Digitale Identitäten

Materialien

- Whitepaper Ökosystem digitaler Identitäten (Bundeskanzleramt) (Aufbau eines solchen Ökosystems ist das Ziel des Projekts „Europäische Digitale-Identitäten-Initiative“)
- European Digital Identity
- Zum Status: https://www.heise.de/news/eHealth-Digitale-Identitaeten-fuer-Gesundheitsanwendungen-kommen-2023-7081367.html
- „Strategie“ der Bundesregierung: https://netzpolitik.org/2023/online-ausweis-keine-strategie-bei-der-elektronischen-identitaet/?s=09#netzpolitik-pw
- Antrag CDU zur eID-Strategie https://dserver.bundestag.de/btd/20/053/2005354.pdf (Doku des parlamentarischen Prozesses: https://www.bundestag.de/dokumente/textarchiv/2023/kw04-de-digitale-identitaet-930080)

Videoident

Vergangene Hacks

Institut für Visual Computing (IVC) der Hochschule-Bonn-Rhein-Sieg im Auftrag des BSI Überlagerung eines mit dem Farbdrucker gefälschten Ausweises mit computergenerierten Hologrammen. (2017)

Deep-Fake-Angriff. Gesicht der Person im Videostream wurde in Echtzeit mit dem Gesicht aus dem Ausweis ersetzt (etwas später als der erste)

Hack des CCC (Tschirsich, 2022). Tschirsich beschreibt, dass der Angreifer sich selbst filme, wie er einen Personalausweis in die Kamera hält und das erforderliche Prozedere durchgeht. Danach filme er den Personalausweis einer anderen Person. Anschließend lege der Angreifer Teile des Videos des fremden Personalausweises – das Passbild, die Anschrift, etc. – über sein Originalvideobild. Diese Techniken existieren im Wesentlichen seit mehr als einem Jahrzehnt. ⇒ Der Angriff ist wesentlich einfacher durchführbar als die ersten beiden!

Der Angriff basiert auf der videotechnischen Kombination zweier oder mehrerer echter ID-Dokumente im Videobild zu einem künstlichen neuen ID-Dokument. Dazu werden Bildausschnitte aus einem Video in ein zweites Video übertragen.

Seit 2019 existiert in in Anlage 4b BMV-Ä § 2 eine Übergangslösung zur Identifikation bei der Videosprechstunde.

nPA als eID

Ende Mai 2023 hat das Kabinett einen Gesetzesentwurf zur Überarbeitung des Onlinezugangsgesetzes (OZG) beschlossen. Das alte OZG sah vor, dass jedes Bundesland und der Bund je ein Nutzerkonto für Onlineanträge anbietet. Künftig dürfen Behörden nur noch das „Bund-ID“ genannte Bundeskonto anbinden.

Detailinfos zum neuen Personalausweis gibt es auf dem Personalausweisportal des BMI.

Den neuen Personalausweis (**nPA**) im Scheckkartenformat gibt es seit dem **1.11.2010**, den **elektronischen Aufenthaltstitel** seit **1.9.2011**. Mit beiden Ausweiskarten ist die **Online-Ausweisfunktion** etabliert worden, die **seit Juli 2017** bei neu ausgegebenen Ausweiskarten immer **eingeschaltet** ist. Seitdem steigt der Anteil der eingeschalteten Online-Ausweise jährlich um rund 8 Millionen.[1)]

Zudem wurde im Februar 2022 von der Bundesdruckerei im Auftrag des BMI ein Online-Rücksetzdienst (PRS = PIN-Reset-Service) für die PIN eingerichtet, der den Gang zum Amt erspart, wenn die PIN vergessen oder noch nicht aktiviert wurde. Am 25.5.2023 meldet die Bundesdruckerei die 1.000.000ste Bestellung.[2)]

Der nPA ist **keine SSEE**, aber ermöglicht **Fernsignatur**.

