mit klar umrissenem Einsatzzweck vor. Im zweiten Fall dagegen handelt es sich um einen hochkomplexen Multifunktionscomputer mit jeweils konkret sehr unterschiedlichen Sicherheitseigenschaften: ein Smartphone.

Die IT-Sicherheit eines Smartphones hat komplexe Bedingungen und hängt ganz allgemein gesprochen im Wesentlichen von drei Faktoren ab, die als Heuristik verwendet werden können: Marke und Alter des Gerätes und seiner Software und Update-Verhalten der Besitzerin. Erstens weisen eher hochpreisige Gerätemarken tendenziell einen eher hohen IT-Sicherheitsstandard auf, was Hardware, Anzahl der Updates und die Reaktion auf bekannt gewordene Sicherheitslücken angeht. Zweitens weisen eher neue Geräte tendenziell einen höheren IT-Sicherheitsstandard auf, allein schon weil aktuellere Software zu vermuten ist und auch Hersteller in der Regel nur für eine begrenzte Zeit überhaupt Sicherheitsupdates anbieten; im ungünstigsten Falle werden alte Geräte gar nicht mehr mit Updates versorgt. Drittens ist das Update-Verhalten der Besitzerin relevant, weil vom Hersteller angebotene Sicherheitsupdates natürlich auch installiert werden müssen, um ihre Schutzwirkung zu entfalten.

Um nun eine hoheitliche Funktion wie den elektronischen Identitätsnachweis mit dem mobilen Endgerät – vulgo Smartphone – zu nutzen, ist ein Mindeststandard bezüglich der IT-Sicherheit dieser Geräte selbstredend unabdingbar. Dies wird in § 2 Absatz 13 PAuswG-E entsprechend neu geregelt und soll in Verbindung mit § 2 Satz 2 PAuswV sowie den technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik[3] sichergestellt werden. Damit sollen dann die elektronischen Speicher- und Verarbeitungsmedien mobiler Endgeräte die geforderten IT-Sicherheitsanforderungen aufweisen („substanziell“ der eIDAS-Verordnung), inklusive Freigabe durch das BSI.

Auch wenn dieses Vorgehen sicherheitstechnisch gesehen vorbildlich ist, hat es die Gesetzgeberin bislang trotz diverser IT-Sicherheitsgesetze oder Produkthaftungsvorstöße versäumt, sichere und auch erschwingliche Endgeräte für die breite Bevölkerung auf dem Markt zu begünstigen. In der Folge erfüllen aktuell nur Samsung-Geräte der Modellreihe „Galaxy S20“ die Anforderungen, weil diese konkret dafür gefördert worden sind.[4] Bislang ist der vorliegende Entwurf quasi ein „Lex Samsung“. Doch auch später werden es – wenn überhaupt – vermehrt die hochpreisigen Modelle sein, welche die geforderten Standards erfüllen und somit zertifiziert werden können. Es findet also auch hier eine Digitalisierung entlang der sowieso schon

---

[3] BSI TR-03165 Trusted Service Management System, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03165/TR-03165_node.html

[4] OPTIMOS - praxistaugliches Ökosystem sicherer Identitäten für mobile Dienste, https://www.bundesdruckerei.de/de/Innovation/Optimos

vorherrschenden gesellschaftlichen sozio-ökonomischen Benachteiligungen statt.

Langfristig werden auch andere Digitalisierungsvorhaben unter dieser Logik leiden. Also sollte langfristig und systemisch gegengesteuert werden, etwa mit Mindeststandards, Haftungsregeln oder gar Angeboten aus der öffentlichen Hand.

Wohlwissend um dieses Manko der geringen Zahl nutzbarer Geräte hat der Bundesrat in seiner Stellungnahme nicht etwa langfristig und sozialverträglich gefordert, die IT-Sicherheit von Endgeräten im Allgemeinen zu erhöhen, sondern drängte darauf, „zu überprüfen, ob zugunsten einer schnellen und breiten Einsatzfähigkeit auf derartige Zulassungserfordernisse möglichst ganz verzichtet oder das Zertifizierungsverfahren zumindest einfach und mit kurzen Prüffristen ausgestaltet werden kann“.[5] Auch wenn auf diesen Vorschlag nicht eingegangen worden ist, zeigt dieser Vorschlag doch das grundlegende Problem unsicherer IT-Systeme für Endanwenderinnnen. Aus IT-Sicherheitssicht kann diesbezüglich mittlerweile durchaus von breitem Marktversagen gesprochen werden.

Geltungsdauer

Vor diesem Hintergrund der unzureichenden und generell schnelllebigen Situation bezüglich der IT-Sicherheit von Endgeräten mutet auch die angedachte Geltungsdauer von fünf Jahren[6] für den elektronischen Identitätsnachweis mit dem mobilen Endgerät zu lang an. Das angedachte Provisorium, dass „in der Personalausweisverordnung […] zunächst eine kürzere Geltungsdauer von zwei Jahren normiert werden [soll]“, muss aufgelöst und die reguläre Geltungsdauer auf maximal zwei Jahre gesetzt werden.

Nicht zuletzt sind die wesentlichen Regelungen dieses Gesetzes, nämlich die Anforderungen an das Speicher- und Verarbeitungsmedium, nicht im Gesetz definiert und folglich unbestimmt. Hier handelt es sich aus Sicht des Parlaments um eine „Katze im Sack“. Man könnte auch sagen, dass dem Bestimmtheitsgebot nicht ausreichend Genüge getan ist und dass eine Regelung im Rahmen einer späteren Verordnung nicht möglich ist, da wesentliche Regelungen gesetzlich vorzunehmen wären. So ist beispielsweise im Gesetzestext keine Trennung zwischen dem Verarbeitungsmedium und dem mobilen Betriebssystem vorgesehen.

---

[5] Stellungnahme des Bundesrates, Buchstabe a.

[6] Artikel 1 – Änderungen des Personalausweisgesetzes, Nummer 8 Abs 2 und Artikel 2 – Änderungen des eID-Karte-Gesetzes Nummer 5 Abs. 2

Metadatenfrage bei Einrichtung und Nutzung

Im Entwurf wird den Infrastrukturbetreibenden die Erlaubnis gegeben, einige Metadatenpunkte zu erfassen und auszuwerten. Dieses Recht wird durch den Änderungsantrag vom 30. April sogar noch weiter gefasst.

Bei den Metadaten, die bei der Einrichtung eines Ausweises anfallen, handelt es sich um höchst sensible personenbezogene Daten. Insbesondere zur Sicherstellung der gesellschaftlichen Akzeptanz der Infastruktur muss rechtlich geregelt werden, dass diese Informationen nicht zu anderen Zwecken als der Einrichtung und dem Betrieb von digitalen Ausweisen selbst verwendet werden dürfen. Deshalb sollte explizit festgelegt werden, dass die Metadaten-Verwendung , ähnlich wie z. B. Daten der Mautdatenerfassung, auf die Verwendung zum Zwecke des Gesetzes beschränkt[7] und danach auch gelöscht werden.

Es muss in diesem Kontext weiterhin beachtet werden, dass durch die Authentifizierung von Ausweisinhabenden auf keinen Fall Metadaten bei den Betreibenden der App-, TSM- sowie der eID-Infrastruktur anfallen dürfen. Denn eine Datensammlung darüber, wann sich welche Bürger gegenüber wem identifiziert haben, kann implizites Wissen über z. B. Diskriminierungsmerkmale im Sinne des Allgemeines Gleichbehandlungsgesetzes beinhalten. Da das Verarbeiten solcher Informationen für den Betrieb der Infrastruktur nicht notwendig ist, sollte es explizit ausgeschlossen werden.

Weiterhin sollte hier mehr in die Entwicklung datensparsamer Infrastrukturkonzepte investiert werden, bei denen einem Infrastrukturbetreiber (aus Architektursicht) überhaupt nicht offenbart werden kann, wer sich gegenüber wem ausweist.

Auswirkungen: Beispiel Personenkontrollen

Ein Ausweisdokument auf einem Smartphone zu speichern, kann in einigen Situationen problematisch werden. Wenn eine elektronische Identität einem Ausweisdokument gleichgestellt werden sollte, stellt sich die Frage der Ausweispflicht gegenüber berechtigten Stellen. So sollte beispielsweise von einer Person nicht verlangt werden dürfen, ein elektronisches Gerät in Gegenwart von Polizeivollzugsbeamten zu entsperren oder gar entsperrte Geräte „zur Identitätsfeststellung“ auszuhändigen.

