Digital Gipfel

Dortmund 2019

Ökosystem „Sichere digitale Identität“

Fokusgruppe Sichere Identitäten

Ökosystem „Sichere digitale Identität“

Fokusgruppe Sichere Identitäten, Digitalgipfel 2019

AUTOR*INNEN

Tobias Enke, Verimi GmbH
Martin Meingast, Deutschland sicher im Netz e. V.
André Nash, Bundesverband deutscher Banken e. V.
Rudolf Philipeit, buergerservice.org e. V.
Leslie Romeo, 1&1 De-Mail GmbH
Gabriele Sieck, Gesamtverband der Deutschen Versicherungswirtschaft e.V.
Dr. Jan Sürmeli, FZI Forschungszentrum Informatik
Rebekka Weiß, Bitkom e. V.
Stephan Wollny, T-Systems Int. GmbH
und weitere Mitglieder der Fokusgruppe

"Charakteristisch für digitale Plattformen ist ihre Netzwerkstruktur. Viele Teilnehmer der Plattformen tauschen Informationen aus und sind miteinander vernetzt -- der Nutzen und die Attraktivität der Plattform steigen mit der Anzahl ihrer Teilnehmer."

-- Bundesministerium für Wirtschaft und Energie[1]

Hintergrund

Digitale Plattformen vernetzen physisch weit voneinander entfernte Personen[2], um Transaktionen zwischen ihnen zu ermöglichen und so einen Mehrwert zu generieren. Doch dieser Mehrwert kann letztlich nur entstehen, wenn gewisse Annahmen über das "Gegenüber", also den Partner in einer Transaktion, mit einer hinreichenden Sicherheit getroffen werden können. Diese Annahmen können sich über unterschiedliche abstrakte Charakteristika des Transaktions-Partners erstrecken, wie zum Beispiel die Kreditwürdigkeit, Volljährigkeit oder ein Wohn- oder Geschäftssitz in Deutschland, oder konkrete Informationen über den Partner betreffen, wie beispielsweise einen Namen, eine Adresse oder eine Mitgliedsnummer. Welche Annahmen erforderlich sind und mit welcher Sicherheit diese Annahmen korrekt sein müssen, damit eine Transaktion zustande kommen darf, ist von ökonomischen und regulatorischen Faktoren abhängig.

Während in der physischen Welt "Papier-Identitäten" wie Ausweise oder beglaubigte Dokumente zur Prüfung herangezogen werden, bedient man sich in der digitalen Welt sogenannten "digitalen Identitäten". Die Sicherheit und Vertrauenswürdigkeit dieser

[1] https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/digitale-plattformen.html
[2] Sowohl juristische wie natürliche Personen; das Positionspapier beschränkt sich jedoch zunächst auf die digitalen Identitäten natürlicher Personen.

digitalen Identitäten ist daher essentiell für den erfolgreichen Abschluss einer digitalen Transaktion, somit Erfolgsfaktor für jede digitale Plattform und letztlich Grundstein einer Plattformökonomie.

DIGITALE IDENTITÄTEN

Eine digitale Identität eines Menschen ist seine Abbildung in einem digitalen System, sein "digitales ich". Eine digitale Identität kann verschiedene Informationen über den Menschen enthalten, z.B. grundlegende Stammdaten, wie seinen Namen oder Geburtsdatum, oder anwendungsfallspezifische Attribute wie beispielsweise seine Kundennummer bei einem Dienstanbieter.

Eine digitale Identität kann beispielsweise dafür verwendet werden ein neues Konto auf einer Plattform zu eröffnen, sich bei der Plattform anzumelden oder auf der Plattform mit anderen zu kommunizieren oder zu handeln. Problematisch hierbei ist, dass zu einem Menschen theoretisch beliebig viele digitale Identitäten existieren können, und sogar solche, die falsche, unvollständige oder veraltete Informationen beinhalten. Gerade bei digitalen Plattformen, deren Grundlage die Interaktion zwischen Akteuren ermöglichen, ist ein (häufig durch die Plattform vermitteltes) Vertrauen zwischen den Akteuren elementar. Basierend auf dem Anwendungsfall muss daher – aus ökonomischen Gründen oder gesetzlichen Vorgaben folgend – sorgfältig geprüft werden, ob die digitale Identität hinreichend korrekt, vollständig und aktuell ist. Das heißt, es muss sichergestellt werden, dass die hinterlegten Attribute mit einer für den Anwendungsfall ausreichenden Sicherheit mit den tatsächlichen Attributen des Menschen übereinstimmen.

