Deutscher Bundestag **Drucksache 20/9185**

20. Wahlperiode 08.11.2023

Antwort

der Bundesregierung

auf die Kleine Anfrage der Fraktion der CDU/CSU
– Drucksache 20/8930 –

Smart-eID

Vorbemerkung der Fragesteller

Die Einführung des Personalausweises mit der Online-Ausweisfunktion im Jahr 2010 legte in Deutschland den Grundstein für die Entwicklung staatlicher digitaler Identitäten. Darauffolgend wurde mit dem Onlinezugangsgesetz (OZG) eine wichtige Grundlage für die Digitalisierung und die Bereitstellung von Verwaltungsdienstleistungen in Deutschland gelegt. Dieses Gesetz ebnete gleichzeitig den Weg für die Einführung eines elektronischen Identitätsnachweises über mobile Endgeräte, wie im Smart-eID-Gesetz (Bundestagsdrucksache 19/28169, www.bundestag.de/dokumente/textarchiv/2021/kw20-de-elektronischer-identitaetsnachweis-840256) vom 25. Juni 2021.

Aktuell arbeitet die Bundesregierung an der Umsetzung und Weiterentwicklung der sogenannten Smart-eID, wie in der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU „Stand der Umsetzung der eIDAS-2.0-Verordnung“ dargelegt (Bundestagsdrucksache 20/8201; insbesondere zu den Fragen 26 und 55 bis 62).

Eine entscheidende Rolle bei der Sicherheitszertifizierung und Prüfung von IT-Lösungen, insbesondere im Bereich digitaler Identitätslösungen, kommt unter anderem dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu.

Die geplante Einführung der Smart-eID steht bis heute aus. Die Smart-eID verspricht die Erleichterung der Authentifizierung bei Dienstleistungen der öffentlichen Verwaltung und im privatwirtschaftlichen Kontext, wie beispielsweise der Kontoeröffnung, und hat damit auch das Potenzial, die Digitalisierung in Deutschland weiter voranzutreiben und somit die Wettbewerbsfähigkeit in einer globalisierten, von der Digitalisierung geprägten Welt nachhaltig zu stärken. Angesichts dieser Bedeutung ist nach Ansicht der Fragesteller die zeitnahe Umsetzung dieses Vorhabens von großer Relevanz.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 2. November 2023 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

1. Wie gedenkt die Bundesregierung, die Smart-eID in das Gesamtökosystem von digitalen Identitäten und insbesondere im Rahmen der EUDI-Wallet (EUDI = European Digital Identity) einzubetten?

   Existiert hierzu ein Austauschformat zwischen dem Bundesministerium für Digitales und Verkehr (BMDV) und dem Bundesministerium des Innern und für Heimat (BMI)?

Die Smart-eID setzt auf dem bestehenden Online-Ausweis auf und erweitert diesen um das Komfortmerkmal, die Karte bei der Nutzung nicht an das mobile Endgerät halten zu müssen. Es handelt sich somit nicht um eine Änderung des bestehenden Systems, die neu in das bestehende Ökosystem zu integrieren ist, sondern ergänzt das bestehende System. Ein Austausch mit anderen Ressorts ist über das GovLab.DE Digitale Identitäten sichergestellt (vgl. Antwort zu Frage 4).

2. Ist die Smart-eID-Funktion schon in der Ausweisapp2 freigeschaltet?

Die Smart-eID ist in eine Preview-Version der AusweisApp2 integriert. Eine Freischaltung in der öffentlich verfügbaren Version der AusweisApp2 erfolgt zum öffentlichen Start der Smart-eID.

3. Für wann ist der Launch der Smart-eID geplant, und in welcher Form?

Ein Datum für den öffentlichen Start der Smart-eID steht noch nicht fest. Nach Aufnahme des Wirkbetriebs, in dem mit „echten“ Ausweisen Smart-eIDs erzeugt werden können, ist zunächst eine kurze nicht öffentliche Testphase geplant. Anschließend soll die öffentliche Freischaltung erfolgen, so dass alle Nutzerinnen und Nutzer mit geeignetem mobilen Endgerät Smart-eIDs erzeugen können.

