Wegweiser digitale Identitäten und Nachweise

(WIN)

Ziel dieses Wegweisers ist es, einen Einstieg in die Begriffswelt digitaler Identitäten und ihrer Anwendungen bereitzustellen, die Einzug in den öffentlichen Sprachgebrauch unserer digitalisierten Gesellschaft finden.

Aufgrund der Zunahme der Bedeutung digitaler Identität(en) in der Lebenswelt entwickeln sich neue technische Ansätze. Ziele der vielschichtigen Entwicklungen sind,

- die Verifikation von Informationen zu vereinfachen,
- Sicherheit durch Standardisierung und stabile Rahmenbedingungen (EU-Regulatorik) zu gewährleisten,
- Prozesse zu automatisieren und zu beschleunigen.

Eine Besonderheit dieser dynamischen technischen Entwicklung liegt darin, dass Nutzenden mehr Verantwortung übertragen wird, und daher ein Grundverständnis dieser neuen Formen des Daten- und Identitäten Management zu gewährleisten ist.

Um entsprechend ein Basisverständnis der Grundüberlegungen und technischen Funktionsweisen aufzubauen und Prozesse des Life Long Learning (lebenslanges Lernen) zu unterstützen, wurde dieser Wegweiser erstellt.

Nachstehende Begriffe werden im WIN erläutert:

Wallet
Digitaler Nachweis
Digitale Identität
Signatur

Der „Wegweiser digitale Identitäten und Nachweise“ entstand im Rahmen des Programms „Schaufenster Sichere Digitale Identitäten“, gefördert durch das Bundesministerium für Wirtschaft und Klimaschutz. An seiner Erstellung waren Personen aus den folgenden Projekte beteiligt: ID-Ideal (FKZ 01MN21001*), IDunion (FKZ 01MN21002*), SDIKA (FKZ 01MN21004*).

Insbesondere wirkten mit: Benjamin Burde, Timo Burkhard, Sascha Dobratz, Matthias Fuhrland, Jonas Hammer, Christopher Praas und Jan Sürmeli.

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

✧ Wallet

Eine Wallet ist ein Speicherort für Daten. Diese Daten können in unterschiedlicher Form vorliegen und dementsprechend digital oder visuell ausgelesen werden (z.B. Kreditkarten, Eintrittskarten, Boarding Tickets oder auch Ausweise/Zertifikate).

Wallet-Typen

Es gibt verschiedene Wallet-Typen, welche sich in Bedienung sowie im Funktions- und Sicherheitsumfang unterscheiden können:

- webbasierte Anwendungen (Browser z.B. Chrome, Firefox, Safari)
- Applikationen auf Endgeräten (z.B. Wallet-Apps auf Smartphones)
- In Form speziell gesicherter Hardware (z.B. Cold-Wallets)

Einzelne Wallets können aktuell nur spezifische digitale Formate aufnehmen.

Wallet-Inhalt

Aktuell werden in gängigen Wallet-Apps beispielsweise Kreditkarten, Eintritts- oder auch Bordkarten verwahrt. Diese unterscheiden sich von Digitalen Nachweisen, die in ihrem technischen Design und ihrer Funktionalität weit über vorgenannte Nutzungen hinausgehen. Um dieses „Design“ besser zu verstehen ist es sinnvoll das Begriffspaar „Digitaler Nachweis“ anzuschauen.

✧ Digitaler Nachweis

Nachweis

Mit einem Nachweis wird eine Behauptung belegt. Beispielsweise, dass ein Individuum ein Flugzeug führen (Pilotenschein), eine Baustelle betreten (Zugangsberechtigung), oder eine Fortbildung abgeschlossen (Zertifikat) hat.

Digitaler Nachweis

Ein digitaler Nachweis wird von einer ausstellenden Entität (Person, Organisation, Objekt) für eine empfangende Entität ausgestellt. Die Daten/Informationen in einem Nachweis werden als Attribute bezeichnet. Diese können beispielsweise aus einem öffentlichen Register stammen (z.B. Vereinsregister). Ein Nachweis kann einzelne oder mehrere Attribute enthalten.

Ein digitaler Nachweis besteht, bildlich formuliert, aus einem Umschlag und dessen Inhalt. Der Umschlag dient einem doppelten Zweck: er stellt die Identität der ausstellenden Entität sicher und schützt den Inhalt (Nachweis) vor Fälschung.

Die Besonderheit des digitalen Nachweises liegt in seiner Signatur. Diese ist

- fälschungssicher, nicht nachahmbar, unveränderlich und
- sowohl der ausstellenden als auch der empfangenden Entität eindeutig zuzuordnen.

Der Kernaspekt digitaler Nachweise ist, dass deren Echtheit Orts- und zeitunabhängig überprüft und belegt werden kann. Dies in Echtzeit.

Eine weitere Besonderheit digitaler Nachweise liegt in der Möglichkeit einzelne Attribute, anstelle des gesamten Nachweises, zu präsentieren. Dieses als „selective disclosure“ (Selektive Weitergabe) bezeichnete Verfahren ermöglicht es der empfangenden Entität, nur jene Attribute weiterzugeben, die erforderlich oder relevant erscheinen.

Postsystem

Um ein Ökosystem für digitale Nachweise zu begründen (Erstellen, Senden, Empfangen, Überprüfen), braucht es ein Postsystem. Hierzu wird jeder Entität ein Identifikator zugewiesen, vergleichbar einer Postadresse. Dieser ermöglicht es, einen Kommunikationskanal zum Austausch von Nachweisen zwischen zwei Entitäten einzurichten. Je nach eingesetzter Technologie kann eine Entität über beliebig viele Identifikatoren verfügen, die sie unabhängig voneinander einsetzen kann.

✧ Digitale Identität

Digitale Identitäten werden benötigt, um Kommunikation (Austausch von Daten/Informationen) im virtuellen Raum/Netzwerken sowie Zugang zu Dienstleistungen zu ermöglichen. Diese können natürliche Personen und weitere Entitäten (Organisationen und Objekte) der analogen Welt im digitalen Raum repräsentieren. Eine Entität kann mehrere digitale Identitäten besitzen.

Aktuell erhalten natürliche Personen eine digitale Identität beispielsweise über Service-Anbieter. Diese können vielfältig zum Einsatz kommen (Social Media Plattformen, E-Commerce). Bei jeder Nutzung dieser Services, beispielsweise für einen Login zur Nutzung einer Dienstleistung, fließen vielfältige Informationen über die Person (Nutzerverhalten). Diese Datenflüsse sind für Nutzende nicht transparent und können damit auch nicht begrenzt werden.

Eine weitere Möglichkeit, eine digitale Identität zu erhalten, besteht darin, sich von einer Behörde eine hoheitliche digitale Identität (eID) ausstellen zu lassen.

Merkmale

Eine digitale Identität umfasst jene Merkmale, die einer Entität im spezifischen Kontext (Social Media, eID…) zugeordnet werden. Bei natürlichen Personen sind dies z.B. körperliche Merkmale (Größe, Augenfarbe). Es können auch nicht-körperliche Merkmale hinzukommen, wie eine Steuer-ID, Mitgliedsnummer oder auch Führerschein-Nummern. Inwieweit der digitale Fußabdruck, beispielsweise Konsumverhalten natürlicher Personen, einer digitalen Identität zuzuordnen sind, ist diskutabel und wird hier nicht vertieft. Entsprechend unterliegt die Definition des Begriffs der digitalen Identität auch Wandlungen, und kann nicht als fix angenommen werden.

Im Bereich der Objekte sind vorgenannte Merkmale in der Regel Identifikationsnummern (MAC-Adressen, IP-Adressen, …). Bei Organisationen kann dies beispielsweise die HR-Nummer (Handelsregister) oder Steuernummer sein.

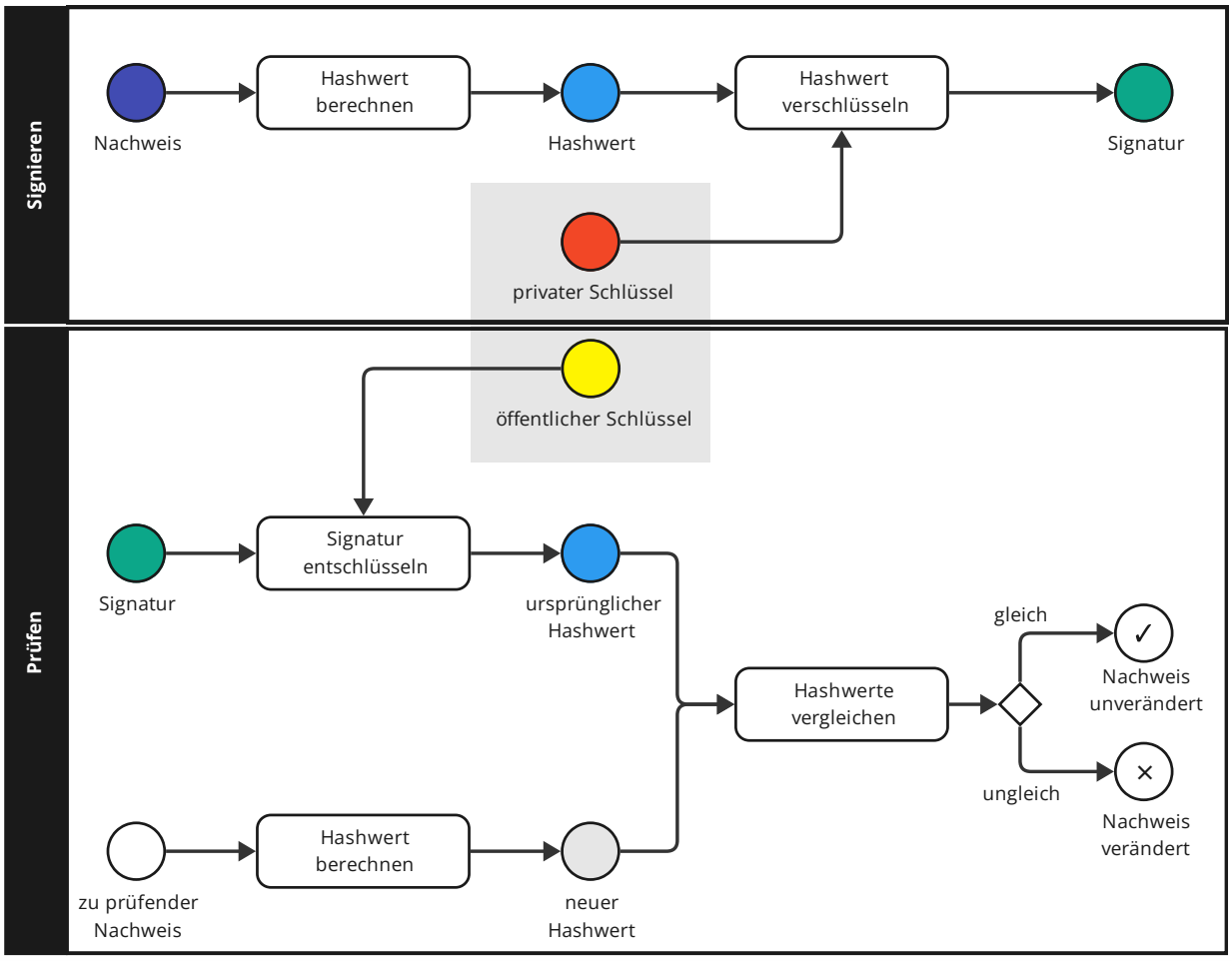
✧ Signatur

Wird ein digitaler Nachweis ausgestellt, ist sicherzustellen, dass die ausstellende und die empfangende Entität eindeutig zu identifizieren sind, und der Inhalt des Nachweises unverfälscht bleibt. Dies ermöglicht es Dritten, den präsentierten Nachweis in Echtzeit zu prüfen und zu vertrauen. Ein wichtiger technischer Baustein sind digitale Signaturen.

Eine digitale Signatur der ausstellenden Entität ist eine Zeichenkette, die es ermöglicht, die Integrität eines Nachweises mit Verschlüsselungs- und Entschlüsselungsverfahren zu prüfen.

Voraussetzung für die Erstellung einer digitalen Signatur ist ein kryptographisches Schlüsselpaar:

- Ein privater Schlüssel, der nur der ausstellenden Entität bekannt ist, für den Signiervorgang.
- