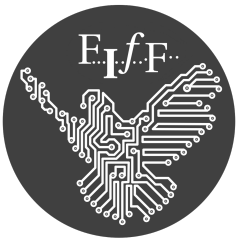
Chaos Computer Club



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.