4. Welche Erkenntnisse wurden in der interministeriellen Arbeitsgruppe GovLabDE hinsichtlich des Launches und der Weiterentwicklung der Smart-eID besprochen?

   a) Wann wurde die Smart-eID das letzte Mal in einer Arbeitsgruppensitzung besprochen?

   b) Wurde über den genauen Zeitpunkt des Launches der Smart-eID gesprochen, und wenn ja, wann?

   c) Wann wurde das letzte Mal über die Weiterentwicklung der Smart-eID gesprochen, und wie soll diese nach Ansicht der Bundesregierung weiterentwickelt werden?

Die Fragen 4 bis 4c werden gemeinsam beantwortet.

Das Projekt Smart-eID ist im GovLab.DE Digitale Identitäten vertreten und berichtet daher wöchentlich über den aktuellen Status mit der Möglichkeit zur Diskussion. Das umfasst auch Informationen zum Zeitplan und weitere geplante Schritte. Der Fokus lag zuletzt auf der Fertigstellung und der Vorbereitung des Starts der Smart-eID. Die nächsten vorgesehenen Schritte der Weiterentwicklung umfassen vor allem die Erhöhung der Reichweite nutzbarer Geräte einerseits durch Aufnahme weiterer Hersteller und andererseits durch die Nutzung weiterer Technologien. Hier ist insbesondere die eSIM von Interesse, da hier eine positive Marktentwicklung anzunehmen ist.

5. Wie genau soll die Smart-eID weiterentwickelt werden (bitte die jeweiligen technischen Spezifikationen auflisten)?

Die wesentliche Herausforderung bei der Smart-eID ist der Zugang zu einer möglichst großen Anzahl an mobilen Endgeräten. Deshalb soll die Smart-eID neben Secure Elements zukünftig auch auf embedded SIMs (eSIM) zurückgreifen können, um die Marktreichweite zu erhöhen. Technische Vorbetrachtungen dazu laufen bereits.

Aktuell wird in der internationalen Vereinigung der GSM-Mobilfunkanbieter (GSMA) und GlobalPlatform der neue Standard „Secured Applications for Mobile (SAM)“ spezifiziert. SAM hat das Potential, den Zugang zu Secure Elements und eSIM deutlich zu vereinfachen und ist damit auch für die Smart-eID relevant. Ein Positionspapier des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu SAM ist unter folgendem Link zu finden:

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/SecureElements/SAM/SAM PositionPaper vl-0.html

Link zum Anforderungsdokument der GSMA:

https://www.gsma.com/newsroom/wp-content/uploads//SAM.01-v1.0.pdf.

Eine technische Spezifikation der GlobalPlatform ist noch nicht öffentlich verfügbar.

6. Wann wurde das letzte Mal mit dem bisher einzigen in die Smart-eID eingebundenen Hersteller Samsung Electronics Gespräche hinsichtlich des Launches der Smart-eID geführt?

Das letzte Gespräch auf Management-Ebene zwischen dem Bundesministerium des Innern und für Heimat (BMI) und Samsung Electronics Deutschland fand im September 2023 statt. Hierbei wurde Samsung über den derzeitigen Status transparent informiert.

7. Wie bewertet das BSI die Sicherheit der Smart-eID in Deutschland, und gibt es hierzu ein entsprechendes Dokument?

Für die Realisierung der Smart-eID wird die Funktionalität der Online-Ausweisfunktion, welche beim Kartenausweis auf einem dedizierten Chip implementiert ist, analog auf einem eingebetteten Sicherheitselement (Secure Element) in einem Mobilgerät implementiert, wie in der BSI TR-03127 beschrieben. Wesentlicher Sicherheitsanker ist die Verwendung eines (zertifizierten) Secure Elements zur sicheren Speicherung und Verwendung kryptographischer Schlüssel und der Identitätsdaten. Für die sichere Kommunikation werden die etablierten kryptographischen Protokolle eingesetzt, welche bereits beim elektronischen Personalausweis zum Einsatz kommen.