Beispiel: Die Nutzung eines Mietwagens erfordert die Überprüfung der Identität und ob eine gültige Fahrerlaubnis vorliegt. Im Falle moderner Mobilitätsdienste findet die Registrierung nicht in einer Filiale sondern digital statt, z.B. in einer Smartphone-App.

Diese Prüfung kann auf unterschiedlichen Wegen erfolgen, z.B. durch die Nutzung einer eID-Anwendung (vgl. Online-Ausweis) oder durch den Einsatz eines Drittanbieters (online durch ein Video-Ident-Verfahren oder offline durch Post-Ident).

Abhängig vom gewählten Lösungsansatz sind diese Prüfungen mit Kosten und Zeitaufwand verbunden – und liegen üblicherweise außerhalb des Kerngeschäfts von Unternehmen. Daher ist es erstrebenswert, die Prüfung zwar so häufig wie nötig doch so selten wie möglich durchzuführen. Anstatt eine digitalen Identität bei jeder Verwendung aufwändig zu überprüfen, kann unter Umständen auf vorherige Prüfungen zurückgegriffen und sich auf einfachere Prüfschritte beschränkt werden. Dafür ist es essentiell, nachvollziehen zu können, dass die vorherige Prüfung von einer vertrauenswürdigen Instanz oder Technologie vorgenommen wurde.

Beispiel: Eine Person möchte bei einem (fiktiven) Mobilitätsanbieter CarShare24 einen Mietwagen nutzen. Bei der Registrierung könnte die Überprüfung der Fahrerlaubnis stark vereinfacht werden, wenn die Person bereits bei einem anderen Anbieter, z.B. dem (fiktiven) Dienst MietMich, diese Überprüfung durchgeführt hat und dies beweisen kann.

Diese Information könnte CarShare24 von MietMich erhalten. CarShare24 muss sich jedoch versichern können, dass MietMich die Überprüfung ordnungsgemäß durchgeführt hat und nicht in Kenntnis einer entzogenen Fahrerlaubnis ist. Die Beziehung zwischen den beiden Mobilitätsanbietern kann auch indirekt über andere Dienste durchgeführt werden, die als Treuhänder auftreten und möglicherweise zusätzliche Garantien aussprechen.

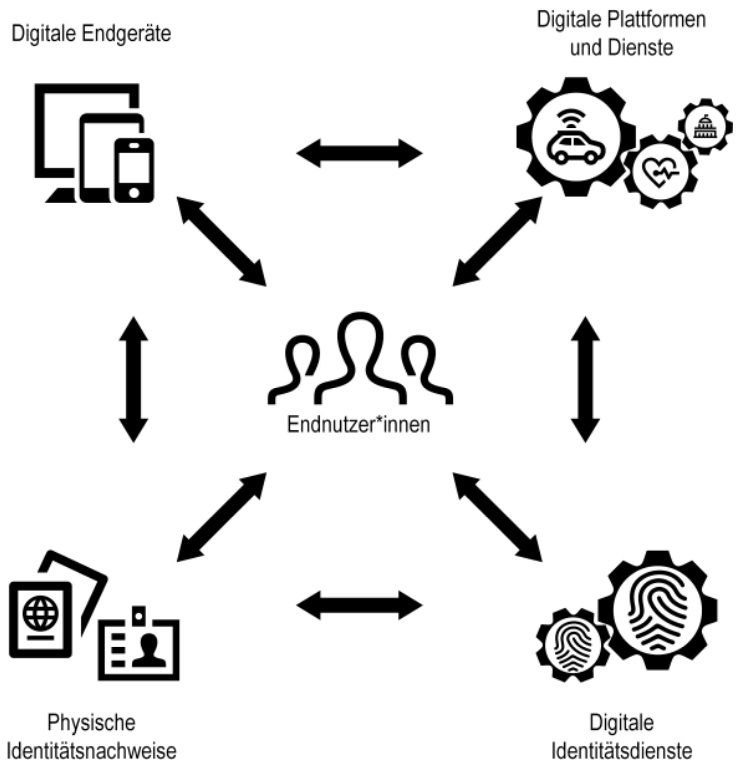
Aus Sicht des Menschen, dessen Identität geprüft wird, ist es auch häufig relevant, dass er der prüfenden Instanz oder Technologie ein gewisses eigenes Vertrauen entgegenbringt. Dies ist insbesondere dann der Fall, wenn bei der Prüfung sensible Attribute inspiziert werden, die nicht in der digitalen Identität enthalten sind. So könnte beispielsweise die digitale Identität nur das Attribut „ist volljährig“ enthalten, die Prüfung jedoch das Geburtsdatum heranziehen.

"SICHERE DIGITALE IDENTITÄT" ALS KERN DES ÖKOSYSTEMS

Eine Wiederverwendung einmal geprüfter digitaler Identitäten und die damit einhergehende Vereinfachung der Prüfschritte ermöglichen es Marktteilnehmern mit weniger Aufwand an digitalen Plattformen teilzunehmen oder solche selbst zu entwickeln. Die Wiederverwendung geprüfter digitaler Identitäten für unterschiedliche Anwendungsfälle erfordert gewisse Vertrauensbeziehungen zwischen den beteiligten Akteuren: Endnutzer*innen mit ihren digitalen Endgeräten, Diensteanbieter und digitale Plattformen, Identitätsdienste, etc. Diese Vertrauensbeziehungen können sich unter anderem in der Form von bilateralen oder multilateralen Vertragsbeziehungen äußern, sowie auch in Zertifizierungen und Nachweisen der Konformität zu den Standards durch die einzelnen Akteure. Insbesondere muss neben der Prüfung und Kennzeichnung zur Wiederverwendbarkeit auch sichergestellt werden, dass als inkorrekt oder veraltet erkannte digitale Identitäten keine weitere Verwendung mehr finden.

Dies motiviert die Etablierung eines Vertrauensnetzwerks „sichere digitale Identität“, das diese Vertrauensbeziehungen zwischen Akteuren abbildet, um so die Wiederverwendung geprüfter digitaler Identitäten in unterschiedlichen Anwendungsfällen zu ermöglichen.

Im Herzen eines solchen Vertrauensnetzwerks müssen die Endnutzer*innen und ihre digitalen Identitäten stehen: Sie verwenden digitale Plattformen und Dienste über digitale Endgeräte, und identifizieren sich dort, um persönliche Dienste angeboten bekommen zu können. Das Rückgrat eines solchen Vertrauensnetzwerks bilden Identitätsdienste, die Identitäten erstellen, prüfen, bestätigen und/oder terminieren. Dabei können diese auch auf physische Identitätsnachweise wie zum Beispiel den elektronischen Personalausweis oder Mitgliedskarten zurückgreifen. Anbieter digitaler Plattformen und Dienste können in ihren jeweiligen Geschäftsprozessen solche geprüften Identitäten verwenden, die den anwendungsfallspezifischen Bedingungen genügen. Die Identitätsdienste treten jedoch auch als Vertrauensinstanzen für Endnutzer*innen auf, das heißt, die Menschen, die die digitalen Plattformen verwenden.



ANFORDERUNGEN AN DAS VERTRAUENSNETZWERK UND SEINE TEILNEHMER

Das Vertrauensnetzwerk soll dabei die folgenden Eigenschaften erfüllen:

SICHERHEIT

Die Sicherheit digitaler Identitäten ist das höchste Gebot, da es sich hierbei um die sensibelsten Daten der Bürgerinnen und Bürger handelt. Diese Daten gilt es zu schützen. Zum einen damit die Nutzer die eigene Datensouveränität wahren können. Zum anderen benötigen Unternehmen und Behörden die Rechtssicherheit und Verbindlichkeit, dass es sich bei einer genutzten digitalen Identität wirklich auch um den Identitätsinhaber handelt.

Die Grundlage dafür bildet die sichere Identifizierung, in der Identitätsattribute wie Name, Alter, Wohnort, etc. zweifelsfrei verifiziert werden, zum Beispiel durch Prüfung physischer Personaldokumente, und der anschließenden Ableitung hin zu einer elektronischen Identität. Geltende Sicherheits- bzw. Vertrauensniveaus (z. B, niedrig, substanziell, hoch) gewährleisten nationale und europäische Anerkennung der Identifizierung.

Die Authentifizierung sichert die Wiedererkennung einer Person, wenn sie erneut Zugang zu einem Service benötigt. Die Anmeldung sollte stets zusätzlich gesichert sein, mittels einer Zwei-Faktor-Authentifizierung, z. B. über biometrische Merkmale.

Auf Seiten der Identitätsanbieter müssen Daten sicher verschlüsselt werden, zu nennen sind dabei die individuelle Datenverschlüsselung, die Trennung von Daten- und

Schlüsselaufbewahrung sowie die verschlüsselte interne und externe Kommunikation. Darüber hinaus muss eine klare Sicherheitsinfrastruktur z.B. durch Multiple Availability Zones, Serverstandorte in Deutschland / Europa und ein geprüftes Sicherheitsmanagement und -monitoring etabliert sein.

TRANSPARENZ UND SOUVERÄNITÄT

Jeder Nutzer muss souverän seine digitale Identität verwalten können. Unerlässlich ist dafür der transparente und faire Umgang mit Daten. Für Anbieter gelten die Prinzipien Privacy-by-Default und Security-by-Design. Den Nutzern muss die Kontrolle über ihre Datenübermittlungen gegeben werden. Dafür sollten Identitätsdiensteanbieter den Nutzern gängige technische Verfahren anbieten, damit diese Übersicht über ihrer Aktivitäten und Transaktionen behalten.

