BERICHTE DES NEGZ NR. 6

IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG LEICHT GEMACHT — DIE NUTZER INS ZENTRUM STELLEN

Petra Hoepner
Christian Welzel
Marianne Wulff

dataport
Fraunhofer FOKUS
Kompetenzzentrum Öffentliche IT
NEGZ
Nationales E-Government Kompetenzzentrum e.V.

Für einen modernen Staat

Das Nationale E-Government Kompetenzzentrum vernetzt Experten aus Politik, Verwaltung, Wissenschaft und Wirtschaft und ist die zentrale, unabhängige Plattform für Staatsmodernisierung und Verwaltungstransformation in Deutschland.

Herausgegeben und gefördert vom
Nationalen E-Government Kompetenzzentrum e. V.
Berlin 2019

INHALT

Zusammenfassende Empfehlungen **4**

1 Einleitung **6**

2 Erfolgsfaktoren für Akzeptanz und Nutzung **9**

3 Verwaltungsverfahren und Vertrauensniveaus **10**

3.1 Vertrauensniveaus 10

3.2 Beispiele 13

4 Empfehlungen **14**

4.1 Vertrauensniveaus nutzerorientiert und realistisch festlegen 14

4.2 Leichte Zugänglichkeit als oberstes Gebot leben 15

4.3 Zusammenarbeit mit privaten Initiativen prüfen 15

4.4 Alternative Verfahren nutzen 16

4.5 Zwang zur Nutzung von digitalen Verwaltungsleistungen prüfen 17

4.6 Nutzungsanreize schaffen 17

4.7 Recht digitaltauglich machen 17

4.8 Registervernetzung vorantreiben 18

Vertiefung **19**

5 Identifizierungs-Lösungen in der EU – Beispiele **19**

5.1 Übersicht 19

5.2 Estland 19

5.3 Österreich 21

5.4 Großbritannien 22

6 Technische Lösungen und Initiativen der Wirtschaft **23**

6.1 OpenID & OAuth 24

6.2 Video-Ident 25

6.3 Social Logins 25

6.4 FIDO Alliance 26

6.5 Verimi 27

6.6 netID 28

6.7 Mobile Connect 28

6.8 YES 29

Quellen- und Literaturverzeichnis **30**

Impressum **34**

ZUSAMMENFASSENDE EMPFEHLUNGEN

Ein möglichst einfacher Zugang zu Verwaltungsleistungen gilt als kritischer Erfolgsfaktor für das E-Government in Deutschland. Identifikation und Authentifikation der Nutzer bilden dabei einen neuralgischen Punkt. Fehler an dieser Stelle eröffnen Missbrauchspotenziale, die teilweise zu erheblichen Schäden führen können. Sind die Verfahren aber zu komplex, wird das Angebot von den Nutzern nicht angenommen. Die Online-Ausweisfunktion des Personalausweises steht sinnbildlich für dieses Spannungsfeld. Sie ist für das höchste Vertrauensniveau geeignet und gesetzlich der Schriftform gleichgesetzt. In der Anwendung stellt sie jedoch hohe Anforderungen an Nutzer und Dienstanbieter, sodass die Nutzungszahlen hinter den Erwartungen zurück bleiben.

Es ist davon auszugehen, dass zahlreiche Verwaltungsleistungen auch mit den geringeren Vertrauensniveaus „normal“ oder „substanziell“ realisiert werden können.[1] Hierfür herrscht allerdings Unsicherheit über die Einsatzmöglichkeiten von niedrigschwelligen Identifikationslösungen, die verwaltungsseitig akzeptiert werden und – für den jeweiligen Einsatzzweck – auch hinreichend rechtssicher sind. Dabei ist der angemessene Ausgleich zwischen Benutzbarkeit und Sicherheit das Eine, das Andere, und vermutlich mindestens ebenso wichtig ist die Frage, ob und wie eine womöglich staatliche Stelle das Risiko für den Bereich übernimmt, der eben nicht technisch abgesichert werden kann oder soll („Restrisiko“) – und nicht die Bürgerinnen und Bürger.

Ein Blick auf erfolgreiche Identifikationslösungen zeigt, dass Identifizierung und Authentifizierung einfach, verständlich und dem Anwendungsfall angemessen sein müssen. Andere Länder wie Estland, Österreich oder Dänemark zeigen, wie man mit leichtgewichtigen und mobilfähigen Identifizierungslösungen E-Government-Angebote wesentlich bürgernäher gestalten kann.

Parallel zu den staatlich entwickelten Lösungen entstehen eine Reihe von Identifizierungslösungen in der Wirtschaft. Eingesetzt werden offene Standards genauso, wie proprietäre Lösungen. Ziel, neben einem Single Sign-on, ist zumeist, bisherige, als unsicher einzustufende Nutzername-Passwort-Authentifizierungs-Verfahren abzulösen. Dabei setzt sich vermehrt die 2-Faktor-Authentifizierung als Mittel durch.

Vor dem Hintergrund der Europäischen Datenschutzgrundverordnung müssen Unternehmen, die mit Kundendaten agieren, zukünftig europaweit einheitliche Regeln für den Umgang mit personenbezogenen Daten einhalten. In Deutschland haben sich inzwischen mehrere Industriekonsortien gebildet, die sich jeweils mit einem eigenen Identitätsmanagementdienst etablieren wollen. Dahinter stehen große namhafte Konzerne mit teilweise großem Kundenstamm.

Diese Entwicklung zeigt, dass die öffentliche Verwaltung auf viele existierende Lösungen und einem breiten Erfahrungsschatz aufbauen kann. Um digitale Verwaltungsangebote attraktiver zu gestalten, wird in diesem Papier empfohlen, leichtgewichtige Ergänzungen zur Online-Ausweisfunktion für die Verwaltung nutzbar zu machen, das heißt konkret:

1 Vgl. ausführlich Abschnitt 3.1.

- **Vertrauensniveaus nutzerorientiert und realistisch festlegen**

  Wir empfehlen grundsätzlich, zunächst die Onlinedienste und damit verbundenen Prozesse aus Nutzersicht zu definieren, dann die Datenströme zu betrachten, den Schutzbedarf festzulegen und erst dann das Vertrauensniveau sowie das „passende" Identifikationsverfahren zu bestimmen.

- **Leichte Zugänglichkeit als oberstes Gebot leben**

  Besonders für Gelegenheitsnutzer ist ein einfacher Zugang zu Verwaltungsleistungen von hoher Bedeutung, wobei möglichst eine Variante zum Einsatz kommen sollte, die den Bürgerinnen und Bürgern aus anderen Lebensbereichen vertraut ist. Für Onlinedienste, die das Vertrauensniveau „substanziell" erhalten, sollte geprüft werden, ob und wie Servicekonten bspw. das ELSTER-Zertifikat zur Identifikation nutzen können.

- **Zusammenarbeit mit privaten Initiativen prüfen**

  Derzeit entstehen viele privatwirtschaftliche Initiativen im Bereich der Identifizierung und Authentifizierung. Noch ist offen, wie erfolgreich die teilweise noch jungen privatwirtschaftlichen Initiativen sind. Sollte die Nutzung schnell Verbreitung finden, bieten sich hier ggf. weitere Möglichkeiten, um Onlinedienste der Verwaltung leicht zugänglich und damit attraktiv zu gestalten.

- **Registervernetzung vorantreiben**

  Der Zugang zu und die Nutzung von Onlinediensten der Verwaltung könnte erheblich erleichtert werden, wenn das Prinzip des Once Only[2] konsequent umgesetzt wird. Hierzu bedarf es einer stärkeren Vernetzung der Register und damit verbunden geeigneter Mechanismen, um registerübergreifend die Daten einer Person zu identifizieren. Hier bestehen in Deutschland vor dem Hintergrund des Grundrechts auf informationelle Selbstbestimmung hohe Hürden. Der Blick auf andere Länder, etwa Österreich, zeigt jedoch, dass es Lösungsansätze gibt, die diesen Anforderungen gerecht werden können. Diese Lösungsansätze sollten weiter verfolgt und an die deutschen Bedingungen angepasst werden.

Schlagworte: Identitätsmanagement, Online-Ausweisfunktion (eID), Personalausweis, Servicekonto, Identifizierung, Authentifizierung

2 Once Only bedeutet, „dass Daten und Dokumente der Bürger und Unternehmen […] nur genau einmal – once only – in der Verwaltung produziert oder dort erfasst und bei Bedarf von anderen Behörden wiederverwendet, soweit dem keine Datenschutzinteressen der Betroffenen entgegenstehen." Siehe Gabriele Goldacker et al. 2019, No-Government, In: Jens Fromm und Mike Weber (Hrsg.), 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT, http://www.oeffentliche-it.de/-/no-government.

1. EINLEITUNG

Die Identifizierung und Authentifizierung von Bürgerinnen[3] und Bürgern sowie Unternehmen gibt seit Jahren immer wieder Anlass zu Diskussionen. Im Mittelpunkt der Auseinandersetzung steht dabei oft das Spannungsverhältnis zwischen Bedienbarkeit und erforderlicher Sicherheit.

Mit der Online-Ausweisfunktion des Personalausweises[4] steht ein starkes Identifizierungs- und Authentifizierungsmittel zur Verfügung, das auch online allen rechtlichen Anforderungen genügt. Allerdings führt das hohe Vertrauensniveau inhärent zu erhöhten Anforderungen an die Nutzer und deren IT-Infrastruktur (Einsatz spezieller Hard- und Software). Studienergebnisse zeigen, dass die Nutzung und Akzeptanz bisheriger Lösungen vergleichsweise gering und der Mehrwert den Nutzern oftmals nicht ersichtlich ist. Hürden sind die wenig komfortable Bedienung über ein zusätzliches kostenpflichtiges Lesegerät, vor allem aber die nach wie vor nur vereinzelten Anwendungsmöglichkeiten. So fehlen zum Beispiel als Partner viele große Onlineplattformen und Onlinebanking-Anbieter.[5] Unter anderem aus diesen Gründen konnte die Verbreitung und vor allem die Nutzung der Online-Ausweisfunktion des Personalausweises bis heute nicht flächendeckend realisiert werden: Lediglich 6% der deutschen Onliner hat neben dem Personalausweis mit aktivierter Online-Ausweisfunktion auch ein Lesegerät. Zwar kennen 48% die Möglichkeit, ihr Fahrzeug auch online abzumelden, aber nur 14% nutzen diese Möglichkeit.[6] Ob die kostenlose „AusweisApp2“, bei der NFC-fähige Smartphones in vielen Fällen das Kartenlesegerät ersetzen, der Online-Ausweisfunktion einen Schub verleihen, bleibt abzuwarten. In Österreich hat erst die sogenannte Handy-Signatur den Durchbruch gebracht.[7]

Für unternehmensinterne Prozesse kommt hinzu, dass der Personalausweis ein Dokument für das private Umfeld ist, sodass Mitarbeiter nicht verpflichtet werden können, ihre privaten Ausweisdokumente im dienstlichen Kontext zu nutzen. Alternativen wie Signaturkarten sind zwar zumindest teilweise vorhanden, sie stellen jedoch ähnliche Anforderungen an die Nutzer bezüglich Hard- und Software wie die Online-Ausweisfunktion. Es besteht daher der Bedarf nach Ergänzungen zur Identifizierung eines Unternehmens. Lösungen entstehen allmählich. Ideen sind etwa die Elster ID, die Nutzung elektronischer Siegel gemäß eIDAS oder Ansätze über das Unternehmenskonto im Kontext der OZG-Umsetzung, wobei der

3 Im folgenden Text ist die weibliche Form der männlichen Form gleichgestellt; lediglich aus Gründen der Vereinfachung wurde teilweise nur die männliche Form gewählt.

4 In diesem Dokument bezeichnet der Begriff „Personalausweis“ stets den sogenannten neuen oder elektronischen Personalausweis mit Online-Ausweisfunktion. Da Online-Ausweisfunktion in Personalausweis und elektronischem Aufenthaltstitel im Wesentlichen identisch sind, beziehen sich Aussagen zur Online-Ausweisfunktion ebenfalls sowohl auf den Personalausweis als auch den Aufenthaltstitel.

5 Vgl. https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Anwendungen/Anwendungen_node.html, Stand 02.07.2019.

6 Vgl. Initiative D21, fortiss (Hrsg.): eGovernment MONITOR 2018, Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich, November 2018, S. 38ff.