Für die Smart-eID kommt ein Provisionierungssystem zum Aufspielen und für den Lifecycle des eID-Applets auf dem Secure Element zum Einsatz. Dieses Trusted Service Management System (TSM-System) besteht im Wesentlichen aus einem Backendsystem. Hier gelten allgemeine Anforderungen wie eine Zertifizierung nach ISO 27001 bzw. IT-Grundschutz. Darüber hinaus gelten spezielle Anforderungen für die Smart-eID wie ein Betrieb der kritischen Funktionen (insbesondere Verwaltung und Nutzung kryptographischen Schlüsselmaterials) in entsprechend geschützten Rechenzentren auf deutschem Staatsgebiet sowie unter Verwendung entsprechender Hardware-Sicherheitsmodule. Speziell auf solche Provisionierungssysteme zugeschnittene Zertifizierungsanforderun-

gen oder Zertifizierungsschemata gibt es derzeit nicht. Dies wird aber aktuell auf europäischer Ebene für die EUDI-Wallet erarbeitet und ist nach Fertigstellung ggf. auch für die Smart-eID anwendbar.

8. Wie beurteilt die Bundesregierung das Secure Element als Hardwarekomponente in den ausgerüsteten Samsung Handys hinsichtlich der spezifischen Sicherheit in Bezug auf die sichere einmalige Einrichtung und hinsichtlich der allgemeinen Sicherheit der Nutzung?

Die für die Smart-eID zum Einsatz kommenden Sicherheitselemente bzw. Secure Elements sind auf hohem Niveau (ab EAL4+AVA VAN.S) nach Common Criteria zertifiziert. Die Zertifizierung deckt neben der eigentlichen Hardware auch das Betriebssystem des Secure Elements und damit verbundene standardisierte Mechanismen für die Verwaltung von Applikationen (inkl. Einrichtung und Nutzung) ab. Die eingesetzte Technologie ist in vielen Belangen mit den in Chipkarten eingesetzten Sicherheitschips vergleichbar. Zwar bringt die Einbindung des Secure Elements in ein komplexes System (Smartphone) spezielle Herausforderungen mit sich, allerdings sind diese mit Secure Elements und der starken Isolierung vom eigentlichen Smartphone Betriebssystem leichter abzudecken als bei Nutzung anderer auf Smartphones verfügbarer Möglichkeiten wie z. B. eines i. d. R. nicht zertifizierten und nicht standardisierten Trusted Execution Environments.

9. Wie beurteilen die Bundesregierung und respektive das BSI die Gefahr des Verlustes des Handys und das damit bestehende mögliche Risiko des Identitätsdiebstahls?

Die Identitätsdaten des Nutzers und das zugehörige Schlüsselmaterial werden ausschließlich im Sicherheitselement des Mobilgeräts abgelegt und eine Verwendung ist nur nach Eingabe der PIN und Übermittlung dieser an das Sicherheitselement möglich. Insofern ist die Gefahr eines Identitätsdiebstahls bei Verlust des Mobilgeräts vergleichbar mit dem Verlust der Ausweiskarte. Die Smart-eID bietet gleichermaßen wie die Ausweiskarte die Möglichkeit, diese bei Verlust über die Sperrhotline zu sperren wodurch eine weitere Verwendung nicht mehr möglich ist. Zudem bietet die Smart-eID zusätzlich die Möglichkeit diese über die Fernlösch-Funktion des Geräteherstellers unwiderruflich unbrauchbar zu machen.

10. Wie beurteilen die Bundesregierung und respektive das BSI die Gefahr des Hackings der „Softwarekomponente“ und das damit mögliche Risiko des Identitätsdiebstahls?

Die sicherheitsrelevanten Funktionen der Smart-eID werden, analog zum Chip in der Ausweiskarte, im Sicherheitselement des Mobilgeräts realisiert. Insbesondere werden die Identitätsdaten ausschließlich über einen Ende-zu-Ende verschlüsselten Kanal zwischen dem Sicherheitselement und dem jeweiligen Diensteanbieter übertragen. Die Softwarekomponente, welche durch die AusweisApp2 realisiert wird, übernimmt im Falle der Smart-eID analog zur Ausweiskarte die Rolle des eID-Clients und hat keine Einsicht in den verschlüsselten Kanal. Die Gefahren, welche sich aus einem Angriff auf die AusweisApp2 ergeben sind somit vergleichbar mit der Verwendung der AusweisApp2 als eID-Client für den Kartenausweis. Des Weiteren wird sichergestellt, dass die Personalisierung einer Smart-eID nur auf dem Gerät des sich hierzu identifizierenden Nutzers erfolgen kann. Dies wird erreicht, indem der Personalisie-

rungsdienst die Ausstellung der Smart-eID nur über den gleichen verschlüsselten Kanal vornimmt, über welchen auch die Ausweiskarte zur initialen Identifizierung des Nutzers ausgelesen wird.

11. Wie bewertet die Bundesregierung das mögliche spezifische Risiko des Identitätsdiebstahls durch die Smart-eID, und wie bewertet sie das mögliche allgemeine Risiko des Identitätsdiebstahls bei dem geplanten softwarebasierten Ansatz im Zuge der Entwicklung einer EUDI-Wallet, und inwiefern arbeitet sie daran, die jeweiligen Risiken zu minimieren und auszuschließen?

Im Falle der hardwarebasierten Smart-eID ist das Risiko eines Identitätsdiebstahls vergleichbar mit der bestehenden Online-Ausweisfunktion. Ein Missbrauch der Identität auf dem Mobilgerät erfordert gleichzeitigen unbeschränkten Zugriff auf das Gerät (den Besitzfaktor) und die PIN (Wissensfaktor) des Nutzers. Durch die Speicherung der Identitätsdaten im Sicherheitselement und die verschlüsselte Obertragung direkt aus diesem, hat zudem weder das Betriebssystem noch eine andere auf dem Mobilgerät installierte Anwendung Zugriff auf die Identitätsdaten. Gegenüber dem Kartenausweis bietet die Smart-eID bei Verlust des Geräts zusätzlich zur Sperrung über die Sperrhotline auch die Möglichkeit die Smart-eID über die Fernlösch-Funktion des Geräteherstellers unwiderruflich unbrauchbar zu machen. Im Rahmen der Erarbeitung eines Architekturkonzepts für eine mögliche EUDI-Wallet werden Sicherheitsmaßnahmen frühzeitig mit einbezogen und Varianten gewählt, die Nutzerfreundlichkeit und Risikominimierung entsprechend gegeneinander abwiegen.

12. Welche Erkenntnisse konnten aus Sicht der Bundesregierung aus den Tests um die Smart-eID gezogen werden, und zu welchem abschließenden Ergebnis kommt sie hier?

Die Funktionalität der Smart-eID wurde im Rahmen von internen Systemtests und Sicherheitstests, durch kontinuierliche Tests parallel zu den Entwicklungsarbeiten und durch Konformitätstest des BSI bestätigt. Damit wurde das Ziel eines stabilen Entwicklungszustandes erreicht.

Zu den Erkenntnissen gehörten u. a. die Verbesserung von Deployment Prozessen, die Weiterentwicklung des Überlastschutzes sowie des Umgangs mit Fehlermeldungen und Gerätekonfigurationen.

13. Wie plant die Bundesregierung die Bewerbung der Smart-eID-Funktion nach deren Launch?

Die Bundesregierung plant, die Smart-eID-Funktion nach ihrem Start in mehreren Schritten zu bewerben. Die Kommunikation beginnt mit grundlegenden Informationen und wird dann an den Fortschritt des Projekts angepasst.

14. Wie viele Mittel wurden bisher für die Entwicklung der Smart-eID in den Jahren 2016, 2017, 2018, 2019, 2020, 2021, 2022 und 2023 im Bundeshaushalt bereitgestellt, und wie viele Mittel sind abgeflossen (bitte getrennt nach Jahren und bereitgestellten sowie abgeflossenen Mitteln auflisten)?

Das Projekt Smart-eID wurde im Jahr 2021 gestartet, daher kann die Betrachtung der Entwicklungskosten (einschließlich Testbetrieb) erst ab diesem Zeitpunkt erfolgen.