Vertrauen in die digitale Identität baut sich durch Transparenz auf. Daher sollte eine Vermengung von Verhaltens-/Transaktionsdaten mit der verifizierten digitalen Identität nicht erfolgen bzw. ausschließlich auf expliziten Wunsch der Endnutzer*innen. Auch die kommerzielle Nutzung persönlicher Daten für Werbezwecke kann nur auf Wunsch und unter Zustimmung der Endnutzer*innen erfolgen.

USABILITY

Um im Wettbewerb mit global agierenden Unternehmen und deren etablierten Lösungen zu bestehen, muss das Vertrauensnetzwerk und die darin tätigen Anbieter sowohl Sicherheit als auch eine hohe Benutzerfreundlichkeit bieten.

Erfolgreiche Lösungen basieren in allen Branchen auf zukunftsgerichteten, nutzerzentrierten Technologien. Daher ist eine verlässliche und barrierefreie Verfügbarkeit auf allen Endgeräten vorrangig. Vor allem das Smartphone ist als „Token“, den alle Nutzer stets und überall mit sich führen und auf dem Sie Einsatzmöglichkeiten ihrer digitalen Identität erwarten, geeignet.

UNABHÄNGIGKEIT

Das Netzwerk sollte dabei offen und gleichberechtigt konzipiert sein: Es darf keinen grundsätzlichen Ausschluss von Marktteilnehmern und keine Diskriminierung über Geschäftsmodelle geben, solange diese mit den hier aufgeführten Leitlinien des Netzwerks einhergehen.

Die Herausforderung dabei ist die Interoperabilität der Systeme, d.h. die Möglichkeit sich mit anderen Systemen zu verknüpfen, um so eine branchenübergreifende Nutzung der digitalen Identität sicherzustellen. Interoperabilität benötigt einheitliche und übergreifende Standards. Ein plattformbasiertes Vertrauensnetzwerk kann diese Interoperabilität herstellen.

STANDARDS

Die Standards und der Nachweis der Konformität zu diesen Standards, wie Zertifizierungen und Herstellererklärungen, bilden die wesentliche Grundlage für die Funktionen im System, das Vertrauen in das System und die Interoperabilität des Systems zwischen den beteiligten Akteuren.

Wichtig ist hier der Einsatz von weit verbreiteten, aktuellen Standards auf dem Stand der Technik für die technischen Belange (z.B. Authentifizierungsstandards wie Open ID Connect, FIDO2, WebAuthn, OAuth2.0) und übergreifenden, EU-weit anwendbaren Regularien (eIDAS, DSGVO, PSD2) für die rechtlichen und regulatorischen Belange.

Bei Letzteren ist unbedingt auf eine Harmonisierung der Anforderungen und Regelungen zu achten, zwischen den Mitgliedsländern der EU, den unterschiedlichen Ressorts und den föderalen Geltungsbereichen in Deutschland. Falls diese Harmonisierung nicht existiert, wäre sie herbei zu führen.

BRANCHENÜBERGREIFENDES VERTRAUENSNETZWERK

Ein Mehrwert entsteht vor allem dann, wenn das Vertrauensnetzwerk Silogrenzen durchbricht und anwendungsfall- und sogar branchenübergreifend funktioniert. So sollten Bürger*innen eine einmal angelegte digitale Identität gleichzeitig unter anderem für digitale Bürgerdienste, eHealth-Anwendungen, Bank- oder Versicherungsgeschäfte, für Nachweise z. B. im Bereich der Telekommunikation oder bei Mobilitätsangeboten sowie auch bei smart-home-Anwendungen oder für einfache Altersverifikationen nutzen können.

Die Berücksichtigung der oben dargestellten Grundelemente Sicherheit, Transparenz und Souveränität, Usability, Unabhängigkeit sowie Schaffung und Einsatz von Standards sind dabei die Voraussetzung für eine erfolgreiche Etablierung von Vertrauensnetzwerken sowie deren Glaubwürdigkeit und Akzeptanz bei den Anwendern. Unabhängig von der Art des Ökosystems, in dem das Vertrauensnetzwerk Anwendung findet, oder von der Art der Darstellung der digitalen Identität sind diese Grundelemente daher stets zu beachten und tragen maßgeblich zu dem Erfolg der jeweiligen digitalen Plattformen bei. Die Kriterien bieten auch die Chance auf ein Level-Playing-Field, welches eine hohe Wettbewerbsfähigkeit und Innovationskraft erhält.