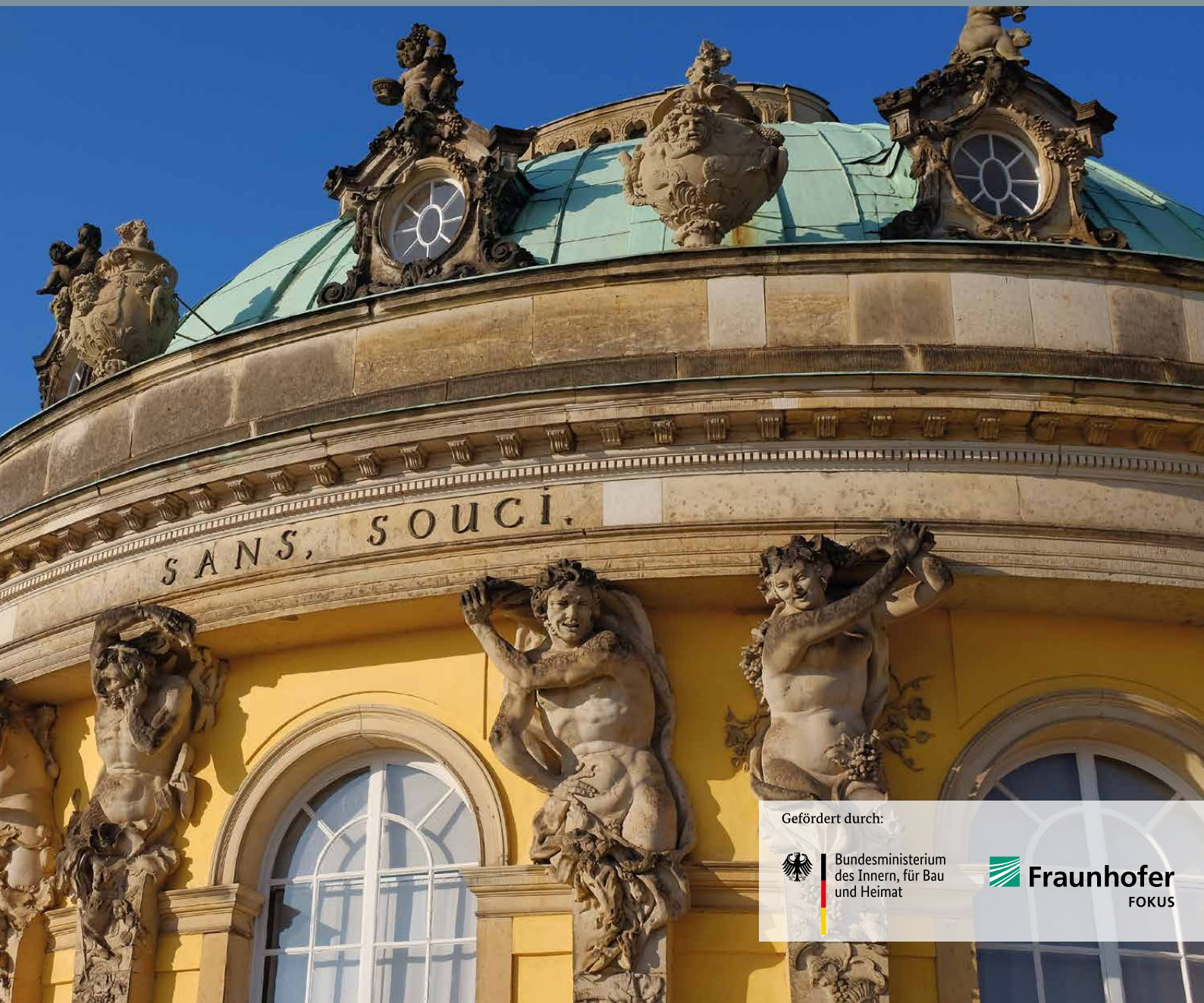
Kompetenzzentrum
Öffentliche IT

FORSCHUNG FÜR DEN DIGITALEN STAAT

SICHERE MOBILE AUTHENTIFIZIERUNG

Thilo Ernst, Nadja Menz, Jaroslav Svacina, Christian Welzel, Johannes Wolf



Gefördert durch:

Bundesministerium
des Innern, für Bau
und Heimat

Fraunhofer
FOKUS

IMPRESSUM

Autoren:
Thilo Ernst, Nadja Menz, Jaroslav Svacina,
Christian Welzel, Johannes Wolf

Gestaltung:
Reiko Kammer

Herausgeber:
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31, 10589 Berlin
Telefon: +49-30-3463-7173
Telefax: +49-30-3463-99-7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

ISBN: 978-3-9819921-1-3

1. Auflage April 2019

Bildnachweise:

Seite	Autor	Quelle	Lizenz
1	Gitta Zahn	flickr	CC BY 2.0
6	Martin Pettitt	flickr	CC BY 2.0
10	Florian Plag	flickr	CC BY 2.0
13	Steffen Zahn	flickr	CC BY 2.0
14	A. Kniesel	wikipedia	CC BY-SA 3.0
17	Andreas Tille	wikipedia	CC BY-SA 4.0
18-19	Katherine Price	flickr	CC BY 2.0
21	wy	wikipedia	Gemeinfrei
22	Ulrich Mayring	wikipedia	CC BY-SA 3.0
25	Bwag	wikipedia	CC BY-SA 4.0
27	Sergei Gussev	flickr	CC BY 2.0
29	Günter Seggebäing	wikipedia	CC BY-SA 3.0
31	Backslash	wikipedia	CC BY 3.0
34	Josh Hallett	flickr	CC BY-SA 2.0

VORWORT

Der technologische Wandel hat unsere Gesellschaft in den letzten Jahrzehnten stark geprägt. Wir gehen online einkaufen, informieren und vernetzen uns oder schalten von unterwegs die häusliche Heizung an. Über Plattformen organisieren wir einen Großteil unserer digitalen Kommunikation. Und spätestens seit dem Smartphone ist das Internet als ständiger Begleiter allgegenwärtig.

Doch während Onlinedienste immer smarter und ausgefeilter werden, scheint eines konstant zu bleiben – die Authentifizierung. 87 Prozent der deutschen Internetnutzer[1] verwenden zum Login Benutzername und Passwort[2]. Während wir überall nach mehr Sicherheit verlangen, verlassen wir uns bei Onlinediensten auf ein Konzept, das mehr als 30 Jahre alt und bekanntermaßen anfällig ist. Wenn es darum geht, den Zugang zu teilweise sehr sensiblen Daten zu schützen, bedienen wir uns steinzeitlicher Methoden. Es gibt wohl kaum einen vergleichbaren IT-Sicherheitsmechanismus, der eine ähnlich lange Erfolgsgeschichte vorweisen kann. Dementsprechend vielfältig sind die Angriffsmethoden auf Passwörter: Da wären beispielsweise Trojaner, Keylogger, Phishing- oder Social-Engineering-Angriffe, das Ausprobieren gängiger Begriffe und bekannter Passwortkombinationen oder sogenannte Brute-Force-Attacken. Onlinedienstanbieter versuchen, ihre Nutzer zu schützen, indem sie bspw. Vorgaben für Passwörter festlegen oder zu viele falsche Passworteingaben unterbinden. Ein Kampf gegen Windmühlen.

IT-Sicherheitsexperten empfehlen seit Langem, auf eine Zwei-Faktor-Authentifizierung umzusteigen. Doch warum ist dieser Umstieg nicht schon längst geschehen? Liegt es am oft beschworenen Trade-off zwischen Usability und Sicherheit? Dabei sind Passwörter alles andere als nutzerfreundlich, wenn man wenigstens halbwegs sichere verwenden möchte. Das BSI empfiehlt beispielsweise, dass Passwörter mind. 8 Zeichen lang sein sollten. Jeder Dienst sollte ein separates Passwort erhalten, die gewählten Passwörter sollten in keinem Wörterbuch stehen, keine Namen oder Geburtsdaten enthalten und regelmäßig geändert werden. Ach ja: Und gut merken können sollte man sich die Passwörter natürlich auch noch.[3] Ist dieser Ansatz bei der Vielzahl unterschiedlicher Onlinezugänge noch zeitgemäß?

Die Datenskandale der letzten Jahre haben womöglich auch ihr Gutes, denn langsam setzt sich die Erkenntnis durch, dass wir modernere Authentifizierungsverfahren benötigen. Die Alternativen sind vielfältig und reichen von mTANs über biometrische Verfahren bis hin zu Hardware-basierten Lösungen, wie Signaturkarten oder sicheren USB-Sticks. Sollen diese Authentifizierungsverfahren eine breite Akzeptanz erreichen, müssen sie vor allem mobil nutzbar sein, verwenden doch bereits heute 4 von 5 Internetnutzern in Deutschland Smartphones.[2] Welche Ansätze gibt es dafür überhaupt und wie funktionieren sie? Wie zukunftssicher und nutzerfreundlich sind solche Verfahren? Diesen Fragen sind wir nachgegangen und wollen Ihnen mit dieser Expertise nicht nur einen Überblick über den Stand der Technik geben, sondern auch aufzeigen, wie eine sichere mobile Authentifizierung aussehen kann.

Wir wünschen eine anregende Lektüre!

Ihr Kompetenzzentrum Öffentliche IT

[1] Wenn wir in diesem Dokument von Menschen als Nutzern, Bürgern usw. reden, sind damit stets Personen jedweden Geschlechts gemeint.

[2] Statistisches Bundesamt: »Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien« in Fachserie 15 Reihe 4, IKT 2018, Artikelnummer: 2150400187004, https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/IT-Nutzung/Publikationen/Downloads-IT-Nutzung/private-haushalte-ikt-2150400187004.html, abgerufen am 22. März 2019.

[3] https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html, abgerufen am 22. März 2019.

INHALTSVERZEICHNIS

1.	**Thesen**	**5**
2.	**Einführung**	**7**
3.	**Bessere mobile Authentifizierung – aber wie?**	**9**
4.	**Stand der Technik und aktuelle Trends**	**11**
4.1	Smartphone-Marktsituation	11
4.2	Erweiterbarkeit durch externe Hardware	11
4.3	Passwort-Authentifizierung im Mobilzeitalter: Vor dem Kollaps	12
4.4	SMS-TAN/mTAN	14
4.5	Push-TAN	15
4.6	Hardware-unterstützte Sicherheit – extern	15
4.7	Hardware-unterstützte Sicherheit – intern	17
4.8	Biometrie	20
4.9	Single Sign-on (SSO)	21
4.10	Offene Protokollstandards für die Authentifizierung	22
4.11	Ungenutzte Potenziale: SIM-Karte und Mobilfunk-Nutzeridentität	24
4.12	Europäische Single-Sign-on-Inititativen	25
5.	**Handlungsfelder**	**28**
5.1	Identifizierung und Authentifizierung in der Privatwirtschaft	28
5.2	Identifizierung und Authentifizierung im staatlichen Sektor	28
5.3	Forschung und Entwicklung	30
6.	**Empfehlungen**	**32**
	Glossar	**34**

1. THESEN

Mobile Authentifizierung entscheidet über Dienstpopularität.

Nutzer verwenden heute primär mobile Geräte – auch im häuslichen Bereich sind Smartphone und Tablet schneller zur Hand als der Laptop. Populäre Cloud-Dienste bieten ausgefeilte Zugangs-Apps an, die zunehmend die Erwartungen an Nutzerfreundlichkeit prägen – und Smartphone-Apps werden nur minutenlang ausprobiert, bis die meist endgültige Nutzungsentscheidung fällt. Ohne anwenderfreundliche (aber auch ausreichend sichere) mobile Authentifizierung gewinnen personalisierte Dienste keine neuen Nutzer.

Das Smartphone wird zentraler Authentifizierungsfaktor.

Passwörter sind unsicher und auf Mobilgeräten unhandlich. Separate Hardware-Sicherheitsschlüssel haben durch Anschaffungskosten sowie Handhabungs- und Koppelprobleme eingeschränkte Akzeptanz. Biometrie ist zur Authentifizierung eher flankierend geeignet und hat zudem spezifische Schwachstellen. Problemlos akzeptiert wird als Authentifizierungsfaktor nutzerseitig vor allem eines: der Gerätebesitz selbst – darum sind SMS-TAN-Verfahren trotz mäßiger Sicherheit ungebrochen populär. Logisch, denn das Smartphone hat der mobile Nutzer stets schon dabei. Bei solider und nutzbarer interner Hardware-Sicherheitsbasis sowie mit Vorkehrungen für den Diebstahl- oder Zerstörungsfall steht einer Hauptrolle des Smartphones in der mobilen Authentifizierung auch nichts im Wege.

Sicherheit braucht dedizierte Hardware – im Smartphone oft vorhanden, aber noch nicht effektiv nutzbar.

Auf offenen Smartphone-Plattformen ist sichere Authentifizierung nicht ohne dedizierte Hardware machbar. Passende Sicherheitshardware ist in immer mehr Mobilgeräten schon ab Werk verbaut; auch die SIM-Karte kann adäquaten Hardwareschutz bieten. Jedoch bleibt beides zur Absicherung von Online-Authentifizierungsprozessen nicht breit nutzbar, solange Plattformanbieter oder Mobilnetzbetreiber nicht die Weichen dafür stellen. Die angekündigte[4] Einführung der Mobile-Connect-Authentifizierungsfunktion durch die deutschen Mobilnetzbetreiber ist ein erster Schritt in diese Richtung.

Akzeptanz erfordert abgestufte Sicherheitsniveaus.

Die Schreibtischschublade wird nicht so aufwändig gesichert wie der Safe – ebenso erfordern unterschiedliche Onlinedienste verschiedene Grade an Authentifizierungssicherheit. Werden substanzielle Risiken für Vermögen oder Privatsphäre wahrgenommen, tolerieren auch verwöhnte Smartphone-Nutzer im Interesse der Sicherheit etwas Zusatzaufwand. Überschaubare, sinnvoll abgestufte Authentifizierungsmechanismen, die dem Anwender nur dem Sicherheitsbedarf des gewünschten Dienstes angemessene Interaktionsarbeit abverlangen, haben kaum Akzeptanzprobleme.

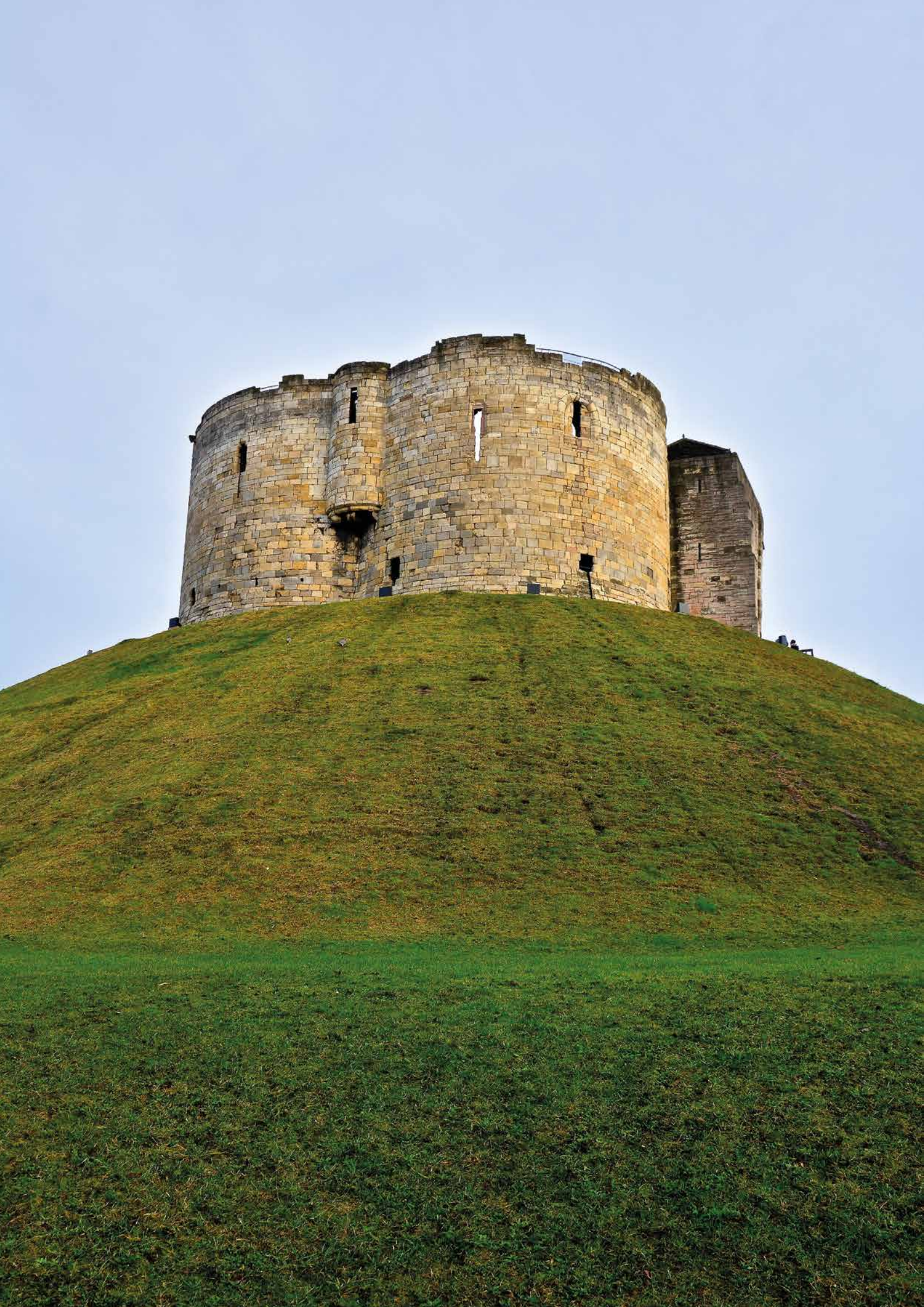
Offene, sichere Protokolle ermöglichen bequeme, einheitliche Authentifizierung.

Authentifizierungsmechanismen sind bisher meist dienstspezifisch – Nutzer sind mit jeweils unterschiedlichen Bedienabläufen konfrontiert. Offene Authentifizierungs-Protokollstandards und darauf basierende Single-Sign-on-Angebote ermöglichen grundlegende Vereinheitlichung: Mit einmal erlernten Abläufen wird bequeme Authentifizierung bei unterschiedlichsten Diensten möglich. Dienstseitig werden Integration und Betrieb einfacher und sicherer. Authentifizierungsinformationen müssen nicht mehr bei jedem Dienstbetreiber gespeichert werden, die Missbrauchsgefahr sinkt und ganze Angriffsklassen werden somit verhindert.

Eine europäische Single-Sign-on-Partnerschaft hat Chancen gegenüber Google und Facebook.

Den von einem oft genutzten Onlinedienst gewohnten Anmeldeprozess direkt bei anderen Dienstanbietern nachnutzen zu können, ist bequem. Jedoch steigt die Wahrnehmung damit verbundener Gefahren für Privatsphäre und Sicherheit. Für deutsche und europäische Anbieter birgt diese Situation Chancen, einen von US-Internetriesen unabhängigen, zu nationalem und EU-Datenschutzrecht konformen Single-Sign-on-Dienst zu etablieren. Initiativen wie Verimi und NetID sind angelaufen, eine kritische Masse an Nutzern ist jedoch noch nicht erreicht. Eine konsequent auf offene Standards setzende, gemeinsam von privatwirtschaftlichem und öffentlichem Sektor vorangetriebene Partnerschaft, die die Stärken der europäischen IT- und Telekommunikationsindustrie nutzt, könnte den Durchbruch schaffen.

[4] Vgl. Abschnitt 4.11



2. EINFÜHRUNG

Im Zeitalter der ubiquitären Nutzung von Mobilgeräten hat der Anwender ständig und überall Zugriff auf das Internet. Eine kaum überschaubare Vielfalt von Onlinediensten erfreut sich breiter Popularität.

Diese Onlinedienste stellen heute überwiegend nicht nur einer anonymen Öffentlichkeit Informationen zur Verfügung (oder nehmen diese entgegen), sondern dienen dem Informationsaustausch mit individuellen und voneinander unterschiedenen Nutzern. Sie arbeiten also personalisiert, wobei nutzerspezifische Informationen dienstseitig in Nutzerkonten oder -profilen verwaltet werden. Um die Nutzer voneinander zu unterscheiden und beim Zugriff sicher zuzuordnen, muss der Dienst zumindest über Basisinformationen zur Identität jedes Nutzers (z. B. Nutzernamen) verfügen und muss sichern, dass ausschließlich legitime Zugriffe zugelassen werden. Beim Authentifizierungsvorgang während der Anmeldung belegt der Nutzer seine Identität und damit seine Legitimität durch Vorweisen eines oder mehrerer Authentifizierungsfaktoren:

– etwas, das (nur) der Nutzer weiß – *Wissensfaktor* (z. B. Passwort oder PIN)
– etwas, das (nur) der Nutzer hat – *Besitzfaktor* (ein fälschungssicherer physischer Gegenstand, z. B. eine Smartcard mit hardwaregeschützt gespeicherten privaten Schlüsseln)
– etwas, das (nur) der Nutzer ist – *Inhärenzfaktor* (z. B. ein spezifisches biometrisches Merkmal wie Fingerabdruck oder Irisgeometrie).

Die mit einem Smartphone oder Tablet ausgestatteten Anwender verlangen von einem Dienst ein hohes Niveau an Nutzerfreundlichkeit, wie von diesen Geräten und den darauf laufenden Apps gewohnt. Das betrifft auch und besonders die als lästige Einstiegshürde wahrgenommene Authentifizierung – von welcher natürlich trotzdem ausreichende Sicherheit verlangt wird. Erwartet wird gerade bei thematisch verwandten Diensten zudem, dass nicht jeweils andere Zugangsmechanismen erlernt werden müssen, sondern diese idealerweise über unterschiedliche Dienste hinweg völlig identisch funktionieren.

Auch die bei der Erstregistrierung für manche Dienste notwendige Identifizierung des Nutzers (also die sichere Feststellung seiner juristischen Identität und deren angemessene Abbildung in einer digitalen Identität) ist von Bedeutung, jedoch handelt es sich hierbei um einen jeweils einmaligen Vorgang. In dieser Phase sind Nutzer bereit, etwas mehr Aufwand zu investieren, solange die normale Nutzung des Dienstes als unkompliziert und angenehm empfunden wird. In Bezug auf den Authentifizierungsmechanismus, der den alltäglichen Zugang zum Dienst kontrolliert, kann diese Toleranz jedoch nicht erwartet werden. Verursacht dieser eine hohe kognitive Belastung (z. B. durch komplexe Interaktion oder starke Gedächtnisbeanspruchung), erschwert dies den Zugang zum Dienst und in der Konsequenz die Gewinnung neuer Nutzer massiv.

Die Mehrzahl der Onlinedienste wird von kommerziellen Anbietern betrieben, die bereits seit einigen Jahren bestrebt sind, ihre Angebote auch für die mobile Nutzung zu optimieren oder dieser sogar den Vorrang gewähren (»mobile first«-Strategie). Bei E-Government-Diensten ist dies in Deutschland noch nicht in vergleichbarem Umfang der Fall. Insbesondere wurden die Verfahren zur Identifizierung und Authentifizierung häufig noch nicht ausreichend an die mobile Nutzung angepasst, was schwerwiegende Folgen für die Nutzerzahlen hat.

Authentifizierung und Identifizierung sind Teilaspekte des übergreifenden Gebiets Identitätsmanagement[5]. Insbesondere für im öffentlichen Sektor betriebene Onlinedienste gelten in Deutschland strikte gesetzliche Anforderungen an die Identifizierung der Nutzer, die auch Auswirkungen auf die Auswahlmöglichkeiten von Authentifizierungsverfahren haben können. Darauf wird hier aber nur nach Bedarf punktuell eingegangen.

Dieses Papier erklärt und bewertet Begriffe, Ansätze und Techniken der mobilen Authentifizierung, gibt einen Überblick über den Stand der Technik, erklärt wesentliche Trends und zeigt Dienstbetreibern insbesondere im öffentlichen Sektor sinnvolle Wege und Handlungsoptionen auf.

Um eine breite Dienstnutzung zu ermöglichen, dürfen Authentifizierungsmechanismen dabei keinesfalls Nutzergruppen signifikanter Größe ausschließen, z. B. durch mangelnde Gerätekompatibilität.

[5] Eine Einführung in das Thema Digitale Identitäten und Identitätsmanagement finden Sie im White Paper: »Vertrauenswürdige digitale Identität: Baustein für öffentliche IT«. Abrufbar unter: https://www.oeffentliche-it.de/publikationen, abgerufen am 25. März 2019.

ANGEMESSENE SICHERHEITSNIVEAUS VERMEIDEN UNNÖTIGEN NUTZERAUFWAND.

Sicherheitsniveaus in der Authentifizierung

Wie in der Einleitung dargestellt, ist es sinnvoll, Authentifizierungsverfahren bezüglich ihres Sicherheitsniveaus so auszuwählen und einzusetzen, dass der resultierende Aufwand aus Nutzersicht (für die Interaktion, aber auch bezüglich der benötigten Hard- und Software) dem Sicherheitsbedarf des abgesicherten Dienstes angemessen ist – welcher wiederum vom anzunehmenden Schadensumfang bei illegitimem Zugriff abhängt. Zur genaueren Definition und Charakterisierung konkreter Sicherheitsniveaus bei der Authentifizierung (und im umfassenderen Gebiet Identitätsmanagement) ist in verschiedenen Anwendungskontexten und in unterschiedlichen Gremien eine Anzahl ähnlicher, aber nicht deckungsgleicher nationaler und internationaler Standards entstanden[6]. Diese Standards definieren konkrete Sicherheitsniveaus (»Levels of Assurance/LoA« oder »Security Levels/SL«) und legen für jedes Niveau Mindestanforderungen der Umsetzung fest. Über die technische Ebene hinaus werden derartige Festlegungen auch in der Gesetzgebung adressiert[7]. Die technische Richtlinie TR-03107-1 des BSI beispielsweise definiert die Niveaus »normal«, »substantiell« und »hoch« und beschreibt dazu jeweils zugehörige Gefährdungsgrade, z. B. bezogen auf finanzielle Auswirkungen: »finanzieller Schaden überschaubar«, »substantieller finanzieller Schaden möglich«, »beträchtliche finanzielle Verluste«. Im Folgenden wird analog dazu grob von normalem, substanziellem oder hohem Sicherheitsniveau bzw. Sicherheitsbedarf von Diensten die Rede sein. Oberhalb des niedrigsten Sicherheitsniveaus (in der BSI-Kategorisierung also ab »substanziell«) wird üblicherweise verlangt, zwei unabhängige Faktoren im Authentifizierungsprozess zu kombinieren. Wenn also im Weiteren eine Methode als »bis zum Niveau substanziell« empfohlen wird, bedeutet dies nicht notwendigerweise, dass diese Methode allein ausreichen würde.

[6] ISO/IEC 29115:2013 Information technology – Security techniques – Entity authentication assurance framework https://www.iso.org/standard/45138.html, abgerufen am 25. März 2019.
Technische Richtlinie TR-03107-1Elektronische Identitäten und Vertrauensdienste im E-Government, Teil 1: Vertrauensniveaus und Mechanismen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf, abgerufen am 25. März 2019.
IEC62443-3-3 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels. https://webstore.iec.ch/publication/7033, abgerufen am 25. März 2019.
NIST Special Publication 800-63B Digital Identity Guidelines/Authentication and Lifecycle Management. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf, abgerufen am 25. März 2019.

[7] DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015R1502&from=EN, abgerufen am 25. März 2019.

3. BESSERE MOBILE AUTHENTIFIZIERUNG – ABER WIE?

Mit Authentifizierung wird die programmgesteuerte Überprüfung der Legitimität von Zugriffen auf IT-Systeme bezeichnet. Das Konzept entstand mit den Multi-User-Großrechnern der 1960er Jahre, bei denen erstmals mehreren Nutzern Zugriff mit jeweils unterschiedlichen Rechten zu gewähren und illegitimer Zugriff auszuschließen war.

Damals wurde Rechentechnik nur von einem kleinen Kreis technischer Experten bedient, und die Folgen einer eventuellen illegitimen Nutzung waren überschaubar. In der Informationsgesellschaft der Gegenwart hingegen greift jedermann alltäglich und überall auf IT-Systeme zu. Vorwiegend sind dies cloudbasierte Onlinedienste, die von einer Vielfalt von Endgeräten (stationären PCs, Laptops, Tablets und Smartphones …) aus nutzbar sind. Illegitime Zugriffe können heute schwere materielle oder ideelle Schäden bewirken. Auf den inzwischen bereits überwiegend verwendeten Mobilgeräten ist die überkommene Nutzername/Passwort-Authentifizierung als Relikt anzusehen – eine Kombination unzureichender Sicherheit und mangelhafter Nutzerfreundlichkeit. Für viele Dienste ist diese Art der Authentifizierung eigentlich inakzeptabel und sollte dringend abgelöst werden. Welche Eigenschaften muss eine zeitgemäße mobile Authentifizierung haben?

Angemessen sicher: Die Sicherheit von Authentifizierungsmechanismen wird immer wichtiger, denn mit der fortschreitenden IT-Durchdringung aller Lebensbereiche bestehen heute für praktisch jeden Einzelnen erhebliche und weiter wachsende Risiken, wenn illegitime Zugriffe nicht verlässlich ausgeschlossen werden. Wirklich hohe Risiken bestehen allerdings nur bei einem Teil der Dienste, z. B. dem Onlinebanking. Wo so klar ein höherer Sicherheitsbedarf wahrgenommen wird, akzeptieren Nutzer auch höheren Aufwand und geringere Bequemlichkeit als notwendigen Preis für die gewünschte Sicherheit. Das Sicherheitsniveau der Authentifizierung muss also dem Sicherheitsbedarf des abgesicherten Dienstes angemessen sein. Eine »one size fits all«-Authentifizierung ist unrealistisch – sinnvoll sind dagegen überschaubar abgestufte Konzepte.

Mobilnutzer-freundlich: Die mobile Nutzung steht seit einigen Jahren immer stärker im Vordergrund, da die entsprechenden Geräte praktisch immer, überall und sofort verfügbar sind. Damit sind allgemein gesteigerte Erwartungshaltungen an die Nutzerfreundlichkeit (Usability) entstanden – auch für Authentifizierungsvorgänge werden einfache Prozesse ohne allzu hohen Interaktionsaufwand erwartet, sonst leidet die Popularität des so abgesicherten Dienstes schnell. Zumindest teilweise haben diese Erwartungshaltungen objektive Ursachen: Mobilgeräte besitzen kleinere Bildschirme und fehlerträchtige Touch-Tastaturen, was eine geringere nutzbare »Interaktionsbandbreite« gegenüber stationären Geräten mit Hardware-Tastatur bewirkt. Vergleichbare Interaktionsschritte werden auf Mobilgeräten als aufwändiger empfunden, die »Unzumutbarkeitsschwelle« ist schneller erreicht. Auch die Option, externe Hardware in die Problemlösung einzubeziehen, ist nur eingeschränkt praktikabel, da Mobilgeräte hierfür nur wenige und uneinheitliche Schnittstellen besitzen. Nutzer wollen zudem nur ungern zusätzliche Hardware mitführen und ggf. auch noch deren Batteriezustand im Auge behalten. Smartphones verfügen jedoch zunehmend auch selbst über geeignete interne Sicherheitshardware zur Absicherung der Authentifizierung.

Breitentauglich: Um weitverbreiteten Einsatz zu erreichen, darf ein Authentifizierungsverfahren keine Nutzergruppen substanzieller Größe ausschließen. Insbesondere muss es auf allen marktbestimmenden Mobilgeräteplattformen einsetzbar sein. Auch von der Nutzermehrheit als zu hoch wahrgenommene Einstiegshürden (z. B. substanzielle Kosten für zusätzliche Hardware, unangemessener Bürokratieaufwand zur Erstregistrierung) können die Breitentauglichkeit kritisch beeinträchtigen. Im Interesse der Verbreitung bei vielen Dienstbetreibern dürfen aber auch Einführung und Betrieb des Verfahrens dienstseitig keine unangemessenen Kosten oder Risiken verursachen.

Idealerweise einheitlich: Die Vielzahl mobil zugreifbarer Dienste konfrontiert die Nutzer auch mit einer erheblichen Anzahl unterschiedlicher Authentifizierungskonzepte, was kognitive Mehrbelastung und Unwillen erzeugt. Es wird als angenehmer empfunden, für unterschiedliche Dienste einen einheitlichen Bedienablauf zur Authentifizierung und idealerweise auch dieselben Authentifizierungsfaktoren verwenden zu können.

Zusammenfassend ist festzustellen, dass dem jeweiligen Bedarf angemessen sichere, die vorhandene Hardware sinnvoll nutzende und konsequent auf die Bedürfnisse mobiler Nutzer abgestimmte, breitentaugliche und idealerweise einheitliche mobile Authentifizierungsverfahren gefragt sind.

4. STAND DER TECHNIK UND AKTUELLE TRENDS

4.1 SMARTPHONE-MARKTSITUATION

Die noch vor wenigen Jahren stärkere Fragmentierung des Smartphone-Markts ist einer faktischen Duopol-Konstellation gewichen, in welcher sich Google mit Android und Apple mit der iOS-Plattform als marktbestimmende mobile Ökosysteme behaupten. Im Juli 2018 lagen die Marktanteile in Deutschland bei 80,5 Prozent (Android) und 18,8 Prozent (iOS)[8]. Innerhalb dieser auf absehbare Zeit stabilen Duopol-Situation wird sich die Marktkonsolidierung fortsetzen: Es ist davon auszugehen, dass sich mit voranschreitender Marktsättigung[9] die Anzahl aktiver Android-Smartphone-Hersteller verringert[10].

Die gravierenden technischen Detailunterschiede der Plattformen erfordern aus Sicht von Anwendungsanbietern zwar die separate Entwicklung von Apps, andererseits stellt sich der Leistungsumfang der Plattformen und Endgeräte aus Nutzersicht inzwischen als sehr ähnlich dar, abgesehen von einigen (für das Thema Authentifizierung allerdings sehr relevanten) Hardware-Unterschieden. Apple ist für das iOS-Betriebssystem gleichzeitig einziger Hardware-Hersteller und hat somit vollständige Kontrolle über alle Plattformdetails. Google lizensiert Android an eine Vielzahl von Hardware-Herstellern in der »Open Handset Alliance«[11] und kontrolliert seine Plattform weniger strikt, was allerdings eine beträchtliche Fragmentierung der Android-Welt verursacht hat. Eine Folge davon ist, dass für viele Android-Geräte herstellerseitig nur unzureichende Softwareaktualisierungs-Zyklen realisiert werden. Ein erheblicher Teil der im Einsatz befindlichen Android-Geräte besitzt daher ein veraltetes Betriebssystem oder erhält nicht einmal wichtige Sicherheitsupdates. Einige Markenhersteller liefern zwar (bezogen auf das Gerätealter) im Mittel länger Updates und Google ergreift bereits Maßnahmen[12], um die Situation generell zu bessern. Trotzdem ist der durchschnittliche Sicherheitsstatus von im Feld anzutreffenden Android-Geräten weiterhin schlechter als der von iOS-Geräten[13]. Bei Betrachtung der Sicherheit eines mobilen Authentifizierungsverfahrens muss eine mögliche Kompromittierung des Smartphones aufgrund nicht verfügbarer Sicherheitsupdates folglich auch in Zukunft stets einkalkuliert werden[14].

Bezüglich der Breitentauglichkeit mobiler Authentifizierungsverfahren bedeutet die geschilderte Marktsituation, dass ein Kandidatenverfahren definitiv Android und iOS abdecken muss, wofür jeweils angepasste Software und ggf. auch Hardware benötigt wird. Andere Plattformen spielen wegen ihrer verschwindend geringen Marktanteile keine nennenswerte Rolle und werden deshalb in diesem Papier nicht diskutiert.

4.2 ERWEITERBARKEIT DURCH EXTERNE HARDWARE

Die Erweiterbarkeit durch externe Hardware spielt für sichere Authentifizierungsmechanismen eine besondere Rolle. Hierzu stehen auf beiden relevanten Smartphone-Plattformen nur beschränkte Optionen zur Verfügung (nur bei wenigen Produkten vorhandene Schnittstellen, z. B. Infrarot-Kommunikation, werden dabei nicht berücksichtigt).

iOS-Geräte sind drahtgebunden nur durch den Apple-proprietären Lightning-Port erweiterbar. Ein Anschluss externer Komponenten über USB ist auf wenige, von Apple festgelegte Geräteklassen (z. B. Digitalkameras) eingeschränkt und erfordert ein Adapterkabel. Auch der früher stets vorhandene 3,5-mm-Audiosteckverbinder taucht in den aktuellsten iPhones nicht mehr auf. An drahtlosen Verbindungen werden Bluetooth, WLAN und NFC durchgängig unterstützt, allerdings z. T. mit strikten, von Apple festgelegten Einschränkungen bezüglich

[8] Erhebung von Kantar WorldPanel/ComTech, zitiert in: https://www.computerbase.de/2018-07/marktanalyse-smartphone-betriebssysteme-q2-2018/, abgerufen am 22. März 2019.

[9] https://www.gartner.com/en/newsroom/press-releases/2018-02-22-gartner-says-worldwide-sales-of-smartphones-recorded-first-ever-decline-during-the-fourth-quarter-of-2017, abgerufen am 22. März 2019.

[10] https://economictimes.indiatimes.com/tech/hardware/exits-in-smartphone-market-up-six-fold-on-rising-competition-says-report/articleshow/63966438.cms, abgerufen am 22. März 2019. In anderen Marktsegmenten wie Unterhaltungselektronik, SmartWatches und Internet of Things ist für spezifische neue Android-Varianten jedoch mit weiterem Wachstum, auch bezüglich der Zahl der beteiligten Hersteller, zu rechnen.

[11] https://www.openhandsetalliance.com/, abgerufen am 22. März 2019.

[12] https://www.wired.co.uk/article/android-phone-updates-security-google, abgerufen am 22. März 2019.

[13] https://www.androidpolice.com/2017/11/02/android-versus-ios-software-updates-revisited-two-years-later, abgerufen am 22. März 2019. Sogar wenn auf Android-Seite nur die (bestunterstützten) Flaggschiffmodelle der »Nexus/Pixel«-Serie betrachtet werden, ergibt sich eine mittlere Unterstützungsdauer mit OS-Updates von 31 Monaten, gegenüber 50 Monaten bei iOS-Geräten

[14] https://www.cl.cam.ac.uk/~drt24/papers/spsm-scoring.pdf, abgerufen am 22. März 2019.

DUTZENDE PASSWÖRTER
UND PASSWORTRICHTLINIEN
ÜBERFORDERN NUTZER.

der durch Apps nutzbaren Schnittstellen-Funktionalität. Aus diesem Grund ist auf der iOS-Plattform derzeit keine NFC-basierte Kommunikation mit für Authentifizierungszwecke interessanten externen Komponenten, wie der eID-Funktion in Personalausweis oder Aufenthaltstitel oder mit anderweitigen NFC-Smartcards, möglich[15].

Viele aktuelle Android-Geräte unterstützen den USB-OTG-Standard, erlauben also eingeschränkt Kommunikation mit über die USB-Schnittstelle angeschlossenen Geräten. Die Funkschnittstellen Bluetooth und WLAN werden praktisch durch alle Android-Geräte unterstützt. Bezüglich NFC verfolgt Google zwar keine zu Apple vergleichbar restriktive Produktpolitik, allerdings bewirken eine in Details nicht ausreichend klare Spezifikation sowie die Marktfragmentierung von Android, dass in der Praxis viele Geräte ebenfalls nicht verlässlich mit den oben genannten Komponenten über NFC kommunizieren können.

Diese Hardwaresituation hat für mobile Authentifizierungslösungen weitreichende Konsequenzen, die im Abschnitt 4.5 näher dargestellt werden.

Versuche, Apple von der geschilderten restriktiven Politik bzgl. NFC abzubringen, u. a. seitens der britischen Regierung und großer australischer Banken, blieben bisher erfolglos[16]. Auch die neueste Version iOS12 brachte nur eine geringfügige und unzureichende Liberalisierung der NFC-Restriktionen[17]. Bei Android dagegen bewirkt die Herstellervielfalt und Produktfragmentierung, dass eine ausreichende NFC-Nutzbarkeit in der Breite ebenfalls nicht absehbar ist. Für eine zukünftige Integration geeigneter zusätzlicher Schnittstellen sind bei beiden Plattformen keine Anzeichen erkennbar.

4.3 PASSWORT-AUTHENTIFIZIERUNG IM MOBILZEITALTER: VOR DEM KOLLAPS

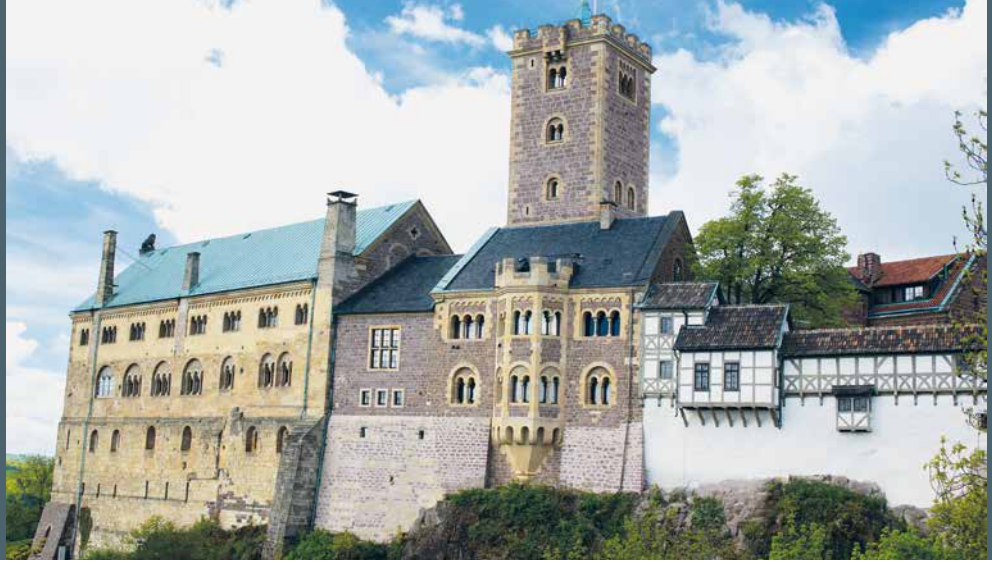
Eine direkte passwortbasierte Authentifizierung bei Onlinediensten ist letztlich immer unzureichend sicher, denn sie erlaubt skalierbare Angriffe – einmal gestohlene Passwort-Datenbanken können weiterverteilt und von praktisch beliebig vielen Angreifern genutzt werden. Dies gilt insbesondere, wenn Passwörter dienstseitig in unverschlüsselter Form gespeichert oder zu deren Verschlüsselung veraltete, schwache Kryptoverfahren verwendet werden – beides kommt in der Praxis leider immer wieder vor. Um »stärkere« (also komplexere und längere) Passwörter zu erzwingen, bewerten Dienstbetreiber inzwischen die Eignung von Passwörtern während deren Festlegung durch den Nutzer, wobei strenge und pro Anbieter subtil unterschiedliche »Password Policies« zum erlaubten Passwort-Format durchgesetzt werden. In manchen Fällen wird zusätzlich ein regelmäßiger Passwortwechsel gefordert. Schon 2016 verfügte fast die Hälfte der Nutzer über 10 oder mehr Online-Konten, inzwischen wird von bis zu 200 Konten pro Nutzer ausgegangen[18]. Zwar sollte aus Sicherheitsgründen kein Passwort für mehr als ein Konto benutzt werden, das menschliche Gedächtnis ist jedoch zum Speichern vieler verschiedener starker Passwör-

[15] https://www.heise.de/mac-and-i/meldung/Personalausweis-mit-eID-AusweisApp2-fuer-iPhone-muss-ohne-NFC-auskommen-3648693.html, abgerufen am 25. März 2019.
https://www.bbc.com/news/uk-politics-46043668, abgerufen am 25. März 2019.

[16] https://www.nfcworld.com/2017/04/03/351418/australian-banks-lose-fight-to-gain-access-to-nfc-functionality-in-apple-iphones/, abgerufen am 25. März 2019.
https://www.bbc.com/news/uk-politics-46043668, abgerufen am 25. März 2019.
https://9to5mac.com/2018/11/01/uk-government-nfc-brexit/, abgerufen am 25. März 2019.

[17] https://www.macworld.com/article/3307191/iphone-ipad/what-apples-background-tag-reading-nfc-update-means-for-you-and-businesses.html, abgerufen am 25. März 2019.

[18] https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/moving-beyond-passwords-cybersecurity.html, abgerufen am 25. März 2019.



ter ungeeignet, sodass diese Forderung regelmäßig ignoriert wird. Die prinzipiellen Probleme der Passwort-Authentifizierung werden auf Mobilgeräten noch durch deren beschränkte Interaktionsbandbreite verschärft.

Auch die von einigen Nutzern verwendeten Passwortmanager-Programme sind kein Allheilmittel: Sie unterstützen zwar die Verwendung stärkerer Passwörter, indem sie diese an Stelle des Nutzers automatisiert generieren, speichern und z. T. sogar in die Nutzerschnittstelle der Anwendungsebene eintragen. Jede dieser Techniken eröffnet jedoch auch neue Angriffsflanken[19]. Vor allem aber stellt ein einmal geknackter Passwortmanager für den Angreifer einen Jackpot dar, der ihm unmittelbaren Zugriff auf alle so verwalteten Onlinekonten des Nutzers verschafft. Obwohl es bisher nicht zu massenhaften Angriffen auf Passwortmanager z. B. mittels Malware kam, ist dies für die Zukunft durchaus zu befürchten, denn auch aktuelle Passwortmanager-Versionen weisen erhebliche Sicherheitsmängel auf[20].

Angesichts der durch die IT-Durchdringung weiter anwachsenden Schadenspotenziale wird es immer dringlicher, das Passwort als unzeitgemäße Form der Authentifizierung abzulösen oder zumindest mit zusätzlichen Sicherheitsmechanismen in einer zwei- bzw. Mehrfaktor-Authentifizierung zu kombinieren, um belastbaren Schutz gegen Angriffe zu erzielen.

Für die Zukunft empfohlen werden können allenfalls noch die mobiltauglicheren Passwort-Verwandten »PIN« und »Touchscreen-Wischmuster« – diese sollten allerdings keinen eigenständigen Faktor in der Authentifizierung bei einem Dienst darstellen (und daher auch in keiner Form dienstseitig bekannt oder gespeichert werden), sondern lediglich den lokalen Zugang zum Mobilgerät absichern. Damit ist im Diebstahl- oder sonstigen Verlustfall der eigentliche mit dem Gerät mögliche Authentifizierungsprozess einem illegitimen Nutzer von Anfang an unzugänglich.

4.4 SMS-TAN / MTAN

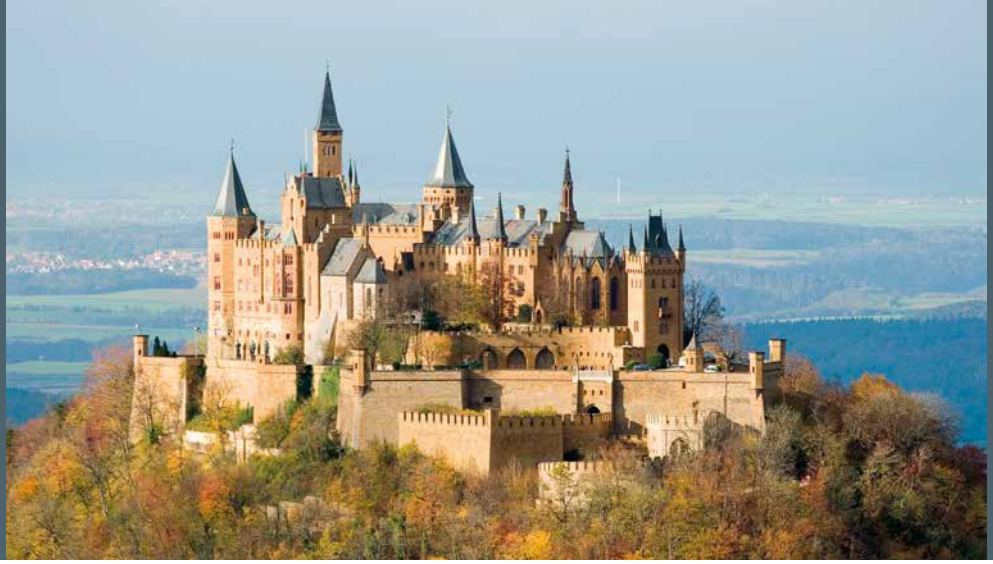
TANs (Transaktionsnummern, also z. B. aus sechs Ziffern bestehende Einmalpasswörter) werden seit Langem im Onlinebanking eingesetzt – üblicherweise nach einer klassischen Passwort-Authentifizierung, welche den initialen Zugriff zum persönlichen Onlinebanking-Bereich freigibt. Die TAN muss also als zweiter Faktor vorgewiesen werden, um eine Transaktion (z. B. eine Überweisung) auszulösen. In der Vergangenheit entstammten TANs einer dem Kunden vorab in Papierform übergebenen, nur den beiden Parteien der Transaktion bekannten TAN-Liste, deren Besitz insofern den zweiten Faktor manifestierte. Seit etwa 2009 wurde dieses System durch den Versand von transaktionsspezifisch zufällig serverseitig erzeugten TANs per SMS an den Nutzer abgelöst (»SMS-TAN« oder »mTAN«). Dabei stellt letztlich der Besitz einer bei einem Mobilnetzbetreiber registrierten SIM-Karte mit der bei der Bank für das SMS-TAN-Verfahren hinterlegten Rufnummer den zweiten Authentifizierungsfaktor dar.

Die dem Verfahren zugrundeliegende Annahme, dass SMS einen sicheren und unabhängigen Kanal darstellt, mittels dessen die generierte TAN risikolos dem Nutzer übermittelt werden kann, stellt sich inzwischen jedoch als nicht ausreichend tragfähig dar:

– Die Transportmechanismen für SMS gemäß den hierfür gültigen internationalen Kommunikationsstandards (die durch bei Mobilfunkbetreibern verwendete Software umgesetzt werden), haben sich als unsicher erwiesen. Es ist dadurch nicht ausreichend schwierig, SMS durch dritte im Netz registrierte

[19] https://team-sik.org/trent_portfolio/password-manager-apps/, abgerufen am 25. März 2019.

[20] https://www.zdnet.com/article/critical-vulnerabilities-uncovered-in-popular-password-managers/, abgerufen am 25. März 2019.
https://www.securityevaluators.com/casestudies/password-manager-hacking/, abgerufen am 25. März 2019.



Mobilgeräte illegitim abzufangen bzw. gefälscht zu versenden. Diese bereits seit einigen Jahren bekannten Schwächen sind weiterhin breit ausnutzbar[21].

- Auf durch Malware infizierten Smartphones besteht die Gefahr, dass SMS verdeckt beim Empfang abgegriffen und evtl. direkt und vom Nutzer unbemerkt zur Authentifizierung illegitimer Transaktionen verwendet werden[22].
- Den Mobilfunkbetreibern gelingt es nicht zuverlässig, sogenannte »Social Engineering«-Attacken (»SIM Hijacking«) abzuwehren, mittels derer Angreifer sich unberechtigt SIM-Karten für Anschlüsse Anderer beschaffen und somit Zugang zur illegitimen SMS-TAN-Verwendung verschaffen können[23]

Durch Ausnutzung dieser und weiterer Schwächen gab es in den letzten Jahren verschiedene Angriffe auf SMS-basierte Authentifizierungsverfahren, die im Onlinebanking erhebliche wirtschaftliche Schäden verursachten.

Ein weiterer Schwachpunkt ergibt sich daraus, dass eine SIM-Karte keinen vom Smartphone physisch separaten Authentifizierungsfaktor darstellt – sie bleibt normalerweise darin eingesteckt (oder ist in manchen neuen Geräten sogar als eSIM fest verbaut). Aus Nutzersicht sind also Smartphone und SIM-Karte in einem einzigen Gegenstand vereint. Eine echte Zwei-Faktor-Konstellation ist insofern nur vorhanden, wenn die abzusichernde Anwendung auf einem anderen Gerät ausgeführt wird. Ist dies nicht der Fall, muss der Zugriff auf die SIM zusätzlich abgesichert sein (durch eine PIN, ein Touchscreen-Wischmuster oder Biometrie), womit dann wieder ein separater zweiter Faktor im Spiel ist.

[21] https://www.ptsecurity.com/ww-en/analytics/ss7-vulnerability-2018, abgerufen am 25. März 2019.

[22] https://blog.avast.com/de/banking-trojaner-gm-bot-zielt-auf-postbank-und-sparkassenkunden-ab, abgerufen am 25. März 2019.

[23] http://www.spiegel.de/wirtschaft/service/deutsche-telekom-betrug-beim-online-banking-die-wichtigsten-antworten-a-1058840.html, abgerufen am 25. März 2019.

Aus Nutzersicht sind SMS-TAN und mTAN relativ benutzerfreundlich und daher populär (insbesondere da sie ohne Zusatzhardware auf allen Smartphone-Plattformen funktionieren). Zur Neueinführung können sie jedoch wegen der genannten Probleme nicht mehr uneingeschränkt empfohlen werden.

Die Ablösung SMS-basierter Verfahren hat bereits begonnen. Momentan werden -Push-TAN-Verfahren als sinnvollster Ersatz angesehen und gewinnen im Onlinebanking-Sektor immer stärker an Bedeutung.

4.5 PUSH-TAN

Als Alternative zu unsicheren SMS-TAN-Verfahren haben sich Softwarelösungen etabliert, die üblicherweise als Apps zu installieren sind und den Transport der serverseitig generierten TAN zum Endnutzer übernehmen. Dieser Transport wird durch kryptografische Kommunikationsprotokolle abgesichert.

Die Gefahren innerhalb des Smartphones (z. B. durch Abgreifen oder Vortäuschen einer übertragenen PIN[24] durch Malware) lassen sich bei Einhaltung zusätzlicher Einschränkungen (insbesondere keine automatische Übergabe der übertragenen TAN aus der Push-TAN-App an die eigentliche Banking-App) und fachgerechter Implementierung gering halten. Das Sicherheitsniveau solcher Verfahren ist dann zumindest höher als bei SMS-basierten Methoden. Natürlich bilden auch bei diesem Ansatz Smartphone und Push-TAN-App physisch eine Einheit; analog zur Situation beim SMS-TAN-Verfahren (SIM-Zugriff) sollte der Zugriff auf die Push-TAN-App also durch einen weiteren Authentifizierungsfaktor abgesichert werden.

Bei Beachtung dieser Rahmenbedingungen kann die Anwendung von Push-TAN-Verfahren auch in Zukunft für Anwendungsdienste bis zu substanziellem Sicherheitsbedarf empfohlen

[24] Persönliche Identifikationsnummer.

NFC-TOKEN PLUS SMARTPHONE:
DERZEIT NOCH FEHLANZEIGE.

werden, allerdings wäre im Interesse der Einheitlichkeit die Verwendung einer einzigen, gemeinsamen Implementierung über mehrere Dienste hinweg, vorzugsweise unter Nutzung von Hardware-Sicherheit des Mobilgerätes (also z. B. als »Trustlet«, siehe Abschnitt 4.7), wünschenswert.

4.6 HARDWARE-UNTERSTÜTZTE SICHERHEIT – EXTERN

Ein Authentifizierungsprozess kann nur so sicher sein wie die Hardware, auf welcher seine wesentlichen Prozessschritte ablaufen. Ist diese kompromittiert, kann ein Angreifer stets eine illegitime Authentifizierung erreichen. Da bei Smartphones eine Kompromittierung z. B. durch Malware nicht ausgeschlossen werden kann, bleibt eine Einbindung unabhängiger externer (und möglichst gut abgesicherter) Hardware in den mobilen Authentifizierungsprozess zumindest für Anwendungsfälle mit hohem Sicherheitsbedarf wünschenswert. Konkret bieten sich hierfür u. a. die eID-Funktion in Personalausweis und Aufenthaltstitel, Smartcards und elektronische Sicherheitsschlüssel (externe Hardwaretoken) an. Potenziell erscheinen auch Bankkarten und die deutsche Gesundheitskarte geeignet, allerdings können hier rechtliche oder technische Hürden bestehen. Während des Authentifizierungsvorgangs muss die externe Komponente Informationen mit dem Smartphone austauschen – die dafür nötige Kopplung stößt allerdings in der Praxis auf erhebliche Hürden:

– Eine drahtgebundene Kopplung kommt realistisch kaum in Betracht: Zum einen ist mangels einer einheitlichen (plattformübergreifend verfügbaren) Hardware-Schnittstelle (vgl. Abschnitt 4.2) Breitentauglichkeit nur erzielbar, indem das Token über verschiedene Hardware-Schnittstellen verfügt oder in Varianten produziert wird. Akzeptanzprobleme wären trotzdem zu erwarten, da bei Smartphones der drahtgebundene Anschluss externer Geräte nicht (wie bei PCs und Notebooks mit USB) als einfach und relativ verlässlich, sondern als unhandlich und eher fehleranfällig gilt: Viele Android-Geräte unterstützen USB OTG, trotzdem wird die Funktionalität oft nicht verwendet, da zusätzliche Adapterkabel benötigt werden oder die Softwareunterstützung für den intendierten Anwendungsfall mangelhaft ist.
– Die WLAN-Schnittstelle dient primär anderen Zwecken. Eine Umschaltung nur zur kurzzeitigen Nutzung eines externen Authentifizierungstokens würde ohne Modifikationen in den Smartphone-Betriebssystemen erhebliche Interaktion erfordern, also die Usability beeinträchtigen. Eine simultane Verbindung des Smartphones mit dem Authentifizierungstoken und dem entfernten Dienst wäre ggf. unmöglich. Schließlich bedeutet eine WLAN-Schnittstelle auch noch beträchtlichen Energiebedarf im Zusatzgerät, was dessen Größe und Gewicht sowie die Gefahr, dass im entscheidenden Moment der Akku leer ist, steigert. Daher bietet diese Schnittstelle für die hier diskutierte Integration keine adäquate Grundlage.
– Die NFC-Schnittstelle unterstützt Peripheriegeräte ohne eigene Energieversorgung (indem im Betrieb eine geringe, jedoch ausreichende Energiemenge induktiv, also drahtlos, übertragen wird) und wäre damit eigentlich die ideale Lösung für die hier diskutierte Kopplung. Auf beiden großen Smartphone-Plattformen bestehen jedoch weiterhin erhebliche Hürden, diesen Weg in der Praxis zu beschreiten (siehe Abschnitt 4.2).
– Bei der Bluetooth-Funkschnittstelle bestehen die für WLAN und NFC beschriebenen Probleme nicht – der Bluetooth-Standard wurde, insbesondere in seinen neueren Versionen, klar auf die Anforderungen kleiner Peripheriegeräte mit schmalem Energiebudget ausgerichtet und wird ohne kritische Einschränkungen auf beiden marktbestimmenden Smartphone-Plattformen unterstützt. Bluetooth-Geräte erfordern zwar eine eigene Energieversorgung mit dem dabei unvermeidlichen Usability-Minuspunkt der Batterie-Leer-Gefahr. Der Energiebedarf ist hier jedoch sehr gering und kann bei einem selten und kurzzeitig benutzten Gerät (was bei einer Authentifizierungskomponente ja gegeben ist) z. B. durch eine langlebige Knopfzelle gedeckt werden.

EXTERNE KOMPONENTEN:
HOHE SICHERHEIT MIT USABILITY-MINUS.

– Alternative Kopplungsmethoden zur Verbindung von Smartphone und Sicherheitstoken, z. B. optisch (Flackermuster oder Barcode auf dem Bildschirm) oder über den Headset-Klinkenstecker wurden in einzelnen Produkten z. T. erfolgreich angewendet, konnten aber keine ausreichende Popularität erreichen. Das gilt analog auch für Hardwaretoken nach dem zeitbasierten Einmalpasswort-Prinzip (Time-based One-Time Password, TOTP), die keine physische Kopplung mit dem Mobilgerät erfordern – stattdessen allerdings dauerhafte Batterieversorgung und stets genaue Uhrzeitsynchronisation.

Als geeignete Schnittstelle zur Ankopplung externer Hardware-Sicherheitskomponenten kann derzeit im Sinne der Breitentauglichkeit nur Bluetooth empfohlen werden. (Bei der konkreten Ausgestaltung der Kommunikation zwischen Smartphone und externer Sicherheitshardware müssen allerdings kürzlich aufgedeckte, in älteren Versionen der Bluetooth-Standardspezifikationen und entsprechenden Implementierungen ggf. vorhandene Sicherheitsmängel[25] berücksichtigt werden.)

Ein unvermeidbarer Usability-Minuspunkt jeder externen Komponente ist, dass diese neben dem Smartphone überhaupt als zusätzlicher Gegenstand mitgeführt werden muss – eine Bereitschaft zur Anschaffung und Nutzung derartiger Hardware-Sicherheitsschlüssel bzw. Lesegeräte kann wohl nur bei Diensten mit hohem Sicherheitsbedarf erwartet werden. Die Einbeziehung externer Sicherheitshardware ermöglicht jedoch auch, vom Hersteller zu verantwortende Schwachstellen des Smartphones (z. B. durch mangelnde Sicherheitsupdates) wirksam zu kompensieren, sodass ein sicherer Authentifizierungsprozess trotzdem gewährleistet bleibt. Ebenso können vom Smartphone-Hersteller verfügte Restriktionen, die die Nutzung etwaig eingebauter Sicherheitshardware des Smartphones (siehe Abschnitt 4.7) behindern, durch Rückgriff auf externe Sicherheitshardware wirksam ausgeglichen werden.

Die Akzeptanz externer Hardware-Sicherheitstoken wurde bisher auch dadurch behindert, dass diese lediglich als proprietäre, nur spezialisiert (und oft gar nicht mobil) einsetzbare Produkte verfügbar waren. Mit der Spezifikation und der aktuell laufenden breiten Umsetzung der Authentifizierungsstandards FIDO/WebAuthn (siehe Abschnitt 4.10) sowie deren Implementierung in mobiltauglichen Tokenprodukten entsteht hier gerade eine neue Situation, da Nutzer ein einmal angeschafftes Hardwaretoken für eine Vielzahl von Zwecken und Diensten (und z. T. auch sowohl mit Mobilgeräten als auch stationären PCs) einsetzen können. Der wahrgenommene Nutzen einer solchen Anschaffung steigt also an und die Hemmschwelle sinkt effektiv. Ein Beispiel hierfür ist das kürzlich von Google auf den Markt gebrachte Produkt »Titan Security Keys«[26], das primär im Rahmen der Google-Cloud-Dienste vermarktet wird, für welches aber auch (durch FIDO-Konformität) Nutzbarkeit für eine wachsende Zahl von anderen Diensten beworben wird.

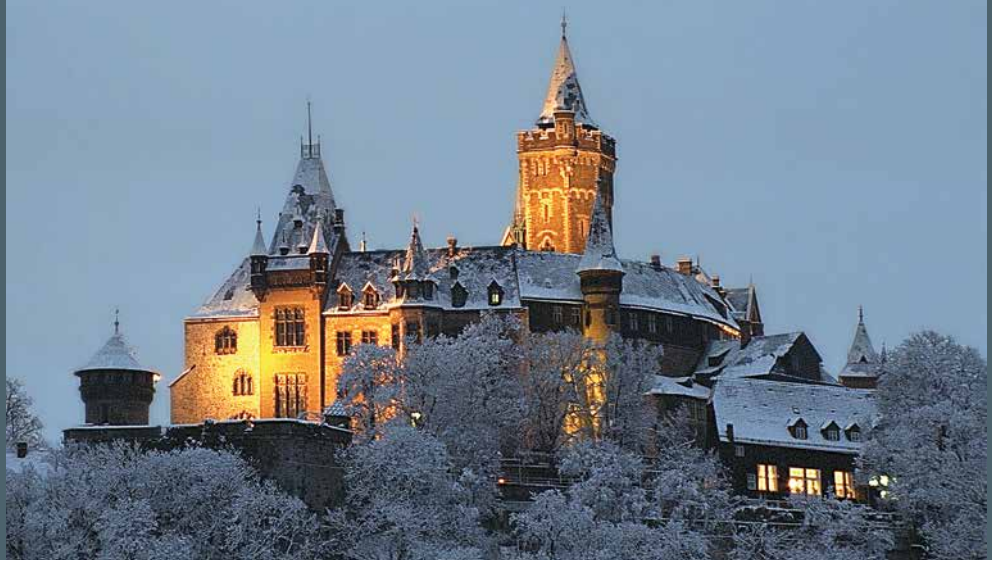
Externe Sicherheitstoken können bei substanziellem bis hohem Sicherheitsbedarf empfohlen werden; bei hohem Sicherheitsbedarf sollten sicherheitszertifizierte Komponenten verwendet werden, die nachgewiesenermaßen (z. B. durch eine Common Criteria-Zertifizierung) einem hohen Angriffspotenzial widerstehen. Für alle mit einem externen Hardwaretoken abgesicherten Dienste ist für den Fall des Tokenverlustes ein unabhängiger, anderweitig abgesicherter Ersatzzugang vorzusehen. Im einfachsten Fall ist dies ein zweites, ebenfalls registriertes Ersatztoken, das für diesen Zweck sicher zu verwahren ist.

4.7 HARDWARE-UNTERSTÜTZTE SICHERHEIT – INTERN

Moderne Smartphones werden herstellerseitig mit internen Hardware-Sicherheitskomponenten ausgerüstet, die ausgewählte, besonders sensible Daten, wie z. B. kryptografische

[25] https://www.kb.cert.org/vuls/id/304725/, abgerufen am 25. März 2019.

[26] https://cloud.google.com/security-key, abgerufen am 25. März 2019.



Schlüssel, mit deutlich erhöhter Sicherheit speichern und verarbeiten können. Diese Daten bleiben so vor Angriffen geschützt, selbst wenn das Smartphone ansonsten z. B. durch Malware kompromittiert ist. Einen sehr starken Schutz bietet ein im Mobilgerät verbautes Sicherheitselement (Secure Element), bestehend aus einem separaten Chip, der wie eine Smartcard einen Mikrocontroller, Speicherzellen sowie einen Krypto-Koprozessor (Spezialprozessor für kryptografische Berechnungen) enthält und durch spezielle Hardware-Sicherheitsmaßnahmen geschützt ist. Zunehmend bieten aber auch die CPUs von Smartphones selbst ähnliche Funktionalität in Gestalt eines abgegrenzten, gesicherten Subsystems innerhalb des Prozessor-Chips an (z. B. ARM TrustZone). Im Gegensatz zur ansonsten relativ offenen, durch Apps erweiterbaren Software-Ausstattung des Smartphones steht Software, die privilegierten Zugriff auf diese abgesicherten Bereiche hat bzw. darin ausgeführt wird (u. a. als »Trustlet« bezeichnet), wie das Betriebssystem des Mobilgerätes unter strikter Kontrolle des Herstellers. Durch diese im Interesse der Sicherheit sinnvolle Einschränkung sind allerdings auch nur die Gerätehersteller in der Position, die beträchtlichen Chancen, die interne Sicherheitshardware für die Unterstützung sicherer mobiler Authentifizierungsprozesse bietet, auch tatsächlich nutzbar zu machen. Eine herstellerübergreifende Initiative hierzu ist bisher nicht in Sicht:

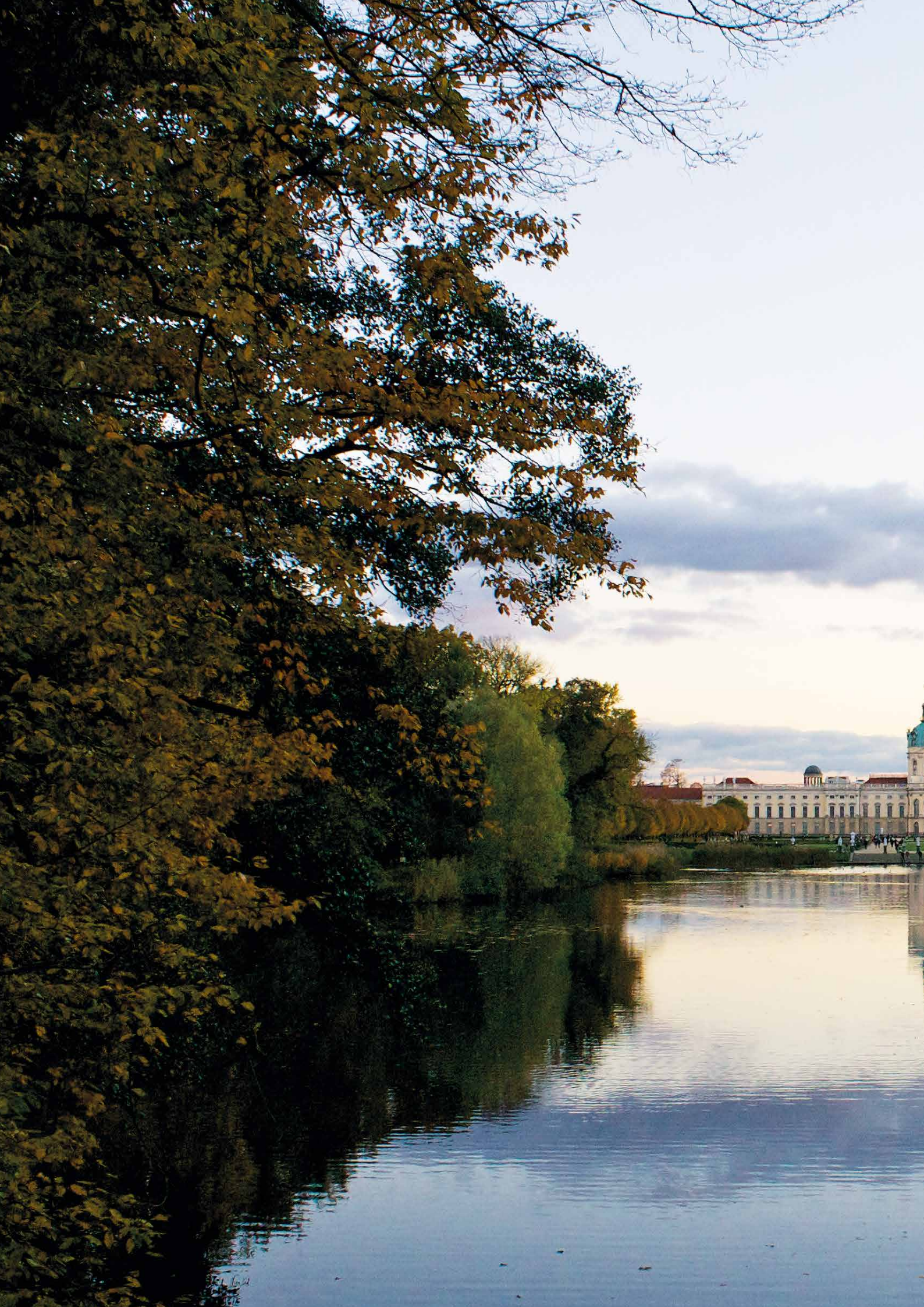
- Die iOS-Plattform bringt hardwareseitig seit Längerem gute Voraussetzungen mit, durch die restriktive Haltung von Apple kann die vorhandene Sicherheitshardware jedoch nur sehr eingeschränkt für herstellerfremde Zwecke genutzt werden.
- In der fragmentierten Android-Welt ist die Hardwaresituation uneinheitlich. Einige Hersteller statten ausgewählte Smartphones mit Sicherheitselementen aus oder nutzen die ggf. vorhandenen CPU-Funktionalitäten zur Verwaltung sicherer Bereiche. Eine vereinheitlichte und breite Initiative ist von einem entsprechenden Vorstoß des Plattformanbieters Google abhängig. Mit der im August 2018 veröffentlichten Android-Version 9 («Pie«) wurden hierfür die Grundlagen geschaffen: Das Betriebssystem wurde nicht nur dahingehend erweitert, dass kryptografische Schlüssel in einer sogenannten »Strongbox« nachweislich geschützt gespeichert und verrechnet werden, sondern es enthält jetzt neuerdings auch eine »Protected Confirmation«-genannte Funktion, die eine kryptografisch abgesicherte interaktive Transaktionsbestätigung durch den Nutzer ermöglicht. Durch die Hardware-Absicherung ist eine Fälschung dieser Interaktion oder ein illegitimer Zugriff auf das geschützte Schlüsselmaterial somit sehr stark erschwert, selbst wenn das Smartphone ansonsten z. B. durch Malware kompromittiert ist[27]. Weiterhin wird Geräteherstellern, die das Google-Kompatibilitätssiegel erhalten wollen, nunmehr »stark empfohlen«, Common-Criteria-zertifizierte Sicherheitshardware im Gerät zu verbauen[28]. Somit werden zumindest in naher Zukunft wesentliche Bausteine für eine Authentifizierung, die konsequent durch interne Sicherheitshardware des Smartphones geschützt ist, auf der Android-Plattform breit verfügbar.

Falls in der Zukunft beide marktbestimmenden Smartphone-Hersteller die Voraussetzungen schaffen, die in den Geräten vorhandene Hardware-Sicherheitsfunktionalität für eine sichere Authentifizierung bei beliebigen Dienstanbietern einsetzbar zu machen, kann dieser Weg für Dienste mit bis zu substanziellem Sicherheitsbedarf klar empfohlen werden sowie für hohen Sicherheitsbedarf, falls im Smartphone ein separates Sicherheitselement verbaut ist, dessen Widerstandsfähigkeit gegen hohes Angriffspotenzial durch eine Zertifizierung belegt ist. Erfüllung dieser Voraussetzungen erscheint derzeit nur durch Umsetzung der offenen Protokollstandards FIDO/Webauthn realistisch (vgl. Abschnitt 4.10). Mittelfristig dürften alle Gerätehersteller daran interessiert sein, den Sicherheitsmehrwert der jetzt verbauten Hardware für den Endkunden umfassend sichtbar zu machen.

---

[27] https://developer.android.com/about/versions/pie/android-9.0#security, abgerufen am 25. März 2019.

[28] https://source.android.com/compatibility/android-cdd#9_11_keys_and_credentials, abgerufen am 25. März 2019.



BIOMETRIEFAKTOREN: BEI ERFOLGREICHER FÄLSCHUNG DAUERHAFT »VERBRANNT«.

Wird im Smartphone fest installierte Sicherheitshardware im Authentifizierungsprozess genutzt, ist das Gerät selbst Besitzfaktor. Um einen Fremdzugriff bei Diebstahl des Geräts auszuschließen, ist die Einbeziehung mindestens eines weiteren (Wissens- oder Inhärenz-)Faktors notwendig, der während des Authentifizierungsvorgangs abgefragt wird oder zumindest den initialen Gerätezugang absichert (Displaysperre). Für alle mit dieser Faktorenkombination abgesicherten Dienste sollte allerdings für den Fall des Geräteverlusts ein unabhängiger, anderweitig abgesicherter Ersatzzugang verfügbar sein.

4.8 BIOMETRIE

Biometrische Verfahren wie Fingerabdruck-, Iris-, Gesichts- oder Stimmerkennung ermöglichen eine Bestätigung der Nutzeridentität durch individuelle körperliche Merkmale. Die Entwicklung entsprechender Sensoren und Analyseverfahren ist inzwischen sehr weit vorangeschritten – stark verringerter Platz- und Energiebedarf haben bereits verbreitet die Integration von Fingerabdruckscannern und Gesichtserkennung in Smartphones ermöglicht, bei hoher und weiter steigender Verlässlichkeit der Erkennung. Allerdings werden fehlerhafte Identifikationen auch zukünftig nicht auszuschließen sein, insbesondere solange nicht durchgängig Lebenderkennungsfunktionalität[29] integriert ist.

Die Verwendung biometrischer Inhärenzfaktoren in einem Authentifizierungsprozess erscheint aus Nutzersicht bei effizienter und ausreichend verlässlicher Umsetzung sehr bequem und wird daher aktuell immer populärer. Sie bleibt allerdings prinzipiell dadurch fragwürdig, dass – im Gegensatz zu allen Wissens- oder Besitzfaktoren – der Besitzer nicht die Möglichkeit hat, einen einmal kompromittierten Biometriefaktor einfach zu ersetzen. Sobald sich bei einer in vielen Geräten verbauten Biometrieerkennung eine Schwäche zeigt, die einem Angreifer ermöglicht, das Vorhandensein des Inhärenzfaktors erfolgreich vorzutäuschen und die Schwäche nicht z. B. durch ein Update nachträglich behebbar ist, muss der Faktor dauerhaft als »verbrannt« gelten.

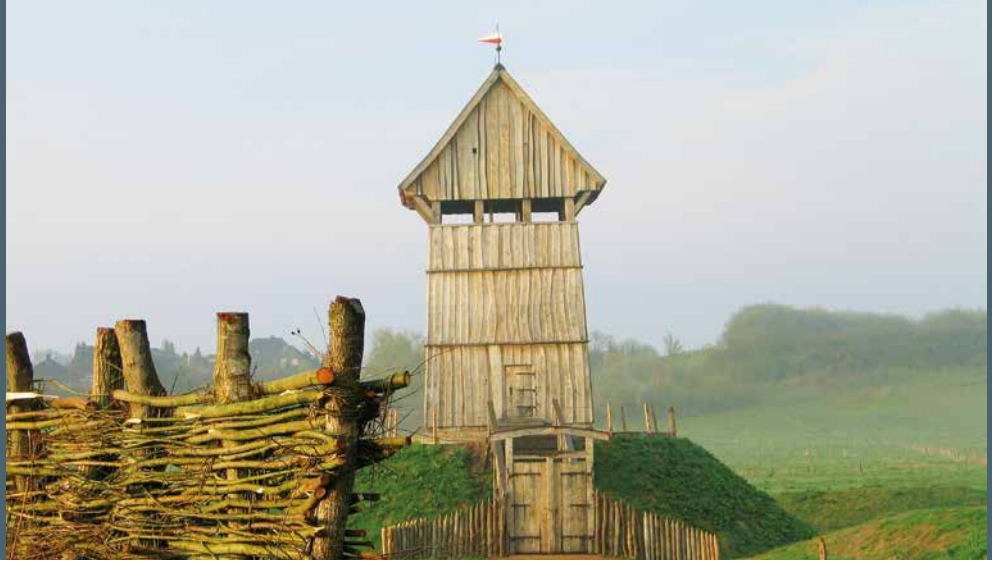
Seit Jahren werden trotz ständiger Weiterentwicklung bei vielen von in Mobilgeräten eingesetzten (und somit erheblichen Größen-, Kosten- und Energiebeschränkungen unterliegenden) Biometrietechnologien bereits kurz nach deren Erscheinen erfolgreiche und oft mit erstaunlich geringem Aufwand durchführbare Angriffe gemeldet[30]. Selbst als sicherer geltende Verfahren wie die Handvenen-Erkennung wurden bereits mit relativ simplen Mitteln gebrochen[31].

Erfolgreiche Biometriehacks waren bisher gezielte Angriffe, bei denen biometrische Merkmale eines legitimen Nutzers auf ein Ersatzmedium kopiert wurden, welches (nur) vom Sensor nicht als gefälscht erkannt wird. Kürzlich wurde jedoch eine neue und prinzipiell andere Kategorie von Angriffen bekannt, die ohne kopierte Biometriemerkmale individueller Nutzers auskommt und sich potenziell gegen alle Nutzer richtet: Mithilfe maschineller Lernverfahren werden generelle Schwächen des von einem gegebenen Biometriesensor verwendeten Erkennungsalgorithmus identifiziert, und auf dieser Basis wird ein Biometriedatenmuster (z. B. ein Fingerabdrucksbild) synthetisch erzeugt, das einem Masterschlüssel ähnelt: Damit kann jeder baugleiche Sensor mit einer gewissen Erfolgswahrscheinlichkeit getäuscht werden, ohne dass ein existierendes, beim Sensor als

[29] Zusätzlich zur Erkennung eines statischen Musters (wie Fingerabdruck oder Irisgeometrie) wird hierbei versucht, auch festzustellen, ob das präsentierte Objekt tatsächlich ein Körperteil einer lebenden Person ist.

[30] Gesichtserkennung: https://www.forbes.com/sites/thomasbrewster/2018/12/13/we-broke-into-a-bunch-of-android-phones-with-a-3d-printed-head/#70facf7e1330, abgerufen am 25. März 2019.
Fingerabdruckerkennung: https://www.syss.de/pentest-blog/2018/hacking-fingerprint-readers-without-making-a-mess/, abgerufen am 25. März 2019.
Iriserkennung: https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security, abgerufen am 25. März 2019.

[31] Venenerkennung: http://www.spiegel.de/netzwelt/gadgets/biometrie-hack-venen-scanner-fallen-auf-wachshaende-herein-a-1243583.html, abgerufen am 25. März 2019.



legitim registriertes Nutzer-Biometriemuster dem Angreifer bekannt sein muss. Es handelt sich also um einen skalierbaren Angriff (der allerdings physischen Gerätezugriff erfordert und dadurch in der Praxis limitiert ist). Auch wenn die derzeit erzielbare Erfolgswahrscheinlichkeit von etwa 20 Prozent (allerdings bei einem Biometriesensor, der eigentlich nicht mehr als 0,1 Prozent falsch positive Erkennungen liefern darf!) nicht allzu hoch ist, wird die Eignung von Biometrieerkennung für Authentifizierungszwecke dadurch zusätzlich stark infrage gestellt[32].

In einem Authentifizierungsprozess mit substanziellem oder hohem Sicherheitsniveau (z. B. für Bezahlsysteme/Banking) sollte Biometrie wegen dieser vielfachen und erheblichen Unsicherheitsfaktoren daher trotz der Usability-Vorteile niemals den primären oder gar einzigen Faktor bilden, sondern nur eine ergänzende Rolle spielen – eine Empfehlung, die inzwischen auch von manchen Mobilgeräteherstellern geteilt wird. Für den Fall, dass eine Sicherheitsschwäche der Biometriekomponente nicht behebbar ist, muss es dem Nutzer stets möglichsein, einen dann unnützen Biometriefaktor dauerhaft zu sperren und durch einen Besitz- oder Wissensfaktor zu ersetzen[33].

4.9 SINGLE SIGN-ON (SSO)

Sowohl Google als Smartphone-Plattformanbieter als auch Anbieter verbreitet genutzter cloudbasierter Dienste wie Facebook und Twitter sind zusätzlich als Identitätsprovider tätig und haben ihre Authentifizierungsmechanismen zur Nutzung durch Drittanbieter geöffnet, die auf diese Weise den Zugriff auf ihre eigenen Dienste kontrollieren können. Auch Apple betreibt mit Apple ID einen Identitätsservice, der allerdings nur zur Authentifizierung bei diversen von diesem Unternehmen selbst betriebenen Onlinediensten genutzt werden kann. Die so erzielte Einheitlichkeit (Anwendung eines bereits bekannten und häufig genutzten Authentifizierungsprozesses auf viele Dienste) ist aus Sicht des Endnutzers ein klarer Pluspunkt bei der Usability. Wenn der jeweilige Identitätsprovider besonders sichere Mechanismen zur Authentifizierung anbietet, wird diese zusätzliche Sicherheit bei allen den Provider nutzenden Diensten wirksam, ohne dass deren Anbieter in eigene Authentifizierungslösungen investieren und diese ständig aktuell halten müssen. Dem stehen jedoch auch Nachteile gegenüber: Der Nutzer öffnet zusätzliche Teile seines Internet-Nutzungsprofils dem Identitätsprovider (bisher meist einem US-Internetkonzern) mit zumindest schwer absehbaren und kontrollierbaren Folgen für den Schutz der Privatsphäre. Aber auch für den Dienstanbieter können Nachteile aus den so verfügbaren Daten resultieren, da diese Daten dem Identitätsprovider nutzerindividuelle Rückschlüsse auf Nutzungshäufigkeit und -verteilung des abgesicherten Dienstes erlauben. Zudem können z. T. proprietäre Protokolle und Schnittstellen einen eventuell später gewünschten Wechsel zu einem anderen Identitätsprovider erschweren.

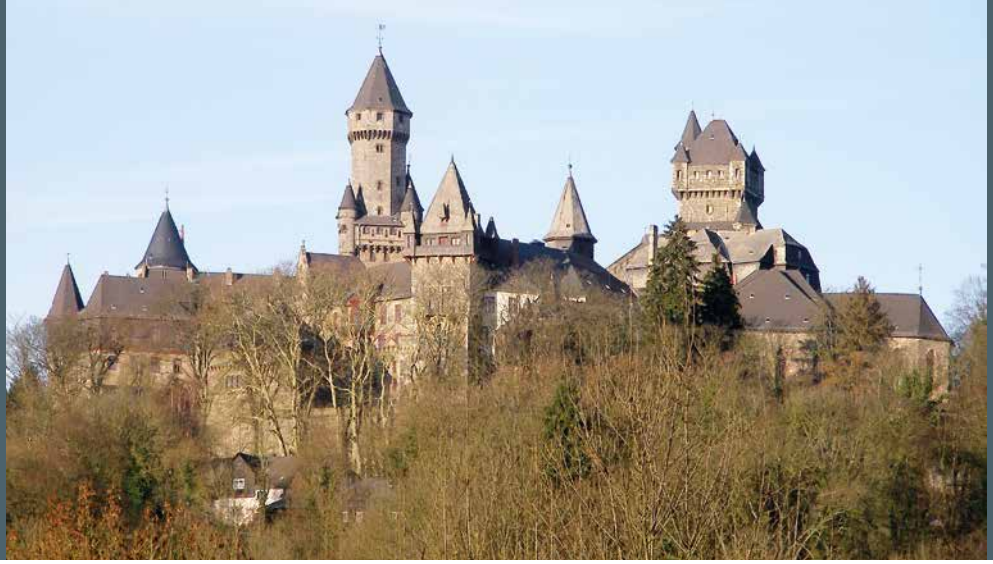
Single Sign-on verbindet lediglich den abzusichernden Dienst mit einem oder mehreren durch den Identitätsprovider dem Endnutzer angebotenen konkreten Authentifizierungsverfahren. Daher sind zur Sicherheit dieses Ansatzes keine generellen Aussagen möglich. Die theoretische zusätzliche Angriffsmöglichkeit, bei der der Angreifer dem Dienstanbieter nur vortäuscht, dass die Authentifizierung beim Identitätsprovider erfolgreich abgeschlossen wurde, ist bei Nutzung moderner, offener und sicherer Protokollstandards (vor allem OAuth und OpenID Connect) jedoch praktisch ausgeschlossen.

SSO kann daher für die Realisierung eines mobilen Authentifizierungsverfahrens empfohlen werden, wenn der SSO-Anbieter Authentifizierungsverfahren anbietet, die dem Sicherheitsbedarf der jeweiligen Anwendungsdienste angemessen sind – aber auch sonstige Anforderungen, wie der Schutz der Privat-

---

[32] »DeepMasterprints«: https://www.theguardian.com/technology/2018/nov/15/fake-fingerprints-can-imitate-real-fingerprints-in-biometric-systems-research, abgerufen am 25. März 2019.
https://arxiv.org/pdf/1705.07386.pdf, abgerufen am 25. März 2019.

[33] C. Busch, H.-W. Heibey, G. Quiring-Kock, T. Kniess; H: Herzog: Biometrische Authentisierung. TeleTrusT Deutschland e.V., 2010.



sphäre des Endnutzers durch den Identitätsprovider erfüllt sind. (Siehe auch Abschnitt 4.11.)

Generell zielt Single Sign-on zumindest in den bisher realisierten Ausprägungen auf (jeweils bei einem Identitätsprovider) zentralisiertes Identitätsmanagement inklusive Authentifizierung ab. Diesem Anbieter fällt also erhebliche Verantwortung bezüglich der Identitätsinformationen aller registrierten Nutzer zu. Die aus einem zentralisierten Modell bezüglich des Datenschutzes resultierenden Gefahren können vollständig nur durch alternative, von Grund auf dezentrale Ansätze ausgeschlossen werden, bei welchen die Nutzer selbst die Hoheit über ihre Daten behalten. Es existieren Initiativen, die sich diesem auch unter dem Begriff »Selbst-souveräne Identitäten« bekannten Ziel verschrieben haben, z. B. ID4me[34] (Identitätsmanagement basierend auf dem Internet-Namensverwaltungssystem DNS) und Sovrin[35] (Blockchain-basiertes Identitätsmanagement). Bisher scheinen diese Projekte überwiegend auf die Verwaltung an die Identität geknüpfter, für Anwendungsdienste relevanter Attribute fokussiert zu sein und das Thema Authentifizierung noch nicht abzudecken. Insgesamt ist ihre technische Entwicklung auch noch in einem relativ frühen Stadium. Daher kann ihre Bedeutung für das hier im Vordergrund stehende Thema derzeit nicht bewertet werden.

4.10 OFFENE PROTOKOLL-STANDARDS FÜR DIE AUTHENTIFIZIERUNG

Wegen der Vielzahl alltäglich genutzter Dienste und IT-Ressourcen wird die Einheitlichkeit der Authentifizierungsprozesse für Nutzer immer wichtiger. Auch auf Dienstbetreiberseite ist es vorteilhaft, für Authentifizierungsprozesse auf einheitliche und (insbesondere in puncto Sicherheit) bewährte Ansätze zurückgreifen zu können, ohne sich jedoch zu stark an konkrete Anbieter zu binden. Aus diesen Motivationen heraus wurden seit einigen Jahren offene Protokollstandards für Authentifizierung (und allgemeiner Identitätsmanagement) entwickelt. Diese spezifizieren die zu benutzenden Datenformate und Kommunikationsprozesse, auch bezüglich sicherheitsrelevanter Details wie der zur Verschlüsselung des Datenaustauschs genutzten kryptografischen Verfahren. Relevant sind hier vor allem folgende Standards:

- **OAuth**[36] als ältester der hier aufgeführten Standards ist nicht primär auf Authentifizierung fokussiert, sondern auf die Autorisierung (also die Gewährung von Rechten) externer Dienste, auf Daten des Nutzers, die von einem bereits genutzten Dienst verwaltet werden, ebenfalls zuzugreifen. Dazu werden sogenannte Autorisierungstoken[37] vergeben, die beispielsweise einen Fotodruck-Service temporär dazu berechtigen, ausgewählte Fotos abzurufen, die ein Nutzer in seinem Bereich in einem sozialen Netzwerk archiviert hat. Es handelt sich also primär um einen Mechanismus zur Zugriffsdelegierung im Auftrag des Nutzers.
- **OpenID Connect**[38] baut auf zentrale OAuth-Mechanismen auf und erweitert diese mit klarem Fokus auf »sichere Authentifizierung als Dienst«. OpenID Connect ist eine verlässliche Basis für Single-Sign-on-Angebote und wird hierfür bereits seit mehreren Jahren u. a. von Google eingesetzt.
- **Der FIDO**[39]-Standard regelt (im Unterschied zu den bisher genannten Standards, die primär die Kommunikation zwi-

[34] https://id4me.org/, abgerufen am 25. März 2019.

[35] https://sovrin.org/, abgerufen am 25. März 2019. https://jolocom.io/, abgerufen am 25. März 2019.

[36] https://oauth.net/2/, abgerufen am 25. März 2019.

[37] In diesem Kontext steht »Token« nicht für eine Hardwarekomponente sondern ein Datenobjekt, konkret eine große zufällig generierte und dadurch nicht »erratbare« Zahl.

[38] https://openid.net/connect/, abgerufen am 25. März 2019.

[39] https://fidoalliance.org/, abgerufen am 25. März 2019. Die ursprüngliche Bedeutung der Abkürzung »Fast IDentity Online« wird den tatsächlichen technischen Zielen nicht mehr gerecht. Real spielen personenbezogene Identitätsinformationen nämlich in den FIDO-Protokollen keine Rolle, es geht ausschließlich um einen sicheren und datensparsamen Authentifizierungsprozess.

FIDO/WEBAUTHN: VIELVERSPRECHENDE ABLÖSUNG FÜR DAS PASSWORT.

schen Anwendungsdienst und Identitätsprovider organisieren) konkrete Details des eigentlichen Authentifizierungsvorgangs. Hierbei kommuniziert das vom Nutzer verwendete Endgerät mit dem durch die Authentifizierung geschützten Dienst so, dass der kryptografische Originalschlüssel des Benutzers (dessen Besitz den eigentlichen Authentifizierungsfaktor darstellt) niemals übertragen wird. Somit verfügt der Dienstanbieter gar nicht erst über missbrauchsgeeignete Authentifizierungsgeheimnisse der Nutzer – eine entsprechende Diebstahlsgefahr und skalierbare Angriffe sind daher ausgeschlossen. Für FIDO ist es irrelevant, ob der durch die Authentifizierung geschützte Dienst ein tatsächlicher Anwendungsdienst ist, auf den der Nutzer zugreifen möchte, oder ein zwischengeschalteter Single-Sign-on-Dienst eines Identitätsproviders. FIDO schützt zusätzlich auch die Privatsphäre des Nutzers, indem dienstübergreifende Verfolgung des Nutzers (Tracking) technisch unmöglich gemacht wird und persönliche Daten des Nutzers im Authentifizierungsprozess keine Rolle spielen – somit speichern z. B. auch FIDO-konforme Hardware-Authentifizierungstoken niemals derartige Daten.

- **Web Authentication (WebAuthn)**[40], ein kürzlich in Kooperation mit dem FIDO-Konsortium verabschiedeter W3C[41]-Standard, integriert eine weiterentwickelte Form von FIDO nahtlos in die Infrastruktur des World Wide Web. Alle großen Browserhersteller haben bereits Unterstützung angekündigt oder sogar entsprechende Beta-Versionen veröffentlicht[42]. Auch serverseitig werden dank der auf dem Wege befindlichen Standardisierung in absehbarer Zeit leicht integrierbare Unterstützungskomponenten verfügbar werden. Für geeignete Fälle unterstützt WebAuthn über den Funktionsumfang von FIDO hinaus zusätzlich ein passwortloses (Ein-Faktor-) Login mittels Biometrie oder Hardware-Token. Dieses wurde kürzlich bereits in das Authentifizierungs-Subsystem »Windows Hello« von Microsoft integriert[43].

Da FIDO absehbar im WebAuthn-Standard aufgeht, wird im Folgenden stets die gemeinsame Form »FIDO/WebAuthn« verwendet.

Die Kombination von OAuth und OpenID Connect bildet eine sehr gute Basis für den Datenaustausch zwischen Anwendungsdiensten und Identitätsmanagementdiensten, z. B. einem Single-Sign-on-Dienst. Eine zusätzliche Kombination mit FIDO/WebAuthn schaltet Gefahren bezüglich missbrauchsfähiger Authentifizierungsgeheimnisse des Endnutzers beim Identitätsmanagement-Dienstleister aus, da diese dort nicht mehr gespeichert werden.

FIDO/WebAuthn hat das Potenzial, endlich die Ablösung des Passworts als verbreiteter Authentifizierungsmethode einzuleiten. Der client-seitige Teil von FIDO/WebAuthn kann einerseits komplett in Software realisiert werden, z. B. als Komponente einer App, andererseits erlaubt der Standard auch eine durch interne oder externe Sicherheitshardware unterstützte Ausführung sicherheitskritischer Teile des Verfahrens. Geeignete externe Hardwaretoken sind bereits am Markt verfügbar, einige davon sind dank Bluetooth- oder NFC-Schnittstelle auch mobiltauglich.

Eine entscheidende Voraussetzung für die breite Nutzung von FIDO/WebAuthn wird sein, dass Protokollunterstützung nicht nur im Webbrowser sondern auf Plattformebene gegeben ist, also in den Software Development Kits (SDKs) der Mobil-Betriebssysteme – und idealerweise unter Nutzung der im Gerät vorhandenen Sicherheitshardware. Google wurde hier bereits

[40] https://www.w3.org/TR/webauthn/, abgerufen am 25. März 2019. Synonym wird für WebAuthn bisweilen auch FIDO2 genannt.

[41] World Wide Web Consortium.

[42] https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.en, abgerufen am 25. März 2019.

[43] https://www.microsoft.com/en-us/microsoft-365/blog/2018/04/17/windows-hello-fido2-security-keys/, abgerufen am 25. März 2019.

SIM-GESTÜTZTE AUTHENTIFIZIERUNG: BESONDERS BEQUEM – ABER NOCH NICHT VERFÜGBAR.

initiativ und erhielt kürzlich eine FIDO2-Zertifizierung[44], die (nach einem Update) die gesamte Android-Plattform ab Android 7 abdeckt. Details dazu, insbesondere zur etwaigen Einbindung von Hardware-Sicherheitsfeatures, sind allerdings bisher nicht bekannt.

Auf der iOS-Plattform kann FIDO/WebAuthn absehbar nur rein softwaremäßig (also ohne Hardware-Absicherung und somit angreifbar) oder mittels via Bluetooth gekoppelter externer Hardware-Token realisiert werden, es sei denn, der Plattformanbieter schafft zukünftig ebenfalls hinreichende Unterstützung im Betriebssystem (Nutzung der internen Sicherheitshardware oder Öffnung der NFC-Schnittstelle).

FIDO/WebAuthn-gestützte Authentifizierung mit Hardware-Unterstützung kann für Dienste bis zu substanziellem Sicherheitsbedarf empfohlen werden sowie bis zu hohem Sicherheitsbedarf, wenn zertifizierte Sicherheitshardware genutzt wird, die nachgewiesenermaßen einem hohen Angriffspotenzial widersteht.

4.11 UNGENUTZTE POTENZIALE: SIM-KARTE UND MOBILFUNK-NUTZERIDENTITÄT

In jedem Smartphone repräsentiert die SIM-Karte den im Mobilfunknetz angemeldeten Nutzer und schützt dessen Verfügungsgewalt über den Anschluss durch vom restlichen Gerät abgeschirmte, gegen Manipulationen und Fälschung gesicherte Hardware.

Die erfolgreich im Netz registrierte SIM-Karte ist normalerweise im Gerät eingesteckt, aber meist wechselbar und insofern zwischen interner und externer Hardware-Sicherheitsfunktionalität angesiedelt. (Nur in einigen neuen Geräten ist stattdessen eine vom Netzbetreiber ferngesteuert konfigurierbare eSIM fest verbaut, deren Funktion und Rolle ansonsten jedoch sehr ähnlich ist. Der SIM-Kartenwechsel erfolgt in diesem Fall virtuell.) Die SIM-Karte bildet in jedem Fall einen besonders bequemen (da mit dem Smartphone eine physische Einheit bildenden) Besitzfaktor zur Absicherung mobiler Authentifizierungsprozesse. Sie kann allerdings durch den Mobilfunkbetreiber neuausgestellt, also kopiert werden, woraus zusätzliche Gefahren erwachsen (vor allem »Social-Engineering«-Attacken, vgl. Abschnitt 4.4). Diesen sollte durch flankierende Verwendung eines Wissens- oder Inhärenzfaktors begegnet werden.

Ein SIM-gestütztes Authentifizierungsverfahren kann nur durch die Mobilfunkbetreiber etabliert werden, einerseits da sie die Hoheit über die auf den SIM-Karten bzw. eSIMs laufende Software und die dort gespeicherten Informationen haben, andererseits auch, weil hierfür netzseitig ein dedizierter Authentifizierungsdienst betrieben werden muss. Durch ihren – seit November 2016 in Deutschland gesetzlich vorgeschriebenen[45] – kompletten Durchgriff auf die reale Identität jedes Nutzers bietet sich den Netzbetreibern aber auch einzigartiges Potenzial für weiterreichende Identitätsmanagement-Angebote an Endnutzer und Dienstanbieter.

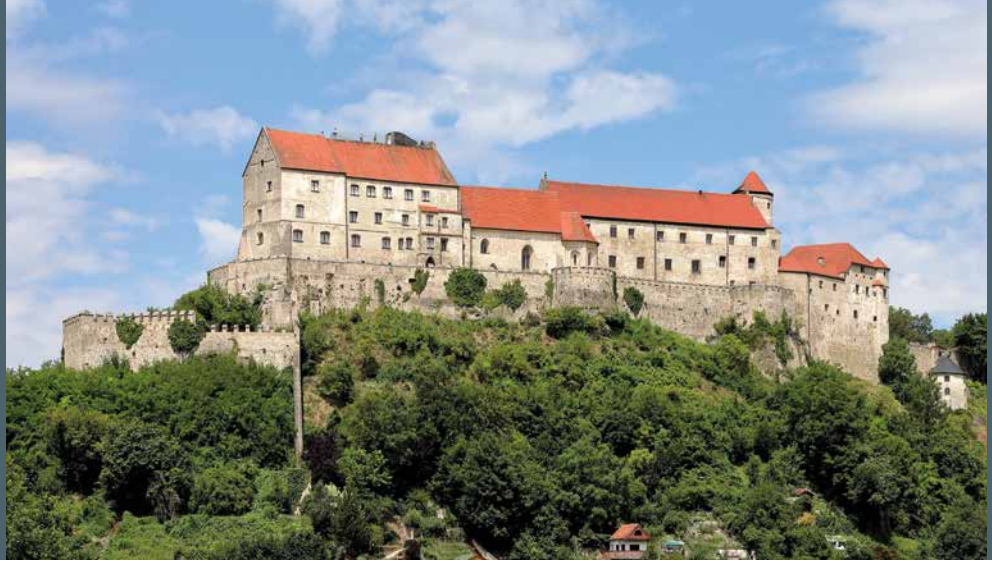
Mobile Connect

Mit dem Mobile-Connect-Standard des internationalen Mobilfunk-Betreiberverbandes GSMA[46] steht seit 2015 die zentrale technische Grundlage (basierend auf einer minimal angepassten Version des OpenID-Connect-Standards) zur Verfügung, um Mobilnetzbetreiber nicht nur als Datenübertragungsdienstleister, sondern auch als Identitätsprovider zwischen Mobilfunk-

[44] https://fidoalliance.org/android-now-fido2-certified-accelerating-global-migration-beyond-passwords/, abgerufen am 25. März 2019.

[45] Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus, Bundesgesetzblatt Jahrgang 2016 Teil I Nr. 37, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl116s1818.pdf, abgerufen am 25. März 2019.

[46] https://www.gsma.com/identity/mobile-connect, abgerufen am 25. März 2019.



kunden und Dienstanbietern vermitteln zu lassen. Die in anderen Ländern bereits erfolgreich eingesetzte Technologie wartet in Deutschland jedoch bisher weiter auf den Roll-out.

Das Zeitfenster, um auch in Deutschland mit Mobile Connect bereits vorhandene Sicherheitshardware in den Dienst sicherer mobiler Authentifizierung zu stellen und gleichzeitig unter Nutzung der bei den Mobilfunkbetreibern bereits verfügbaren Informationen beim Identitätsmanagement voranzukommen, wird nur noch begrenzte Zeit offen sein. Smartphones verfügen inzwischen zunehmend unabhängig von der SIM-Karte auch über integrierte Hardware-Sicherheitsfeatures, die ebenfalls das Potenzial haben, hier einen Durchbruch zu bewirken. Die Ankündigung von Telefonica, Vodafone und Deutsche Telekom vom Februar 2018, den Mobile-Connect-Dienst noch im selben Jahr einzuführen – und zwar in Partnerschaft mit der Single-Sign-on-Initiative Verimi (siehe Abschnitt 4.12) – vermittelte hier Zuversicht, allerdings wurde die Ankündigung bis jetzt (April 2019) noch nicht umgesetzt. Problematisch erscheint auch, dass bisher alle in Deutschland operierenden Mobilfunkbetreiber lediglich die Einführung der Basis-Ausbaustufe »Mobile Connect Basic« des Mobile-Connect-Dienstes vorsehen[47]. Die Ausbaustufe »Mobile Connect Authenticate Plus« (die laut GSMA in allen anderen 30 Ländern, in denen Mobile Connect bereits im operativen oder Pilotbetrieb ist, realisiert ist)[48] unterstützt zusätzlich eine Zwei-Faktor-Authentifizierung, wobei auch der zweite Faktor (PIN-Überprüfung) vom Hardwareschutz durch die SIM-Karte profitieren und so sicher gegen Kompromittierung des Smartphones bleiben kann. Zwar ist eine Kombination mit einem zweiten Authentifizierungsfaktor auch auf Anwendungsebene möglich, äquivalente Sicherheit ist dann aber nur durch Einbindung zusätzlicher externer oder interner Sicherheitshardware erzielbar.

Die bisher für Deutschland vorgesehene Basisfunktion »Mobile Connect Authenticate« ist kaum sicherer als SMS-TAN. (Falls für den Wechsel zur »Plus«-Variante ein SIM-Kartenaustausch erforderlich ist, könnte der an höherer Sicherheit interessierte Nutzer dafür ggf. auch selbst aufkommen.)

Mobile Connect kann nach bisher vorliegenden Informationen zur Absicherung von Diensten mindestens bis zu substanziellem Sicherheitsbedarf empfohlen werden.

Führende amerikanische Mobilfunkbetreiber planen aktuell die US-Markteinführung eines zu Mobile Connect interoperablen mobilen Authentifizierungsdienstes, der gegenüber dem existierenden Standard sogar ein noch höheres Sicherheitsniveau erreichen soll.[49]

4.12 EUROPÄISCHE SINGLE-SIGN-ON-INITITATIVEN

In den letzten Jahren wurden die Themen Datenschutz und Privatsphäre in Deutschland und Europa stärker thematisiert, insbesondere im Licht der weitgehenden Marktdominanz US-amerikanischer Internetkonzerne sowie der Snowden-Enthüllungen. Konkret für das Thema Identitätsmanagement und Single Sign-on wurde ein klarer Bedarf nach unabhängigen und in Europa beheimateten Lösungen identifiziert. Unter dieser Prämisse starteten die deutschen bzw. europäischen Single-Sign-on-/Identitätsmanagement-Industrieallianzen Verimi[50], NetID[51] und YES[52], welche nach Schaffung der technischen Grundlagen z. T. bereits um Nutzer werben. Neben den erwähnten Datenschutz-

[47] https://developer.mobileconnect.io/operators, abgerufen am 25. März 2019.

[48] https://developer.mobileconnect.io/operators, abgerufen am 25. März 2019.

[49] https://www.prnewswire.com/news-releases/att-sprint-t-mobile-and-verizon-unveil-next-generation-mobile-authentication-platform-details-300606054.html, abgerufen am 25. März 2019.

[50] https://verimi.de/de, abgerufen am 25. März 2019.

[51] https://enid.foundation/, abgerufen am 25. März 2019.

[52] https://www.it-finanzmagazin.de/yes-sparkasse-identity-checkout-datenschutz-60434/, abgerufen am 25. März 2019.

SSO: STRATEGISCHE PARTNERSCHAFTEN ENTSCHEIDEND.

Pluspunkten werden gegenüber den global etablierten US-Anbietern auch erweiterte Identitätsmanagement-Funktionalitäten ins Feld geführt, vor allem die Möglichkeit, eigene Identitätsattribute wie z. B. die Postadresse kontrolliert, sicher und bequem an Dienstbetreiber (z. B. Onlineshops) übergeben zu können. Verimi und NetID setzen bei der Kommunikation zum Anwendungsdienstbetreiber auf die offenen Protokollstandards OAuth und OpenID Connect. Eine Sonderstellung nimmt die auf den Bankingbereich fokussierte YES-Initiative ein: Sie bietet zwar auch SSO-Funktionalität, verfolgt aber darüber hinaus nicht nur im Identitätsmanagement besonders weitreichende Ziele, z. B. Weitergabe von Informationen zur Kreditwürdigkeit. Sie strebt darüber hinaus auch an, sich unmittelbar in die Abwicklung von Transaktionen zwischen Händlern und Kreditinstituten einzuschalten und primär darauf ihr Geschäftsmodell aufzubauen. Bei allen anderen Allianzen ist anzunehmen, dass die kommerzielle Weitergabe von Nutzerprofildaten, in unterschiedlichen Ausprägungen, zumindest eine Komponente des Geschäftsmodells darstellt, um ein für den Endnutzer kostenloses Angebot zu ermöglichen.

Bezüglich des erreichbaren Sicherheitsniveaus der angebotenen Authentifizierung nimmt von den bisher diskutierten Anbietern aktuell – soweit dazu Informationen veröffentlicht wurden – Verimi eine Führungsposition ein: Bisher unterstützt nur dieser Anbieter eine mobile Zwei-Faktor-Authentifizierung (mittels Biometrie und zukünftig auch über Mobile Connect). Die geplante Integration von Mobile Connect als Authentifizierungsmethode in diesen Dienst[53] verspricht außerdem hervorragende Breitentauglichkeit, falls das Verfahren zukünftig tatsächlich wie geplant von allen Mobilfunkkunden in Deutschland genutzt werden kann. Aber auch bei den anderen Anbietern, insbesondere bei YES, ist davon auszugehen, dass für Anwendungsfälle mit entsprechendem Bedarf zu gegebener Zeit ebenfalls zusätzliche, besonders sichere Authentifizierungsmethoden unterstützt werden.

Die genannten Allianzen treiben derzeit intensiv strategische Partnerschaften mit weiteren Anwendungsdienstbetreibern voran. Es ist zu erwarten, dass neben Usability und Sicherheit der Authentifizierung auch der »mitgebrachte« Nutzerstamm dieser strategischen Partner substanziell darüber entscheiden wird, in welchem Maß sich die einzelnen Single-Sign-on-/Identitätsmanagement-Dienste in der Praxis durchsetzen werden.

[53] https://www.telekom.com/de/medien/medieninformationen/detail/einfache-nutzer-identifikation-514738, abgerufen am 25. März 2019.

5. HANDLUNGSFELDER

Beim Thema mobile Authentifizierung hat die Marktentwicklung weltweit und auch in Deutschland eine möglicherweise entscheidende Phase erreicht. Es wird immer stärker deutlich, dass die bisher verbreiteten Lösungen – Passwort-Login für normalen Sicherheitsbedarf und SMS-TAN für substanziellen bis hohen Sicherheitsbedarf – nicht zukunftsfähig sind, jedoch ist das Rennen um breitentaugliche, angemessen sichere und idealerweise einheitliche Alternativen noch nicht entschieden. Staat und Politik können und sollten die aktuelle Phase dieses Prozesses mitgestalten. Doch an welchen Stellen und mit welchen Mitteln kann dies gelingen?

Um staatliche und politische Handlungsfelder bei mobilen Authentifizierungsverfahren einzugrenzen, muss auch der für die technischen Verfahren geltende regulatorische Rahmen betrachtet werden. In den einschlägigen Gesetzen, Verordnungen und Normen steht der juristische Begriff der »Identifizierung« im Vordergrund, Authentifizierung stellt demgegenüber nur einen Teilaspekt dar. Eine isolierte Betrachtung nur der Authentifizierung ist insofern auf dieser Ebene nicht sinnvoll möglich. Die folgenden Abschnitte umreißen daher die existierende Praxis und den regulatorischen Rahmen für Identifizierung und Authentifizierung. Dabei ist es sinnvoll, zwischen staatlichen und privatwirtschaftlichen Angeboten zu differenzieren.

Die rechtsverbindliche Identitätsfeststellung ist eine hoheitliche Aufgabe. Digitale Identitäten übernehmen eine wichtige gesellschaftliche Funktion, die nicht allein unter wirtschaftlichen Erwägungen betrachtet werden darf und deren Ausgestaltung und Verwendung nicht allein privatwirtschaftlichen Akteuren überlassen werden sollte. Für E-Government-Dienste kann und muss der Staat die Mittel der Identifizierung und Authentifizierung definieren, wobei eine zu starke Abhängigkeit von einzelnen Anbietern vermieden werden sollte.

5.1 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG IN DER PRIVATWIRTSCHAFT

Kommerziell betriebene Onlinedienste verwenden üblicherweise Informationen, die Nutzer per Selbstregistrierung zur Verfügung stellen. Diese Nutzeridentitäten sind in den meisten Fällen nicht verlässlich an eine hoheitliche Identität gekoppelt. In manchen Fällen wird auf Dienste auch inkognito mittels leerer oder erfundener Login-Informationen zugegriffen. Selbst dann wird jedoch eine Authentifizierung benötigt, denn auch ein Inkognito-Nutzer möchte bei der nächsten Dienstnutzung Zugriff auf die von ihm dienstseitig hinterlassenen Daten haben und ausschließen, dass andere Nutzer darauf Zugriff erhalten[54]. Die Qualität der vom Nutzer bereitgestellten Informationen wie auch die Sicherheit des Authentifizierungsprozesses ist bei kommerziellen Diensten nur in bestimmten Sektoren reguliert (z. B. Onlinebanking[55] oder Abschluss von Mobilfunkverträgen). Ansonsten werden entsprechende Anforderungen nach eigenem Ermessen des Dienstanbieters festgelegt und umgesetzt und vom Nutzer nach eigener Risikoeinschätzung akzeptiert. Aus einer geringen Absicherung der Identitätsdaten bzw. der Authentifizierungsmethode können praktische und wirtschaftliche Herausforderungen entstehen, denen die Dienstbetreiber mit geeignetem Risikomanagement begegnen müssen.

5.2 IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG IM STAATLICHEN SEKTOR

Im öffentlichen Sektor betriebene Dienste, insbesondere im E-Government-Bereich, sind in wesentlich stärkerem Maß Regulationen unterworfen. Insbesondere gelten bei Verwaltungsdienstleistungen für den Schriftformersatz[56] mittels digitaler Dienste in Deutschland strikte Anforderungen bezüglich der Identifizierung des Nutzers[57], welche eine Verwendung ungesicherter, nicht hoheitlicher Identitäten nicht zulassen.

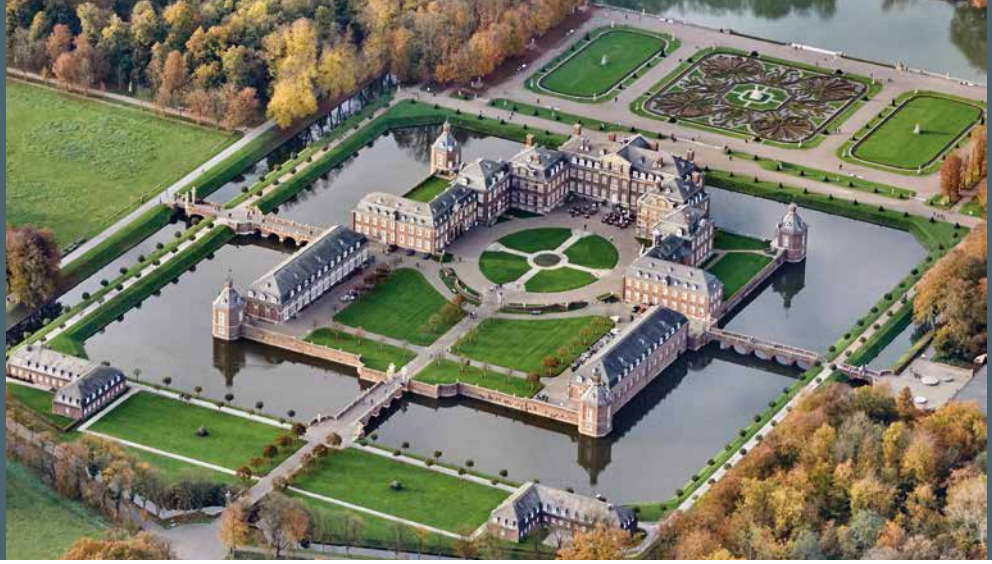
---

[54] Eine Ausnahme bildet der komplett anonyme Zugriff auf nicht personalisierte Dienste. Dieser ist jedoch für dieses Papier irrelevant.

[55] »PSD2«: RICHTLINIE (EU) 2015/2366 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG.

[56] Verwaltungsverfahrensgesetz (Januar 2003, zuletzt geändert Juli 2017), § 3a Elektronische Kommunikation.

[57] BSI-TR-03107 »Elektronische Identitäten und Vertrauensdienste im E-Government«, IT-Planungsrat: »Handreichung mit Empfehlungen für die Zuordnung von Vertrauensniveaus«.



Innerhalb der für den öffentlichen Sektor geltenden Regularien stellt der Einsatz der Fernsignatur[58] gemäß der europäischen eIDAS-Verordnung[59] prinzipiell eine – gerade für die mobile Nutzung besonders attraktive – Option der Dienstabsicherung dar, denn mit dieser Option ist ein bestehendes Schriftformerfordernis sofort rechtssicher erfüllt. Aus Nutzersicht ist dabei vor allem das Authentifizierungsverfahren des Vertrauensdiensteanbieters zur Signaturauslösung relevant, an das strikte Anforderungen durch die eIDAS-Verordnung, ihre Durchführungsbestimmungen[60] bzw. relevante europäische Normen[61] gestellt werden. Alternativ gelten die eID-Funktion in Personalausweis und Aufenthaltstitel sowie gesicherter E-Mail-Versand über die für eGovernment-Zwecke geschaffene »De-Mail«-Plattform als Schriftformersatz. Beide sind derzeit jedoch nur bedingt mobil nutzbar.

Hier lohnt es sich auch einen Blick auf eID-Lösungen anderer Staaten zu werfen. Genannt seien hier nur exemplarisch die Handy-Signatur aus Österreich, die Mobiil-ID aus Estland oder die NemID aus Dänemark.

Bei der Suche nach geeigneten Lösungen werden auch Änderungen bestehender Regularien diskutiert – beispielsweise, die Nutzung kommerzieller Identifikations- und Authentifizierungsdienste zukünftig auch für im öffentlichen Sektor betriebene Dienste zu ermöglichen, für deren Sicherheitsbedarf dies angemessen ist. Diesbezüglich können zwei Handlungsfelder identifiziert werden:

- **Analyse und Neufestlegung des Sicherheitsbedarfs konkreter Dienste:** Für welche Dienste könnten bisher allzu strikt definierte Anforderungen an Identifizierung und Authentifizierung im Interesse der Breitennutzung abgeschwächt werden, um den Einsatz anderweitig bereits etablierter, mobil- und breitentauglicher Authentifizierungsverfahren zur Absicherung dieser Dienste zu ermöglichen?
- **Zulassung alternativer Identifikationsverfahren:** Können Wege geschaffen werden, die bestehenden Anforderungen an die Nutzeridentifikation auf mobil- und breitentauglichere Weise zu erfüllen? Das Verwaltungsverfahrensgesetz enthält eine Öffnungsklausel[62], mit der zusätzliche Mittel zum digitalen Schriftformersatz mit relativ geringem gesetzgeberischem Aufwand eingeführt werden können.

Ein möglicher und vermutlich vielversprechenderer Lösungsansatz wird in Deutschland unter dem Begriff »Abgeleitete Identitäten« seit längerer Zeit diskutiert[63]. Dabei wird von der im Personalausweis repräsentierten hoheitlichen Identität des Nutzers in einem vorbereitenden Schritt eine ausreichend vertrauenswürdige Sekundäridentität abgeleitet, die dann beispielsweise auf einem Smartphone abgespeichert und unmittelbar mobil genutzt werden kann – d. h., ohne dass der Personalausweis im weiteren Prozess (z. B. beim Authentifizierungsschritt) verwendet werden muss. Diese abgeleitete Identität muss hardwaregeschützt gespeichert werden, sodass illegitime Nutzung, Transfer,

[58] Bei der Fernsignatur handelt es sich um eine qualifizierte oder fortgeschrittene elektronische Signatur, die auf einem Server eines Vertrauensdiensteanbieters ausgeführt wird. Nach Authentifizierung des Nutzers signiert der Vertrauensdiensteanbieter im Auftrag des Nutzers unter Verwendung des beim Vertrauensdiensteanbieter abgesichert gespeicherten Signaturschlüssels des Nutzers. Für den Nutzer hat dies den Vorteil, dass er keine Signaturkarte oder sonstige Infrastrukturkomponenten benötigt.