Jahr	Bereitgestellt	Abgeflossen
2021	99.920.815 €	2.426.615 €
2022	97.494.199 €	39.933.508 €
2023*	74.735.513 €	29.865.334 €

*Bis 19. Oktober 2023

15. Ist eine Zertifizierung der Smart-eID durch den Bundesdatenschutzbeauftragten sowie durch das BSI vorgesehen, und wenn ja, wann?

Die Zertifizierung des Smart-eID-Applets gemäß der Technischen Richtlinie durch das BSI ist bereits erfolgt. Eine Zertifizierung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) ist nicht vorgesehen. Die datenschutzrechtliche Dokumentation wird in Abstimmung mit dem zuständigen behördlichen Datenschutz erstellt und soll dem BfDI nach Fertigstellung zur Kenntnis gegeben werden.

16. Ist die Anbindung der Smart-eID an das Nutzerkonto der Bund-ID abgeschlossen?

Ja. Die Freischaltung erfolgt erst zum Start der Smart-eID.

17. Welche konkreten Erkenntnisse wurden aus der bisherigen Pilotphase um die Smart-eID mit insgesamt rund 150 Testkarten gewonnen, und wurden hier Missbrauchsmöglichkeiten festgestellt, und wenn ja, welche?

Durch die Pilotphase konnten signifikante Verbesserungen der Smart-eID erreicht werden. Diese Verbesserungen umfassen sowohl die Optimierung des Workflows in der AusweisApp2 als auch die Verbesserung der Verständlichkeit von Fehlermeldungen. Darüber hinaus konnte die Gerätekompatibilität erweitert, die Bereitstellung und Installation von Applets auf den Geräten optimiert und allgemeine technische Prozesse vereinfacht werden.

Durch eine Umfrage zur Nutzendenführung der Smart-eID wurde festgestellt, dass sowohl die Einrichtung der Smart-eID in der AusweisApp2 als auch die einzelnen Prozessschritte sowie deren Reihenfolge bei der Nutzung der Komfortfunktion reibungslos verliefen. Folglich fanden sich die meisten Benutzer problemlos im Smart-eID-Menü der AusweisApp2 zurecht.

Im Zuge der durchgeführten Umfrage wurden weder der Missbrauch der Smart-eID noch mögliche Manipulationsmöglichkeiten bewertet.

18. Wurde die Smart-eID auf mögliche Schwachstellen bei der Einrichtung und bzw. oder der Anwendung untersucht?

Ja.

19. Welche möglichen Gefahren sind der Bundesregierung bei der Einrichtung und bzw. oder Anwendung der Smart-eID aus Nutzerperspektive bekannt?

Die Sicherheitsfunktionalität wird analog zum Karten-Ausweis durch das Sicherheitselement realisiert. In der Folge gestalten sich die Gefahren bei der Anwendung der Smart-eID vergleichbar zur Nutzung der kartenbasierten Online-

Ausweisfunktion. Im Gegensatz zum Kartenausweis kann das Sicherheitselement bei Nichtnutzung nicht physikalisch vom Gerät getrennt werden, im Gegenzug wird der Verlust des Mobilgeräts als Besitzfaktor in der Regel aber deutlich schneller bemerkt werden, als beim Kartenausweis. Zusätzlich wird auch die Ausstellung der Smart-eID gesondert abgesichert. Wie in der Antwort zu Frage 10 beschrieben, kann eine Smart-eID ausschließlich auf dasjenige Gerät ausgestellt werden, welches der Nutzer zur initialen Identifizierung verwendet. Der Nutzer muss folglich die bereits für den Kartenausweis geltenden Sicherheitsmaßnahmen befolgen, insbesondere Dritten keinen Zugriff auf seinen Kartenausweis bzw. sein Gerät und seine PIN zu gewähren.

20. Arbeitet die Bundesregierung bereits an einer softwarebasierten Authentifizierungsvariante, welche als integraler Bestandteil des Gesamtsystems der deutschen eIDAS-Umsetzung fungiert, und wie ist hier der Stand der Umsetzung?

Im Rahmen der Erarbeitung eines Architekturkonzepts für ein eIDAS2.0-Gesamtsystem wird die Frage nach einer Authentifizierungslösung unterhalb des Vertrauensniveaus Hoch behandelt. Momentan befindet sich das Projekt noch in einer Konzeptionsphase und konkrete Entwicklungsleistungen finden noch nicht statt.

21. Wie beurteilt die Bundesregierung die Konkurrenz aus der Hardware-Authentifizierung (ePersonalausweis und Smart-eID) und der geplanten Software-Authentifizierung im Rahmen der deutschen eIDAS-Umsetzung?

Die Bundesregierung beabsichtigt keine Konkurrenz herzustellen, sondern verfolgt den Ansatz von komplementären Authentifizierungs- und Identifizierungsmöglichkeiten, die für den jeweiligen Schutzbedarf angemessen sind. Lösungen sollten für den jeweiligen Anwendungsfall so nutzungsfreundlich wie möglich und so sicher wie nötig sein.

22. Wie beurteilt die Bundesregierung die Notwendigkeit der Smart-eID im Vergleich zur geplanten softwarebasierten Authentifizierung, welche ohne Online-Ausweis vorgenommen werden kann?

Eine softwarebasierte Authentifizierung wird nicht die gleichen sicherheitstechnischen Anforderungen wir eine hardwarebasierte Lösung erfüllen und somit für Anwendungsfälle, die ein hohes Vertrauensniveau erfordern nicht geeignet sein. Für solche Fälle ist ein hardwarebasiertes Verfahren wie z. B. mit dem Onlineausweis oder einer Smart-eID unumgänglich.

23. Sieht die Bundesregierung die Smart-eID deshalb als Übergangslösung bis zur Einführung einer softwarebasierten Authentifizierungslösung, welche im Rahmen der deutschen eIDAS-Umsetzung geplant ist?

Die Bundesregierung sieht in der Smart-eID keine Übergangslösung, sondern einen technischen Ansatz, wie künftig Hardwaresicherheit auch ohne dedizierte Chipkarte und nur unter Verwendung der Sicherheitshardware in Mobilgeräten gewährleistet werden kann. Zugleich ist sie sich gewahr, dass in der Übergangszeit, bis die Smart-eID auf allen Smartphones nutzbar ist, Lösungen für eine Identifizierung oder Authentifizierung in den Fällen, in denen kein hohes

Vertrauensniveau benötigt wird, sinnvoll sein können. Auf die Antworten zu den Fragen 20 bis 22 wird verwiesen.

24. Welche Haushaltsmittel sind für die Jahre von 2023 bis 2027 für die Smart-eID vorgesehen (bitte getrennt für 2023, den Haushaltsentwurf 2024 und die Mifrif 2025, 2026 und 2027 angeben)?

Im Jahr 2023 sind für die Entwicklung und die Finanzierung des Testbetriebs der Smart-eID im Haushalt bis zu 74 735 513 Euro veranschlagt. Im Haushaltsentwurf für 2024 sowie die fortfolgenden Jahre sind bisher keine Mittel explizit für die Smart-eID vorgesehen. Die Finanzierung soll aus dem Titel für Digitale Identitäten erfolgen, ist aber bisher nicht gesichert, da weder der Haushalt für 2024 beschlossen wurde noch die Höhe eventueller Ausgabereste feststeht.

25. Wie hoch sind die Kosten im Rahmen der Wartung und der Inbetriebnahme für die Smart-eID (bitte getrennt für 2023, den Haushaltsentwurf 2024 und die Mifrifi 2025, 2026 und 2027 angeben)?

Die Kostenschätzungen für die Smart-eID gehen grundsätzlich neben dem Betrieb auch von einer notwendigen Weiterentwicklung aus, um die Anzahl nutzbarer Geräte perspektivisch zu erhöhen. Je nachdem, wieviele weitere Geräte wievieler Hersteller einerseits und welche Technologien andererseits hinzukommen, kann der tatsächliche Kostenverlauf von den Prognosen stark abweichen. Die Planung geht von einem starken Wachstum in den ersten beiden Jahren und einem langsameren Wachstum in den Folgejahren aus.

Jahr	Kosten für Betrieb und Wartung der Smart-eID inkl. Weiterentwicklung zur Steigerung der Reichweite (in Mio. Euro)	Davon Kosten nur für Betrieb und Wartung des Produktivsystems inkl. Herstelleranbindung (in Mio. Euro)
2023	26,2	-/-
2024	34,3	21,9
2025	43,5	30,8
2026*	45,6	33,9
2027*	47,8	37,3

* Die Angaben für 2026 und 2027 basieren auf einer geschätzten Kostensteigerung von 5 Prozent gegenüber dem Vorjahr, da die tatsächliche Höhe stark von den erzielten Ergebnissen beim Reichweitenausbau in den Jahren 2024 und 2025 abhängen wird.

26. Wie bewertet die Bundesregierung das Nutzen-Risiko-Verhältnis für die Smart-eID-Lösung, und überwiegen aus Sicht der Bundesregierung die Vorteile für die Smart-eID und deren Launch?

Mit der Smart-eID wurde auf Basis der mit Fokus auf Sicherheit designten Infrastruktur des Online-Ausweises eine komfortable und zugleich sehr sichere (vgl. Antworten zu den Fragen 7 bis 11) Lösung geschaffen, um sich online ausweisen zu können. Die Notwendigkeit sich auszuweisen ist kein Selbstzweck, so dass bisher häufig deutlich weniger sichere oder weniger komfortable Lösungen genutzt werden. Daher wird die Bereitstellung der Smart-eID als wichtiger Schritt zu mehr Sicherheit im Bereich der online durchgeführten Identifizierung und Authentifizierung angesehen. Zugleich ist die Smart-eID nur ein Angebot an die Nutzenden, die selbstverständlich auch weiterhin den Online-Ausweis in der bisherigen Form weiter nutzen können.

27. Wie beziffert die Bundesregierung das potenzielle Skalierungspotenzial durch die Einführung der Smart-eID, und welches Nutzeraufkommen erwartet die Bundesregierung durch die Einführung der Smart-eID anhand der bisher ausgerüsteten Samsung-Modelle?

Die Smart-eID stellt eine komfortable Ergänzung zum bestehenden Online-Ausweis dar. Dieser wird i. d. R. nicht zum Selbstzweck genutzt, sondern zur Erledigung von konkreten Anliegen. Wesentlich ist daher nicht die Einführung der Smart-eID, sondern eine hohe Zahl attraktiver Einsatzmöglichkeiten für den Online-Ausweis. Mit der Smart-eID wird dessen Nutzung noch komfortabler, da die Karte im Zuge des Ausweisvorgangs nicht mehr an das Gerät gehalten werden muss. Dies macht den Online-Ausweis auch für Diensteanbieter attraktiver. Dennoch ist auch der kartenbasierte Online-Ausweis bereits eine im Vergleich zu den Alternativen sehr komfortable Möglichkeit, sich online sicher zu identifizieren.

28. Hat die Bundesregierung Informationen und Zahlen über die aktuell im Umlauf befindlichen mit Secure-Element ausgerüsteten Samsung-Modelle, und wenn ja, wie hoch sind diese?

Die genauen Zahlen unterliegen dem Betriebsgeheimnis der Firma Samsung. Ausgehend von den bereits im Pilotbetrieb unterstützten Modellen könnten derzeit rechnerisch ca. 10 Prozent der geschätzten Smartphone-Nutzer in Deutschland die Smart-eID zum Start unmittelbar nutzen. Durch Unterstützung weiterer Geräte und weiterer Technologien (vgl. Antwort zu Frage 5) soll dieser Anteil nach dem Start zügig erhöht werden.

29. Welche Maßnahmen unternimmt die Bundesregierung, um bei der Umsetzung und Weiterentwicklung der Smart-eID eine umfassende Barrierefreiheit sicherzustellen?

Die Benutzerschnittstelle zur Nutzung der Smart-eID wird ausschließlich durch die AusweisApp2 realisiert. In der Folge stellen die bereits existierenden und stetig fortgeführten Maßnahmen zur Sicherstellung der Barrierefreiheit innerhalb der AusweisApp2 diese auch für die Smart-eID sicher.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333