Folgende **Daten** stehen auf dem Chip:

- Familienname, Geburtsname, Vorname(n), Doktorgrad, Tag und Ort der Geburt, Anschrift, Ordens- oder Künstlername, Dokumentenart, Landeskürzel „D“, letzter Tag der Gültigkeit,
- dienste- und kartenspezifische Kennzeichen (Pseudonym),
- Angabe, ob ein bestimmtes Aler über- oder unterschritten wird (Altersbestätigung),
- Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht (Wohnortbestätigung)
- Angabe, ob der Personalausweis gültig ist, und Sperrmerkmal.

Die **maschinenlesbare Zone** (englisch: Machine Readable Zone, **MRZ**) befindet sich im unteren Bereich des nPA und entspricht den Vorgaben der Internationalen Zivilluftfahrt-Organisation (ICAO). Dadurch ist sichergestellt, dass die deutschen Ausweise und Pässe zB bei Grenzkontrollen analog zu internationalen Reisepässen maschinell gelesen werden können. Kürzung erfolgt wegen begrenzter Zeichenzahl nach festen Regeln.

Kopien des nPA sind nur mit dem Einverständnis der Ausweisinhaber*innen erlaubt.[3)]. Wurde das Dokument im Original vorgelegt und erfolgte eine Identifizierung reicht in den meisten Fällen ein Vermerk als Dokumentation. Darüber hinaus gibt es gesetzlich geregelte Fälle, in denen Kopien von Ausweisen erstellt werden dürfen bzw. müssen.[4)]

Digitale Funktionen

Digitale Funktionen des nPA:

- Online-Ausweis
- Vor-Ort-Auslesen

- Biometriefunktion.

Online Ausweis

- Vor Übermittlung der Daten können die Nutzer*innen sehen, welche Behörde bzw. welches Unternehmen erhält und prüfen, ob eine staatliche Zulassung (Berechtigung) der Vergabestelle für Berechtigungszertifikate im Bundesverwaltungsamt für diesen Geschäftszweck vorliegt (**gegenseitige Authentifizierung**)
- **PIN**-Eingabe notwendig
- **E2E-Verschlüsselung** bei der Datenübertragung vom Chip an den eID-Server des Dienstanbieters.

Zum Online-Ausweisen benötigen Sie:

- Ausweiskarte mit aktivierter Online-Ausweisfunktion
- Smartphone oder Kartenlesegerät
- (sechsstellige) PIN
- Software, bspw. die AusweisApp2

Mobiles Online-Ausweisen:

Abbildung 1 zeigt die Möglichkeiten des mobilen Online-Ausweisens.

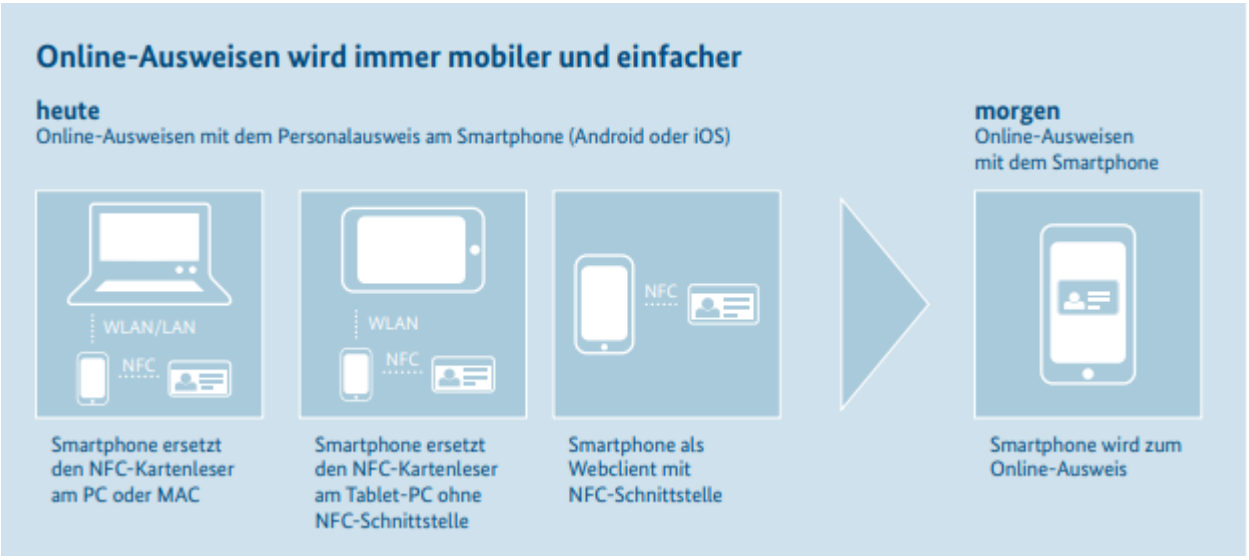

Abb. 1: Mobiles Online-Ausweisen / Quelle: Bundesministerium des Innern, für Bau und Heimat, Hrsg., 2019. Digitale Identifizierung mit dem deutschen Online-Ausweis (abgerufen am 10.10.2022), S. 12.

„On-the-Fly“-Signatur-Signatur

Bisherige Signaturverfahren trennen die Vorgänge der Identifizierung (zum Erhalt des Signaturzertifikats) und der Authentisierung (zum Auslösen der Signatur) in separate Schritte. Mit dem nPA können beide Vorgänge in einem Schritt im Rahmen einer (eIDAS-konformen) Fernsignatur zusammengefasst werden, wie Abbildung 2 zeigt.

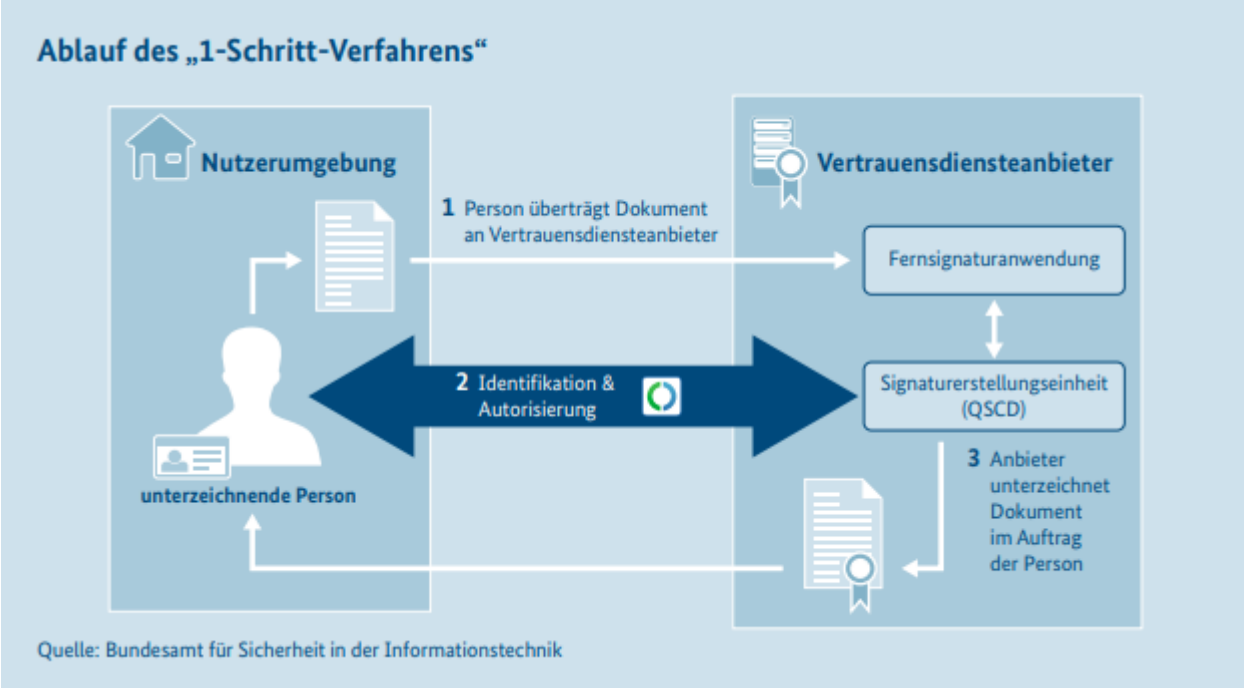

Abb. 2: Fernsignatur mit nPA / Quelle: Bundesministerium des Innern, für Bau und Heimat, Hrsg., 2019. Digitale Identifizierung mit dem deutschen Online-Ausweis (abgerufen am 10.10.2022), S. 21.

Vor-Ort-Auslesen

- Datenübernahme bspw. in ein Formular
- Vorherige Identifizierung per Lichtbild- und Personendatenabgleich von der Ausweiskarte vor Ort
- Eingabe der CAN (Card Access Number, Zugangsnummer), die auf der Vorderseite des nPa aufgedruckt ist.

Das Vor-Ort-Auslesen ist geeignet für die in der Kreditwirtschaft gem. AO und GwG notwendige Legitimationsprüfung natürlicher Personen in den Filialen sowie beim Erwerb von SIM-Karten bzw. dem Abschluss von Mobilfunkverträgen nach TKG.

Biometriefunktion

Seit August 2021 müssen alle Menschen in Deutschland beim Beantragen eines Personalausweises zwei Fingerabdrücke hinterlassen. Dies regelt die Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben und § 5 Abs. 9 des deutschen Personalausweisgesetzes.

Die Biometriefunktion kommt ausschließlich bei hoheitlichen Personenkontrollen an Grenzen oder im Inland zum Einsatz. Diensteanbieter können darauf nicht zugreifen.

Sperren der eID-Funktion

- erfolgt über die Sperrhotline mittels Sperrpasswort

- Wenn das Sperrkennwort nicht vorliegt, ist persönliches Erschienen bei der Ausweisbehörde inkl. einer Identitätsfeststellung notwendig.[5)]

Technische Architektur

Abbildung 3 zeigt die technische Architektur.