7 Vgl. Abschnitt 5.3.

zuletzt genannte Ansatz über das entsprechende Projekt des IT-Planungsrates an Fahrt aufgenommen hat.[8] Da etliche Verwaltungsverfahren keine sehr hohen oder hohen Sicherheitsanforderungen haben und auch mit einfacheren Identifikations- und Authentifizierungsdiensten bedienbar wären, ist das Fehlen von niederschwelligen Verfahren einer der Hemmschuhe für die Akzeptanz von E-Government-Services durch die Bürger und Unternehmen.

Erfahrungen der Internetnutzer im E-Commerce, Onlinebanking etc. und den damit verbundenen einfachen Möglichkeiten der Identifikation und Authentifizierung (Nutzername/Passwort, mTAN/SMS-Tan, Video-Identifizierung oder biometrische Verfahren) erschweren die Akzeptanz hochsicherer Verfahren der öffentlichen Verwaltung zusätzlich. Dem E-Government Monitor 2018 zufolge wünschen sich die dort Befragten, für die Inanspruchnahme von Verwaltungsleistungen solche Authentifizierungsvarianten nutzen zu können, die sie aus anderen Lebensbereichen kennen.[9]

Im Kontext der Projekte Servicekonto, Portalverbund und Umsetzung des Onlinezugangsgesetzes (OZG) bekommt das Thema neue Relevanz. Denn wenn Deutschland den Prozess der Verwaltungsdigitalisierung massiv beschleunigen will, braucht es bezogen auf die Identifizierung und Authentifizierung Lösungen, die die Nutzer kennen, mit geringem Aufwand einsetzen und auch für Onlinedienste der Verwaltung nutzen können. Hierfür ist es sinnvoll, die Erfahrungen der Bürger aus anderen Lebensbereichen aufzugreifen, in denen bereits Internet-Transaktionen durchgeführt werden.

Auch die Verwaltung kennt solche Lösungen (z.B. in Hamburg oder Schleswig-Holstein mit Nutzername/Passwort). In anderen Mitgliedstaaten der EU gibt es seit Langem erfolgreich etablierte Lösungen, die als Beispiel dienen können.

Ergänzend eröffnen sich im Zusammenhang mit der Umsetzung der Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS)[10] neue Möglichkeiten der grenzüberschreitenden Zusammenarbeit im E-Government, auf die Deutschland vorbereitet sein muss.

Mit eIDAS sind zudem sogenannte Fernsignaturen möglich. Dabei benötigt ein Nutzer nicht wie bisher eine Signaturkarte mit Lesegerät und Software, sondern beauftragt einen sogenannten Vertrauensdienstanbieter damit, seine Signatur zu verwalten und in seinem Auftrag zu signieren. Rechtlich ist diese Lösung einer qualifizierten elektronischen Signatur gleichgestellt. Erste Beispielanwendungen gibt es auch in Deutschland.[11]

Dieses Papier will Anregungen für Politik, Verwaltung und Entscheider für die Entwicklung gemeinsamer Lösungsstrategien geben.

Dabei handelt es sich um ein Diskussionspapier, das bestehende Methoden und Lösungen beschreibt. Vertiefte Betrachtungen, die sich detailliert den technischen, rechtlichen und organisatorischen Voraussetzungen der jeweiligen Lösungen widmen, bleiben weiteren Untersuchungen vorbehalten. Zudem

8 29. Sitzung des IT-Planungsrats vom 27. Juni 2019. Entscheidung 2019/22 - Unternehmenskont/-en, https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2019/Sitzung_29.html?pos=4

9 Vgl. eGovernment MONITOR 2018, Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich, S. 30f.

10 EU-Verordnung Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910.

11 Vgl.: Aufruf: Bundesdruckerei und kommune.digital suchen Pilotanwender für sign-me, http://kommune.digital/sign-me/

handelt es sich um eine Momentaufnahme – aktuell gibt es zahlreiche Entwicklungen, die weiter beobachtet werden müssen und in diesem Papier nicht vollständig erwähnt werden können. Die Studie wird von zwei Thesen geleitet:[12]

These 1: Ein möglichst einfacher Zugang zu Verwaltungsleistungen ist ein kritischer Erfolgsfaktor für das E-Government in Deutschland. Damit verbunden werden niedrigschwellige Lösungen für die Identifizierung und Authentifizierung benötigt.

These 2: Zahlreiche der 575 Verwaltungsleistungen, die es in den nächsten Jahren nach OZG zu digitalisieren gilt, können in die Vertrauensniveaus „normal“ oder „substanziell“ eingestuft werden. Insbesondere viele Verwaltungsleistungen der Kommunen werden mit dem Vertrauensniveau „normal“ einzuordnen sein.

Ausgehend von einer Darstellung allgemeiner Erfolgsfaktoren für Akzeptanz und Nutzung von Onlinediensten gehen wir auf Verwaltungsverfahren und Vertrauensniveaus in der deutschen Verwaltung ein. Basierend auf diesen Ergebnissen werden Empfehlungen für Verwaltung und Politik formuliert.

Im Teil „Vertiefung“ dieses Papiers beschreiben wir exemplarisch die strategische Ausrichtung anderer Länder. Zudem stellen wir – in einer Momentaufnahme – Lösungen für Identifizierung und Authentifizierung in der Wirtschaft vor. Diese Lösungen und Initiativen haben uns als Anregung für das Papier gedient und können von Entscheidern als weiterführende Quellen genutzt werden.

12 Wir verwenden die in Deutschland gebräuchlichen Begriffe, die von der eIDAS-Verordnung abweichen, also „normal“ für „niedrig“ und „Vertrauensniveaus“ für „Sicherheitsniveaus“.

2 ERFOLGSFAKTOREN FÜR AKZEPTANZ UND NUTZUNG

Erfolgsfaktoren für Akzeptanz und Nutzung elektronischer Identitäten aus Nutzer - und auch aus Anbietersicht - sind einfach zu benennen: **Nutzerfreundlichkeit und Sicherheit**. Im Folgenden werden einige Facetten benannt:

Nutzerfreundlichkeit:

- Identifizierung und Authentifizierung müssen für Nicht-Techniker verständlich und nachvollziehbar sein. Dazu gehört auch, dass die Verfahren sich an etablierten Lösungen orientieren, sodass Nutzer diese wiedererkennen und sich daran orientieren können.
- Die Beantragung (sofern notwendig) und Ausgabe der elektronischen Identitäten muss einfach und komfortabel sein.
- Bei Verfahren, die eine persönliche Identifizierung erfordern, muss die Identifizierungsstelle zeitlich und örtlich gut erreichbar sein.
- Die Lösungen müssen kostenlos oder zumindest kostengünstig zugänglich sein.
- Nutzer müssen zumindest mittel- bis langfristig zwischen verschiedenen Ausprägungen von elektronischen Identitäten wählen können (vergleichbar mit unterschiedlichen Bezahloptionen bei Onlinekäufen).
- Die elektronischen Identitäten müssen für verschiedene Dienste auch in unterschiedlichen Umgebungen und Infrastrukturen wie zum Beispiel mobil und auf dem PC oder im In- und Ausland genutzt werden können. Außerdem muss eine endgeräteübergreifende Nutzbarkeit bzw. Dauerhaftigkeit gegeben sein. Das heißt zum Beispiel: einfacher Übergang von einem Gerät auf ein anderes.
- Die Nutzung darf keine oder nur wenige Anforderungen an die Infrastruktur stellen (zum Beispiel keine lokale Installation erforderlich, keine zusätzlichen Infrastrukturkomponenten wie Kartenleser etc.).
- Das unterstützte Vertrauensniveau muss einfach erkennbar und nachweisbar sein.
- Abgestufte Verfahren hinsichtlich des Vertrauensniveaus müssen verständlich aufgebaut sein, und die zusätzlichen Stufen sollten keine völlig andersartigen Lösungen erfordern (nur Ergänzungen).

Sicherheit:

- Das Risiko für den Nutzer muss so gering wie möglich sein bzw. vertretbar im Verhältnis zum Mehrwert, der durch das Angebot erzielt wird.
- Im Schadensfall muss die Haftung bzw. der Eigenanteil für den Nutzer begrenzt sein.
- Die elektronischen Identitäten dürfen nicht durch Unbefugte kopiert und genutzt werden können.

13 Inzwischen ist die Online-Ausweisfunktion des Personalausweises über die AusweisApp2 auch mobil per Smartphone nutzbar. (vgl. http://www.die-ausweisapp.de/, konsultiert am 03.07.2019). Vgl. auch Ziffer 5.3 zur Handy-Signatur in Österreich.

- Eine hohe Resistenz gegen typische Angriffe (bzw. Schadsoftware, Man-in-the-middle, Phishing, Sessionübernahme) muss gegeben sein.

- Ein Widerruf bei Kompromittierung muss einfach möglich sein.

- Die Nutzung der Daten aus dem Identitätsmanagementsystem muss für den Nutzer immer transparent und nachvollziehbar sein (Datensouveränität).

Infrastrukturen für elektronische Identitäten müssen nicht nur den Nutzer einfach einbinden, sondern auch die Dienstanbieter. Lösungen, die in der Wirtschaft bzw. in Sozialen Netzwerken verwendet werden, setzen auf einen hohen Wiedererkennungswert und hohe Nutzerakzeptanz. Eine intelligente Identifizierungs- und Authentifizierungsinfrastruktur basiert dabei nicht nur auf dem verwendeten Identifizierungs- und Authentifizierungsmittel (bzw. mehreren bei 2-Faktor-Authentifizierung), sondern könnte gegebenenfalls auch auf weiteren kontextabhängigen Faktoren beruhen, wie etwa der Umgebung, den Gerätedetails oder anderen benutzerspezifischen Attributen.

3 VERWALTUNGSVERFAHREN UND VERTRAUENSNIVEAUS

Die in Abschnitt 2 genannten und sich teilweise widersprechenden Anforderungen zeigen, dass eine Universallösung, die allen Aspekten gleichermaßen gerecht wird, nicht möglich ist. Identitätsmanagement-Lösungen werden daher entsprechend ihrem Vertrauens- bzw. Sicherheitsniveau unterschieden. Je nach Schutzbedarf eines Dienstes kann so ein passgenauerer Kompromiss zwischen Nutzerfreundlichkeit und Sicherheit gefunden werden.

3.1 Methodisches Vorgehen

Im Rahmen der Aktivitäten des IT-Planungsrates hat die Projektgruppe Strategie für eID und andere Vertrauensdienste im E-Government „eID-Strategie“ das Papier „Interoperables Identitätsmanagement für Bürgerkonten – Studie“ herausgegeben. Dort heißt es unter anderem:

„Bei der elektronischen Registrierung für ein Bürgerkonto ist zur Überprüfung der Identität grundsätzlich die eID-Funktion erforderlich. Zur Senkung der Einstiegshürden und zur Steigerung der Akzeptanz der Bürgerinnen und Bürger ist auch eine Registrierung mit Benutzername/Passwort möglich. Dies setzt voraus, dass sich die Nutzung des Bürgerkontos zunächst auf Verwaltungsdienstleistungen mit dem Vertrauensniveau „normal“ beschränkt. Im Fall einer späteren Nutzung von Verwaltungsdienstleistungen auf höheren Vertrauensniveaus, ist eine nachträgliche Registrierung mit der Online-Ausweisfunktion möglich. Daneben besteht die Möglichkeit, Verwaltungsprozesse außerhalb einer Registrierung oder Anmeldung pseudonym oder anonym durchführen zu können, so beispielsweise zum Herunterladen öffentlich zugänglicher Statistiken oder Geodaten.“[14]

Um die Nutzungshürden so gering wie möglich zu halten, ist vor dem Hintergrund der geringen Nutzung der Online-Ausweisfunktion des Personalausweises und des Aufenthaltstitels sorgsam zu prüfen,

ob andere Möglichkeiten der Identifizierung und Authentifizierung existieren, die den Bürgern vertraut sind.

Auch nach Auffassung einschlägiger Institutionen wie dem BSI oder NIST ist es sinnvoll, die Art und Weise einer Multi-Faktor-Authentifizierung (MFA) sowohl an den Sicherheitsbedürfnissen der jeweiligen Anwendung zu orientieren als auch an den betroffenen Verfahrensnutzern und deren Akzeptanz einer solchen Lösung.

Das BSI unterscheidet Vertrauensniveaus wie folgt:

- **normal:** Die Schadensauswirkungen bei einer Kompromittierung sind begrenzt und überschaubar;
- **substanziell:** Die Schadensauswirkungen bei einer Kompromittierung sind substanziell;
- **hoch:** Die Schadensauswirkungen bei einer Kompromittierung können beträchtlich sein.

Zusätzliche Anforderungen über Vertrauensniveau „hoch" hinaus können aufgrund rechtlicher **Formvorschriften** bestehen, gekennzeichnet durch **„hoch +"**. Bei Geschäftsprozessen, für die die Schadensauswirkungen bei einer Kompromittierung vernachlässigbar sind, ist das Vertrauensniveau **untergeordnet**, das nicht weiter betrachtet wird.[15]

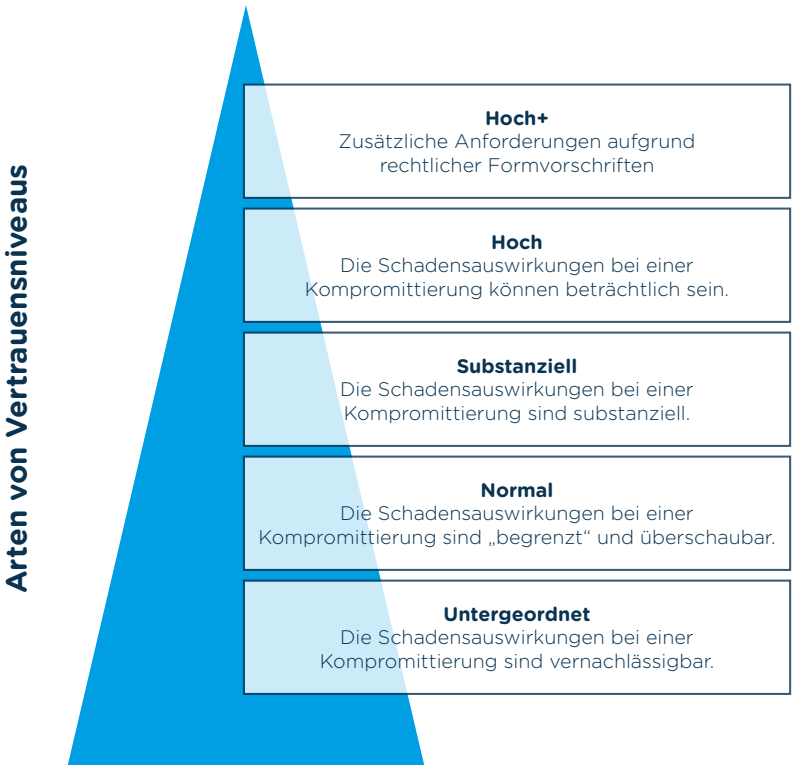

Abbildung 1: Arten von Vertrauensniveaus nach BSI TR-03107[16]

14 IT-Planungsrat: Interoperables Identitätsmanagement für Bürgerkonten – Studie – Stand: 6. Mai 2015, S. 22, http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/eID/Studie_Identitaetsmanagement_BK.pdf

15 Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government. Teil 1: Vertrauensniveaus und Mechanismen. Version 1.1 31.10.2016 S. 8. https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html

16 Ebd.

Vertrauensniveaus sollen in zwei Schritten definiert werden:

- Das initiale Vertrauensniveau für eine Leistung leitet sich aus dem potenziellen Schaden ab, den eine falsche Identifizierung, eine nicht eindeutig zuzuordnende Willenserklärung oder falsch übermittelte Daten erzeugen.
- Das finale Vertrauensniveau wird aus Gewichtung des initialen Vertrauensniveaus mit der Eintrittswahrscheinlichkeit des Schadens gebildet.

Das Verfahren wird anschließend passend zu dem bestimmten finalen Vertrauensniveau ausgewählt.

Die folgende Tabelle aus der Technischen Richtlinie TR-03107[17] illustriert die Bewertungen:

Gefährdung	Potentieller Schaden bedingt Vertrauensniveau		
	Normal	**Substantiell**	**Hoch**
Verstoß gegen Gesetze/Vorschriften	Verstoß mit geringfügigen Konsequenzen	Verstoß mit substantiellen Konsequenzen	Verstoß mit erheblichen Konsequenzen Besondere Formvorschriften (*hoch +*) bei Gefahr eines Verstoßes mit schwerwiegenden Konsequenzen
Unrichtige Identifizierung oder Zuordnung zu einer Identität	Geringfügige Konsequenzen	Substantielle Konsequenzen	Erhebliche Konsequenzen Besondere Formvorschriften (*hoch +*) bei Gefahr von schwerwiegenden Konsequenzen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen beeinträchtigen können.	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen substantiell beeinträchtigen können.	Verarbeitung personenbezogener Daten, die den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen können.
Beeinträchtigung körperlicher/persönlicher Unversehrtheit	Beeinträchtigung erscheint nicht möglich	Beeinträchtigung kann nicht vollständig ausgeschlossen werden	Beeinträchtigung kann nicht ausgeschlossen werden
Beeinträchtigung der Aufgabenerfüllung	Beeinträchtigung wird von den Betroffenen als tolerabel eingeschätzt	Beeinträchtigung wird von einzelnen Betroffenen als tolerabel eingeschätzt	Beeinträchtigung wird als nicht tolerabel eingeschätzt
Negative Innen- oder Außenwirkung	Geringe/nur interne Ansehens- oder Vertrauensbeeinträchtigung zu erwarten	Substantielle Ansehens- oder Vertrauensbeeinträchtigung zu erwarten	Breite Ansehens- oder Vertrauensbeeinträchtigung zu erwarten
Finanzielle Auswirkungen	Finanzieller Schaden tolerabel	Subtantieller finanzieller Schaden möglich	Beachtliche finanzielle Verluste, jedoch nicht existenzbedrohend

Zu beachten: Die Aggregation von Gefährdungen kann zur Erhöhung des notwendigen Vertrauensniveaus führen. Zum Beispiel kann die Verarbeitung personenbezogener Daten mit Schutzbedarf *substantiell* zu einem notwendigen Vertrauensniveau *hoch* führen, wenn viele Personen von einer Beeinträchtigung betroffen sind.

Sind mehrere Gefährdungen relevant, so ist für die Gesamtbewertung das Maximum der einzeln ermittelten notwendigen Vertrauensniveaus anzunehmen.

Tabelle 1: Gefährdungen und Vertrauensniveaus, Quelle: BSI TR-03107

17 Ebd. S. 14.

Das BSI schreibt: „Es wird empfohlen, die Feststellung des notwendigen Vertrauensniveaus auf Basis einer Schutzbedarfsfeststellung nach [BSI100-2][18] unter zusätzlicher Berücksichtigung rechtlicher Vorgaben durchzuführen. Bei Geschäftsprozessen, bei denen im Falle eines Missbrauchs im Wesentlichen keine Schäden entstehen, kann auf Mechanismen gemäß dieser Richtlinie verzichtet werden."[19]

Zu beachten ist, dass immer zwei Varianten zu berücksichtigen sind: Entweder definiert das Fachrecht das Vertrauensniveau der Verwaltungsdienstleistung. Oder dieses ist im Fachrecht nicht vorgegeben, dann definieren die Behörden das Vertrauensniveau.[20]

3.2 Beispiele

Gegenwärtig definieren Verwaltungen die Vertrauensniveaus identischer Verwaltungsdienstleistungen durchaus unterschiedlich. Vergleicht man verschiedene Internetauftritte[21], so sind die Anforderungen der Verwaltungen sehr unterschiedlich. Für die Beantragung von Personenstandsurkunden sind die Anforderungen sehr hoch, vieles muss schriftlich oder mit persönlichem Erscheinen beantragt werden. Andere Behörden ermöglichen eine Registrierung mit Personalausweis bzw. Aufenthaltstitel oder auch nur mit E-Mail-Adresse und Passwort. Ob die dafür erforderlichen Entscheidungen immer auf den vom BSI empfohlenen Verfahren beruhen, ist unklar. Eher ist zu vermuten, dass Erfahrungswerte, Gewohnheiten oder das Bestreben, die Online-Ausweisfunktion des Personalausweises und des Aufenthaltstitels breit einzusetzen, Entscheidungsgründe sind.

Beispiele:

Urkunden des Standesamtes:

- In Düsseldorf können Urkunden online bestellt werden (ohne Registrierung).
- In Schleswig-Holstein muss man mit Identitätsnachweis registriert sein.
- In Köln kann man eine Geburtsurkunde ohne Registrierung online bestellen, bei Zuhilfenahme der eID-Funktion des Personalausweises wird das Formular vorausgefüllt.

Einfache Melderegisterauskunft:

- In Hamburg ist eine Onlineantragstellung möglich, wenn der Anfrager ein Servicekonto mit Identitätsnachweis im Kundenzentrum oder mit dem neuen Personalausweis hat.
- In Schleswig-Holstein ist eine Onlineantragstellung möglich, wenn der Anfrager ein Servicekonto mit E-Mail-Adresse und Name hat.
- In Köln ist die Onlineabwicklung ohne Registrierung möglich. Nach Ausfüllen der Eingabemasken und Eingabe der Bankverbindung werden die Daten geprüft und bei erfolgreicher Prüfung die Melderegisterauskunft sofort erteilt.
- In Düsseldorf müssen ein ausgefülltes und unterschriebenes Antragsformular und die Kopie des Überweisungsbelegs (Gebühren) vorgelegt werden.

18 Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-2. IT-Grundschutz-Vorgehensweise, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile

19 Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government. Teil 1: Vertrauensniveaus und Mechanismen. Version 1.1 31.10.2016 S. 12., https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html

20 Vgl. IT-Planungsrat: Interoperables Identitätsmanagement für Bürgerkonten - Studie - Stand: 6. Mai 2015, S. 15. http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/eID/Studie_Identitaetsmanagement_BK.pdf

21 Für das konkrete Beispiel wurden die Serviceportale von: Hamburg, Schleswig-Holstein, Aachen, Köln, Düsseldorf, Nürnberg, Stuttgart und Ulm konsultiert.

4 EMPFEHLUNGEN

4.1 Vertrauensniveaus nutzerorientiert und realistisch festlegen

Im Rahmen der Umsetzung des OZG wird eine Vereinheitlichung der Vertrauensniveaus angestrebt. Wir empfehlen grundsätzlich, zunächst die Onlinedienste und damit verbundenen Prozesse aus der Nutzersicht zu definieren, dann die Datenströme zu betrachten und erst dann das Vertrauensniveau zu bestimmen und entsprechende Instrumente zur Identifizierung oder Authentifizierung auszuwählen.

Als Zwischenlösung empfiehlt sich, standardmäßig besonders für Leistungen, die von den Kommunen erbracht werden, das Vertrauensniveau „normal“ oder ggf. „substanziell“ anzunehmen. Sollen höhere Niveaus gelten, sollte dies begründet werden (Risiken und Risikoeintrittswahrscheinlichkeit, potenzieller Schaden).

Eine Schutzbedarfsfeststellung in vereinfachter Form sollte für Zweifelsfälle erfolgen, die nach Erfahrung und gesundem Menschenverstand nicht als „normal“ eingestuft werden können.

Ergänzend sollten weitere Kriterien zur Bestimmung des Vertrauensniveaus herangezogen werden:

- **Gebühren- / Steuerpflicht:** Wenn die Zahlung von Gebühren oder Steuern vorgesehen ist, ist das Missbrauchsrisiko voraussichtlich gering. Dies gilt z. B. für die Anmeldung eines Hundes, für den Fischereischein, den Anwohnerparkausweis, das Wunschkennzeichen und ähnliche Leistungen der Verwaltung. Von dieser Regel sollte nur abgewichen werden, wenn besondere Risiken vorliegen (etwa bei der Ausstellung eines Waffenscheins).

- **Transferleistungen:** In der Leistungsverwaltung sind andere Betrachtungen erforderlich, da Transferleistungen an einen unberechtigten Empfänger ggf. erheblichen Schaden verursachen können, wenn die Zahlungen über einen längeren Zeitraum erfolgen. Hier wird man regelhaft das Vertrauensniveau „hoch“ annehmen können. Für solche Verfahren sollte die Online-Ausweisfunktion des Personalausweises bzw. des Aufenthaltstitels die primäre Wahl sein, es sei denn, innerhalb der Verwaltung werden alternative Verfahren für das Vertrauensniveau „hoch“ etabliert (etwa indem Nachweise eine eindeutige Identifizierung ermöglichen). Vor einer solchen Entscheidung ist zunächst allerdings zu betrachten, wie die Fachprozesse im Hintergrund ausgestaltet sind. Wenn die Verwaltung vor Leistungsgewährung die Daten nochmals prüft oder den Empfänger sogar vorsprechen lässt, reicht ein erster Antrag online über das Vertrauensniveau „normal“.