[59] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

[60] Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

[61] Insbesondere DIN EN 419241-1

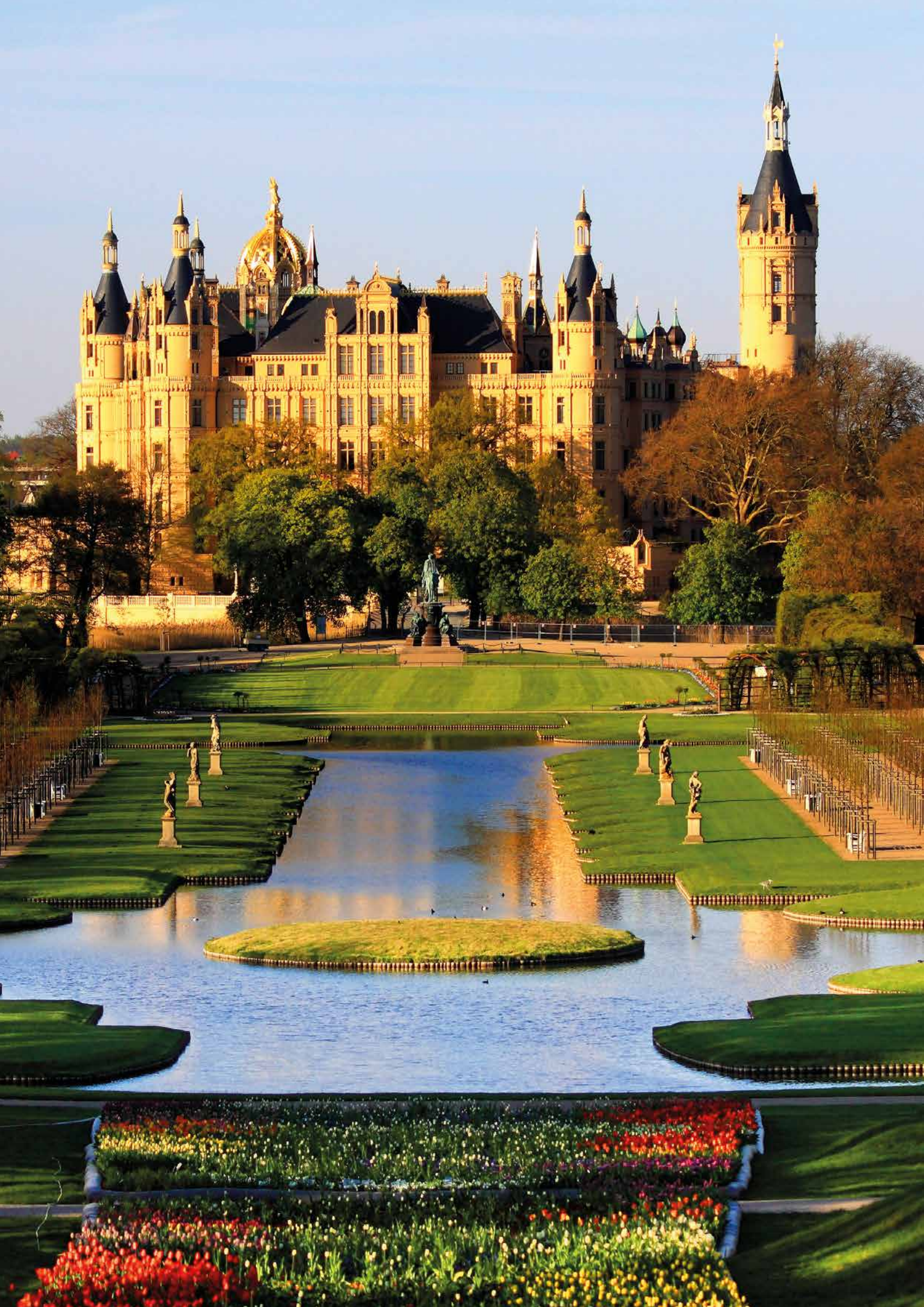
[62] »durch sonstige sichere Verfahren, die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten; der IT-Planungsrat gibt Empfehlungen zu geeigneten Verfahren ab.« (zitiert § 31 Abs. 2 Nr 4 VwVfG)

[63] Schröder, M., Morgner, F.: eID mit abgeleiteten Identitäten. Datenschutz und Datensicherheit-DuD, Volume 37, Issue 8 pp. 530-534, Springer (2013).

Modifikation oder Klonung verlässlich ausgeschlossen sind. Um auf offenen Smartphone-Plattformen verbleibende Gefahren weiter zu reduzieren, kann die Sekundäridentität gegenüber der primären, hoheitlichen Identität von Anfang an substanziellen Einschränkungen unterworfen werden, z. B. begrenzte zeitliche Gültigkeit oder eng zweckgebundener Einsatz. Wenn möglich, kann der Hardwareschutz mittels immer verbreiteter vorhandener interner Smartphone-Sicherheitshardware erreicht werden (beispielsweise durch Nutzung verbauter Secure Elements – vgl. Abschnitt 4.6), alternativ aber auch durch breitentaugliche (Bluetooth-gekoppelte) externe Sicherheitshardware (vgl. Abschnitt 4.6).

5.3 FORSCHUNG UND ENTWICKLUNG

Zusätzlich umfasst das Thema sichere mobile Authentifizierung auch Aspekte, bei denen technische Lösungen und Produkte bisher unzureichend entwickelt sind. Unter Einbeziehung vorhandener Stärken der Industrie und der angewandten Forschung in Deutschland und Europa kann gezielte Innovationsförderung dazu beitragen, diese Lücken zu schließen und resultierende Marktchancen nutzbar zu machen.



6. EMPFEHLUNGEN

Alle E-Government-Vorhaben sollten die Anforderungen an Nutzerfreundlichkeit, Breitentauglichkeit und Sicherheit gleichwertig betrachten und in die Konzeption einbeziehen. Zugleich sollten auch Datenschutz und Datensouveränität des Nutzers bei allen Maßnahmen hohe Priorität eingeräumt werden.

Die Vergangenheit hat gezeigt, dass nationale Alleingänge nur wenig Erfolg versprechen, daher ist eine intensive Abstimmung mit relevanten deutschen und europäischen Initiativen anzustreben. Europäische bzw. internationale Standards sollten gegenüber Ansätzen auf nationaler Ebene bevorzugt und, wo sinnvoll, aktiv mitgestaltet werden.

Bestehende staatliche Lösungen mobilfähig gestalten

Mit der eID-Funktion in Personalausweis und Aufenthaltstitel setzt Deutschland auf NFC für die sichere Kommunikation mit hoheitlichen Dokumenten. Ausreichende Unterstützung hierfür ist jedoch weiterhin auf zu wenigen Mobilgeräten vorhanden. Wenn der Personalausweis im Mobilbereich eine relevante Rolle spielen soll, sollte der Staat bei den Herstellern auf eine aktive und technisch ausreichende Unterstützung des NFC-Standards und entsprechende Öffnung der Schnittstellen hinwirken. Dies wird nicht auf nationaler Ebene gelingen, sondern sollte auf europäischer Ebene verfolgt werden.

Privatwirtschaftliche Lösungen unterstützen und einbinden

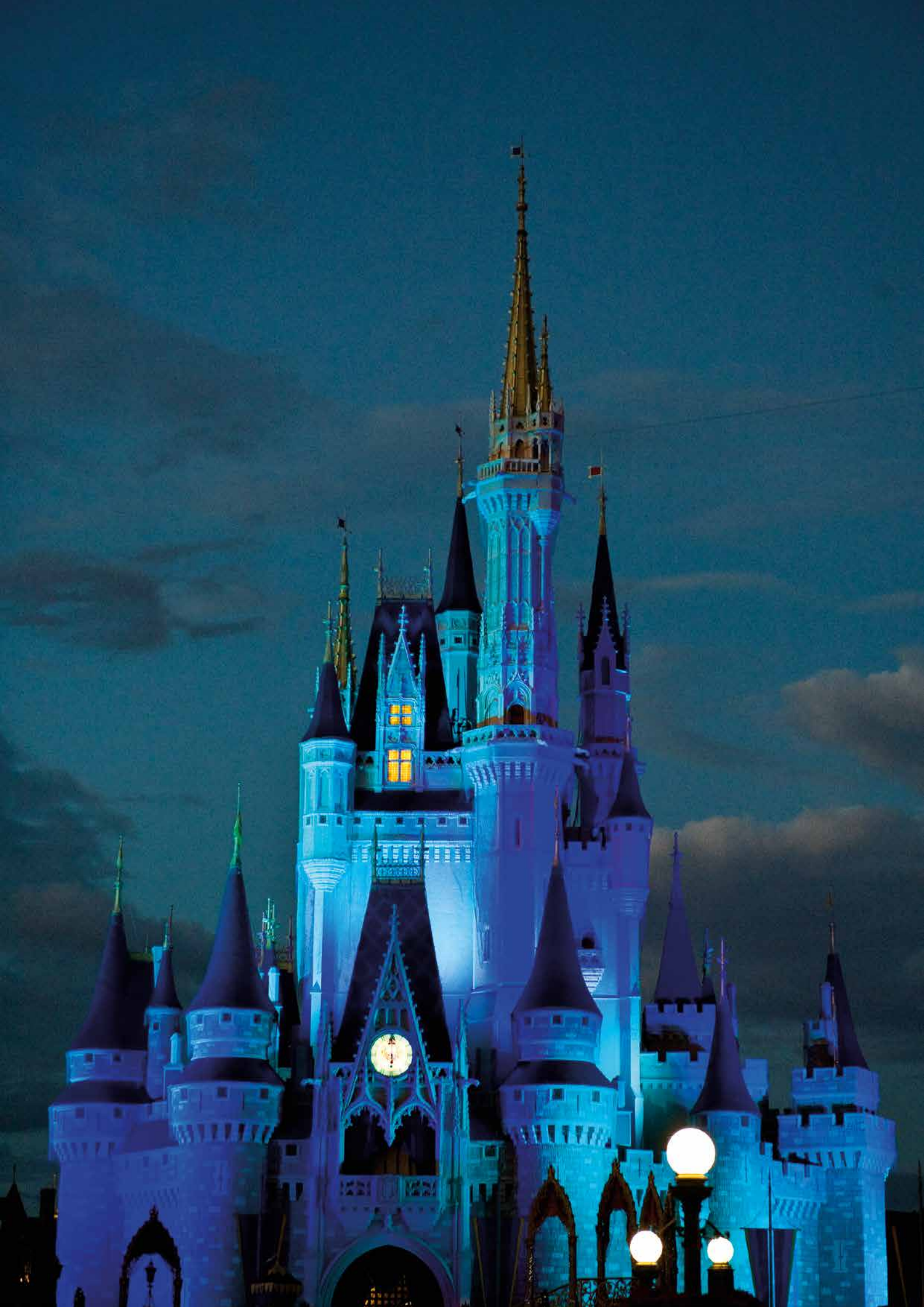
Abzuwarten bleibt, wie sich die gerade in Deutschland etablierenden privatwirtschaftlichen Initiativen entwickeln. Public-Private-Partnerships mit einem oder mehreren relevanten kommerziellen Akteuren im Bereich Identitätsmanagement erscheinen durchaus geeignet, um bei Technologieentscheidungen und Standardisierungsbestrebungen der betreffenden Firmen (bzw. Verbünde) die Interessen und Anforderungen der Dienstbetreiber aus dem öffentlichen Sektor einzubringen und die kommerziellen Anbieter somit als Multiplikatoren zu nutzen. Eine solche Kooperation wäre auch im Interesse der Anbieter sein: Ihre Identitätsmanagement-Dienstleistung wird für ein breiteres Spektrum von Anwendungsdiensten nutzbar und auch attraktiver. Die Zulassung einer privatwirtschaftlichen Identitätsmanagement-Lösung zur Zugangskontrolle auf vom Staat bereitgestellte Onlinedienste sollte allerdings zwingend an die Einhaltung substanzieller Anforderungen bezüglich Datenschutz und Sicherheit geknüpft sein. Damit stellt eine derartige Zulassung eine Art Qualitätssiegel dar. In jedem Fall sollte der Staat auf dem Einsatz offener, sicherer Standards und Protokolle bestehen, um eine zu starke Abhängigkeit von einzelnen Anbietern zu vermeiden. Außerdem sollten Identifikationsdienste angemessene Lösungen für unterschiedliche Vertrauensniveaus anbieten.

Bei der (angekündigten) Einführung des Mobile Connect-Diensts sollten die in Deutschland tätigen Mobilfunkbetreiber dazu angehalten werden, nicht nur die Basis-Ausbaustufe zu realisieren, sondern die Ausbaustufe »Mobile Connect Authenticate Plus«.

Gezielt Innovation fördern

Für Anwendungsfälle mit hohem Sicherheitsbedarf stellt die Nutzung externer Hardware-Sicherheitstoken auch in mobilen Authentifizierungslösungen weiterhin eine sinnvolle Option dar. Insbesondere kann mit diesem Ansatz einer zu starken Abhängigkeit von Smartphone- bzw. Mobilplattformanbietern entgegengewirkt werden. Bisher sind nur wenige entsprechende Produkte auf dem Markt. Mit dem in Gestalt von FIDO/WebAuthn aktuell einsetzenden Durchbruch offener Standards auf diesem Gebiet eröffnen sich neue Marktchancen. Hier könnten vorhandene Stärken der deutschen und europäischen Industrie, insbesondere im Smartcard-Sektor, hervorragend ausgebaut werden. Um diesen Prozess zu beschleunigen, erscheint eine Innovationsförderung sinnvoll, die konkret Forschung, Vor-Produkt-Entwicklung, Sicherheitszertifizierung und Standardisierung für mobil- und breitentaugliche externe Hardware-Sicherheitstoken mit hoher Vertrauenswürdigkeit inklusive innovativer Energieversorgungskonzepte für diese Geräte umfasst.

Auch das in Abschnitt 5.2 genannte Konzept der abgeleiteten Identitäten kann durch Innovationsförderung vorangebracht werden, z. B. in Form eines mehrstufigen Wettbewerbs, in dem Konsortien aus Industrie und angewandter Forschung unterschiedliche, konkurrierende Konzepte entwickeln, als Grundlage für die Umsetzung der erforderlichen regulatorischen Anpassungen und Pilotprojekte sowie bestenfalls des bundesweiten Roll-outs einer mobilen eID.



GLOSSAR

Authentifizierung: Anmelde- und Legitimationsvorgang eines Nutzers gegenüber einem Dienst oder sonstigen IT-System. Bei diesem Vorgang wird die zunächst (meist durch Angabe der Nutzerkennung) nur behauptete Nutzeridentität anhand eines oder mehrerer vom Nutzer vorgewiesener Authentifizierungsfaktoren überprüft und bei Erfolg bestätigt. Interpretationsvarianten: a) Bisweilen wird die erste Phase des Vorgangs, in welcher der Nutzer die Authentifizierungsfaktoren vorweist, als separater Prozess angesehen und mit dem Begriff Authentisierung bezeichnet. b) Eine allgemeinere Interpretation des Begriffes Authentifizierung deckt auch Legitimitätsprüfungsvorgänge zwischen verteilten IT-Systemen ohne menschliche Beteiligung ab.

Authentifizierungsfaktoren: Von einem Dienst zur Authentifizierung akzeptierte Informationen, bei welchen durch Geheimhaltung oder fälschungssichere physische Repräsentation ausreichend gesichert ist, dass diese ausschließlich vom legitimen Nutzer stammen können. Unterschieden werden a) Wissensfaktoren – »etwas, das (nur) der Nutzer weiß«, z. B. PIN oder Passwort b) Besitzfaktoren – »etwas, das (nur) der Nutzer hat«, z. B. eine Smartcard, auf der ein kryptografischer Schlüssel abgesichert gespeichert ist c) Inhärenzfaktoren – »etwas, was (nur) der Nutzer ist«, z. B. individuell einmalige biometrische Merkmale wie Fingerabdruck oder Irisgeometrie.

Autorisierung: Erteilung der vorgesehenen Zugriffsrechte (auch »Privilegien« genannt) an einen Nutzer nach erfolgreicher Authentifizierung. Interner Prozessschritt am Beginn der Ausführung eines Dienstes.

Mehrfaktor-Authentifizierung: Authentifizierungsprozess, der zwingend mehr als einen Authentifizierungsfaktor fordert, konkret z. B. »Zwei-Faktor-Authentifizierung«. Die Faktoren sollten dabei unterschiedlichen Kategorien (Besitz, Wissen, Inhärenz) angehören, damit ein Angriff möglichst nicht mehrere Faktoren gleichermaßen betrifft.

Identifizierung: Feststellung der Identität einer natürlichen oder juristischen Person. Im Kontext dieses Dokumentes primär zur Erstregistrierung eines Nutzers bei einem Dienst.

(Erst-)Registrierung: Registrierung der Identität eines neuen Nutzers bei einem Onlinedienst. Umfang und Vertrauenswürdigkeit der anzugebenden Identitätsinformationen richten sich nach Anforderungen des Dienstbetreibers (ggf. auf der Basis gesetzlicher Erfordernisse). Ausgewählte Identitätsdaten des Nutzers werden üblicherweise in Zusammenhang mit einer Nutzerkennung vom Dienstanbieter gespeichert, sodass dieses dienstseitig nach jeder Authentifizierung zur Verfügung stehen.

Near Field Communication (NFC): Standard zur drahtlosen elektromagnetischen Kommunikation im Nahfeldbereich (Geräteabstand wenige cm). Ermöglicht neben der bidirektionalen Datenübertragung auch die induktive Übermittlung geringer Mengen elektrischer Energie, die kurzeitig zum Betrieb eines angekoppelten (sehr energiesparenden) Gerätes ausreichen, ohne dass dieses eine eigene Stromversorgung bräuchte. So werden z. B. kontaktlose Chipkarten während ihrer Benutzung vom mit der Karte kommunizierenden Gerät (bspw. Chipkartenleser oder Smartphone) auch mit Energie versorgt.

Single Sign-on (SSO): Nutzung eines gemeinsamen Authentifizierungsprozesses zur Zugriffskontrolle bei unterschiedlichen Diensten. Der Authentifizierungsprozess kann dabei an eine separate Instanz, den Identitätsprovider, ausgelagert werden. Verbreitet genutzte Onlinedienstleister wie Google oder Facebook treten zusätzlich zu ihrem jeweiligen Kernangebot auch als Identitätsprovider auf.

USB-OTG: Der USB-On-The-Go-Standard ist eine spezielle Variante des USB-Standards, der die USB-basierte Kopplung von Peripheriekomponenten mit Mobilgeräten regelt. Er unterstützt nur eingeschränkte Geräteklassen und Kommunikationsmodi. Nicht alle Smartphones unterstützen USB-OTG.

KONTAKT

Christian Welzel
Kompetenzzentrum Öffentliche IT (ÖFIT)
Tel.: +49 30 3463-7173
Fax: +49 30 3463-99-7173
info@oeffentliche-it.de

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de
www.oeffentliche-it.de
Twitter: @OeffentlicheIT

ISBN: 978-3-9819921-1-3

kre | 1904 (Fotos: flickr; wikipedia)