SICHERE
DIGITALE
IDENTITÄT

„SICHERE DIGITALISIERUNG ERFORDERT SICHERE DIGITALE IDENTITÄTEN“

THESENPAPIER DES VERBANDS SICHERE DIGITALE IDENTITÄT e. V. (VSDI)

Frühjahr 2020

Grußwort

Die reale und digitale Welt haben eines gemeinsam: Es ist wichtig, dass eine Identität nicht gefälscht, kompromittiert oder sogar imitiert werden kann. Denn unsere persönliche Integrität und zwischenmenschliche Beziehungen sind eng mit unserem Identitätsbild verbunden. Je mehr wir im Netz sensible Informationen austauschen, Geschäfte abwickeln oder Behördengänge erledigen, desto wichtiger sind sichere digitale Identitäten. Sie sind das Fundament einer sicheren Online-Welt.

Wir als Verband Sichere Digitale Identität (VSDI) bündeln das Fachwissen zu diesem Thema. Unsere feste Überzeugung ist: Ohne sichere digitale Identitäten gibt es keine sichere Digitalisierung.

Was macht aber eine digitale Identität aus und wie wird sie sicher? Mit dem vorliegenden Papier möchten wir als VSDI einen Beitrag zu dieser Diskussion leisten. Wir verstehen uns als Impulsgeber und nehmen dabei eine lösungsorientierte Haltung ein. Mit diesem Thesenpapier möchten wir politische Entscheidungsträger willkommen heißen, mit uns in einen fachlichen Austausch zu treten.

Antonia Maas

Vorstandsvorsitzende

Einleitung

Herausforderungen der Digitalisierung

Dieses Thesenpapier zeigt die Bedeutung und die Anwendungsbereiche der sicheren Authentifizierung auf und beschreibt den politischen Handlungsbedarf. Damit leistet das Papier einen konkreten Beitrag zur aktuellen politischen Debatte. In diesem Kontext spielt insbesondere der Begriff »Digitale Souveränität« eine große Rolle. Dieser Begriff meint im Kern einen selbstbestimmten und unabhängigen Umgang mit Daten und Informationen, die sichere und vertrauenswürdige Infrastrukturen voraussetzen. Er umfasst Kompetenz, Befähigung und Entscheidungsgewalt im digitalen Raum – sowohl für den Staat als auch für Unternehmen und Privatpersonen, im Sinne von Verfügbarkeit und Unabhängigkeit von spezifischen Hard- und Softwaresystemen sowie technologischen Lösungen.

Mit Blick auf digitale Identitäten ist die Kontrolle über die eigenen Daten essenziell für das nötige Vertrauen und die notwendige Offenheit gegenüber digitalen Anwendungen. Bürger wollen und sollten wissen, wer über ihre Daten verfügt, wer sie wie und wann nutzt und sie sollten in die Lage versetzt werden, Zugriffsrechte selbst zu vergeben und auch wieder entziehen zu können.

Was sind digitale Identitäten?

Digitale Verfahren zum Nachweis einer Identität werden elektronische bzw. digitale Identitäten genannt. Die digitale Identität ist die Voraussetzung für Digitalisierung, ist aber direkt mit der analogen Welt verbunden, da im Vorfeld eine analoge Verifizierung stattfinden muss.

Mit Hilfe einer digitalen Identität kann sich jeder, der im Netz kommuniziert, eindeutig zu erkennen geben – sei es eine natürliche oder eine juristische Person, eine Maschine oder ein Prozess. Digitale Identitäten belegen, dass alle Prozessbeteiligten tatsächlich diejenigen sind, für die sie sich ausgeben. Somit übertragen sie das analoge Vertrauen in die Echtheit einer Identität in die vernetzte Welt. Eine sichere digitale Identität ist auch die Voraussetzung für Datensouveränität, also die Selbstbestimmung über die eigenen Daten im Netz.

Digitale Identitäten können unterschiedliche Formen annehmen. Hierbei greifen Mechanismen, die einer bestimmten Person, Organisation oder Maschine individuelle Attribute zuordnen.