- **Sicherheit:** Bei sicherheitsrelevanten Verwaltungsleistungen wie etwa der Ausstellung von Waffenscheinen wird man ebenfalls regelhaft das Vertrauensniveau „hoch“ annehmen können.

Zu beachten ist, dass sich die Anforderungen an Identifizierung und Authentifizierung verändern, wenn bei einem Onlinedienst auf Registerdaten zugegriffen werden kann (Once Only). Da es sich häufig um den Zugriff auf personenbezogene Daten (oder auf sensible Unternehmensdaten) handelt, wird über das Vertrauensniveau neu zu entscheiden sein.

Wenn die Risikoanalyse ergibt, dass das Vertrauensniveau „hoch“ anzusetzen ist, muss die Online-Ausweisfunktion des Personalausweises bzw. des Aufenthaltstitels genutzt werden, auch wenn sie bisher nicht sehr verbreitet ist.

4.2 Leichte Zugänglichkeit als oberstes Gebot leben

Bei Festlegung des Vertrauensniveaus sollten auch die Nachfragegruppen differenziert werden. Zu unterscheiden sind auf jeden Fall Gelegenheitsnutzer und Power-Nutzer. Besonders für Gelegenheitsnutzer ist ein einfacher Zugang zu Online-Verwaltungsleistungen von hoher Bedeutung, wobei möglichst eine Variante zum Einsatz kommen sollte, die den Bürgern aus anderen Lebensbereichen vertraut ist.

So stellt der eGovernment Monitor 2018 der Initiative D21 fest: „Onliner möchten bewährte Identifizierungsverfahren aus dem privaten Bereich auch für digitale Behördengänge einsetzen."[22] Dem eGovernment Monitor 2018 zufolge sind dies vor allem:

- Benutzername und Passwort,
- PIN-/TAN-Verfahren,
- Bestätigungslink per E-Mail.

Für Onlinedienste, die das Vertrauensniveau „substanziell" erhalten, sollten Servicekonten die Möglichkeit bieten, sich über das ELSTER-Zertifikat zu identifizieren, das sehr viele Bürger besitzen und mit dessen Nutzung sie vertraut sind. Im Juni 2018 waren über 6 Millionen ELSTER-Zertifikate ausgestellt. Die Nutzung des Elster-Zertifikats bietet besonders bei Servicekonten für Unternehmen einen Mehrwert, da Elster auch ein Organisationszertifikat ausstellt. Das würde es ermöglichen, auch das Unternehmen zu identifizieren. Dass das Elster-Zertifikat ggf. eine gute Ergänzung böte, zeigt auch eine repräsentative Bevölkerungsumfrage des Kompetenzzentrums Öffentliche IT. Demnach genießt die Software zur Abgabe der Steuererklärung mit 78% ein hohes Vertrauen und wird von 63% auch regelmäßig verwendet.[23] Bisher liegt allerdings noch keine Entscheidung des BSI vor, ob ELSTER dem Vertrauensniveau „substanziell" genügt (Stand: 03.07.2019).

In Hamburg ist in dem Programm „Digital First" angedacht, analog zu Social Logins z. B. Nutzerkonten bei Universitäten, Banken oder anderen Einrichtungen zu akzeptieren, weil diese identifiziert sind. Im Gegenzug können Banken, Versicherungen etc. das Servicekonto bei der Verwaltung nutzen (in Hamburg).[24]

4.3 Zusammenarbeit mit privaten Initiativen prüfen

Abzuwarten bleibt der Erfolg der Konsortien aus der Privatwirtschaft wie Verimi, netID, Mobile Connect oder YES (ausführlich in Kapitel 6). Sollte die Nutzung schnell Verbreitung finden, bieten sich hier ggf. weitere Möglichkeiten, um Onlinedienste der Verwaltung leicht zugänglich und damit attraktiv zu gestalten. Denn diese Initiativen der Privatwirtschaft bieten ggf. alternative Wege einer nutzerorientierten Identifizierung für Verwaltungsleistungen – besonders wenn wichtige Partner wie etwa große Onlinehändler oder Banken den Allianzen beitreten bzw. selbst die Allianzen bilden wie die Sparkassen und Volksbanken bei YES. In anderen Ländern hat sich eine Kooperation mit Banken als besonders erfolgreich erwiesen – so z.B. in Estland oder Dänemark.

Zu prüfen sind allerdings Fragen

- der rechtlichen Zulässigkeit,

22 eGovernment Monitor 2018, S. 30.

23 Vgl. Kompetenzzentrum Öffentliche IT: Repräsentative Bevölkerungsumfrage „Vertrauen in die Digitale Verwaltung", durchgeführt im November & Dezember 2018. https://www.oeffentliche-it.de/umfragen?entry=vertrauen

24 Das Servicekonto von Dataport bietet inzwischen unterschiedliche Authentifizierungsarten an (Registrierung mit E-Mail Adresse und Name, Registrierung mit der Online-Ausweisfunktion des Personalausweises, Signaturkarte (in Vorbereitung sind ELSTER, Elster-Zertifikat).

- der Sicherheit (digitale Souveränität), denn es ist entscheidend, wie die Identifizierung erfolgt, ob ggf. auch sensible Daten der Bürger gespeichert werden („Logbücher“ des Bürgers) und, wenn ja, wie und wo diese Daten gespeichert werden[25] sowie

- der Wirtschaftlichkeit (die Geschäftsmodelle der Konsortien müssen in einer Kosten-Nutzen-Analyse geprüft werden, zum Beispiel Kosten der Partnerschaft gegenüber sinkenden Verwaltungskosten bei einer prognostizierbar wachsenden Akzeptanz von Onlinediensten der Verwaltung).

Bezogen auf die Identifizierung von Unternehmen ist zu prüfen, in welcher Weise die öffentliche Verwaltung mit privatwirtschaftlichen Dienstleistern kooperieren kann. Es gibt einige Unternehmen, die für ihre Kunden als Identity Provider agieren und teils sehr viele Daten von sehr vielen Unternehmen vorhalten.

Von der Nutzung der Identifizierungen bei den Sozialen Netzwerken oder weiteren globalen Plattformanbietern wird aus Gründen der digitalen Souveränität abgeraten.

4.4 Alternative Verfahren nutzen

Um einen Bürger oder ein Unternehmen eindeutig zu identifizieren und einem Verwaltungsvorgang zuzuordnen, sollten auch alternative Verfahren in Betracht gezogen werden. Dies gilt insbesondere dann, wenn Verwaltungsleistungen vor allem für den Bürger „leicht“ nutzbar sein sollen. Zur Verdeutlichung einige Beispiele:

- **Wohngeld:** Das Digitalisierungslabor Wohngeld (Stand September 2018) schlägt vor, dass es zur Authentifizierung ausreicht, wenn Antragsteller den Antrag ausfüllen, Nachweise hochladen und den Antrag an die Verwaltung senden. Über die Nachweise ist eine eindeutige Authentifizierung möglich.

- **Anhörung bei Ordnungswidrigkeitsverfahren:** Die Verwendung elektronischer Formulare (und die Möglichkeit des elektronischen Bezahlens) kann den Prozess „Anhörung bei Ordnungswidrigkeitsverfahren“ beschleunigen und günstiger machen, wie bereits einige Kommunen zeigen. Da weder ein Schriftformerfordernis noch eine Identifikationsnotwendigkeit besteht, reicht eine kontextbezogene Identifikation mit dem Aktenzeichen des Bußgeldvorgangs in einem elektronischen Formular „Anhörung“ vollkommen aus.

- **Hund anmelden:** Bei „Ablösung“ eines Hundes durch einen anderen ist möglich, das Kassenzeichen zur Identifizierung anzugeben (so in der Landeshauptstadt Düsseldorf).

  In Hamburg ist die Anmeldung eines Hundes mit Benutzername und Passwort des Halters möglich.

  Die Anmeldung kann ohne Identifizierung erfolgen, da die Zustellung der Anmeldung an die Meldeadresse erfolgt.

- **Zustellung von Wahlunterlagen:** Die Zustellung von Wahlunterlagen kann ohne Identifizierung erfolgen, da die Zustellung an die Meldeadresse erfolgt.

- **Offene Schnittstellen für Unternehmen schaffen:** Für Onlinedienste, die von Unternehmen sehr häufig nachgefragt werden, sollte die Realisierung von Maschine-Maschine-Kopplung über APIs geprüft und wenn möglich realisiert werden. Dies kann ggf. über die Grenzen einzelner Unternehmen hinaus branchenbezogen erfolgen. Neben der Authentifizierung der

25 Vgl. die unterschiedlichen Ansätze unter den Ziffern 6.4 bis 6.8.

Kommunikationspartner ist bei der Maschine-Maschine-Kommunikation vor allem die Absicherung der Datenübertragung und die Sicherung der Datenverwendung relevant.[26]

4.5 Zwang zur Nutzung von digitalen Verwaltungsleistungen prüfen

Es sollte geprüft werden, bei welchen Verwaltungsleistungen die Nutzer (Bürger und Unternehmen) zur Verwendung vorhandener digitaler Onlineangebote gezwungen werden können. Der Vorteil für die Verwaltung ist, dass auf diese Weise sehr schnell hohe Nutzungsraten erreicht werden können.

Dieser Weg bietet sich in erster Linie bei Angeboten für Unternehmen und Betriebe an. Denn bei Onlinediensten für Bürger gibt es zahlreiche, unter anderem juristische Hürden, die diese Lösung voraussichtlich mindestens kurzfristig ausschließen dürften.

Verpflichtungen zur digitalen Abwicklung von einzelnen Verwaltungsverfahren gibt es für Unternehmen und andere professionelle Nutzer schon seit vielen Jahren. In einem Bericht von KGSt und KoopAADV werden bereits im Jahr 2006[27] beispielhaft genannt: Übermittlung von Umsatzsteuervoranmeldungen, Lohnsteueranmeldungen und Lohnsteuerbescheinigungen, Meldungen und Beitragsnachweise der Arbeitgeber zu sozialversicherungspflichtigen Beschäftigten, Beantragung von Verschmutzungsrechten gemäß Treibhausemissionshandelsgesetz. Inzwischen gibt es eine Reihe weiterer solcher Verpflichtungen. Ein junges Beispiel ist eRechnung.

4.6 Nutzungsanreize schaffen

Die Akzeptanz von Onlinediensten kann gefördert werden, wenn – wie in Österreich[28] – z.B. geringere Kosten für die Nutzer entstehen oder die Verfahren schneller abgewickelt werden oder verbindliche Statusinformationen Teil des Onlineangebotes sind. Allerdings muss die rechtliche Zulässigkeit geprüft werden. Vereinzelt gibt es diese Ansätze auch in Deutschland: In Hamburg beispielsweise ist die elektronische Anmeldung eines Hundes deutlich günstiger als die Anmeldung auf analogem Wege.

4.7 Recht digitaltauglich machen

Öffentliche Verwaltung und Politik müssen die rechtlichen Hürden, d.h. vor allem Formerfordernisse wie Schriftform, persönliches Erscheinen, Vorlage von Nachweisen im Original senken und die Spezifika der Digitalisierung berücksichtigen. Die Technik muss zwar den juristischen Vorgaben folgen, allerdings müssen auch die juristischen Vorgaben digitaltauglich gestaltet sein. So empfiehlt der Normenkontrollrat: „Zusätzlich sollen ausweislich des Koalitionsvertrages und bestärkt durch Empfehlungen des Digitalrates auch zukünftige Gesetze frühzeitig auf ihre Digitaltauglichkeit geprüft werden. Als Orientierung wird auf einen Digitalisierungs-Tauglichkeits-Check im dänischen Gesetzgebungsverfahren verwiesen. Auch der E-Government-Prüfleitfaden von NKR und IT-Planungsrat verfolgt ein solches Ziel.“[29]

26 Dataport hat beispielsweise für einen großen Energieversorger eine API gebaut, so dass der Prozess des Aufgrabescheins direkt in einer Maschine-Maschine-Kommunikation abgewickelt werden kann.

