# Identitätsnachweise im E-Government

Im E-Government ist die sichere Identifikation von Bürgerinnen und Bürgern ein neuralgischer Punkt. Der Beitrag beleuchtet die rechtlichen und praktischen Rahmenbedingungen für Identitätsnachweise in der digitalen Verwaltung und skizziert Wege hin zu einem integrierten und flexiblen System digitaler Identitäten.

## Autoren

**Joachim Dorschel**
ist Managing Partner bei der DPS Engineering GmbH.

**Florian Kühne**
Ist Leiter Public Sector bei der DPS Gruppe.

Deutschlands Verwaltung muss digitaler werden – nicht nur im Wahlkampf führen Mitglieder der meisten Parteien diese Forderung im Munde. Auch Bürgerinnen und Bürger möchten gern ihre Behördengänge vermehrt online erledigen, und das Onlinezugangsgesetz verpflichtet die Verwaltung, dies zu ermöglichen. Doch schaut man sich die Umsetzung von E-Government an, so wird in einer Vielzahl von Verwaltungsprozessen deutlich, dass sich der Nachweis der Identität für die Bürgerinnen und Bürger kompliziert gestaltet, sodass die Angebote in der Praxis eine nur geringe Nutzung erfahren. Verwaltungsdigitalisierung scheint sich so zumindest in Teilen durch die eigenen Anforderungen in ihrer Wirkung zu limitieren. Der Gestaltungsspielraum der Verwaltung ist hier jedoch begrenzt.

## Interessenlage

- **Perspektive der Verwaltung**

Aus Sicht der Verwaltung steht beim Thema Identitätsnachweise notwendigerweise die (Rechts-)Sicherheit im Vordergrund. Urheberin beziehungsweise Urheber, Inhalt und Zeitpunkt von Anträgen, Stellungnahmen oder Bescheiden müssen nachvollziehbar und vor Gericht beweisbar sein. Dies gilt insbesondere in den (häufigen) Fällen, in denen Fristen in Lauf gesetzt oder gewahrt werden müssen.

Zugleich ist es im Interesse der Verwaltung, dass kostenintensive und umständliche analoge Kanäle und Prozesse mittelfristig durch E-Government-Lö-

## Kompakt

- Zur Umsetzung von E-Government bedarf es sicherer und nutzbarer digitaler Identitätsnachweise.
- Die heute zur Verfügung stehenden leicht nutzbaren Lösungen werden von Unternehmen angeboten, deren Geschäftsmodell kommerzielle Datennutzung ist.
- Zugangshürden zum E-Government sind weit höher als zu E-Commerce-Angeboten – die Nutzung ist daher weit weniger verbreitet.
- Self-Sovereign-Identities machen ID-Lösungen für unterschiedliche Sicherheitsanforderungen niederschwellig nutzbar.

sungen ersetzt werden können. Dies ist kein Selbstläufer. Die Erfahrung aus unterschiedlichen Bereichen der Privatwirtschaft zeigt, dass Menschen digitale Angebote nur annehmen, wenn sie niederschwellig erreichbar sind.

Neben dem Vertrauen der Bürgerinnen und Bürger in die Sicherheit des Systems sind vor allem die einfache Nutzbarkeit und die Integration in die alltäglichen digitalen Gewohnheiten für die Akzeptanz der digitalen Verwaltungsangebote entscheidend.

- **Gesellschaftliche Perspektive**

Die Frage, welche Services und Technologien zur Identifikation und Authentifizierung von Bürgerinnen und Bürgern im E-Government zugelassen werden, hat auch eine gesamtgesellschaftliche Dimension. Heute wird die Nachfrage nach leicht zugänglichen, einfach zu handhabenden und nahtlos zu integrierenden Identifikationslösungen vor allem durch Single-Sign-on-Angebote (SSO) der Bigtechs befriedigt. Ein Beispiel ist der weitverbreitete Service „Login über Facebook". Problematisch aus deutscher und europäischer Sicht ist das Geschäftsmodell dieser Dienste, welches, den Vorgaben der Datenschutz-Grundverordnung (DSGVO) zum Trotz, auf die Kommerzialisierung von Daten setzt, die Nutzerinnen und Nutzer im Zusammenhang mit der Inanspruchnahme von Diensten im Internet generieren.

Die Verbreitung von Identitätslösungen folgt dem Prinzip der Netzwerk-Externalität. Je weiter ein Identitätssystem akzeptiert wird, desto höher ist der Anreiz für Nutzerinnen und Nutzer, diese einzusetzen. Welche Identitätslösungen die öffentliche Verwaltung im Rahmen des E-Governments anerkennt, hat also unmittelbaren Einfluss auf die Struktur der in Europa verfügbaren Angebote insgesamt.

## Rechtliche Rahmenbedingungen

Alle Überlegungen der öffentlichen Verwaltung zur Unterstützung von Identitätslösungen müssen sich an den gegebenen rechtlichen Rahmenbedingungen orientieren.

- **Identifikation im Verwaltungsverfahren**

Bundes- und Landesrecht ordnen das nicht-förmliche Verwaltungsverfahren nach § 10 Verwaltungsverfahrensgesetz (VwVfG) als Regelfall an. Soweit keine gesetzlichen Bestimmungen etwas anderes vorschreiben, steht es also im Ermessen der Verwaltung selbst, welche Form der Identifikation sie seitens der Bürgerinnen und Bürger verlangt. Eine wesentliche Ausnahme von diesem Grundsatz sind alle Verwaltungsverfahren, bei denen das Gesetz Schriftform anordnet. Für den Regelfall, dass in einem schriftlichen Verwaltungsverfahren eine elektronische Antragstellung über ein von der Behörde bereitgestelltes Onlineformular erfolgt, schreibt das § 3a VwVfG einen Identitätsnachweis mittels der eID-Funktion des Personalausweises, eines entsprechenden Nachweises für Unionsbürger (eID-Karte) oder elektronischen Aufenthaltstitels (§ 78 Aufenthaltsgesetz, zusammen nachfolgend vereinfachend „eID") vor.

- **Onlinezugangsgesetz (OZG)**

Der Zugang zu OZG-Leistungen soll gemäß § 3 OZG in der Regel über Nutzerkonten erfolgen, über die Bürgerinnen und Bürger sich bundesweit identifizieren können. Das OZG selbst schreibt keine bestimmten Identifizierungsmittel vor, sondern verweist auf § 78 Abs. 6 der Abgabenordnung. Dort ist geregelt, dass ein sicheres Verfahren zu verwenden ist, das „den Datenübermittler authentifiziert und die Vertraulichkeit und Integrität des Datensatzes gewährleistet". Das Gesetz nennt die eID ausdrücklich als Instrument der Authentisierung, ohne deren Nutzung jedoch anzuordnen.

- **Bestimmungen über elektronische Identitäten**

Auf europäischer Ebene macht die eIDAS-Verordnung Vorgaben zur Anerkennung elektronischer Identitäten innerhalb der EU. Artikel 8 Abs. 2 der Verordnung unterteilt die Sicherheitsniveaus „elektronische Identifizierungssysteme" in „niedrig", „substanziell" und „hoch". Die Verordnung macht den Mitgliedstaaten dabei keine Vorgaben dahin gehend, für welche Art von Verwaltungsleistungen sie welche Identifikationssysteme oder Schutzniveaus zu akzeptieren haben. Derzeit wird auf europäischer Ebene eine Weiterentwicklung der Verordnung diskutiert. Der aktuelle Vorschlag der Kommission sieht die Einrichtung einer European Digital Identity Wallet vor, die allen Unionsbürgerinnen und -bürgern zur Verfügung stehen muss. Jeder Mitgliedstaat muss ein Electronic Identification Scheme entwickeln und notifizieren. Die Vorschläge sind offensichtlich von dem Wunsch getragen, ein gesamteuropäisches Ökosystem sicherer digitaler Identitäten zu schaffen.