<table>
<tr><th colspan="4">Formen von digitalen Identitäten</th></tr>
<tr><td rowspan="2"></td><td colspan="2">Personen</td><td rowspan="2">Maschinen</td></tr>
<tr><td>Natürliche Personen</td><td>Juristische Personen</td></tr>
<tr><td rowspan="3">Vertrauenswürdiger Identitätsnachweis im digitalen Raum</td><td colspan="2">Personenzertifikate,
Signatur- und Siegelkarten</td><td rowspan="3">Maschinenzertifikate</td></tr>
<tr><td>Elektronische Ausweise, insbesondere der elektronische Personalausweis / AusweisApp

Biometrie-Lösungen</td><td>Webseitenzertifikate und Siegel</td></tr>
</table>

Hierbei können digitale Identitäten unterschiedlichen Sicherheitsanforderungen entsprechen und somit verschiedene Vertrauensniveaus für die verwendeten Technologien und Verfahren bieten.

Die Rolle der „vertrauenswürdigen Dritten“

Vertrauenswürdige elektronische Dienste, bzw. deren Anbieter überprüfen die Herkunftsidentität der Akteure und der ausgetauschten Datensätze im Internet und sorgen damit für Vertrauen in der elektronischen Interaktion. Damit sind sie ein wesentlicher Baustein des europäischen digitalen Binnenmarkts. Mit der in 2014 verabschiedeten eIDAS-Verordnung[1] wurde ein Meilenstein erreicht, da durch sie ermöglicht wurde, eine Vereinheitlichung der vertrauenswürdigen elektronischen Dienste in ganz Europa anzubieten. Die Verordnung liefert europaweit geltende Regelungen für die Bereiche elektronische Identifizierung und elektronische Vertrauensdienste. Zudem definiert sie die qualifizierten Vertrauensdienste, die darüber hinaus die einschlägigen Anforderungen der eIDAS-Verordnung erfüllen und von einer Aufsichtsbehörde als solches anerkannt sind. Qualifizierte Vertrauensdienste tragen dadurch

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

zur Rechtssicherheit in Europa bei und sind ein Anreiz für Unternehmen, ihre Tätigkeit auch europaweit auszuüben.

Für den VSDI, dem auch qualifizierte Vertrauensdiensteanbieter angehören, ist die Umsetzung und Weiterentwicklung der eIDAS-Verordnung in Deutschland und Europa ein wichtiges Anliegen, das intensiv und vor allem differenziert diskutiert werden muss. Für uns ist klar, dass an einigen Stellschrauben gedreht werden muss, damit die Verordnung ihre intendierte Wirkung entfalten kann und wir damit einem einheitlichen digitalen Binnenmarkt einen großen Schritt näher kommen. Auch zu dieser Debatte möchten wir mit diesem Thesenpapier beitragen.

Unsere Thesen

1) **Sichere digitale Identitäten erfordern verlässliche Vertrauensinfrastrukturen.** Die Technologie für sichere digitale Identitäten entwickelt sich stets weiter. Doch steckt die gleichbleibende Idee der Vertrauensbasis und Verschlüsselung als Grundlage dahinter. Eine intelligente Kombination von bewährten Public-Key-Infrastrukturen (PKI) und der verteilten Blockchain-Technologie (via Distributed Ledger DLT) kann optimale Voraussetzungen für sichere digitale Identitäten schaffen.

2) **Einheitlicher Rechtsrahmen.** Wir begrüßen die politischen Absichten des Europäischen Rates, bzw. der Europäischen Kommission, in Europa ein einheitliches regulatorisches Rahmenwerk für eine europäische digitale Identität zu entwickeln und damit die digitale Souveränität Europas weiter zu stärken. In wenigen Bereichen, wie dem Finanz- und Gesundheitssektor, gibt es bereits detaillierte Vorschriften für die Nutzer-Identifizierung und -Authentifizierung. Wichtig ist, die für die eIDAS-Verordnung geschaffenen Vertrauensniveaus und die entsprechende Standardisierung konsequent zu nutzen und weiterzuentwickeln. Der einheitliche Rechtsrahmen sollte eine höhere Verbindlichkeit (auch gegenüber global agierenden Plattformen) haben als die bisherige eIDAS-Verordnung. Gleichzeitig sollten erforderliche nationale Besonderheiten und Zuständigkeiten insbesondere im Sicherheitsbereich berücksichtigt werden (keine Vollharmonisierung).