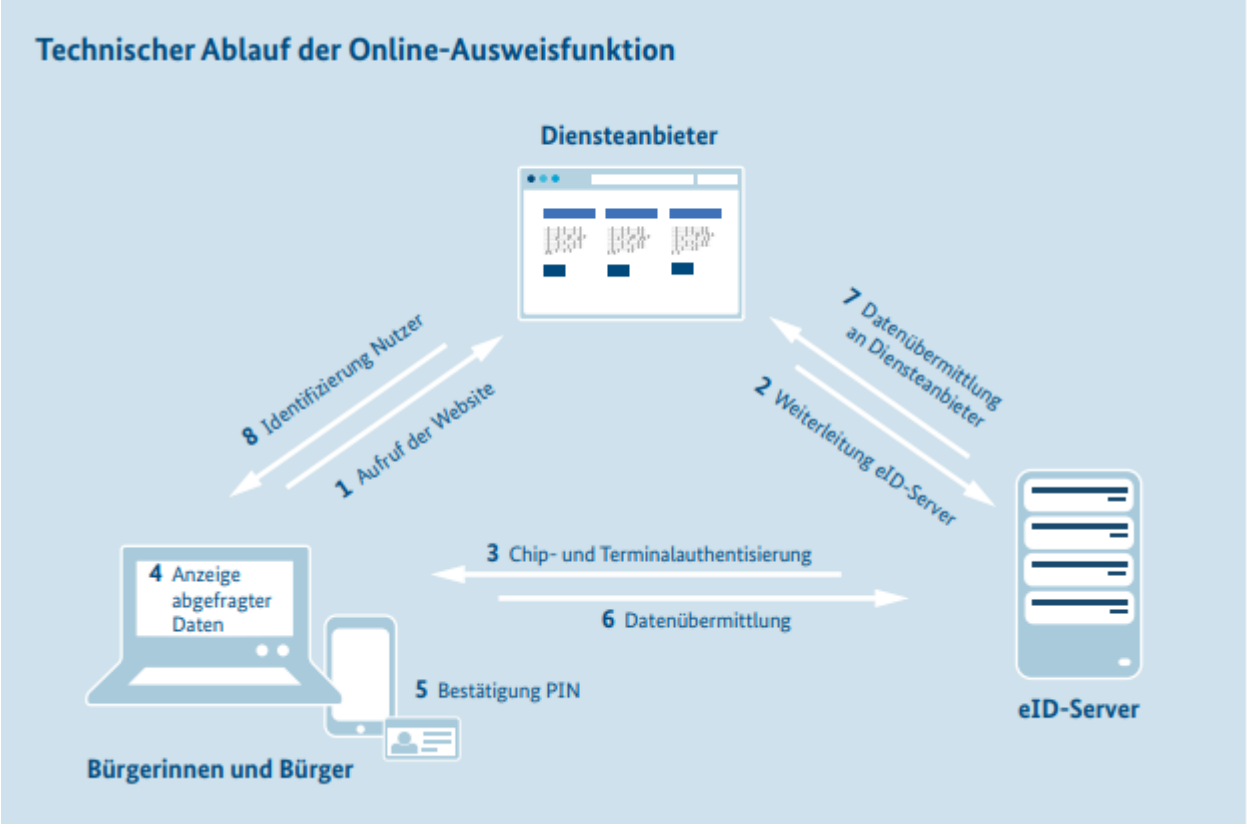

Abb. 3: Technische Architektur / Quelle: Bundesministerium des Innern, für Bau und Heimat, Hrsg., 2019. Digitale Identifizierung mit dem deutschen Online-Ausweis (abgerufen am 10.10.2022), S. 13.

Identifizierungsdienstleistungen

Anbieter von Identifizierungslösungen bieten Dienste an, die von der VfB zugelassen wurden und die TRs des BSI einhalten (gem. § 2 Abs. 3a PAuswG). Der Vorteil ist, dass sie keinen eigenen eID-Server benötigen.

Zu den ersten Identifizierungslösungen zählt bspw. AusweisIDent der Bundesdruckerei und Governikus.

Anwendungen

- Seit 1.10.2019 ist es möglich, den Online-Ausweis für alle Standardzulassungsvorgänge von KfZ im Internet zu nutzen.

Sicherheit

Daten auslesen

Die im Chip des nPA gespeicherten Daten sind durch besondere Sicherheitsmechanismen (**Extended Access Control**) vor unberechtigtem Auslesen geschützt:

- Nutzer muss **PIN** eingeben
- lesende Stelle muss sich mit **Berechtigungszertifikat** autorisieren

Nur wenn dem Chip der richtige Schlüssel übermittelt wird, gibt er die Daten gegenüber dem Lesegerät frei.[6)]

Gem. § 21 Abs. 7 PAuswG sind öffentliche Stellen von **EU-Mitgliedstaaten** berechtigt, Daten des nPA im Wege des elektronischen Identitätsnachweises anzufragen und können diese mit Zustimmung und PIN-Eingabe der Nutzer*innen auslesen. Gem. eIDAS-VO stellt die BRD den anderen Mitgliedstaaten eine entsprechende Software zur Anbindung an das deutsche eID-System bereit.[7)]

Darüber hinaus dürfen Inspektionssysteme von Kontrollbehörden in der EU im Rahmen ihrer Kontrollaufgaben nach einer erfolgreichen Authentisierung unter Verwendung der MRZ oder der CAN auf Daten zugreifen.[8)]

Daten ändern

Ändern ist nur über sog. Visualisierungs-Änderungsterminals in den Personalausweisbehörden möglich. Diese Terminals müssen sich täglich bei den Ausweisherstellern mit einer Smartcard elektronisch autorisieren; bei Verlust werden die Geräte unmittelbar gelöscht.[9)] Die Terminals sind über eine mittels TLS abgesicherte Online-Verbindung an die durch den Ausweishersteller im Hintergrund betriebenen Systeme angeschlossen. Über diesen Kanal werden Softwareaktualsiierungen, aktuelle TLS-Zertifikate, CSCA-Zertifikate und -Masterlisten sowie die Zertifikate aus der CVCA-eID-PKI bezogen, die für den Zugriff der Terminals auf die nPAs notwendig sind. Initiiert wird die Kommunikation dabei ausschließlich durch die Firmware der Terminals. Darüber hinaus erfolgt keinerlei Kommunikation über externe Datennetze.[10)]

Der Betrieb der Terminals ist nur mittels eines Bedienerkarte inkl. zugehöriger PIN möglich, die nur Mitarbeitern der Pass- und Ausweisbehörden vorliegt.[11)]