Sowohl der klassische Grundsatz, dass niemand sich selbst belasten muss, als auch die bestehenden Regelungen bezüglich nicht vorhandener Mitwirkungspflicht und dem Richtervorbehalt bei Durchsuchungen von digitalen Geräten spricht hier für eine unterschiedliche Behandlung der verschiedenen Ausweisungsformen. Ansonsten könnte die möglichst sofortige

[7] Vgl. BT-Dr. 14/7013, S. 14.

Identifizierung einer Person und die damit verbundene Herausgabe von Zugangsdaten zu einem Gerät z. B. in einer Festnahmesituation zu einem weiteren Druckmittel der Polizei werden, um an Zugangsdaten zu kommen, die im weiteren Verfahren dann auch für die Durchsuchung des Gerätes verwendet werden könnten. Das wäre ein erheblicher Eingriff in die informationelle Selbstbestimmung und unter Umständen sogar in den unantastbaren Kernbereich privater Lebensgestaltung.

In diesem Kontext muss beachtet werden, dass ein Abruf des Ausweises via Technologien wie NFC nur nach einer Freigabe durch explizite Einwilligung des Benutzers möglich sein darf. Ermittlungsbehörden dürfen keine weitere Kompetenzen zugesprochen werden, die ihnen die Möglichkeit eröffnen, Menschen dazu zu zwingen, Endgeräte zum Zwecke der Identifizierung auszuhändigen.

Fehlende Umsetzungsaufwände

Diverse Umsetzungsaufwände sind im Gesetzentwurf nicht dokumentiert:

1.) Es sind keine Umsetzungsaufwände für die Wirtschaft dokumentiert, um als TSM-Anbieter auf dem Markt aufzutreten.

2.) Es sind keine Umsetzungsaufwände für die Wirtschaft dokumentiert, um als App-Anbieter die Funktionen nutzen zu können.

3.) Es sind keine Umsetzungsaufwände für die Zivilgesellschaft dokumentiert, um als TSM-Dienst sichere Infrastruktur verwalten zu können.

4.) Es sind keine Umsetzungsaufwände für die Zivilgesellschaft dokumentiert, um als App-Anbieter die Funktionen nutzen zu können, beispielsweise für das Sammeln von Unterschriften für Petitionen.

Die Umsetzungskosten sind hier keinesfalls nebensächlich, sondern ein wesentliches Kriterium, das über den Erfolg oder Misserfolg einer Maßnahme entscheiden kann. Geschlossene Ökosysteme, die in Form eines Monopols oder Oligopols konzipiert werden, zeichnen sich in der Regel durch hohe Adaptionskosten aus. Dann geht die Akzeptanz für eine solche Lösung stark zurück. Die damals vorgesehenen Gebühren pro einzelner „De-Mail“-Nachricht sind hier ein Beispiel, das zu denken geben sollte. Wenn der Staat eine solche Basisinfrastruktur etablieren möchte, sollte darüber nachgedacht werden, alle Personen mit der Möglichkeit einer elektronischen Signatur auszustatten. Wie bei Plattformen üblich, gibt es hier Fixkosten für den Betrieb einer Lösung, deren Kosten nicht wesentlich steigen, wenn mehr Personen Zertifikate bekommen.

Die von der Bundesregierung genannten Kosten sind, wie der Nationale Normenkontrollrat bereits in seiner Stellungnahme beschrieben hat, unerklärbar hoch. Eine Kalkulation zum Gesetzentwurf liegt uns nicht vor. Allein schon aufgrund der absolut unverhältnismäßigen Kosten sollte das Projekt an diesem Punkt überdacht und neu geplant werden.

Änderungsantrag „Zentralisierung von Biometriedaten“

Nach dem Änderungsantrag sollen die Regelungsbefugnisse dahingehend geändert werden, dass in den Ländern zentrale Personalausweisregister-datenbestände zur Speicherung des biometrischen Lichtbilds und der Unterschrift für die Durchführung eines automatisierten Abrufs des Lichtbilds[8] eingerichtet werden können. Zentralisierte Bestände biometrischer Daten bedeuten immer immense Machtzuwächse – hier für die Exekutive – und sind in freiheitlichen Demokratien stets begründungspflichtig, mindestens hinsichtlich der Erforderlichkeit oder Verhältnismäßigkeit. Darüber hinaus entstehen durch schlecht gesicherte Übertragungssysteme einerseits sowie durch den zentralisierten Datenbestand andererseits gefährliche Einfallstore für Kriminelle oder andere unbefugte Dritte.

Die Erweiterungen des Gesetzentwurfes um die Regelung zum Zugriff auf die Passregister und auf die biometrischen Fotos sind inhaltlich mit den sonstigen eID-Regelungen nicht verwandt, stellen aber eine erhebliche Neuregelung und Erweiterung beim Biometrieabruf und der Speicherung von Körperdaten dar. Die richtigerweise als „besonders sensibel“ benannten biometrischen Daten werden damit der Gefahr ausgesetzt, trotz aller gegenteiligen Beteuerungen nun doch zentral festgehalten und von ursprünglich dafür nie vorgesehenen Dritten verwendet zu werden, auch durch die notorisch schlecht kontrollierten Geheimdienste oder durch Zweckentfremdung von Polizeien wie im Fall des „NSU 2.0“. Bereits jetzt dürfen alle deutschen Geheimdienste mit Beginn des Jahres 2021 im automatisierten Verfahren auf die Daten der Meldeämter mit den biometrischen Passbildern zugreifen. Mit der Zentralisierung wird das nun technisch erheblich erleichtert.

Wie schon bei der letzten Neuregelung des eID-Gesetzes ist die nun geplante Zentralisierung der Biometriedaten kurz vor Ende des parlamentarischen Prozesses in einem Änderungsantrag hinzugefügt worden. Als Begründung ist lediglich eine bessere Praktikabilität benannt: Dass es für Polizeien und Geheimdienste mühsam sein kann ist, an die biometrischen Daten in den Ämtern zu kommen, kann jedoch kein Grund für einen so erheblichen Grundrechtseingriff wie die zentralisierte Speicherung von Körperdaten sein. Dezentralität ist keine zu behebende „Hinderung“ für staatliche Stellen, sondern eine absichtliche Sicherheitsvorkehrung und Machteinhegung. Solch ein Vorhaben fast gänzlich ohne Diskussion in ein ansonsten wesensfremdes Gesetz zu schmuggeln, zeigt auch angesichts laufender Verfassungs-beschwerden gegen den automatisierten Biometriezugriff[9] von hoher Ignoranz gegenüber den Grundrechten und den Prinzipien des Datenschutzes.

---

[8] Nach § 25 Absatz 2 Satz 1 und 4 sowie eines automatisierten Abrufs des Lichtbilds und der Unterschrift nach § 25 Absatz 2 Satz 5.

[9] Vgl. Beschwerdeschrift der Gesellschaft für Freiheitsrechte, https://freiheitsrechte.org/home/wp-content/uploads/2018/07/2018-07-14-VB_Passgesetz-ohne-Adressen.pdf

Das vor mehr als einem Jahrzehnt landesweit begonnene und mit Terrorfurcht begründete Vorhaben, alle Menschen in Deutschland biometrisch zu erfassen, um deren Ausweisdokumente fälschungssicher zu machen, wäre damit endgültig zu einem kaum mehr verborgenen nationalen Biometriesammelprojekt degeneriert. Denn mit der Fälschungssicherheit der Pässe gab es keine ernsthaften Probleme:[10] Sie war bereits ohne den Biometriezwang auch im internationalen Vergleich konstant hoch und ist es seitdem geblieben. Die Notwendigkeit der Speicherung von biometrischen Merkmalen war also nie gegeben, dennoch sollen die Biometriedaten von der gesamten Bevölkerung, übrigens inklusive Kinder und Jugendliche, nun auch noch zentralisiert gespeichert werden.

Die Verknüpfung mit anderen personenbezogenen Daten soll zwar vermieden werden, jedoch ist das nach einem automatisierten Abruf in der Praxis kaum oder gar nicht mehr prüfbar. Denn der automatisierte Zugriff wird ohne eine Protokollierung bei den Meldeämtern vollzogen. Für den automatisierten Abruf sollen als Auswahldaten entweder der Familienname, die Vornamen, der Tag der Geburt, der letzte Tag der Gültigkeit des Ausweisdokuments oder die Seriennummer des Ausweisdokuments verwendet werden. Damit werden alle wesentlichen Informationen der Ausweisdokumente auch automatisiert durchsuchbar.

Fazit

Auch wenn sichere digitale Identitäten auf mobilen Endgeräten grundsätzlich begrüßenswert wären, wurden im Falle des vorliegenden eID-Gesetzentwurfes leider die Erfahrungen aus den vorherigen Regelungen (insbesondere elektronischer Personalausweis und De-Mail) schlicht ignoriert. Es soll wieder eine geschlossene, proprietäre und monopolistisch betriebene Infrastruktur geschaffen werden, und wieder wurden spezifische Regelungen für die digitale Welt nicht sinnvoll getroffen.

Eine ganzheitlich gedachte Grundarchitektur fehlt. Es werden nur kleine Insellösungen geschaffen, die gerade so den angedachten Nutzungszweck erfüllen, aber nicht helfen, eine sichere und vielseitig nutzbare eGovernment-Infrastruktur aufzubauen, etwa zur Signierung von Dokumenten.

Auch hinsichtlich der IT-Sicherheit der mobilen Endgeräte weist der Entwurf gravierende Probleme auf oder ist Symptom anderweitig verfehlter IT-Sicherheits- und Digitalstrategien. Es herrscht aktuell ein Mangel an sicheren Geräten, die für die eID-Nutzung zugelassen sind. Perspektivisch werden das auch nur hochpreisige Smartphones sein. Hier zeigen sich die allgemeinen

[10] Die Bundesregierung teilte mit, die Bundespolizei habe von 2001 bis 2006 insgesamt sechs Fälschungen festgestellt: BT-Drucksache 16/5507, S. 1, http://dipbt.bundestag.de/dip21/btd/16/055/1605507.pdf vom 29. Mai 2007.

Versäumnisse der deutschen Digitalpolitik: Sozio-ökonomische Ungleichheiten werden wieder perpetuiert. Sichere Geräte sind nicht breit vorhanden, Mindeststandards und Verantwortlichkeiten dafür fehlen, letztlich entscheidet dann der Geldbeutel.

Zusätzlich sollte die Gültigkeitsdauer auch regulär auf zwei Jahre verringert werden, nicht wie aktuell fünf Jahre und nur temporär durch eine Verordnung reduziert.

Anfallende Metadaten bei Einrichtung und Nutzung der hochsensiblen eID-Funktion müssen auf ein absolut notwendiges Minimum reduziert, dann gelöscht und Zweckentfremdung explizit ausgeschlossen werden.

Die neuerliche Identifizierungsmöglichkeit hat dann auch weitere Auswirkungen in der Gesellschaft. Die Praxis von Personenkontrollen etwa ist im Rahmen des Gesetzes in den Blick zu nehmen. Eine Entsperrung von Smartphones zum Zwecke der Identifikation darf nicht verpflichtend, sondern muss explizit rechtlich verhindert werden.

Zudem fehlen diverse Umsetzungsaufwände, etwa um als Service- oder App-Anbieter aufzutreten. Auch hier wird wieder ersichtlich, das dem Gesetz keine digitale Vision zugrunde lag, wo etwa Vereine digital Unterschriften sammeln können, sondern einzig in analoger Verwaltungsdenke verharrt worden ist.

Zuletzt wird das Gesetz durch den Änderungsantrag vom 30. April auch noch dazu missbraucht, um die wesensfremde Zentralisierung von biometrischen Daten zu ermöglichen. Dieses Vorhaben ist entschieden abzulehnen.
Ein biometrische Datenabgriff bei den Bürgerämtern war schon 2017 abzulehnen, aber es ist mitnichten funktional das Gleiche, diese Daten nun zentralisiert für solche Abrufe vorzuhalten. Hier sind weder Erforderlichkeit noch Verhältnismäßigkeit gegeben.

Wir fordern abschließend dazu auf, für ein sinnvolles und zukunftsorientiertes eID-Konzept in einem dreischrittigen Prozess mit folgenden Punkten zu verfahren:

1.) Entwurf eines ganzheitlichen Architekturplanes für Authentifizierungs- und Signierungsverfahren,

2.) Erarbeitung eines neuen ressortübergreifenden Gesetzentwurfs zur Einführung einer sicheren Basis-Infrastruktur basierend auf 1.,

3.) Erarbeitung eines Gesetzentwurfs zur Einführung eines elektronischen Identitätsnachweises an Kommunikationsendpunkten basierend auf 2.

Erst mit diesem Ansatz lassen sich in der Folge weitere Dienste und Nutzungsszenarien integrieren. Von der Kontoeröffnung bei einer Bank über die Anmeldung bei einem Verein bis hin zur Identifizierung im Rahmen eines Verwaltungsvorgangs gäbe es unzählige Nutzungszenarien für digitale Identitäten.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)845 D

Niedersächsisches Studieninstitut
für kommunale Verwaltung e. V.

Kommunale Hochschule
für Verwaltung in Niedersachsen

NSI | Wielandstraße 8 | 30169 Hannover

Deutscher Bundestag
Ausschuss für Inneres und Heimat
z. Hd. der Vorsitzenden
MdB Andrea Lindholz

Platz der Republik 1
10117 Berlin

Prof. Dr. Isabell Peters
Telefon: 0511 1609-2478
Fax: 0511 15537
isabell.peters@nsi-hsvn.de

Datum: 15. Mai 2021

Öffentliche Anhörung des Ausschusses für Inneres und Heimat am 17. Mai 2021 zum Gesetzesentwurf der Bundesregierung zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät

Sehr geehrte Frau Vorsitzende,

Sie haben mich freundlicherweise als Einzelsachverständige für die öffentliche Anhörung des Ausschusses in die Sitzung am 17.05.2021 eingeladen und Gelegenheit zur Stellungnahme zum Gesetzentwurf der Bundesregierung zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät (Drucksache 19/28169) gegeben. Ich möchte zu dem Gesetzesentwurf wie folgt Stellung nehmen.

ZUSAMMENFASSUNG

I. Allgemeines

Eine Erweiterung des elektronischen Identitätsausweises für mobile Anwendungen ist eine sinnvolle erste Maßnahme, um die Verbreitung und Akzeptanz dieser Lösung am Markt zu steigern. Darüber hinaus empfehle ich zur Zielerreichung folgende weitere Schritte:

a. Bereitstellung einer sektorübergreifenden eID-Lösung,
b. mindestens jedoch einer einheitlichen Lösung für hoheitliche Anwendungsbereiche und Bereiche mit besonderer Datensensibilität (eGovernment, einschl. Finanzverwaltung, elektronische Patientenakte, usw.),
c. Erweiterung um die Funktion einer für den Nutzer kostenlosen elektronischen Signatur.

II. Einzelausführungen

Ich empfehle, folgende Einzelausführungen anzupassen:

a. Zu §§ 10a Abs. 2 PAuswG-E, 8a Abs. 1 eIDKG-E: Begrenzung der Gültigkeitsdauer des elektronischen Identitätsausweises auf einem mobilen Endgerät auf zwei Jahre (anstatt fünf Jahre).
b. Zu §§ 10a Abs. 4 PAuswG-E, 8a eIDKG-E: Für den Fall, dass auf dem mobilen Endgerät gespeicherte Daten unrichtig werden, sollte eine Regelung aufgenommen werden, die

Änderungen auf dem Speichermedium des Personalausweises durch die Ausweisbehörde mit einer Änderung der Daten im Speichermedium des mobilen Endgeräts verknüpft.

c. Zu Pkt. VII. Befristung; Evaluierung: Erhöhung der jährlichen Identifizierungsvorgänge um mindestens 200 Prozent auf rd. 34 Mio. Identifizierungsvorgänge (anstatt um 50 Prozent) binnen fünf Jahren mit einer besseren Ausnutzung von Skalen- und Verbundeffekten.

I. Allgemeines

Sichere und nutzerfreundliche Identitätsnachweise sind ein elementarer Bestandteil der Nutzung elektronischer Leistungen. Die meisten Online-Prozesse im Bereich eBusiness und eGovernment setzen die Identifikation einer Person oder eines Objektes voraus. Die elektronische Identifikation stellt damit ein Eingangstor zur Nutzung von online-Leistungen dar. Die Erweiterung des elektronischen Personalausweises (nPA) um eine mobile Komponente der Identifizierung soll insofern den Anwendungsgewohnheiten der Nutzer gerecht werden und für eine größere Akzeptanz und Verbreitung sorgen. Dies gewinnt insbesondere mit Umsetzung des Onlinezugangsgesetzes für den Bereich öffentlicher Verwaltungsleistungen Ende des Jahres 2022 an Relevanz, wenn über 575 Dienstleistungen auch online angeboten werden müssen[1].

Der Gesetzesentwurf enthält Änderungen im Personalausweisgesetz, im eID-Karte-Gesetz und im Aufenthaltsgesetz, die sämtlich um eine mobile Möglichkeit des elektronischen Identitätsnachweises erweitert werden. Insgesamt geht es um eine Ausweitung der Nutzungsmöglichkeiten des im November 2010 eingeführten elektronischen Identitätsnachweises mittels elektronischen Personalausweises (nPA) für mobile Anwendungen. Zum nPA liegen damit bereits über zehn Jahre Nutzungserfahrung vor, die zeigen, dass der nPA eine bisher anbieter- sowie nachfrageseitig wenig genutzte Lösung darstellt. Von den rd. 33,8 Mio. Personalausweisen mit aktivierter Online-Ausweisfunktion (bis Oktober 2020) nutzen knapp 15% aktiv die AusweisApp2. Die Schwierigkeit auf der Nachfrage- bzw. Nutzerseite liegt in einer mangelnden Benutzerfreundlichkeit des Verfahrens. Vor allem schreckt ein hoher Aufwand vor der Anwendung ab; erst seit dem Jahr 2017 (Android-Smartphones) bzw. seit Ende des Jahres 2019 (iPhones ab iOS 13.2) ist die Nutzung ohne ein zusätzliches Kartenlesegerät möglich. Hinzu kommt eine nur geringe Anzahl an Anwendungsmöglichkeiten: Derzeit gibt es nur 28 privatwirtschaftliche Dienste, die auf der eID-Lösung aufbauen (Stand Oktober 2020)[2]. So führen nutzerseitige Hürden zu einem sinkenden Anbieterinteresse sich dieser Lösung anzuschließen, während eine geringe Anzahl von Angeboten wiederum negativ auf den Verbreitungsgrad und die Akzeptanz der Nutzer auswirken.
Am Markt haben sich indes alternative Identifikationslösungen herausgebildet. Diese bieten Nutzern, deren eID-Funktionen entweder nicht freigeschaltet sind oder die über kein Smartphone mit kompatibler NFC-Schnittstelle verfügen (nutzbar z.B. erst ab iOS 13.2 für iPhones), die Möglichkeit eines Video-, Bank- oder PostIdent-Verfahrens an.

Insgesamt fehlt in Deutschland damit eine sektorübergreifende einheitliche eID-Lösung. In der Folge wird allen Akteuren am Markt eine elektronische Identitätsfeststellung erschwert.

[1] Von den über 575 auch online bereitzustellenden Verwaltungsleistungen gem. OZG erfordern nicht alle eine Identifizierung über das Vertrauensniveau „hoch“, das die eID gewährleistet.
2 Mit Stand 2020 wurde 142 Diensteanbietern die Berechtigung erteilt, die elektronische Ausweisfunktion des nPA in ihre Dienste einzubinden (vgl. BMI 2020, https://download.gsb.bund.de/VfB/npavfb.pdf). Davon sind etwa zwei Drittel der Verfahren Dienste einzelner Kommunen oder Ländern, die auch nur dort gemeldeten Bürgern zur Verfügung stehen. Von dem übrigen Drittel (45 Dienste) stammen 28 Dienste von privatwirtschaftlichen Anbietern, die auf der eID-Lösung aufbauen.

Kontakt
info@nsi-hsvn.de
www.nsi-hsvn.de
Telefon 0511 1609-0

Hannover
Wielandstraße 8
30169 Hannover
Fax: 0511 15537

Braunschweig
Wendenstraße 69
38100 Braunschweig
Fax: 0511 1609-5310

Oldenburg
Rosenstraße 14 – 16
26122 Oldenburg
Fax: 0511 1609-6098

Bankverbindung
Deutsche Bank Hannover
IBAN: DE35 2507 0024 0201 5733 00
BIC (SWIFT): DEUTDEDBHAN
St.-Nr. 25/207/44515

Des Weiteren bestehen unterschiedliche regulatorische Anforderungen in den für eID-relevanten Bereichen Online-Banking, eHealth und eGovernment[3]. Die Bundesregierung hat fehlende digitale Nachweise als eines der größten Digitalisierungshemmnisse unserer Zeit erkannt und mit dem „Schaufenster Sichere Digitale Identitäten“ einen Innovationswettbewerb ausgerufen. Ziel des Wettbewerbs ist es, ID-Lösungen in Zusammenarbeit von Technologieanbietern und Kommunen zu erarbeiten, die eIDAS-konform sind. Auf diese Weise sollen die digitale Souveränität und Datensicherheit in Deutschland und innerhalb der EU gestärkt werden. Zudem erarbeiten auch internationale Technologiekonzerne eID-Lösungen. Das Technologieunternehmen Apple Inc. hat im vergangenen Jahr ein Patent für eine Anwendung beantragt (Controlled Identity Credentials Release), mit der hoheitliche Identitätsdokumente auf mobilen Geräten genutzt werden können[4].

Der Blick auf erfolgreiche eID-Lösungen im europäischen Ausland wie skandinavischen und baltischen Staaten zeigt, dass *erstens* eGovernment-Dienste insgesamt nur einen geringen Anteil von unter zehn Prozent an allen eID-Transaktionen einnehmen, während die weitaus meisten Transaktionen im Finanzsektor und Online-Banking zu verzeichnen sind. *Zweitens* haben diese Länder frühzeitig eine sektorübergreifende eID-Lösung etabliert, die vor allem den Finanzsektor eingebunden hat. *Drittens* haben Länder wie Estland, Dänemark oder Schweden die elektronische Identität mit einer elektronischen Signatur versehen und damit um einen zusätzlichen Funktionsbereich erweitert. Elektronische Signaturen haben insbesondere für eGovernment-Leistungen eine ganz wesentliche Bedeutung, da sie Schriftformerfordernisse deutlich vereinfachen. Insgesamt weisen elektronische Signaturen die Eigenschaft eines Netzwerkgutes aus; sodass mit zunehmender Anzahl der Gesamtnutzer der Wert für jeden einzelnen Nutzer steigt.
Die deutsche eID-Lösung sah in der elektronischen Signatur keine staatliche Aufgabe, die im nPA integriert werden sollte, sondern setzte für die Umsetzung auf private Zertifikatsanbieter. Seit dem Jahr 2020 bietet die Bundesdruckerei eine kostenpflichtige Signaturlösung an (sign-me), die eIDAS-konform ausgestaltet ist.

Die Bundesregierung verfolgt mit dem Gesetzesentwurf die Ziele, den Verbreitungsgrad des elektronischen Identitätsnachweises zu steigern und die Nutzerfreundlichkeit zu erhöhen. Eine Ausweitung der Nutzung des elektronischen Identitätsnachweises auf mobilen Anwendungen kommt insofern den Lebensgewohnheiten der Nutzer entgegen. Allerdings ist zu bezweifeln, dass der Gesetzesentwurf die der bisherigen geringen Verbreitung und mangelnden Akzeptanz zugrunde liegenden Problemfelder in geeignetem Maß adressiert, sodass eine hohe Akzeptanz und ein gelingendes eGovernment erzielt wird.

Zur Erreichung der von der Bundesregierung verfolgten Ziele erscheinen folgende über den Gesetzesentwurf hinaus gehenden Maßnahmen sinnvoll:

a. Bereitstellung einer sektorübergreifenden eID-Lösung: eID-Angebote können aus den vorgenannten Gründen nur dann erfolgreich in der Verbreitung und Nutzung sein, wenn sie sektorübergreifend genutzt werden. Die bisherige Lösung des nPA hat anbieter- sowie nutzerseitig keine Attraktivität entwickelt, die zu einer nennenswerten Marktdurchdringung geführt hat. Daher sollten anbieterseitig sektorübergreifend nutzbare Lösungen entwickelt werden, indem entweder

[3] Im Banking bestehen Auflagen zur Identitätsfeststellung nach dem Geldwäschegesetz unter Aufsicht der BaFin, eGovernment-Anwendungen sind gem. eIDAS-Verordnung zu zertifizieren; zudem sind die technischen Richtlinien des BSI und Konformitätsprüfungen durch den TÜV zu erfüllen.
[4] United States Patent Application Publication, Appl. No.: 16/840,200, Pub. No.: US 2020/0320188 A1 vom 8.10.2020.

Kontakt
info@nsi-hsvn.de
www.nsi-hsvn.de
Telefon 0511 1609-0

Hannover
Wielandstraße 8
30169 Hannover
Fax: 0511 15537

Braunschweig
Wendenstraße 69
38100 Braunschweig
Fax: 0511 1609-5310

Oldenburg
Rosenstraße 14 – 16
26122 Oldenburg
Fax: 0511 1609-6098

Bankverbindung
Deutsche Bank Hannover
IBAN: DE35 2507 0024 0201 5733 00
BIC (SWIFT): DEUTDEDBHAN
St.-Nr. 25/207/44515

i. die eID zu einem sektorübergreifend nutzbaren Angebot weiterentwickelt wird (dafür seien insbes. die Interessen der zahlenmäßig relevanten Branchen zu berücksichtigen) oder
ii. die im Innovationswettbewerb „Schaufenster Sichere Digitale Identitäten“ beste Lösung zusammen mit der Finanzbranche zu einer neuen nationalen elektronischen Identifizierung ausgebaut wird;

b. im Mindesten sollte eine einheitliche Lösung für hoheitliche Anwendungsbereiche und Bereiche mit besonderer Datensensibilität (eGovernment, einschl. Finanzverwaltung und Gerichtswesen, Gesundheitsbereich (elektronische Patientenakte, ePA) geschaffen werden. Mehrere verschiedene elektronische Identitätsnachweise mindern die Akzeptanz und den Verbreitungsgrad jeder einzelnen Lösung und erschweren damit erfolgreiche eGovernment-Prozesse. Elektronische Identitätsnachweisverfahren der Finanzverwaltung (ELSTER-ID „EKONA“) und aus dem Gesundheitsbereich (ePA) sollten auf einem identischen Verfahren beruhen.

c. Erweiterung um die Funktion einer für den Nutzer kostenlosen elektronischen Signatur: Die eID sollte um eine kostenlos nutzbare elektronische Signatur erweitert werden. Eine derartige Funktion würde den Nutzen und damit die Akzeptanz und Verbreitung der Lösung erheblich steigern und die Schriftformerfordernis in eGovernment-Prozessen umzusetzen helfen.

II. Einzelausführungen

a. Zu §§ 10a Abs. 2 PAuswG-E, 8a Abs. 1 eIDKG-E: Begrenzung der Gültigkeitsdauer des elektronischen Identitätsausweises auf einem mobilen Endgerät auf zwei Jahre (anstatt fünf Jahre). Zur Gewährleistung der Datensicherheit sollte ein elektronischer Identitätsnachweis nicht länger als maximal zwei Jahre auf dem Mobiltelefon seine Gültigkeit behalten. Dies ist der Zeitraum von marktüblichen Smartphoneanbietern, für den Patches mindestens ab Kaufdatum angeboten werden. Auch dann bestehen Sicherheitsrisiken fort, sollten Ausweisinhaber die AusweisApp2 erst gegen Ende dieses Zeitraums installiert haben oder Patches nicht regelmäßig installieren.

b. Zu §§ 10a Abs. 4 PAuswG-E, 8a eIDKG-E: für den Fall, dass auf dem mobilen Endgerät gespeicherte Daten unrichtig werden, sollte eine Regelung aufgenommen werden, die Änderungen auf dem Speichermedium des Personalausweises durch die Ausweisbehörde mit einer Änderung der Daten im Speichermedium des mobilen Endgeräts verknüpft. Die reine Regelung, dass ein Ausweisinhaber einen elektronischen Identitätsnachweis im Falle von Änderungen der Daten nicht durchführen darf, wird als nicht ausreichend erachtet.

c. Zu Pkt. VII. Befristung; Evaluierung: Erhöhung der jährlichen Identifizierungsvorgänge von derzeit etwa 8,5 Mio. um mindestens 200 Prozent auf rd. 34 Mio. Identifizierungsvorgänge (anstatt um 50 Prozent). Bei den zugrunde gelegten Kosten des jährlichen Erfüllungsaufwands in Höhe von 26,1 Mio. Euro sowie einem einmaligen Erfüllungsaufwand in Höhe von 19,1 Mio. Euro, ergeben sich auf einen Zeitraum von fünf Jahren berechnet jährliche Kosten in Höhe von 29,92 Mio. Euro. Dies entspricht für die angestrebte Anzahl von bislang nur 12,75 Mio. jährlichen Identifizierungsvorgängen Kosten in Höhe von rund 2,35 Euro pro Identifizierungsvorgang. Neben den unter Pkt. I meiner Stellungnahme genannten Gründen sollten auch aus finanzieller Perspektive die Anwendungszahlen deutlich erhöht und Skalen- sowie Verbundeffekte ausgenutzt werden.

Kontakt
info@nsi-hsvn.de
www.nsi-hsvn.de
Telefon 0511 1609-0

Hannover
Wielandstraße 8
30169 Hannover
Fax: 0511 15537

Braunschweig
Wendenstraße 69
38100 Braunschweig
Fax: 0511 1609-5310

Oldenburg
Rosenstraße 14 – 16
26122 Oldenburg
Fax: 0511 1609-6098

Bankverbindung
Deutsche Bank Hannover
IBAN: DE35 2507 0024 0201 5733 00
BIC (SWIFT): DEUTDEDBHAN
St.-Nr. 25/207/44515

Ich wäre Ihnen dankbar, wenn Sie die Stellungnahme zur Kenntnis nehmen würden.

Mit freundlichen Grüßen

[redacted]

Isabell Peters

Kontakt
info@nsi-hsvn.de
www.nsi-hsvn.de
Telefon 0511 1609-0

Hannover
Wielandstraße 8
30169 Hannover
Fax: 0511 15537

Braunschweig
Wendenstraße 69
38100 Braunschweig
Fax: 0511 1609-5310

Oldenburg
Rosenstraße 14 – 16
26122 Oldenburg
Fax: 0511 1609-6098

Bankverbindung
Deutsche Bank Hannover
IBAN: DE35 2507 0024 0201 5733 00
BIC (SWIFT): DEUTDEDBHAN
St.-Nr. 25/207/44515

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)845 E

Bonn, den 17.05.2021

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Ausschusses für Inneres und Heimat
am 17.05.2021

zum **Entwurf eines Gesetzes zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät** – BT-Drs. 19/28169

unter Berücksichtigung der mit **Anträgen der Fraktionen der CDU/CSU und der SPD** –

A-Drs. **19(4)825** und **19(4)826** vom 30.04.2021 – vorgeschlagenen Änderungen

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

1. Allgemeines

Mit dem Entwurf des Gesetzes zur Einführung eines elektronischen Identitätsnachweises sollen durch Änderungen im Personalausweisgesetz (PAuswG), im eID-Karte-Gesetz (eIDKG) und im Aufenthaltsgesetz rechtliche Grundlagen für einen elektronischen Identitätsnachweis mit einem mobilen Endgerät geschaffen werden. Diese zusätzliche Nachweis-Funktion soll neben der hochsicheren eID-Funktion des Personalausweises, der eID-Karte bzw. des elektronischen Aufenthaltstitels ermöglicht werden.

Dem Gesetzentwurf ist bisher nicht zu entnehmen, ob der elektronische Identitätsnachweis mittels eines mobilen Endgeräts die gleichen Sicherheitsanforderungen wie die bisherigen elektronischen Identitätsnachweise mittels Personalausweis, eID-Karte oder elektronischen Aufenthaltstitel erfüllt bzw. erfüllen soll. Insbesondere fehlen Informationen, welches Sicherheitsniveau gemäß der eIDAS-Verordnung durch den elektronischen Identitätsnachweis mit einem mobilen Endgerät erreicht werden soll. Hier sollte der Gefahr, dass das Sicherheitsniveau zugunsten der erwünschten Nutzerfreundlichkeit abgeschwächt wird, vorgebeugt werden. Unbeantwortet bleibt auch die Frage, ob für denjenigen, dem gegenüber die elektronische Identifikation erfolgt, die Wahl des Mittels (eID-Karte oder mobiles Endgerät) erkennbar sein muss, etwa weil auf Seiten des Empfängers besondere Voraussetzungen für den Fall der Nutzung des elektronischen Identitätsnachweises mittels mobilem Endgerät vorliegen müssen. Hierzu sollten zumindest in der Gesetzesbegründung Ausführungen gemacht werden.