3) **eIDAS-Evaluierung als Chance.** Die Evaluation der eIDAS-Verordnung durch die EU-Kommission sollte auch in Deutschland als Chance genutzt werden, bestehende Gesetze eIDAS-konform auszugestalten. Dazu zählen aktuelle Vorhaben wie das IT-Sicherheitsgesetz 2.0. Für Deutschland bietet sich die Chance mit der EU-Ratspräsidentschaft in der zweiten Jahreshälfte 2020, die Debatte um eine konsequente eIDAS-Umsetzung und -Weiterentwicklung voranzubringen. Bei der anstehenden Evaluation dieser Verordnung ist daher die weitere Stärkung der Verbindlichkeit, insbesondere mit Blick auf den bestehenden Standardisierungsrahmen von ETSI (deutsch: Europäisches Institut für Telekommunikationsnormen) und CEN (deutsch: Europäisches Komitee für Normung) nötig. Zudem empfehlen wir, einen Standard für Objektidentitäten einzuführen.

4) **Einheitliche Zulassung von eIDAS-Diensten.** Im Grundsatz sollte die eIDAS-Verordnung alle Anforderungen für die Zulassung von eIDAS-Diensten selbst definieren und entsprechende Vorgaben für die Zulassungsprozesse der Aufsichtsbehörden machen. Zusätzliche nationale Regeln müssen die absolute Ausnahme bleiben. Dazu sollte auch die Benennung einer Aufsichtsbehörde je

Mitgliedsstaat gehören. Die strikte Trennung der Zuständigkeit zwischen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Themen eID, Identifikation und Webseitenzertifikate sowie der Bundesnetzagentur (BNetzA) für andere Vertrauensdienste erhöht den Aufwand für Unternehmen und widerspricht dem Grundprinzip, Identifikationsdienste mit Vertrauensdiensten wie z.B. der elektronischen Signatur und dem Siegel in Einklang zu bringen.

5) **Nötiger Ausbau von E-Government.** Die eIDAS-Verordnung kann in ihrer Gänze erst dann Anwendung finden, wenn Verwaltungsprozesse entsprechend digitalisiert worden sind. Potenzielle Anwendungsmöglichkeiten wie qualifizierte Siegel, Signaturen und Zertifikate werden aktuell längst nicht ausgeschöpft. Dabei verspricht das Portfolio Effizienz und Nutzerfreundlichkeit. Der Ausbau des E-Governments ist deshalb absolute Grundbedingung für eine konsequente eIDAS-Umsetzung.

6) **Volle Kontrolle für Nutzer.** Zugriffsrechte auf die Daten einer digitalen Identität müssen stets in der Hand des Nutzers bleiben. Dies muss durch den „Privacy by Design"-Ansatz und im Rahmen der Datenschutz-Grundverordnung (DSGVO) gewährleistet werden. Dabei sollte darauf geachtet werden, dass je nach Lösung auch die Nutzung des immer gleichen Zertifikats ein Privatsphären-Risiko darstellen kann. Volle Kontrolle der Nutzer bedeutet zudem, dass diese das Recht haben, Daten gezielt und nach Freigabe weiterzugeben. Rechtliche Barrieren, die das erschweren, sollten beseitigt werden.

7) **Interoperabilität für einen One-for-all-Ansatz.** Es ist für die Akzeptanz entscheidend, dass natürliche Personen mit einer digitalen Identität staatliche und private Dienste unterschiedlicher Bereiche nutzen können. So sollten sich Bürger beispielsweise in der App für den öffentlichen Nahverkehr mit der gleichen Identität anmelden können wie auch an der Ladestation für das Elektroauto oder im Onlineportal des Bürgeramts. Auch Firmen sollten mit einem Unternehmenskonto alle Anwendungen nutzen können, unabhängig von regionalen Verwaltungszuständigkeiten für verschiedene Unternehmensteile. Dafür braucht es eine grundsätzliche Schnittstellen-Interoperabilität und einen klaren Abgleich des Vertrauensniveaus. Hierbei hat die eIDAS-Verordnung, mit dem Ziel einheitliche Rahmenbedingungen für elektronischer Identifizierungsmittel zu schaffen, eine besondere Relevanz.

8) **Besserer Zugang zu digitalen Diensten.** Die Barrieren bei der Identifizierung und Authentifizierung von Nutzern bei deutschen Vertrauensdiensten sind hoch. Zudem sind sie oft umständlich und unbequem für den Nutzer. Das führt zu hohen

Abbruchquoten und einer schlechten Akzeptanz. Besonders schwierig gestaltet sich der Einsatz von Video- und Fernidentifikation. Gleichzeitig geht es in anderen europäischen Ländern schon um den eIDAS-konformen Einsatz neuer Innovationen, wie Methoden der automatisierten Identifikation und Authentifizierung. Es gilt, diese Anforderung europaweit zu vereinheitlichen, um digitale Dienste bequemer und besser zugänglich machen zu können.

9) **Online-Ausweisfunktion als die eID in Deutschland stärken**. Damit die Bürger den Mehrwert der eID-Funktion erkennen und sie stärker nutzen, sollte eine breit angelegte Kommunikationskampagne aufgesetzt werden. Die Kampagne sollte die unterschiedlichen Anwendungsbereiche und die Vorteile der Nutzung aufgreifen. Es ist wichtig aufzuzeigen, was der Online-Ausweis leisten kann, um dadurch seine Akzeptanz und Nutzung zu erhöhen. Der Antragsprozess für Diensteanbieter zur Verwendung der eID-Funktion sollte so einfach wie möglich sein. Auch die Nutzung muss vereinfacht werden, um mehr Dienste zu erschließen und damit Nutzer zu gewinnen. Das Ableiten der eID und die sichere Speicherung von Identitätsdaten auf dem Mobiltelefon spielt hierbei eine wichtige Rolle. Das von der Bundesregierung geförderte Projekt OPTIMOS hat hierfür wichtige Grundlagen geschaffen. Wenn es darum geht, weitere Berechtigungen und Dokumente hinzuzufügen, sollten weitere Ansätze ebenfalls einbezogen werden. Dies ist im Self-Sovereign-Identity-Ansatz dann ein ergänzender Schritt, durch den viele Use Cases erst praktisch erschlossen werden. Sei es ein digitaler Schlüssel, ein Studierendenausweis oder ein digital abgeleiteter Führerschein. Wir befürworten zudem eine europäische Vorschrift, die Gerätehersteller zur Öffnung ihrer NFC-Schnittstelle in diesem Zusammenhang verpflichtet.

10) **Das Smartphone als Identity Manager.** Die Bedeutung des Smartphones dürfte zukünftig eher noch zunehmen, nicht nur im privaten, sondern auch im betrieblichen Umfeld. Es muss ermöglicht werden, einzelne Attribute einer sicheren Identität auf ein Smartphone zu übertragen. Ein offenes Ökosystem, wie in der OPTIMOS-App geplant, welches z.B. aus dem Personalausweis abgeleitete Identitäten in den Sicherheitselementen von Mobilgeräten abspeichert, ist hierfür ein willkommener Ansatz. Dazu müssen die Sicherheitselemente der Mobilgeräte dringend weiter standardisiert werden. Die Bundesregierung wird dazu aufgerufen, die Arbeit der zuständigen Gremien zu unterstützen. Die zur Realisierung des OPTIMOS-Ansatzes notwendige Infrastruktur sollte sowohl auf nationaler Ebene als auch auf europäischer Ebene bereitgestellt werden. Zusätzlich sollten auf europäischer Ebene Mindestanforderungen für Secure Elements in Mobiltelefonen verbindlich festgelegt werden.

