bitkom

#4
Digitalisierung von Identitäten

Digitalisierung von Identitäten in der Verwaltung

eIDAS und das OZG: europäisches Recht auch in Deutschland?

Digitalisierung von Identitäten in der öffentlichen Verwaltung

Einleitung

Das 2017 erlassene Onlinezugangsgesetz (OZG) verpflichtete Bund, Länder und Gemeinden, bis spätestens Ende 2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten und diese miteinander zu einem Portalverbund zu verknüpfen. Das E-Government-Gesetz (EGovG) unterstützt das OZG hierbei, indem es die Abwicklung von Verwaltungsverfahren mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien regelt. Da das Ziel des OZG bis heute sehr deutlich verfehlt wurde, wird aktuell eine Reform beider Gesetze angestrengt. Es wurde hierzu bereits ein erster Entwurf durch das BMI im Januar 2023 und ein zweiter Entwurf am 23.05.2023 veröffentlicht. Der zweite Entwurf wurde bereits im Kabinett beschlossen.

Die eIDAS-Verordnung aus 2014 stellt einen harmonisierten Werkzeugkasten für elektronische Identifizierung und Vertrauensdienste zur Verfügung. Auch hier befindet sich eine Revision derzeit im Trilog. Mit ihr sollen eine EUDI-Wallet und zusätzliche neue Vertrauensdienste etabliert werden, wie zum Beispiel die qualifizierte elektronische Attestierung von Attributen (QEAA).

Mit Gesamtblick bietet sich die Verwendung der umfangreichen Mittel der eIDAS an, um die Ziele des OZG nachhaltig zu unterstützen und deren Erreichung zu fördern. Dennoch werden diese eIDAS-Mittel derzeit in der Novellierung nur lückenhaft im OZG und EGovG aufgenommen und referenziert.

Es lassen sich hierbei drei grundsätzliche Themenfelder herauskristallisieren: Identität – Ersetzung der Schriftform und Zustellung – Integrität.

1. Identität

Im Bereich der elektronischen Identifizierung gemäß eIDAS-Verordnung Kapitel II. legt die eIDAS drei Vertrauensniveaus (hoch, substanziell und niedrig) fest und gibt den Mitgliedsstaaten die Möglichkeiten, eIDs auf einem entsprechenden Vertrauensniveau zu notifizieren, wodurch sie EU-weit gleichwertig einsetzbar werden. Die deutsche eID ist bereits auf „hoch“ notifiziert, im OZG-Kontext als Identifizierungsmittel zugelassen und für Behörden verpflichtend (§ 2 Abs. 3 EGovG). Daneben ersetzt sie, neben anderen Werkzeugen, auch Schriftformerfordernisse. Im Übrigen ist ELSTER mittels juristischer Fiktion nur bis zum 30.06.2023 auf „substanziell“ zugelassen, soll aber mit der OZG-

Novellierung um weitere drei Jahre verlängert werden. Die Verlängerung ist jedoch aufgrund fehlender zweifelsfreier Identifizierung für die Mehrheit der genutzten Konten (Elster-Nutzung auf Basis von Softwarezertifikaten) und der möglichen EU-Rechtswidrigkeit durch die rein deutsche Legalfiktion eines Vertrauensniveaus nicht ratsam. Weitere Identifizierungsmittel sind grundsätzlich nach Prüfung durch das BSI möglich. Hierbei ist jedoch zu beachten, dass das BSI bezüglich der Vertrauensniveaus eigene Technische Richtlinien heranzieht, die sich zwar an den eIDAS-Vertrauensniveaus orientieren, aber in vielen Punkten davon abweichen. Ferner wird auch durch die geplante OZG-Novellierung, welche die eID zunächst als Standardidentifizierungsmittel festlegt, keine Festlegung des entsprechenden Vertrauensniveaus für die einzelne Verwaltungsleistung vorgenommen. Diese Festlegung ist hierbei für eine nutzerfreundliche Ausgestaltung der Verwaltungsprozesse unerlässlich und sollte dabei zwingend unter der Einbeziehung der Vertrauensniveaus der eIDAS-Verordnung erfolgen.

Hierdurch wird die Zugangsbarriere zu allen Verwaltungsleistungen pauschal auf das anfängliche Vertrauensniveau „hoch“ gehoben, wodurch Leistungen der Verwaltungen, die auch auf einem niedrigeren Vertrauenslevel unproblematisch umsetzbar wären, benachteiligt bzw. quasi verhindert werden würden. Die drohende fehlende Abwärtskompatibilität führt zu einer unangemessenen Benachteiligung der Nutzenden, verhindert eine breite Akzeptanz, und damit Reichweite, sowie die Nutzung der jeweiligen Verwaltungsleistung. Dem Angebot fehlt damit jede Relevanz in der Wahrnehmung und eine erfolgreiche Digitalisierung wird nachhaltig verhindert.

2. Ersetzung der Schriftform und Zustellung

Im Bereich der Vertrauensdienste (eIDAS Kapitel III. und IV.) gibt es im bestehenden OZG-Kontext nur wenige Referenzierungen. Die qualifizierte elektronische Signatur (QES) sowie die DE-Mail ersetzen gemäß § 3a VwVfG jeweils dabei die Schriftform und Behörden müssen gemäß § 2 Abs. 1 EGovG einen Zugang für die QES und nach § 2 Abs. 2 EGovG einen Zugang für DE-Mail eröffnen. Andere Arten elektronischer Signaturen und qualifizierte elektronische Siegel für juristische Personen werden jedoch derzeit nicht referenziert

Durch den ersten Entwurf der OZG-Reform aus Januar 2023 sollte in § 9 Abs. 6 OZG eine Vorschrift geschaffen werden, mit der Bescheide aus dem Nutzerkonto von der Behörde qualifiziert fakultativ gesiegelt werden können. Mit dem zweiten OZG-Reform-Entwurf vom 23.05.2023 wurde mit § 2a EGovG-E zusammen mit § 9a Abs. 6 OZG-E, welcher das qualifizierte elektronische Siegel als schriftformersetzend bei elektronischen Dokumenten der Verwaltung an den Bürger festlegt, die Bereitstellung eines zentralen Siegeldienstes statuiert, welcher ausdrücklich als Fortschritt begrüßt wird. So kann eine einheitliche Digitalisierung gewährleistet und gleichzeitig der wirtschaftliche und organisatorische Aufwand bei der Beschaffung qualifizierter elektronischer Siegel minimiert werden. Dennoch sollte Anspruch einer ganzheitlichen Digitalisierung die umfassende, rechtssichere und beweiswerterhaltende Verarbeitung von elektronischen Daten und Dokumenten sein. Der in § 9a Abs. 6 OZG-E vorgesehene bloße Hinweis auf die Möglichkeit, dass ein gesetzlich vorgeschriebenes Schriftformerfordernis durch ein qualifiziertes elektronisches Siegel der Behörde

ersetzt werden kann, reicht jedoch aber nicht aus. Die von Behörden erstellten Dokumente müssen grundsätzlich auch außerhalb des geschlossenen vertrauenswürdigen Systems der Verwaltung, also bspw. gegenüber Banken, Versicherungen oder gegenüber Behörden anderer EU-Mitgliedstaaten, genutzt werden können. Gesetzlich vorgesehene Schriftformerfordernisse sind in dieser Hinsicht irrelevant. Daher muss die Siegelung elektronischer Dokumente standardmäßig vorgesehen werden und die bereits vorhandenen Standards zur QES und qualifizierten Zustelldiensten zur nachhaltigen Anwendung kommen. Ebenfalls sollte in diesem Zusammenhang zwingend erwogen werden, ob es nicht sinnvoll ist, durch geeignete Maßnahmen die Voraussetzung dafür zu schaffen, dass qualifizierte elektronische Signaturen und Siegel sowie qualifizierte Zustelldienste auch von Bürgerinnen und Bürger in größerem Umfang genutzt werden. Vor allem in Hinblick darauf, dass die geplante EUDI-Wallet gemäß dem Entwurf der eIDAS-Novellierung sowohl qualifiziert signieren als auch bei juristischen Personen siegeln kann und somit die bisher bestehende Einstiegshürde zur Verwendung der qualifizierten elektronischen Signatur und Siegel wegfällt. Mit qualifiziert signierten Anträgen würde die Rechtswirkung inklusive einer Verkehrsfähigkeit unmittelbar erzeugt werden, die § 9a OZG-Entwurf erst durch die Verknüpfung von Identifikation im Benutzerkonto mit den Inhaltsdaten schafft.