Die mit A-Drs. 19(4)826 vom 30.04.2021 zum Ausdruck gebrachte Unterstützung dieses Anliegens begrüße ich daher.

Ebenfalls auf Antrag der Fraktionen der CDU/CSU und der SPD (A-Drs. 19(4)825) soll der Gesetzentwurf u. a. eine Erweiterung dahingehend erfahren, dass sowohl im Passgesetz (PassG) als auch im PAuswG eine Regelungsbefugnis zugunsten der Länder eingeräumt wird, ein zentrales Register zur vereinfachten Durchführung eines automatisierten Abrufs des Lichtbilds und der Unterschrift in den Fällen des § 22a Absatz 2 PassG bzw. § 25 Absatz 2 PAuswG einzurichten. Dieses Vorhaben stößt auf nachstehend erläuterte grundsätzliche datenschutzrechtliche Bedenken.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

2. Zu einzelnen Änderungsbefehlen

a) Zu **Artikel 1 – Änderung des Passgesetzes** (§ 27a – neu PassG-E)

Die hier durch einen neu einzufügenden § 27a PassG-E eingeräumte Befugnis, auf Länderebene zentrale Passregisterdatenbestände zum Zweck des automatisierten Abrufs des Lichtbilds und der Unterschrift einrichten zu können, wird hauptsächlich damit begründet, dass es für viele Kommunen bereits eine große Herausforderung bedeuten würde, allein die technischen Voraussetzungen für den automatisierten Abruf sicherzustellen, und dass eine zentrale Datenhaltung neben einer Erleichterung der Umsetzung der Abrufe auch die Möglichkeit der Einbindung spezialisierter Einrichtungen zur Gewährleistung eines hohen Maßes an Datensicherheit biete.

Diesen Erwägungen steht allerdings gegenüber, dass der in den Pass- und Personalausweisbehörden für einen automatisierten Abruf vorhandene Datenbestand auf Landesebene zusätzlich noch einmal gespiegelt und dauerhaft für die gesetzlich vorgesehenen Abrufzwecke vorgehalten würde. Da jeder neu und auf Dauer geschaffene Bestand an personenbezogenen Daten das Risiko einer zweckfremden Verwendung oder eines Missbrauchs potenziell deutlich erhöht, ist seine Einrichtung vor allem an den datenschutzrechtlichen Grundsätzen der Datenminimierung und Erforderlichkeit zu messen. Schon in dieser Hinsicht bedarf es unabweisbarer Gründe, um einen solchen zusätzlichen Datenbestand zu legitimieren.

Die Anforderungen an diesen Prüfungsmaßstab steigen noch, wenn – wie hier hinsichtlich des biometrischen Lichtbilds – eine Verarbeitung von besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO erfolgt. An dieser Stelle sehe ich auch einen entscheidenden Unterschied zu den bereits etablierten zentralen (Spiegel-)Melderegistern der Länder zum Zweck eines automatisierten Abrufs bestimmter Meldedaten nach § 39 Abs. 3 Bundesmeldegesetz – denn hierbei handelt es sich nicht um eine Verarbeitung besonders sensibler Daten im Sinne des Art. 9 DSGVO.

Im Lichte dessen kann die Begründung des Änderungsantrags daher nicht überzeugen. Insbesondere ist ein erhebliches öffentliches Interesse an der Errichtung eines solchen Registers auf der Grundlage eines nationalen Gesetzes, wie es Art. 9 Abs. 2 lit. g) DSGVO verlangt, wenn die Betroffenen nicht ausdrücklich in diese Datenverarbeitung eingewilligt haben, nicht herauslesbar.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Dieser strenge Maßstab kommt nach meiner Auffassung bereits dann zum Tragen, wenn mit dem nationalen Gesetz zunächst lediglich eine entsprechende Ermächtigung im Wege einer Öffnungsklausel für den darauf tätig werdenden Landesgesetzgeber geschaffen wird. Denn die Festlegung, es bestehe ein erhebliches öffentliches Interesse an der Errichtung zentraler Abrufregister für Lichtbild und Unterschrift auf Landesebene, trifft der (Bundes-)Gesetzgeber bereits an dieser Stelle der Aufnahme der Öffnungsklausel, vor allem, wenn er sich die von Länderseite dazu vorgebrachten Argumente zu eigen macht.

Wie in der Begründung zum Änderungsantrag ausgeführt, müssen die technischen Voraussetzungen eines bundesweiten automatisierten Abrufs im Wege einheitlicher Kommunikationsstandards ohnehin noch geschaffen werden. Eine Einbindung sämtlicher Pass- und Personalausweisbehörden in diesen Prozess ist technisch sicherlich möglich, wenn auch aufwändiger. Das grundsätzlich nachvollziehbare Motiv einer Verfahrenserleichterung reicht für die Bejahung eines „erheblichen“ öffentlichen Interesses jedenfalls nicht aus – hierzu bedarf es vielmehr eines qualifizierten Interesses mit ausreichend Gewicht, wie beispielsweise im Fall humanitärer Notlagen infolge von Naturkatastrophen oder zur Überwachung von Epidemien und deren Ausbreitung (siehe ErwGr. 46 DSGVO).

Aus den genannten Gründen kann ich der vorgeschlagenen Änderung bzw. Ergänzung des PassG durch die Aufnahme eines § 27a nicht zustimmen.

Mit den gleichen Erwägungen bitte ich, den inhaltlich deckungsgleichen Regelungsvorschlag eines neu einzufügenden **§ 34a PAuswG-E** (**Änderungsbefehl Nr. 19** des o. g. Änderungsantrags **A-Drs. 19(4)825**) ebenfalls nicht zu berücksichtigen.

b) Zu **Artikel 2 – neu – Änderungsbefehl Nr. 8** (§ 10a – neu PAuswG-E)

Mit dem neu einzufügenden § 10a PAuswG-E soll die Einrichtung des elektronischen Identitätsnachweises mit einem mobilen Endgerät generell regelt werden.

aa) Gültigkeitsdauer der Anwendung (§ 10a Absatz 2 PAuswG-E)

§ 10a Absatz 2 PAuswG-E befasst sich mit der Gültigkeitsdauer des elektronischen Identitätsnachweises mit einem mobilen Endgerät. Sie soll maximal fünf Jahre betragen. Durch Rechtsverordnung soll aber eine kürze Gültigkeitsdauer festgelegt werden können. Laut

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Gesetzesbegründung soll zunächst sogar eine kürzere Geltungsdauer von zwei Jahren in der Personalausweisverordnung (PAuswV) normiert werden, da gerade zu Beginn damit zu rechnen sei, dass sich der Stand der Technik in einem entsprechenden Zeitintervall verändern werde. Eine entsprechende Änderung der PAuswV fehlt allerdings im Gesetzentwurf.

Generell halte ich eine Gültigkeitsdauer von fünf Jahren für einen elektronischen Identitätsnachweises mit einem mobilen Endgerät für deutlich zu lang. Für die vorgesehene Funktion sind besondere sicherheitstechnische Anforderungen an das mobile Endgerät zu stellen. Um Missbrauch zu vermeiden, ist darauf zu achten, dass das jeweilige Endgerät aus Gründen der Datensicherheit immer auf dem aktuellsten Stand ist, also alle vom Hersteller bereitgestellten Sicherheitspatches installiert wurden. In der Regel stellen die Hersteller von mobilen Endgeräten längstens fünf Jahre lang Sicherheitspatches zur Verfügung. Danach dürften die mobilen Endgeräte die Sicherheitsanforderungen für einen elektronischen Identitätsnachweis nicht mehr erfüllen. Es ist somit davon auszugehen, dass ein elektronischer Identitätsnachweis auch auf einem mobilen Endgerät eingerichtet werden kann, das ab dem Zeitpunkt der Einrichtung keine fünf Jahre lang mehr durch den Hersteller mit Sicherheitspatches versorgt wird und somit Sicherheitslücken aufweist, die negative Auswirkungen auf die Zuverlässigkeit der Identifizierung und Anerkennung als sicheres Identifizierungsverfahren haben könnten. Die gesetzlich festgelegte Gültigkeitsdauer muss diesem Umstand Rechnung tragen und grundsätzlich auf einen kürzeren Zeitraum begrenzt werden. Zudem ist zu berücksichtigen, dass sich der Stand der Technik im Bereich der mobilen Endgeräte erfahrungsgemäß in immer kürzeren Abständen weiterentwickelt und nicht erst nach Ablauf von fünf Jahren überholt sein dürfte.
Zwar soll durch die im Gesetzentwurf angeführte, aber im Rahmen dieses Rechtsetzungsvorhabens von der Bundesregierung nicht vorgelegte, Rechtsverordnung die Festlegung einer kürzeren Gültigkeitsdauer für den elektronischen Identitätsnachweis mit einem mobilen Endgerät ermöglicht werden. Da die zeitliche Bemessung der Gültigkeit jedoch einen unmittelbaren Einfluss auf die Zuverlässigkeit einer Identifizierung hat, handelt es sich hierbei um eine wesentliche Regelung, die im PAuswG selbst festgelegt werden sollte. Demgemäß halte ich es für erforderlich, die Gültigkeitsdauer des elektronischen Identitätsnachweises mit einem mobilen Endgerät gesetzlich generell auf zwei Jahre zu begrenzen. Entsprechend müsste § 10a Absatz 2 Satz 1 PAuswG-E wie folgt gefasst werden:

(2) Die Gültigkeitsdauer eines elektronischen Identitätsnachweises nach § 18 Absatz 2 Satz 1 Nummer 2 auf Grundlage einer Übermittlung der Daten nach Absatz 1 beträgt höchstens zwei Jahre.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Der mit der Verkürzung der Gültigkeitsdauer verbundene Mehraufwand für eine häufigere Wiedereinrichtung des elektronischen Identitätsnachweises durch die Nutzenden steht dabei, gerade mit Blick auf das damit verbundene Mehr an Sicherheit, der Schaffung eines nutzerfreundlichen elektronischen Identitätsnachweises und seiner Akzeptanz sicherlich nicht im Wege.

bb) Ergänzende Regelung für Fälle einer Sperrung der Nachweisfunktion

§ 10a Absatz 4 PAuswG-E regelt den Fall, dass die auf das elektronischen Speicher- und Verarbeitungsmedium des mobilen Endgeräts übermittelten Daten unrichtig werden. An dieser Stelle fehlt eine Regelung, die die Änderung von Daten auf dem Personalausweis oder auf dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises durch die Personalausweisbehörde mit einer Änderung der Daten im Speicher- und Verarbeitungsmedium des mobilen Endgeräts koppelt. Zwar dürfte der Ausweisinhaber einen elektronischen Identitätsnachweis mittels mobilem Endgerät nicht durchführen, wenn die Daten unrichtig sind. Jedoch kann nicht ausgeschlossen werden, dass sich der Ausweisinhaber an diese Vorgabe nicht hält.
Zudem fehlt im Gesetzentwurf eine § 10 Absatz 5 PAuswG-E entsprechende Regelung für die Sperrung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät, z. B. für den Fall, dass das mobile Endgerät abhandenkommt.

Daher halte ich es für angezeigt, § 10a PAuswG-E um einen Absatz 6 wie folgt zu ergänzen:

(6) Die zuständige Personalausweisbehörde hat zur Aktualisierung der Sperrliste unverzüglich die Sperrsumme des elektronischen Identitätsnachweises mit einem mobilen Endgerät an den Sperrlistenbetreiber nach § 7 Absatz 4 Satz 2 zu übermitteln, wenn sie Kenntnis erlangt von

1. *dem Abhandenkommen eines mobilen Endgeräts mit elektronischem Identitätsnachweis,*
2. *dem Versterben eines Ausweisinhabers,*
3. *der Ungültigkeit eines Ausweises nach § 28 Absatz 1 oder Absatz 2 oder*
4. *der Unrichtigkeit der auf das elektronischen Speicher- und Verarbeitungsmedium des mobilen Endgeräts übermittelten Daten nach Absatz 1 Satz 1.*

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

c) Zu **Artikel 3 – neu – Änderungsbefehl Nr. 5** (§ 8a – neu eIDKG-E)

Das zu § 10a – neu PAuswG-E Ausgeführte trifft auch auf den Regelungsinhalt des § 8a – neu eID-Karte-Gesetz zu. Zur Vermeidung von Wiederholungen verweise ich insoweit auf meine Ausführungen zu Gliederungspunkt 2. b) aa) oben und rege an, § 8a Absatz 2 Satz 1 eIDKG-E wie folgt zu ändern:

(2) Die Gültigkeitsdauer eines elektronischen Identitätsnachweises nach § 12 Absatz 2 Satz 1 Nummer 2 auf Grundlage einer Übermittlung der Daten nach Absatz 1 beträgt höchstens 2 Jahre.

Darüber hinaus wäre – entsprechend meinen Ausführungen oben zu Gliederungspunkt 2. b) bb) – § 8a eIDKG-E ebenfalls um einen neuen Absatz 6 wie folgt zu ergänzen:

(6) Die zuständige Personalausweisbehörde hat unverzüglich zur Aktualisierung der Sperrliste die Sperrsumme des elektronischen Identitätsnachweises mit einem mobilen Endgerät an den Sperrlistenbetreiber nach § 7 Absatz 4 Satz 2 zu übermitteln, wenn sie Kenntnis erlangt von

1. *dem Abhandenkommen eines mobilen Endgeräts mit elektronischem Identitätsnachweis,*
2. *dem Versterben eines Karteninhabers,*
3. *der Ungültigkeit einer eID-Karte nach § 21 oder*
4. *der Unrichtigkeit der auf das elektronischen Speicher- und Verarbeitungsmedium des mobilen Endgeräts übermittelten Daten nach Absatz 1 Satz 1.*

Auf meine Stellungnahme vom 22.03.2021 gegenüber dem Ausschuss für Inneres und Heimat zu diesem Gesetzgebungsvorhaben nehme ich ergänzend Bezug.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Deutscher Bundestag
Ausschuss für Inneres und Heimat
z. Hd. der Vorsitzenden
Frau Andrea Lindholz, MdB

Platz der Republik 1
11011 Berlin

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-5000
FAX (0228) 997799-5550
E-MAIL referat21@bfdi.bund.de
INTERNET www.bfdi.bund.de
DATUM Bonn, 22.03.2021
GESCHÄFTSZ. 21-206-6/002#0003

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Gesetzentwurf zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät**

ANLAGEN - 1

Sehr geehrte Frau Vorsitzende,

im Rahmen meiner Beteiligung an der Ressortabstimmung des im Betreff genannten Gesetzentwurfs hat die Bundesregierung nicht allen von mir aufgeworfenen datenschutzkritischen Punkten Rechnung getragen.

Daher leite ich Ihnen meine als Anlage beigefügte Stellungnahme zu und wäre dankbar, wenn meine Formulierungsvorschläge in den Beratungen berücksichtigt werden.

Für die Weiterleitung an die für den Gesetzentwurf noch zu benennenden Berichterstattenden und die übrigen Ausschussmitglieder wäre ich Ihnen ebenfalls dankbar.

Mit freundlichen Grüßen

[redacted]

Ulrich Kelber

26327/2021

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Bonn, den 22.03.2021

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Gesetzes zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät

vom 12. Februar 2021

BR-Drs. 139/21

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

1. Allgemeines

Mit dem Entwurf des Gesetzes zur Einführung eines elektronischen Identitätsnachweises sollen durch Änderungen am Personalausweisgesetz (PAuswG), am eID-Karte-Gesetz (eIDKG) und am Aufenthaltsgesetz rechtliche Grundlagen für einen elektronischen Identitätsnachweis mit einem mobilen Endgerät geschaffen werden. Dieser soll neben der hochsicheren eID-Funktion des Personalausweises, der eID-Karte bzw. des elektronischen Aufenthaltstitels, ermöglicht werden. Dem Gesetzentwurf ist nicht zu entnehmen, ob der elektronische Identitätsnachweis mittels eines mobilen Endgeräts die gleichen Sicherheitsanforderungen wie die bisherigen elektronischen Identitätsnachweise mittels Personalausweis, eID-Karte oder elektronischen Aufenthaltstitel erfüllt bzw. erfüllen soll. Insbesondere fehlen Informationen, welches Sicherheitsniveau gemäß der eIDAS-Verordnung durch den elektronischen Identitätsnachweis mit einem mobilen Endgerät erreicht werden soll. Hier sehe ich die Gefahr, dass zugunsten der erwünschten Nutzerfreundlichkeit das Sicherheitsniveau abgeschwächt wird. In diesem Zusammenhang stellt sich auch die Frage, ob für denjenigen, dem gegenüber die elektronische Identifikation erfolgt, erkennbar ist, ob ein elektronischer Identitätsnachweis mittels Karte oder mittels mobilem Endgerät durchgeführt wurde und ob bei ihm besondere Voraussetzungen für den Fall der Nutzung des elektronischen Identitätsnachweises mittels mobilem Endgerät vorliegen müssen. Hierzu sollten zumindest in der Gesetzesbegründung Ausführungen gemacht werden.

2. Zu einzelnen Änderungsbefehlen

1. Zu Artikel 1 Änderungsbefehl Ziffer 8 zu § 10a PAuswG-E

Mit dem § 10a PAuswG-E soll die Einrichtung des elektronischen Identitätsnachweises mit einem mobilen Endgerät generell regelt werden.
§ 10a Absatz 2 PAuswG-E befasst sich mit der Gültigkeitsdauer des elektronischen Identitätsnachweises mit einem mobilen Endgerät. Sie soll maximal fünf Jahre betragen. Durch eine Rechtsverordnung soll aber eine kürze Gültigkeitsdauer festgelegt werden können. Laut Gesetzesbegründung soll zunächst sogar eine kürzere Geltungsdauer von zwei Jahren in der Personalausweisverordnung (PAuswV) normiert werden, da gerade zu Beginn damit

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

zu rechnen sei, dass sich der Stand der Technik in einem entsprechenden Zeitintervall verändern werde. Eine entsprechende Änderung der PAuswV fehlt allerdings im Gesetzentwurf.

Generell halte ich eine Gültigkeitsdauer des elektronischen Identitätsnachweises mit einem mobilen Endgerät von 5 Jahren für viel zu lang. Es sind besondere sicherheitstechnische Anforderungen an das mobile Endgerät zu stellen. Um Missbrauch zu vermeiden, ist darauf zu achten, dass das jeweilige Endgerät aus Gründen der Datensicherheit immer auf dem aktuellsten Stand ist, d. h. ob alle vom Hersteller bereitgestellten Sicherheitspatches installiert wurden. Grundsätzlich stellen die Hersteller von mobilen Endgeräten längstens fünf Jahre lang Sicherheitspatches zur Verfügung. Nach dieser Zeit dürften die mobilen Endgeräte die Sicherheitsanforderungen für einen elektronischen Identitätsnachweis nicht mehr erfüllen. Es ist davon auszugehen, dass ein elektronischer Identitätsnachweis auch auf einem mobilen Endgerät eingerichtet werden wird, das ab dem Zeitpunkt der Einrichtung keine fünf Jahre lang mehr durch den Hersteller mit Sicherheitspatches versorgt wird und somit Sicherheitslücken aufweist, die negative Auswirkungen auf die Zuverlässigkeit der Identifizierung und Anerkennung als sicheres Identifizierungsverfahren haben könnten. Die Gültigkeitsdauer müsste mit dem Zeitraum, in dem der Hersteller die Sicherheitspatches zur Verfügung stellt, gekoppelt werden oder generell auf eine kürzere Zeit begrenzt werden. Zudem entwickelt sich der Stand der Technik im Bereich der mobilen Endgeräte erfahrungsgemäß rasant weiter und ist nach fünf Jahren mehr als einmal überholt. Zwar soll - wie bereits erwähnt - durch die im Gesetzentwurf angeführte, aber im Rahmen dieses Rechtsetzungsvorhabens von der Bundesregierung nicht vorgelegte Rechtsverordnung eine kürzere Gültigkeitsdauer für den elektronischen Identitätsnachweis mit einem mobilen Endgerät festgelegt werden. Jedoch handelt es sich hier um eine wesentliche Regelung, die Einfluss auf die Zuverlässigkeit einer Identifizierung hat und sich daher im PAuswG selbst wiederfinden sollte.
Ich schlage daher vor, in § 10a Absatz 2 PAuswG-E die Gültigkeitsdauer des elektronischen Identitätsnachweises mit einem mobilen Endgerät auf 2 Jahre zu begrenzen. Entsprechend müsste § 10a Absatz 2 Satz 1 PAuswG-E wie folgt gefasst werden:

(2) *Die Gültigkeitsdauer eines elektronischen Identitätsnachweises nach § 18 Absatz 2 Satz 1 Nummer 2 auf Grundlage einer Übermittlung der Daten nach Absatz 1 beträgt 2 Jahre.*

Der mit der Verkürzung der Gültigkeitsdauer verbundene zeitliche Mehraufwand bei den Bürgerinnen und Bürgern von durchschnittlich 3 Minuten für eine einmalige Einrichtung des elektronischen Identitätsnachweises verhält sich dabei in einem sehr akzeptablen

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Rahmen, gerade im Hinblick auf das Mehr an Sicherheit, und steht daher der Schaffung eines nutzerfreundlichen elektronischen Identitätsnachweises nicht im Wege.

§ 10a Absatz 4 PAuswG-E regelt den Fall, dass die auf das elektronischen Speicher- und Verarbeitungsmedium des mobilen Endgeräts übermittelten Daten unrichtig werden. An dieser Stelle fehlt eine Regelung, die die Änderung von Daten auf dem Personalausweis oder auf dem elektronischen Speicher- und Verarbeitungsmedium des Personalausweises durch die Personalausweisbehörde mit einer Änderung der Daten im Speicher- und Verarbeitungsmedium des mobilen Endgeräts koppelt. Zwar dürfte der Ausweisinhaber einen elektronischen Identitätsnachweis mittels mobilem Endgerät nicht durchführen, wenn die Daten unrichtig sind. Jedoch kann nicht ausgeschlossen werden, dass sich der Ausweisinhaber an diese Vorgabe nicht hält.
Zudem fehlt im Gesetzentwurf eine § 10 Absatz 5 PAuswG-E entsprechende Regelung für die Sperrung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät, z. B. für den Fall, dass das mobile Endgerät abhandenkommt.

Daher halte ich es für angebracht, § 10a PAuswG-E um einen Absatz 6 wie folgt zu ergänzen:

(6) Die zuständige Personalausweisbehörde hat unverzüglich zur Aktualisierung der Sperrliste die Sperrsumme des elektronischen Identitätsnachweises mit einem mobilen Endgerät an den Sperrlistenbetreiber nach § 7 Absatz 4 Satz 2 zu übermitteln, wenn sie Kenntnis erlangt von

1. *dem Abhandenkommen eines mobilen Endgeräts mit elektronischem Identitätsnachweis,*
2. *dem Versterben eines Ausweisinhabers,*
3. *der Ungültigkeit eines Ausweises nach § 28 Absatz 1 oder Absatz 2 oder*
4. *der Unrichtigkeit der auf das elektronischen Speicher- und Verarbeitungsmedium des mobilen Endgeräts übermittelten Daten nach Absatz 1 Satz 1.*

2. Zu Artikel 2 Änderungsbefehl Ziffer 5 zu § 8a eIDKG-E

Zur Vermeidung von Wiederholungen verweise ich auf meine Ausführungen zu Artikel 1 Ziffer 8 oben und schlage vor, § 8a Absatz 2 Satz 1 eIDKG-E wie folgt zu ändern:

(2) Die Gültigkeitsdauer eines elektronischen Identitätsnachweises nach § 12 Absatz 2 Satz 1 Nummer 2 auf Grundlage einer Übermittlung der Daten nach Absatz 1 beträgt 2 Jahre.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Darüber hinaus wäre § 8a eIDKG-E ebenfalls um einen Absatz 6 zu ergänzen:

(6) Die zuständige Personalausweisbehörde hat unverzüglich zur Aktualisierung der Sperrliste die Sperrsumme des elektronischen Identitätsnachweises mit einem mobilen Endgerät an den Sperrlistenbetreiber nach § 7 Absatz 4 Satz 2 zu übermitteln, wenn sie Kenntnis erlangt von

1. *dem Abhandenkommen eines mobilen Endgeräts mit elektronischem Identitätsnachweis,*
2. *dem Versterben eines Karteninhabers,*
3. *der Ungültigkeit einer eID-Karte nach § 21 oder*
4. *der Unrichtigkeit der auf das elektronischen Speicher- und Verarbeitungsmedium des mobilen Endgeräts übermittelten Daten nach Absatz 1 Satz 1.*

[redacted]

Prof. Ulrich Kelber

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de