Politik

* Schaufensterprogramm "Sichere Digitale Identitäten" des BMWI

EU-Wallet

- eIDAS 2.0 Entwurf
- Kritik:

https://netzpolitik.org/2022/eidas-2-0-europaeische-id-wallet-fuer-das-digitale-panoptikum/
- https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

- eIDAS 2.0 verpflichtet die Mitgliedstaaten zur Einführung einer nationalen eID und gegenseitigen Anerkennung dieser.
- Die nationalen Identitäten werden dann in einem interoperablen, EU-einheitlichen Wallet gespeichert.
- Zudem werden weitere Vertrauensdienste eingeführt:
  - Electronic Ledger
  - Long Time Archiving
  - Attribute Attestation
  - Online Service Authentication

Graf Zahl

eGovernment Monitor 2022[12)]

- **40 Prozent** der Bundesbürger geben an, dass ihre Online-Ausweisfunktion **aktiviert** ist. Das ist ein Plus von 5 Prozentpunkten gegenüber dem Vorjahr.
- Mit **10 Prozent** bleibt der Anteil der Personen, die die eID nach eigenen Angaben bereits tatsächlich **verwendet** haben, aber fast auf Vorjahresniveau: 2021 lag die Quote bei 9 Prozent.
- 74 Prozent der Anwender des Digitalausweises verwenden die NFC-Schnittstelle ihres Smartphones
- 31 Prozent ein spezielles Lesegerät
- Eine persönliche PIN haben sich bisher nur 6 Prozent aller Ausweisinhaber besorgt.
- 20 Prozent der Befragten geben als Ursache für die Abstinenz an, dass sie kein Vertrauen in die eID-Funktion haben. 19 Prozent kennen sie gar nicht. Ebenso vielen sind keine Anwendungsoptionen geläufig. 18 Prozent sehen keinen Mehrwert, 13 Prozent ist die Handhabung zu umständlich. In Österreich und der Schweiz gebrauchen dagegen schon rund 63,5 Prozent eine digitale staatliche Identität.

1)
Bundesministerium des Innern, für Bau und Heimat, Hrsg., 2019. *Digitale Identifizierung mit dem deutschen Online-Ausweis* (abgerufen am 10.10.2022), S. 7.
2)
Pressemitteilung der Bundesdruckerei vom 25.5.2023.
3)
§ 20 Abs. 2 S. 1 PAuswG
4)
zB § 8 Abs. 2 S. 2 GwG; § 7 Abs. 3 S. 1 TTDSG; § 64 Abs. 1 Nr. 2 FeV.
5)
s. BT-Drs. 20/3759, 4.
6)
BT-Drs. 20/3759, 4.
7) , 9)
BT-Drs. 20/3759, 5.
8)
s. auch vor-ort-auslesen Die hoheitlichen Inspektionssystem werden ausschließlich im Netz der Bundespolizei betrieben und beziehen darüber im Bedarfsfall elektronisches Zertifikatsmaterial zur Prüfung der Echtheit der Ausweisdokumente und der biometrischen Verifikation des Ausweisinhabers.((BT-Drs. 20/3759, 6.

[10] [11]
,
BT-Drs. 20/3759, 6.
[12]
INITIATIVE D21 e.V. und TECHNISCHE UNIVERSITÄT MÜNCHEN, Hrsg., 2022. *eGovernment Monitor 2022* o. O.: o. V. [Zugriff am: 12.10.2022]. ISBN 78-3-9821601-6-0. Verfügbar unter: https://initiatived21.de/app/uploads/2022/10/egovernment_monitor_2022.pdf; Zusammenfassung der Ergebnisse auch in folgendem Online-Artikel: KREMPL, Stefan, 2022. E-Government-Studie: Der digitale Ausweis kommt immer noch nicht vom Fleck. In: *heise online* [online]. 12.10.2022 [Zugriff am: 12.10.2022]. Verfügbar unter: https://www.heise.de/news/E-Government-Studie-Der-digitale-Ausweis-kommt-immer-noch-nicht-vom-Fleck-7305607.html.