Für die Zustellung innerhalb des Nutzerkontos gibt es jedoch eine weitere Besonderheit. Ohne Nachweis der Zustellung muss eine physische Ersatzvornahme, also eine spätere alternative Zustellung per physischem Brief, falls das digitale Dokument nicht abgeholt wurde, erfolgen. Diese jedoch gilt es im Rahmen der Digitalisierung zu verhindern. Für viele Anwender tritt eine tatsächliche Prozessvereinfachung – und damit Kostenersparnis – auch nur ein, wenn es garantiert keine physische Ersatzvornahme geben muss. Es muss daher eine gesetzliche Basis für die Zustellung, insbesondere konfrontative Zustellung, geben. Dies ist durch die qualifizierten Zustelldienste – in Deutschland explizit nur im Rahmen des De-Mail-Standards – der Fall, da im Rahmen der elektronischen Kommunikation ausschließlich nach dem De-Mail-Gesetz (De-Mail-G) nicht nur schriftformersetzend und nachweisbar (Evidenz des Versands und des Empfangs einer Nachricht) kommuniziert werden kann, sondern explizit die Besonderheit der dreitägigen Zustellfiktion, sowie die Möglichkeit der konfrontativen, sowie förmlichen Zustellung, existiert und in keinem Fall eine physische Ersatzvornahme notwendig wird, um die verbindliche Zustellung zu „beweisen“.

Es ist daher erforderlich, die qualifizierten Vertrauens- und Zustelldienste in die Novellierung des OZG mit aufzunehmen und explizit darauf zu referenzieren. Da in Bezug auf eine verbindliche Zustellung in Deutschland das De-Mail-G die Anforderungen der eIDAS-Verordnung mit abdeckt, darüber hinaus jedoch, als einziger gesetzlicher Standard, die physikalische Zustellung vollständig ersetzen kann (Zustellfiktion und konfrontative, sowie förmliche Zustellung), ist damit zu fordern, dass alle Postfächer der Nutzerkonten im Rahmen des OZG zwingend nach den Grundsätzen des De-Mail-G, und damit auch der eIDAS-Verordnung, ausgestaltet sind und damit einen interoperablen qualifizierten Zustelldienst beinhalten.

3. Integrität

Die eIDAS-Mittel finden derzeit ebenfalls keine Verwendung in den Anforderungen an die IT-Sicherheit und die Kommunikationsstandards (§§ 5 und 6 OZG), obwohl auch hier qualifizierte Zertifikatslösungen einfache, nutzerfreundliche und europäisch standardisierte Lösungen für Authentisierung, Zeitstempelung und Integritätsschutz bieten. Auch der eIDAS-Vertrauensdienst der qualifizierten Zertifikate für die Website-Authentifizierung (QWAC), der bislang und auch nicht durch die geplante OZG-Revision referenziert wird, sollte Verwendung finden, auf diese Weise könnten Onlineauftritte von Behörden abgesichert werden. So können Betrugsfälle, wie z. B. Phishing-Attacken auf Bürgerinnen und Bürger, wie sie auch im Falle der Coronahilfen durchgeführt wurden, verhindert werden und ihnen die Sicherheit gegeben werden, dass die ihnen zur Verfügung gestellten Informationen aus einer vertrauenswürdigen Quelle stammen. Weiterhin sollten Schnittstellen der Verwaltung über QWAC abgesichert werden, damit Dritte, die auf diese zugreifen, sicherstellen können, dass sie auf authentische Daten zugreifen. Im Falle der Verarbeitung von personenbezogenen Daten über Schnittstellen, insbesondere solche Maschinen-Maschinen-Schnittstellen nach 9a Abs. 3 Nr. 4 EGovG-E, sollte eine gegenseitige Authentisierung mittels eIDAS-Mittel und einem Rollenkonzept vergleichbar dem Konzept der 2. Zahlungsdiensterichtlinie (PSD2 RTS on SCA Artikel 34) umgesetzt werden. Bereits jetzt sollte auch der geplante neue Vertrauensdienst QEAA im OZG-Kontext etabliert werden, um dem Bürger zu erlauben, digitale Nachweise auch als QEAA in den Verwaltungsprozess einbringen zu können und somit den Erfolg der EUDI-Wallet in Deutschland sicherzustellen. In diesem Zusammenhang sollten die Erleichterungen im Beweis-/Verfahrensrecht angepasst werden, um alle qualifizierten Vertrauensdienste aufzunehmen (bspw. enthalten §§ 371a ZPO und 33 VwVfG noch keinen Hinweis auf Siegel).

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Clemens Schleupner | Referent Vertrauensdienste und Digitale Identitäten
T 030 27576-424 | c.schleupner@bitkom.org

Autoren
Franca Löwenstein, Bundesdruckerei GmbH
Leslie Romeo, 1&1

Verantwortliches Bitkom-Gremium
AK Digitale Identitäten