27 Vgl. KGSt / KoopAADV: Erfolgsfaktoren von E-Government. KGSt-Bericht 1/2006.

28 Vgl Ziffer 5.3.

29 Normenkontrollrat: Monitor Digitale Verwaltung #2. Mai 2019, S. 9.

4.8 Registervernetzung vorantreiben

Der Zugang und die Nutzung von Onlinediensten der Verwaltung könnte erheblich erleichtert werden, wenn das Prinzip des Once Only[30] konsequent umgesetzt wird. Hierzu bedarf es einer stärkeren Vernetzung der Register und damit verbunden geeigneter Mechanismen, um registerübergreifend die Daten einer Person zu identifizieren. Hier bestehen in Deutschland vor dem Hintergrund des Grundrechts auf informationelle Selbstbestimmung hohe Hürden.[31] Solche Identifier sind nur für einzelne Bereiche zulässig, beispielsweise die Steuer-ID für das Finanzwesen. Seine Nutzung ist daher auch gesetzlich nur zu sehr eingeschränkten Zwecken möglich.

Als Beistellung zum NKR-Gutachten 2017 zur Registermodernisierung hat die Deutsche Universität für Verwaltungswissenschaften Speyer, Deutsches Forschungsinstitut für öffentliche Verwaltung, geprüft, ob das österreichische Modell in Deutschland anwendbar ist. Die Autoren kommen zu einem positiven Ergebnis.[32] Das Verfahren in Österreich ist allerdings aufwändig und kennt verschiedene Herstellungsphasen: Jeder in Österreich gemeldete Bürger ist durch eine Zahl aus dem Zentralen Melderegister (Melderegisterzahl bzw. ZMR-Zahl) eindeutig identifizierbar. Auf der Bürgerkarte wird die ZMR nicht gespeichert, sondern kryptografisch wird eine Stammzahl berechnet. Aus der Stammzahl kann man die ZMR nicht wiederherstellen. Aus Datenschutzgründen wird auch die Stammzahl bei Nutzung der Bürgerkarten nicht direkt verwendet, sondern kryptografisch in sogenannte bereichsspezifische Personenkennzeichen (bPK) für unterschiedliche Verwaltungsbereiche umgewandelt.[33] Wegen der Komplexität sind weitere Möglichkeiten zu untersuchen, die weniger komplex und gleichzeitig sicher und datenschutzkonform sind. Hier sind weitere Prüfungen von Lösungen aus dem europäischen Ausland vonnöten.[34]

Bewegung kommt durch den Beschluss der Innenministerkonferenz vom Juni 2019 zum „verfahrensübergreifenden Identitätsmanagement“ in die Entwicklung: In der Anlage zum Beschluss (TOP 12) wird ausgeführt, es solle ein Kerndatensystem geschaffen werden, „in dem die Grunddaten aller Personen mit Verwaltungskontakt in Deutschland gepflegt werden […] Eine eindeutige Zuordnung der Personalienidentität über alle Register hinweg ist herzustellen. Dies kann mithilfe eines Identifiers geschehen.“[35] Wie genau die Lösung aussehen wird, bleibt abzuwarten.

30 Once Only bedeutet, „dass Daten und Dokumente der Bürger und Unternehmen […] nur genau einmal – once only – in der Verwaltung produziert oder dort erfasst und bei Bedarf von anderen Behörden wiederverwendet, soweit dem keine Datenschutzinteressen der Betroffenen entgegenstehen.“ Vgl. Goldacker et al. 2019, No-Government

31 Vgl. Mario Martini, David Wagner, Michael Wenzel: Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer, Version 1.0, Speyer 2017, Stand 17.09.2017.

32 Vgl. ebd.

33 Vgl. https://www.buergerkarte.at/sicherheit-datenschutz.html

34 In den skandinavischen Ländern gibt es z.B. eine sogenannte personnummer. Diese Nummer wird sowohl von öffentlichen als auch nicht-öffentlichen Stellen als Schlüssel verwendet. Vgl. http://www.schwedentor.de/auswandern-leben/durchfuehrung/personnummer; http://de.sonderborgkommune.dk/soenderborg-kommune-auf-deutsch/cpr-nummer-personenkennzahl

35 Bundesministerium des Innern, für Bau und Heimat: Vorschlag des Bundesministeriums des Innern, für Bau und Heimat zur Verbesserung des Identitätsmanagements als Teil der Registermodernisierung, Februar 2019, https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/20190614_12/anlage-zu-top-12.pdf?__blob=publicationFile&v=2.

5 IDENTIFIZIERUNGS-LÖSUNGEN IN DER EU – BEISPIELE

5.1 Übersicht

Die zunehmende Bedeutung von elektronische Identifizierungslösungen und Vertrauensdiensten wird durch die EU-eIDAS-Verordnung deutlich. Dort wird die gegenseitige Anerkennung notifizierter elektronischer Identifizierungssysteme[36] auf EU-Ebene geregelt. Seit dem 29. September 2018 sind alle EU-Mitgliedstaaten verpflichtet, nationale elektronische Identifizierungssysteme anderer Mitgliedstaaten anzuerkennen, die notifiziert sind und die Verordnung erfüllen. Am 22. August 2017 hat Deutschland als erster EU-Mitgliedsstaat die Online-Ausweisfunktion (eID-Funktion) des Personalausweises und des Aufenthaltstitels auf dem höchstmöglichen Vertrauensniveau gemäß eIDAS-Verordnung bei der EU-Kommission notifiziert.[37] Die deutsche Online-Ausweisfunktion kann für Verwaltungsverfahren mit einer elektronischen Identifizierung auf „substanziellem“ oder „hohem“ Vertrauensniveau genutzt werden. Inzwischen haben auch weitere Länder, wie Italien, Luxemburg, Spanien, Kroatien, Estland das Notifizierungsverfahren (fast) abgeschlossen. Weitere Mitgliedstaaten haben den Prozess gestartet.

Betrachtet man bereits existierende Identifizierungssysteme verschiedener EU-Staaten[38], so findet man häufig zertifikatsbasierte Lösungen auf Smartcards und zunehmend auch eIDs auf mobilen Geräten. In Verbindung mit den eIDs werden häufig staatliche Portale für den Zugang zu verschiedenen Onlinediensten der Verwaltung unterstützt. Einige Beispiele werden im Folgenden beschrieben.

5.2 Estland

Der estnische Personalausweis[39] dient der physischen Identifikation und besitzt zusätzlich elektronische Funktionen für die Authentifizierung und digitale Signatur. Auf dem Chip sind persönliche Daten sowie X.509-Zertifikate[40] für die Authentifizierung und qualifizierte

36 What is eID?, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+eID

37 Bundesamt für Sicherheit in der Informationstechnik (BSI): eIDAS-Notifizierung der Online Ausweisfunktion, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/Online-Ausweisfunktion/eIDAS-Notifizierung/eIDAS-Notifikation_node.html

38 Joinup, Digital Government Factsheets and Infographics 2018 [der EU-Länder], https://joinup.ec.europa.eu/page/egovernment-factsheets#eGov2017

39 Estonia eID, A Short Introduction to eID, https://eid.eesti.ee/index.php/A_Short_Introduction_to_eID

40 Eine in 2017 gefundene Sicherheitslücke basierte darauf, dass die Zertifikate fehlerhafte RSA-Schlüssel verwenden. Die Zertifikate wurden im November 2017 zurückgezogen und somit ca. 750.000 e-ID-Karten blockiert. Vgl. Estland: Sicherheitslücke in fast 750.000 ID-Cards, https://heise.de/-3822597.

elektronische Signatur sowie die zugehörigen privaten Schlüssel gespeichert.[41] Die Zertifikate enthalten den Namen und die nationale ID-Kennung und sind 5 Jahre gültig. Das Authentifizierungszertifikat enthält eine staatlich vergebene E-Mail-Adresse (Vorname.Nachname@eesti.ee) für die Kommunikation mit der Verwaltung. Die Nutzung der elektronischen Funktionen erfolgt mit PINs.

Die gleichen elektronischen Funktionen bietet die sogenannte Digi-ID.[42] Diese Smartcard dient allerdings nicht als Sichtausweis und enthält keine persönlichen Daten.

Auf Smartphones kann eine mobile ID (Mobiil-ID) für die Authentifizierung und Signatur verwendet werden. Die Beantragung erfolgt bei den Mobilfunkanbietern, die dann eine spezifische SIM-Karte zur Verfügung stellen.

Estland ist digitalpolitisch sehr fortschrittlich. Einer der wesentlichen Erfolgsfaktoren der elektronischen ID-Lösung ist ihre Vielseitigkeit. Estnische IDs können sowohl für staatliche als auch private Dienste eingesetzt werden. Unter anderem können die elektronischen IDs für E-Tickets, Zugang zur Patientenakte, E-Voting, E-Banking oder die Unternehmensgründung genutzt werden.

Estland hatte 2017 1.315.635 Einwohner.[43] Die Anzahl[44] aktiver ID-Karten wird mit 1.299.804 und aktiver Mobiil-IDs mit 159.903 angegeben. Im Dezember 2017 wurden mit elektronischen IDs 20.668.629 Transaktionen getätigt.

Kommunikation mit öffentlichen Stellen im Jahr 2017	**Prozent der Personen Estland (Deutschland)**
Interaktion mit staatlichen Behörden	78 (53)
Informationsbeschaffung auf Websites öffentlicher Stellen	65 (52)
Herunterladen amtlicher Formulare	40 (34)
Übermittlung ausgefüllter Formulare	70 (18)

Tabelle 2: Übersicht elektronische Kommunikation Bürger / Verwaltung Estland[45]

41 ID-card documentation, https://www.id.ee/index.php?id=35772.

42 What is Digi-ID?, https://www.id.ee/index.php?id=34410

43 Statistische Datenbank Estland, http://andmebaas.stat.ee/Index.aspx?lang=en

44 Tagesaktuelle Statistik (3.1.2018) https://www.id.ee/

45 Eurostat, Einzelpersonen, die das Internet zur Kommunikation mit öffentlichen Stellen nutzen, http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15ei&lang=de

Über das zentrale Onlineportal (eesti.ee) können persönliche Daten geprüft und die verschiedenen Dienste genutzt werden. Hier kann auch die Historie der durchgeführten Authentifizierungs- und Signaturvorgänge eingesehen werden.

5.3 Österreich

Die österreichische Bürgerkarte[46] ist ein funktionales Konzept, das verschiedene Trägermedien für die elektronische Identifikation unterstützt. Derzeit sind zwei Lösungen verfügbar: Signaturkarten (beispielsweise die Krankenkassen-Chipkarte e-Card) oder das Mobiltelefon für die sogenannte Handy-Signatur.

Bei der Aktivierung der Bürgerkartenfunktion[47] auf der e-card wird auf dem Chip ein qualifiziertes Zertifikat und die Personenbindung gespeichert. Das Zertifikat enthält Titel, Vorname, Nachname und die E-Mail-Adresse (auf Wunsch). Die Personenbindung enthält Vorname(n), Nachname, Geburtsdatum und Stammzahl.[48] Die Personenbindung dient dazu, eine Verbindung zwischen dem qualifizierten Zertifikat der Person und ihrer Stammzahl herzustellen, damit Verwechslungen bei gleichem Namen im Zertifikat vermieden werden. Damit die Bürgerkarte als Chipkarte verwendet werden kann, muss ein Kartenleser und eine Bürgerkartensoftware eingesetzt werden.

Bei der Handy-Signatur ist kein Kartenleser notwendig. Die Handy-Signaturfunktioniert analog zu den aus dem Onlinebanking bekannten mTAN-Lösungen: Der Nutzer identifiziert sich mit seiner österreichischen Handynummer und einem Signatur-Passwort auf der Behörden-Website und erhält einen Code per SMS zugesandt, den er auf der Website eingeben muss. Damit wird die elektronische Signatur im Hochsicherheits-Server der A-Trust[49] ausgelöst. Bei der Handy-Signatur wird die Personenbindung auf dem Hochsicherheits-Server der A-Trust gespeichert. Seit 2016 kann die Handy-Signatur auch mit einer App genutzt werden. Dabei wird die TAN direkt in die App übermittelt.

Derzeit sind ca. 850.000 Handy-Signaturen aktiviert. Jede/r dritte Österreicherin und Österreicher mit Internetanschluss ist im Besitz einer Handy-Signatur-Funktion oder einer Karte mit aktivierter Bürgerkartenfunktion.[50] Haupteinsatzgebiete sind die Finanzverwaltung über das Portal FinanzOnline und die Nutzung für Auszüge aus der Sozialversicherung. Seit 2016 sind die Gebühren für diverse Anträge um 40 Prozent günstiger, wenn der Antrag mit der Bürgerkarte oder der Handy-Signatur eingebracht wird.

46 Website Bürgerkarte, http://www.buergerkarte.at/ und Das österreichische E-Government-ABC, https://www.digitales.oesterreich.gv.at/das-e-government-abc

47 Häufige Fragen zur Bürgerkarte, https://www.buergerkarte.at/faq-karte.html

48 Jeder in Österreich gemeldete Bürger ist durch eine Zahl aus dem Zentralen Melderegister (Melderegisterzahl bzw. ZMR-Zahl) eindeutig identifizierbar. Auf der Bürgerkarte wird die ZMR nicht gespeichert, sondern kryptografisch wird eine Stammzahl berechnet. Aus der Stammzahl kann man die ZMR nicht wiederherstellen. Aus Datenschutzgründen wird auch die Stammzahl bei Nutzung der Bürgerkarten nicht direkt verwendet, sondern kryptografisch in sogenannte bereichsspezifische Personenkennzeichen (bPK) für unterschiedliche Verwaltungsbereiche umgewandelt. (https://www.buergerkarte.at/sicherheit-datenschutz.html)

49 A-Trust: qualifizierter Vertrauensdienstanbieter für elektronische Zertifikate, https://www.a-trust.at

50 Initiative D21, fortiss (Hrsg.): eGovernment Monitor 2017. Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich, Oktober 2017, http://www.egovernment-monitor.de/die-studie/2017.html

Kommunikation mit öffentlichen Stellen im Jahr 2017	Prozent der Personen Österreich (Deutschland)
Interaktion mit staatlichen Behörden	62 (53)
Informationsbeschaffung auf Websites öffentlicher Stellen	50 (52)
Herunterladen amtlicher Formulare	38 (34)
Übermittlung ausgefüllter Formulare	37 (18)

Tabelle 3: Übersicht elektronische Kommunikation Bürger / Verwaltung Österreich[51]

Einen Durchbruch hat die österreichische Lösung mit der Handy-Signatur erreicht. Nachdem auf zusätzliche Hardware wie Kartenlesegeräte verzichtet wurde, sind die Nutzungszahlen signifikant angestiegen. Ein weiterer Erfolgsfaktor sind zusätzlich geschaffene Anreize wie Gebührensenkung oder schnellere Verfahrensabwicklung.

5.4 Großbritannien

GOV.UK Verify[52] dient dem Online-Identitätsnachweis von Personen für E-Government-Dienste. Bei der Erstregistrierung wird ein Nutzerkonto bei einem zertifizierten Identitätsdienstleister eingerichtet. Solche Identitätsdienstleister sind etwa Banken, die Post oder klassische Identity-Provider. Die Identitätsdaten werden dabei durch den Identitätsdienstleister bestätigt, er definiert auch, welche Nachweise vom Nutzer zur Identitätsfeststellung erbracht werden müssen. Nach der Erstregistrierung kann man sich auf dem Portal GOV.UK beispielsweise mit Nutzername / Passwort authentifizieren. Das Nutzerkonto fungiert als Single Sign-on (Nutzer müssen sich nur einmal authentifizieren und können anschließend viele Dienste nutzen) für unterschiedliche staatliche Dienstleistungen.[53]

Technisch basiert die Lösung auf OIX[54] (Open Identity Exchange). OIX legt Regeln fest, um eine sichere Identifizierung von Personen zu ermöglichen. Die eigentliche Identifizierung erfolgt durch den Identitätsdienstleister, basierend auf dem OIX-Katalog.

51 Eurostat, http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15ei&lang=de

52 GOV.UK ist das zentrale Online-Portal für E-Government im Vereinigten Königreich. GOV.UK Verify, https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

53 Übersicht über Dienstleistungen, die GOV.UK Verify nutzen: https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify#government-services

54 OIX ist eine gemeinnützige Organisation, www.openidentityexchange.org

Kommunikation mit öffentlichen Stellen im Jahr 2017	Prozent der Personen Großbritannien (Deutschland)
Interaktion mit staatlichen Behörden	49 (53)
Informationsbeschaffung auf Websites öffentlicher Stellen	35 (52)
Herunterladen amtlicher Formulare	25 (34)
Übermittlung ausgefüllter Formulare	35 (18)

Tabelle 4: Übersicht elektronische Kommunikation Bürger / Verwaltung Großbritannien[55]

6 TECHNISCHE LÖSUNGEN UND INITIATIVEN DER WIRTSCHAFT

Parallel zu den staatlich entwickelten Lösungen entsteht eine Reihe von eID-Lösungen in der Wirtschaft. Zum Einsatz kommen offene Standards, wie zum Beispiel OpenID oder OAuth, genauso wie proprietäre Lösungen. In den letzten Jahren wurden eine Reihe privatwirtschaftlicher Initiativen gestartet, die teilweise von großen Industriekonsortien getragen werden. Diese Entwicklung unterstreicht die zunehmende Bedeutung des Themas.[56]

Ziel der meisten Initiativen, neben einem Single Sign-on, ist in der Regel, eine Alternative zu den als unsicher einzustufenden Nutzername-Passwort-Identifizierungs-/Authentifizierungs-Verfahren bereitzustellen. Immer häufiger setzt sich die 2-Faktor-Authentifizierung als Mittel durch, wie etwa FIDO zeigt. Aufgrund der Komplexität und hohen Sicherheitsanforderungen werden die Standards in der Regel von größeren Verbünden entwickelt, die dann über die gemeinsame Marktmacht eine kritische Zahl von Nutzern erschließen wollen.

Vor dem Hintergrund der Europäischen Datenschutzgrundverordnung (EU-DSGVO) und der angekündigten ePrivacy-Verordnung müssen Unternehmen, die mit Kundendaten agieren, zukünftig europaweit einheitliche Regeln für den

55 Eurostat, http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15ei&lang=de

56 Vgl. auch Thilo Ernst, Nadja Menz, Jaroslav Svacina, Christian Welzel, Johannes Wolf: Sichere Mobile Authentifizierung, Kompetenzzentrum Öffentliche IT, April 2019, https://www.oeffentliche-it.de/documents/10181/14412/Sichere+Mobile+Authentifizierung.

Umgang mit personenbezogenen Daten einhalten. Auch in Deutschland haben sich mehrere Industriekonsortien gebildet, die sich jeweils mit einem eigenen Identitätsmanagementdienst etablieren wollen.

Zu beachten ist, dass für keinen der Anbieter (Ziffern 6.4 bis 6.8) bisher geklärt ist, welche Vertrauensniveaus nach BSI TR-03107 über den jeweiligen Identitätsmanagementdienst abgedeckt werden.

6.1 OpenID & OAuth

Bereits seit 2005 steht mit OpenID[57] ein dezentrales Identifizierungs- und Authentifizierungssystem für Onlinedienste zur Verfügung. OpenID ist ein Identitätsmanagementsystem, das auf URLs basiert. Nutzer melden sich zunächst bei einem OpenID-Anbieter (auch Provider genannt) an. Dieser stellt für den Nutzer eine URL zur Verfügung, die als eindeutiger Identifizierer (Unique Identifier) fungiert. Mit dieser URL kann sich der Nutzer nun bei anderen Diensten (Relying Parties) anmelden, ohne einen Nutzernamen oder ein Passwort verwenden zu müssen. Auf diese Weise kann ein Single Sign-on realisiert werden. Da das OpenID-Protokoll offen und frei nutzbar ist, existieren mittlerweile zahlreiche Implementierungen.

Die Identitätsdaten liegen jedoch nicht direkt bei den Nutzern, sondern beim OpenID-Anbieter, der als vertrauenswürdiger Dritter (Trusted Third Party) agiert. Zu den bekannten OpenID-Providern zählen unter anderem Yahoo, Google, IBM oder Microsoft, die jeweils OpenID als optionalen Zusatzdienst anbieten. Jede Anmeldung bei einer Relying Party bzw. Nutzung der OpenID erfordert die Einbeziehung des OpenID-Anbieters. Das System ist Multi-Provider-fähig, sodass prinzipiell jeder als OpenID-Anbieter auftreten kann. Neben den genannten Anbietern gibt es daher auch zahlreiche kleinere Onlinedienste, die eine OpenID-Identität für ihre Nutzer anbieten. OpenID-Identitäten werden zudem von vielen Open-Source-Softwarelösungen als alternativer Registrierungs- und Login-Mechanismus unterstützt.

Aus Nutzersicht bietet der Ansatz diverse Vorteile. So wird die Authentifizierung bei einem Dienst reduziert auf die Eingabe der OpenID-URL. Weitere personenbezogene Daten müssen nicht eingegeben werden. Außerdem kann der Nutzer seine Daten an einer zentralen Stelle pflegen, nämlich beim OpenID-Anbieter. Der Nutzer entscheidet dann selbst, welche Daten der OpenID-Anbieter an die Relying Parties weitergeben soll. Jedoch hat sich der Ansatz in der Breite bei den Nutzern nicht durchgesetzt.

Nach einigen Sicherheitslücken wurde 2007 OpenID 2.0 entwickelt, das heute noch aktuell ist. Der Ansatz ist allerdings anfällig für Phishing-Angriffe, zum Beispiel durch gefälschte OpenID-Anbieter-Seiten. Seit 2007 wird OpenID durch die eigenen Stiftungen OpenID Foundation und OpenID Europe Foundation gefördert.

Während OpenID ein Ansatz zur Identifizierung und Authentifizierung der Nutzer ist, ermöglicht OAuth[58] die Autorisierung von Onlinediensten. OAuth ist ebenfalls ein technisches Protokoll, das offen, frei nutzbar und standardisiert ist. Mit OAuth kann ein Nutzer anderen Anwendungen Zugriff auf seine Daten bei einem Onlinedienst gewähren, ohne dabei seine Zugangsdaten preisgeben zu müssen. Zum Einsatz kommt das Protokoll beispielsweise, um einer App Zugang zu einem Social Media Account gewähren zu können, etwa um aus der App heraus automatisch Beiträge erstellen zu lassen oder Freundeslisten in die App zu integrieren. OAuth ist API-basiert und richtet sich primär an Entwickler von Onlinediensten und Apps. Die Autorisierung erfolgt über

57 Vgl. https://openid.net/

58 Vgl. https://oauth.net/

Access Token, die vom Onlinedienst generiert werden. Das Protokoll ermöglicht über den sogenannten Scope eine feingranulare Vergabe von Zugriffsrechten. So ist es möglich, zum Beispiel nur lesenden Zugriff zu gewähren oder den Zugriff nur für bestimmte Bereiche freizugeben. In der Verknüpfung mit OpenID Connect ist es zusätzlich möglich, die Identität des Nutzers zu überprüfen.

OAuth wurde 2007 erstmals veröffentlicht und 2012 auf die Version OAuth 2.0 aktualisiert. Kritisiert wird, dass das Protokoll eine hohe Komplexität mit sich bringt, was zu Fehlern bei der Entwicklung führen und damit potenziell Sicherheitsprobleme verursachen kann. Wird es korrekt eingesetzt, ermöglicht es jedoch eine sichere Verknüpfung unterschiedlicher Onlinedienste. Heute kommt das Protokoll bei vielen Webdiensten und mobilen Anwendungen zum Einsatz, viele Soziale Netzwerke bieten basierend auf dem OAuth-Konzept eigene Lösungen an.

Auch in Deutschland gab es immer wieder Überlegungen, OpenID-basierte-Lösungen für die Verwaltung einzusetzen. Es gab Forschungsprojekte, um OpenID mit der Online-Ausweisfunktion des Personalausweises zu verknüpfen[59], die oftmals jedoch nicht über den Status von Prototypen hinausgekommen sind, was eher organisatorisch und rechtlich denn technisch begründet ist.

6.2 Video-Ident

Das Video-Ident-Verfahren (Video-Identifikation) ist eine Lösung für die Erst-Identifizierung bei Onlineverfahren.[60] Dabei wird über einen Video-Chat eine Fernüberprüfung der Identität eines Nutzers vorgenommen. Dieser muss in der Regel ein Identifikationsmittel (zum Beispiel Personalausweis oder Reisepass) im Rahmen eines Video-Chats präsentieren. Ein Mitarbeiter des Anbieters überprüft über das Videobild die Echtheit und Plausibilität des Identifikationsmittels. Verschiedene Absicherungsmechanismen sollen verhindern, dass ein aufgezeichnetes Video oder ein gefälschtes Identifikationsmittel präsentiert werden. Einzige Voraussetzung auf Nutzerseite ist ein Gerät mit Videokamera, was heutzutage nahezu alle Laptops, Smartphones und Tablets mitbringen. Zur Klärung der Rechtmäßigkeit in Deutschland hat im Jahr 2014 eine Neuauslegung des Geldwäschegesetzes durch das Bundesfinanzministerium (BMF) beigetragen, indem das Video-Ident-Verfahren für die Kontoeröffnung ermöglicht wurde. In einer überarbeiteten und angepassten Version des ursprünglichen Rundschreibens des BMF wurde nach erneuter Prüfung und Bewertung – wegen der unstrittigen Sicherheitsrisiken – Mindestkriterien an die Verfahren formuliert.

6.3 Social Logins

Social Logins sind eine Form der Authentifizierung, die sich in den letzten Jahren stark verbreitet hat. Dabei werden Nutzerkonten von Sozialen Netzwerken genutzt, um sich bei Drittanbietern anzumelden. Die Anbieter der Sozialen Netzwerke stellen dafür eine eigene – in der Regel proprietäre – Schnittstelle (API) zur Verfügung. Beispiele sind Facebook, Twitter, Google+ oder LinkedIn. Auf der Drittanbieter-Seite kann dabei auf die Einrichtung eines separaten Nutzerkontos verzichtet werden, womit für die Nutzer ein Single Sign-on realisiert werden kann. Drittanbieter nutzen dazu in der Regel ein Plugin oder Widget[61], das vom Betreiber des Sozialen Netzwerks angeboten wird. Die Nutzer melden sich mit ihren

59 Vgl. zum Beispiel http://www.eid-connect.de/

60 Aus einem Video-Ident-Verfahren resultiert nicht zwangsläufig eine elektronische Identität. Das Verfahren erlangt jedoch zunehmende Relevanz für die Erstregistrierung und wird deshalb hier explizit erwähnt.

61 Plugin, Widget: Ein Quellcode-Schnipsel, den Entwickler und Webseitenbetreiber in ihre Anwendung übernehmen.

Zugangsdaten bei dem Sozialen Netzwerk an, welches dann die Informationen an den Drittanbieter weiterleitet. Social Logins fungieren sowohl zur Authentifizierung als auch zur Autorisierung. Als technische Basis kommen dabei unter anderem OpenID oder OAuth zum Einsatz. Teilweise werden diese aber um proprietäre Erweiterungen ergänzt.

Der mit Abstand am häufigsten verwendete Social-Login-Mechanismus ist Facebook-Connect, mit dem Nutzer sich mit ihrer Facebook-ID bei anderen Onlinediensten anmelden können. Die Lösung ähnelt dem OpenID- und OAuth-Ansatz, enthält jedoch zusätzliche Funktionen. So können etwa nach Zustimmung des Nutzers weitere Daten aus dem Facebook-Profil des Nutzers an den anfragenden Dienst übermittelt werden. Außerdem können mit Zustimmung des Nutzers Informationen durch den Drittanbieter-Dienst zum Profil des Nutzers hinzugefügt werden.

Im Wesentlichen sind zwei Faktoren für den Erfolg von Social Logins entscheidend. Aus Nutzersicht lässt sich mit Social Logins ein Single Sign-on realisieren: Nutzer müssen nicht mehr viele unterschiedliche Zugänge verwalten. Der Vorteil für die Drittanbieter liegt darin, verlässlichere Daten sowie tendenziell mehr demografische Daten über ihre Nutzer zu erhalten. Die Betreiber der Sozialen Netzwerke wiederum schaffen durch Social Logins eine engere Bindung der Nutzer an ihren Dienst. Außerdem erhalten sie auf diesem Weg zusätzliche Informationen zu den Nutzungsgewohnheiten ihrer Nutzer bezüglich anderer Dienste, zum Beispiel wo und wie oft sich ein Nutzer bei einem bestimmten anderen Dienst anmeldet.

Social Logins sind weit verbreitet und bieten prinzipiell eine niedrigschwellige Form der Registrierung und Wiederanmeldung. Sie sind theoretisch für Dienste mit niedrigem Vertrauensniveau geeignet. Allerdings sind Social Logins unter Datenschutzaspekten und unter Aspekten der Datensouveränität ausgesprochen kritisch zu bewerten. Außerdem steht diese Form der Authentifizierung ausschließlich den Nutzern zur Verfügung, die einen Account bei dem betreffenden Sozialen Netzwerk besitzen. Von einem Einsatz in der Verwaltung wird daher abgeraten.

6.4 FIDO Alliance

Eine der größten privatwirtschaftlichen Initiativen ist die FIDO Alliance. In der 2013 gegründeten Allianz haben sich mittlerweile mehr als 250 Organisationen zusammengeschlossen, um technische Standards für eine sichere Identifizierung und Authentifizierung zu erarbeiten. Im Mittelpunkt steht dabei eine 2-Faktor-Authentifizierung, wobei unterschiedliche Token kombiniert werden können. Standardisiert wird dabei ein sogenannter universeller zweiter Faktor (Universal Second Factor U2F). Das kann beispielsweise eine PIN, ein Passwort oder ein Einmal-Token sein, ein biometrisches Merkmal (zum Beispiel Fingerabdrücke, Stimme, Iris-Scan, Gesicht) oder ein physisches Token zum Beispiel in Form eines USB-Sticks.

Die Lösung basiert auf kryptografischen Public-Key-Verfahren, wobei die privaten Schlüssel immer auf dem Gerät des Nutzers verbleiben. Besonderer Wert wurde bei der Entwicklung auf eine möglichst einfach und intuitiv bedienbare Benutzerschnittstelle, den Schutz der Privatsphäre sowie die Standardisierung gelegt. Entstanden ist der offene FIDO-Standard, der das Authentifizierungsprotokoll zwischen Client und Onlineservice beschreibt und für den es mittlerweile mehr als 300 zertifizierte Lösungen gibt.

Zu den teilnehmenden Organisationen gehören viele namhafte Unternehmen, unter anderem Google, Microsoft, Amazon, Alibaba Group, Mastercard, American Express, Visa, ARM, Intel, Infineon, Gemalto, RSA oder PayPal. Allein aufgrund der hinter diesen Unternehmen stehenden Marktmacht kann man davon ausgehen, dass FIDO in Zukunft eine bedeutende Rolle bei Online-Authentifizierungen einnehmen wird. Seit 2015 ist das BSI ebenfalls Teil

der FIDO Alliance, um den neuen Personalausweis mit FIDO zu verknüpfen.[62] Das BSI arbeitet an Sicherheitsanforderungen mit. Angeschlossen hat sich auch das Trust-Center der Bundesdruckerei (D-TRUST).

6.5 Verimi

Verimi entwickelt eine Plattform für digitale Identitäten und Payment. Gesellschafter des Konsortiums sind unter anderem Allianz, Axel Springer, Bundesdruckerei, Core, Daimler, Deutsche Bahn, Deutsche Bank und Postbank, Deutsche Telekom, Giesecke+Devrient, Here Technologies, Lufthansa, Samsung Electronics und Volkswagen Financial Services.[63] Bei weiteren Partnern kann man sich inzwischen mit Verimi einloggen. Die Plattform fungiert als Identitätsanbieter im Sinne eines vertrauenswürdigen Dritten (Trusted Third Party). Schrittweise sind weitere Funktionen geplant, unter anderem eine qualifizierte elektronische Signatur nach eIDAS, Bezahlmöglichkeiten sowie ein Dokumentenspeicher zur Archivierung sensibler Dokumente.

Anfang 2019 hat die BaFin Verimi die Erlaubnis erteilt, Dienstleistungen als Zahlungsinstitut nach dem Zahlungsdiensteaufsichtsgesetz (ZAG) zu erbringen. Auf dieser Basis können Nutzer ihre bei einer Bank hinterlegte Identität in die Verimi-Plattform übertragen. Verimi kann durch die ZAG-Lizenz bestehende GwG-konforme Identitäten von Bankkunden annehmen, speichern und weitergeben. So hat der Bankkunde und Verimi-Nutzer die Möglichkeit, seine bereits geprüfte Identität in die Verimi-Plattform zu übertragen oder sich bei Verimi nach dem deutschen Geldwäschegesetz (GwG) zu legitimieren.

Technisch basiert die Plattform auf den Standards OAuth 2.0 und OpenID Connect. Für Dritte wird eine offene API zur Verfügung gestellt, die allerdings erst genutzt werden kann, wenn eine vertragliche Beziehung mit Verimi besteht. Die API soll schrittweise erweitert werden und enthält zu Beginn die Funktionalitäten für Login und den Austausch von kundenspezifischen Daten sowie eine Bezahlfunktion.

Die Verimi-Plattform erzeugt auf Basis unterschiedlicher Quellen (zum Beispiel Reisepässe, Personalausweise oder Führerscheine) mit Hilfe eines WebID-Videochecks eine abgeleitete Identität, die auf einem – nach Angaben der Plattformbetreiber – „anerkannten" Vertrauensniveau basiert. Verimi soll zukünftig zudem eine 2-Faktor-Authentifizierung unterstützen. Die Plattform richtet sich an Bürger, Unternehmen und Verwaltung.

Verimi fungiert als zentraler Identitätsprovider. Dies hat zur Folge, dass jegliche Identifizierungs- und ggf. auch Authentifizierungsvorgänge der Nutzer Verimi bekannt werden. Verimi speichert die Daten, die ein Nutzer hinterlegt. Der Nutzer gibt sie – je nach Onlineanwendung – für die jeweilige Nutzung frei. Kritisiert wird u.a., dass damit eine sehr umfangreiche Datensammlung in einer Hand entsteht.[64] Denn auf diese Weise ist es möglich, detaillierte Nutzerprofile darüber anzulegen, wann welcher Nutzer sich bei welchem Dienst identifiziert oder gar authentifiziert.

Der Freistaat Thüringen nutzt als erstes Bundesland den Verimi-Log-in für das neu entstehende E-Government-Portal Thüringens. Im Januar 2019 unterzeichneten Verimi und das Thüringer Finanzministerium die Verträge. Auch das Land NRW sowie der Bund führen Gespräche mit Verimi, allerdings bisher ohne

62 Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI): Certification Report, https://www.commoncriteriaportal.org/files/ppfiles/pp0096a_pdf.pdf

63 Vgl. https://verimi.de/de/ueber-uns

64 Vgl. z.B. Marie Bröckling, Eine Identität für alles: Das schwierige Geschäftsmodell von Verimi, 18.12.2018, https://netzpolitik.org/2018/eine-identitaet-fuer-alles-das-schwierige-geschaeftsmodell-von-verimi/.

Ergebnisse. Da Verimi für die Nutzung seiner Angebote Entgelte pro Authentifizierung verlangt, zudem bisher unklar ist, welche Vertrauensniveaus mit dem Verimi-Angebot abgedeckt sind, bleibt die weitere Entwicklung abzuwarten.

6.6 netID

Einen ähnlichen Ansatz verfolgt EnID. Die Stiftung European netID Foundation (EnID) wurde im März 2018 von der Mediengruppe RTL Deutschland, ProSiebenSat.1 und United Internet gegründet. Die Stiftung entwickelt netID und überprüft alle Standards, Partner und Account-Anbieter innerhalb der Initiative. „Sie verfolgt das Ziel, mit der netID als Single Sign-on eine europäische Alternative zu den US-Anbietern zu etablieren. Mit der netID können Nutzer ihre Einwilligung zur Nutzung von Internet-Diensten (Opt-ins) datenschutzkonform und transparent in einem sogenannten Privacy Center organisieren. Dazu hat die Stiftung einen offenen Standard entwickelt, der es Nutzern branchenübergreifend ermöglicht, auf alle Internet-Angebote der Partner der European netID Foundation mit denselben Log-in-Daten zuzugreifen."[65]

Mit der persönlichen netID kann man sich bei den netID-Partnern einloggen und einen Überblick über die eigenen Daten erhalten. Dafür kann der Nutzer ein bestehendes Login bei einem netID Account-Anbieter nutzen oder einen separaten netID Account (Kombination aus E-Mail-Adresse und Passwort) anlegen. Dieser Zugang erreicht damit das Niveau niedrig/normal.