## Konvergenz und Convience

**Die eID als zentrales Identifikationssystem** – Die gesetzlichen Regeln zur Identifikation im E-Government kennen als Identifikationssystem nur die eID. Deren Nutzungsgrad ist bislang niedrig. Der Grund für die geringe Akzeptanz dürfte vor allem in der umständlichen Handhabung liegen. Neben dem physischen Personalausweis wird entweder ein Kartenlesegerät oder ein Smartphone neueren Modells mit einer eigenen App (AusweisApp2) benötigt. Zusätzlich wird eine PIN vergeben, welche viele Bürgerinnen und Bürger bereits kurz nach der Aushändigung des Ausweises vergessen oder verlegen.

Der Gesetzgeber hat sich Mitte dieses Jahres zumindest der Notwendigkeit eines physischen Personalausweises angenommen und die Möglichkeit eines „elektronischen Identitätsnachweises mit einem mobilen Endgerät" geschaffen. Letztlich handelt es sich hierbei um eine Kopie der auf dem Chip des Personalausweises gespeicherten Daten in einer eigens hierfür geschaffenen Wallet.

Ob diese Neuerung aber dazu beiträgt, den Nutzungsgrad des elektronischen Personalausweises wesentlich zu erhöhen, bleibt abzuwarten. Kurzfristig dürfte die Verbreitung insbesondere durch die Hardware-Anforderungen gebremst werden. Die Technologie benötigt ein sogenanntes „Secure Element", das nur auf Smartphones neuester Generation vorhanden ist. Es handelt sich bei der eID trotz allen Bemühens um eine benutzerfreundliche Lösung um ein Identifikationssystem mit hohem Sicherheitsniveau. Die hiermit verbundenen technischen Restriktionen bringen zwingend Einschränkungen mit sich, die zulasten der Nutzbarkeit einerseits und der Möglichkeiten der nahtlosen Integration andererseits gehen.

**Handhabung in der Praxis:** In der Praxis zeichnet sich ab, dass die Verwaltung einen Zugang zu E-Government-Leistungen auf zwei Arten zulässt:

- Einerseits werden Verwaltungsleistungen ganz ohne Identifikation oder lediglich auf Basis eines Nutzerkontos angeboten, dessen Anlage wiederum keiner Prüfung der Identität bedarf.
- Andererseits gibt es Leistungen, deren Online-Inanspruchnahme nur auf Basis der eID möglich ist.

Damit ist für eine große Anzahl der Verwaltungsleistungen, für die eine Identifikation der Bürgerinnen und -bürger notwendig oder sinnvoll ist, nur die eID als Identifikationssystem verfügbar. Die Zugangshürden zum E-Government sind damit deutlich höher als etwa zu E-Commerce-Leistungen in der Privatwirtschaft. So ist es rechtlich möglich und in der Praxis üblich, auch großvolumige Verträge online zu schließen und zur Legitimation nur Zahlungsinstrumente mit Online-Autorisierung, zum Beispiel eine Kreditkarte, vorzulegen. Vieles spricht dafür, auch für Alltagsleistungen im E-Government neben der eID weitere, niederschwelligere Identifikationssysteme zuzulassen.

**Beispiel Schweden** – Das Land verfügt mit der BankID über ein Identifikationssystem mit enorm hohem Verbreitungsgrad. Die BankID ist das Produkt eines Konsortiums schwedischer Banken, wird aber auch im E-Government als Identifikationssystem anerkannt. Alle Personen mit einer schwedischen Identitätsnummer und einer Kundenbeziehung zu einer der beteiligten Banken können die BankID bei ihrer Bank beantragen. Die BankID ist als Softwarezertifikat, als Smartphone-App und als physischer Token verfügbar.

Die universelle Einsetzbarkeit und die einfache Form der Beantragung für einen großen Teil der Bürgerinnen und Bürger dürften wesentliche Gründe für den hohen Nutzungsgrad sein.

## Lösungsansätze für Deutschland

Das Beispiel Schweden zeigt, dass Banken als Identitätsprovider eine entscheidende Rolle auch für das E-Government spielen können. Banken sind nach dem Geldwäschegesetz verpflichtet, die Identität ihrer Kundinnen und Kunden zu überprüfen. Es liegt mehr als nahe, diese Identitäten auch für andere Zwecke zu nutzen. Die Finanzwirtschaft selbst ist bestrebt, entsprechende Identitätsservices zu entwickeln – ein prominentes Beispiel in diesem Zusammenhang ist yes.com. Das in der Zweiten Zahlungsdiensterichtlinie (PSD 2) festgeschriebene Prinzip des Open Bankings verpflichtet alle Banken, Schnittstellen zu den Konten ihrer Kunden bereitzustellen, die von Drittanbietern (TPPs) im Auftrag der Kunden genutzt werden können. Über solche Schnittstellen lassen sich Bankdienstleistungen ebenso bereitstellen wie Identitäts-Services. Eine von einer Bank emittierte Kreditkarte mit Online-Autorisierung oder die Legitimation mittels Karte-PIN an einem Selbstbedienungsterminal kann ebenfalls als elektronisches Identifizierungssystem genutzt werden.

Vorgeschlagen wird auch die Nutzung etablierter Identitätssysteme aus anderen Bereichen der öffentlichen Verwaltung. So könnte etwa das Elster-Zertifikat auch als Identifikationssystem im E-Government genutzt werden. Unternehmen, die bereits über eine qualifizierte elektronische Signatur verfügen, etwa weil sie regelmäßig mit dem elektronischen Handelsregister kommunizieren, sollten die Möglichkeit haben, diese auch für die Identifikation im E-Government zu nutzen.

Es wäre allerdings wenig erstrebenswert, wenn öffentliche Verwaltung und Privatwirtschaft auf eine Vielzahl unterschiedlicher, miteinander nicht kompatibler Identitätslösungen setzen, sodass Kundinnen und Kunden sowie Bürgerinnen und Bürger in jeder Situation, in der sie sich online legitimieren müssen, ein anderes Identitätssystem benötigen. Einem solchen Szenario kann das Prinzip der Self-Sovereign-Identities (SSI) vorbeugen. Self-Sovereign-Identities sind digitale Identitäten, bei denen verschiedene Attribute des Identitätssubjekts (Credentials) unter der Kontrolle des Identitätssubjekts selbst (Holder) in einer Wallet gespeichert werden. SSI-Wallets können verschiedene Identitätssysteme mit unterschiedlichen Sicherheitsniveaus aufnehmen, sodass je nach Kritikalität des Einsatzszenarios ein mehr oder weniger aufwendiger Legitimationsprozess angestoßen wird.

Erfreulicherweise investiert der Bund derzeit erheblich in den Aufbau von SSI-basierten Ökosystemen. So unterstützt das BMWi mehrere sogenannte Schaufensterprojekte mit dem Ziel, miteinander kompatible Identitätsökosysteme für Sichere Digitale Identitäten zu etablieren. Die Bundesregierung entwickelte im Jahr 2020 gemeinsam mit Unternehmen der Privatwirtschaft eine ID Wallet, die in einem ersten MVP einen digitalen Hotel Check-in erlaubte.

Es bleibt zu hoffen, dass die aktuelle Dynamik rund um die SSI-Technologie anhält. Die Umsetzung des OZG wäre eine ideale Gelegenheit, dem Thema einen weiteren Schub zu geben, indem man die notwendige Identifizierung und Authentifizierung bei der Inanspruchnahme von OZG-Leistungen für entsprechende SSI-basierte Lösungen öffnet. ■