11) **Sicherheit und Effizienz in Balance.** Nicht jede Authentifizierung erfordert die Nutzung der Online-Ausweisfunktion des hoheitlichen Ausweisdokuments und nicht jedes Dokument erfordert die Absicherung durch eine qualifizierte Signatur. Die Verwaltung sollte allen digitalen Verwaltungsdienstleistungen ein bestimmtes Vertrauensniveau zuordnen. Dabei ist stets auf die Balance zwischen Effizienz, Nutzbarkeit, Komfort und Sicherheit zu achten. Außerdem sollte diese Zuordnung bundesweit einheitlich geregelt sein. Die relevanten Initiativen des IT-Planungsrates zeigen hier den richtigen Weg. Diese müssen gestärkt und zeitnah umgesetzt werden.

12) **Best-Practices für den Einsatz des Online-Personalausweises**. Bislang variieren die Einsatzmöglichkeiten des neuen Personalausweises zwischen den Kommunen zum Teil stark. Hier sollten zentral Best-Practice-Empfehlungen bereitgestellt werden, um eine gleichartige und möglichst breite Herangehensweise – zum Beispiel bei Bürgerkonten – zu ermöglichen. Denkbar wäre auch, die kommunalen Verwaltungen mit Basiskomponenten und Fachkomponenten zu unterstützen, um Technologie und Anwendung voneinander zu entkoppeln.

13) **Bei der OZG-Umsetzung auf die Synergien zur Single Digital Gateway (SDG) achten.** Wir halten es für wichtig, dass die einzelnen Umsetzungserfordernisse der europäischen SDG-Verordnung in die Digitalisierungsinitiativen zur OZG-Umsetzung (Onlinezugangsgesetz) einfließen, damit digitale Verwaltungsdienstleistungen zukünftig auch europaweit genutzt werden können.

14) **Qualifizierte Fernsignatur als Standard für die Bürgerkommunikation.** Die entsprechende Infrastruktur und die Anwendungsmöglichkeiten von elektronischen Signaturen sollten zentral bereitgestellt werden. So hätte jede Person eine sichere und einfach einsetzbare elektronische Signatur, die sie einwandfrei identifiziert.

15) **Leitlinien statt Eingriffe in die Industrie**. Sichere digitale Identitäten in Produktions- und Fertigungsprozessen müssen grundsätzlich im Gestaltungsbereich der Unternehmen liegen. Eine Zertifizierung von Herstellern durch staatliche Behörden wie das BSI sichert den Schutz digitaler Identitäten. Eine staatliche Zertifizierung von Prozessen und Kommunikation innerhalb der Unternehmen ist – sofern es nicht um kritische Infrastrukturen geht – jedoch kontraproduktiv, denn sie behindert den Wettbewerb und Innovation im Bereich der Vertrauensdienste.

16) **Innovative Angebote stärker im Blick haben**. Der steigende Bedarf an digitaler Authentifizierung – etwa bei Carsharing-Angeboten, im Bereich des Internets der Dinge, der Industrie 4.0 oder bei Transport und Logistik – erfordert einen stärkeren

Fokus legislativer Arbeit. Durch kluge Regulierung auf Basis der eIDAS-Verordnung sollten diese Prozesse mit passenden Standardisierungen und Zertifizierungen aus Unternehmensperspektive effizienter und aus Verbraucherperspektive praktischer gestaltet werden. Digitale Identitäten sind unerlässlich, um Datenintegrität zu gewährleisten. Denkt man z.B. an Sensortechnik in Smart Cities und dadurch generierte Daten, die Steuerungsentscheidungen als Grundlage dienen, ist es dringend erforderlich, dass die digitale Infrastruktur über abgesicherte Identitäten verfügt.

17) **Nachhaltigkeit fördern.** Nicht zuletzt ist auch die Bedeutung digitaler Identitäten für die Erfüllung nationaler, europäischer und globaler Nachhaltigkeitsziele in diesen Branchen enorm. Authentifizierung und Nachverfolgung können zur Bekämpfung der Umweltausbeutung, der Ausbeutung von Personen und auch der Produktpiraterie beitragen.