Als Partner sind bereits eine Reihe von namhaften Unternehmen im Wesentlichen aus dem E-Commerce-Bereich gelistet.[66]

Nach eigenen Angaben erreicht die Stiftung über ihre Mitglieder etwa 35 Millionen Benutzer.

Analog zu Verimi fungiert auch netID als zentraler Identitätsprovider, mit der Folge, dass detaillierte Nutzerprofile über die Dienstnutzung angelegt werden können.

6.7 Mobile Connect

Aus dem Mobilfunk-Bereich ist die Lösung Mobile Connect entstanden. Sie wurde von der GSMA (Global System for Mobile Communications Association), einer Industrievereinigung der weltweiten Mobilfunkanbieter, entwickelt.[67]

Bei Mobile Connect treten die Mobilfunkanbieter als vertrauenswürdige dritte Instanz (Trusted Third Party) auf. Nutzer müssen sich zunächst für Mobile Connect registrieren. Möchte sich ein Nutzer anschließend bei einem Onlinedienst anmelden, übermittelt er dem Onlinedienst dazu seine Mobilfunknummer. Über Mobile Connect kontaktiert der Onlinedienst den Mobilfunkanbieter. Anschließend erhält der Nutzer eine Nachricht auf seinem Mobiltelefon, mit einem Verifikationslink, über den der Nutzer die Anmeldung bestätigt. Je nach Schutzbedarf kann auch zusätzlich die Eingabe einer PIN verlangt werden. Im Anschluss bestätigt der Mobilfunkanbieter die Identität des Nutzers gegenüber dem Onlinedienst. Darüber hinaus können Nutzer ihren Mobilfunkanbieter anweisen, weitere Daten zu übermitteln (zum Beispiel Name, Anschrift oder Kontodaten), wobei die Nutzer die Hoheit darüber haben, wem sie welche Daten zur Verfügung stellen.

Mobile Connect wird weltweit in ca. 30 Ländern eingesetzt. Im Februar 2018 haben die drei führenden Mobilfunkanbieter in Deutschland (Vodafone, Deutsche Telekom und Telefónica) angekündigt, den

65 https://enid.foundation/stiftung/.

66 Vgl. https://netid.de/#netid-standard

67 https://www.gsma.com/identity/mobile-connect

Dienst auch hierzulande einzuführen.[68] Verimi hat angekündigt, dieses Identifikationsverfahren ebenfalls zu unterstützen. Da Mobilfunkanbieter verpflichtet sind, die Identität ihrer Kunden eindeutig festzustellen, kann bei den Identitätsdaten von einer hohen Qualität ausgegangen werden. Mit diesem Ansatz erweitern die Mobilfunkbetreiber ihr Geschäftsmodell und positionieren sich damit als Identitätsanbieter.

Ist das Verfahren in Deutschland etabliert, kann es auch für die öffentliche Verwaltung ein interessantes Identifikations- und Authentifizierungsmittel darstellen, nicht zuletzt aufgrund einer großen Nutzerabdeckung mit Mobilgeräten. Auch bei diesem Ansatz fungieren die Netzbetreiber als zentrale Identitätsprovider, die dadurch detaillierte Informationen über die Dienstnutzung ihrer Nutzer erhalten.

6.8 YES

Die Identitätsplattform YES soll 2019 starten. Anbieter sind die Sparkassen-Finanzgruppe sowie die Volks- und Raiffeisenbanken. Kunden brauchen keine zusätzliche Anmeldung, um den Dienst zu nutzen, sondern verwenden ihr bestehendes Online Banking Login bei einer der teilnehmenden Banken. Dabei wird die Identität des Kunden von der Sparkasse oder Volksbank auf Basis des Online-Banking-Logins gegenüber Unternehmen und Dienstleistern bestätigt. Dazu bindet die Fiducia & GAD IT AG, Dienstleister für Informationstechnologie der genossenschaftlichen FinanzGruppe den Identitätsdienst CAS (Central Authentication Services) der Genossenschaftsbanken an. Technologisch basiert YES auf OpenID und OAuth.

"Der Dienst übernimmt [...] die Rolle eines Vermittlers und sorgt dafür, dass die Identität eines Kunden auf dessen Wunsch von einer Sparkasse oder einer Genossenschaftsbank gegenüber einem anderen Unternehmen bestätigt wird [...] Statt sich per Post- oder Video-Ident auszuweisen, sollen Nutzer auf einen Yes-Button klicken. Das Login erfolgt über die Zugangsdaten für das Online-Banking. Eine zusätzliche Anmeldung ist nicht erforderlich. Yes fokussiert sich aktuell auf die Identifizierung der Nutzer und wirbt damit, dass es selbst keine Daten speichert. Es stelle nur eine einheitliche Infrastruktur für Banken bereit."[69]

Auch dieses Verfahren kann für die öffentliche Verwaltung ein interessantes Identifikations- und Authentifizierungsmittel darstellen, nicht zuletzt aufgrund der zahlreichen Online Banking-Nutzer der Sparkassen und Volksbanken.

68 Vgl. Alexander Geckeler, Deutsche Telekom, Telefónica und Vodafone führen sichere und einfache Nutzer-Identifikation per Mobilfunknummer ein, 08.02.2018, https://blog.telefonica.de/2018/02/mobile-connect-deutsche-telekom-telefonica-und-vodafone-fuehren-sichere-und-einfache-nutzer-identifikation-per-mobilfunknummer-ein/

69 Elisabeth Atzler, Katharina Schneider, Genossenschaftsbanken und Sparkassen investieren in Identitätsdienst „Yes", 18.12.2018, https://www.handelsblatt.com/finanzen/banken-versicherungen/online-login-genossenschaftsbanken-und-sparkassen-investieren-in-identitaetsdienst-yes-/23769102.html?ticket=ST-4021257-Nof4d7fFDRZDxJJAbkbv-ap1.

QUELLEN- UND LITERATURVERZEICHNIS

29. Sitzung des IT-Planungsrats vom 27. Juni 2019. Entscheidung 2019/22 - Unternehmenskont/-en, https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2019/Sitzung_29.html?pos=4

Elisabeth Atzler, Katharina Schneider, Genossenschaftsbanken und Sparkassen investieren in Identitätsdienst „Yes“, 18.12.2018, https://www.handelsblatt.com/finanzen/banken-versicherungen/online-login-genossenschaftsbanken-und-sparkassen-investieren-in-identitaetsdienst-yes-/23769102.html?ticket=ST-4021257-Nof4d7fFDRZDxJJAbkbv-ap1

Aufruf: Bundesdruckerei und kommune.digital suchen Pilotanwender für sign-me, http://kommune.digital/sign-me/

Marie Bröckling, Eine Identität für alles: Das schwierige Geschäftmodell von Verimi, 18.12.2018, https://netzpolitik.org/2018/eine-identitaet-fuer-alles-das-schwierige-geschaeftsmodell-von-verimi/

Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-2. IT-Grundschutz-Vorgehensweise, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile

Bundesamt für Sicherheit in der Informationstechnik (BSI): Certification Report, https://www.commoncriteriaportal.org/files/ppfiles/pp0096a_pdf.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI): eIDAS-Notifizierung der Online Ausweisfunktion, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/Online-Ausweisfunktion/eIDAS-Notifizierung/eIDAS-Notifikation_node.html

Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government. Teil 1: Vertrauensniveaus und Mechanismen. Version 1.1 31.10.2016, https://www.bsi.bund.de/DE/Publikationen/ TechnischeRichtlinien/tr03107/index_htm.html

Bundesministerium des Innern, für Bau und Heimat: Vorschlag des Bundesministeriums des Innern, für Bau und Heimat zur Verbesserung des Identitätsmanagements als Teil der Registermodernisierung, Februar 2019, https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/20190614_12/anlage-zu-top-12.pdf?__blob=publicationFile&v=2

Das österreichische E-Government-ABC, https://www.digitales.oesterreich.gv.at/das-e-government-abc

Thilo Ernst, Nadja Menz, Jaroslav Svacina, Christian Welzel, Johannes Wolf: Sichere Mobile Authentifizierung, Kompetenzzentrum Öffentliche IT, April 2019, https://www.oeffentliche-it.de/documents/10181/14412/Sichere+Mobile+Authentifizierung

Estland: Sicherheitslücke in fast 750.000 ID-Cards, https://heise.de/-3822597

Estonia eID, A Short Introduction to eID, https://eid.eesti.ee/index.php/A_Short_Introduction_to_eID

EU-Verordnung Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910

Eurostat, Einzelpersonen, die das Internet zur Kommunikation mit öffentlichen Stellen nutzen, http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15ei&lang=de

Alexander Geckeler, Deutsche Telekom, Telefónica und Vodafone führen sichere und einfache Nutzer-Identifikation per Mobilfunknummer ein, 08.02.2018, https://blog.telefonica.de/2018/02/mobile-connect-deutsche-telekom-telefonica-und-vodafone-fuehren-sichere-und-einfache-nutzer-identifikation-per-mobilfunknummer-ein/

Gabriele Goldacker et al. 2019, No-Government, In: Jens Fromm und Mike Weber (Hrsg.), 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT, http://www.oeffentliche-it.de/-/no-government

Häufige Fragen zur Bürgerkarte, https://www.buergerkarte.at/faq-karte.html

ID-card documentation, https://www.id.ee/index.php?id=35772

Initiative D21, fortiss (Hrsg.): eGovernment Monitor 2017. Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich, Oktober 2017.

Initiative D21, fortiss (Hrsg.): eGovernment Monitor 2018. Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich, November 2018.

IT-Planungsrat: Interoperables Identitätsmanagement für Bürgerkonten – Studie – Stand: 6. Mai 2015, http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/eID/ Studie_Identitaetsmanagement_BK.pdf

Joinup, Digital Government Factsheets and Infographics 2018 [der EU-Länder], https://joinup.ec.europa.eu/page/egovernment-factsheets#eGov2017

KGSt / KoopAADV: Erfolgsfaktoren von E-Government. KGSt-Bericht 1/2006.

Kompetenzzentrum Öffentliche IT: Repräsentative Bevölkerungsumfrage „Vertrauen in die Digitale Verwaltung", durchgeführt im November & Dezember 2018. https://www.oeffentliche-it.de/umfragen?entry=vertrauen

Mario Martini, David Wagner, Michael Wenzel: Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, Version 1.0, Speyer 2017, Stand 17.09.2017.

Statistische Datenbank Estland, http://andmebaas.stat.ee/Index.aspx?lang=en

What is Digi-ID?, https://www.id.ee/index.php?id=34410

What is eID?, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+eID

IMPRESSUM

Die Kurzstudie basiert auf einer Initiative des Nationalen E-Government Kompetenzzentrum e. V.

Ansprechpartner

Christian Welzel
Kompetenzzentrum Öffentliche IT
christian.welzel@fokus.fraunhofer.de

Dr. Marianne Wulff
Dataport AöR
marianne.wulff@dataport.de

Nationales E-Government Kompetenzzentrum e. V.

Pressehaus / 4102
Schiffbauerdamm 40
10117 Berlin

+49 (0)30 80494747
info@negz.org
negz.org

Gestalterische Umsetzung
made in – Design & Strategieberatung
www.madein.io

BERICHTE DES NEGZ

Folgende Kurzstudien sind in der Reihe „Berichte des NEGZ“ bereits erschienen:

Nr. 1 Schuppan, T., Köhl, S., Off, T. (2018). Vollzugsorientierte Gesetzgebung durch eine Vollzugssimulationsmaschine, Berlin. » DOI

Nr. 2 Ogonek, N., Distel B., Ben Rehouma, M., Hofmann, S., Räckers, M. (2018). Digitalisierungsverständnis von Führungskräften, Berlin. » DOI

Nr. 3 Djeffal, C. (2018). Künstliche Intelligenz in der öffentlichen Verwaltung, Berlin. » DOI

Nr. 4 Fadavian, B., Franzen-Paustenbach, D., Rehfeld, D., Schmitt, M., Schweikart, D., Djeffal, C. (2019). Data Driven Government, Berlin. » DOI

Nr. 5 Balta, D., Hofmann, S., Kuhn, P., Krcmar, H., (2019). Sharing Economy: Potential im öffentlichen Sektor, Berlin. » DOI

Nationales E-Government Kompetenzzentrum e. V.
Pressehaus / 4102
Schiffbauerdamm 40
10117 Berlin

+49 (0)30 80494747
info@negz.org
negz.org

ISSN (online) 2626-6032
DOI 10.30418/2626-6032.2019.06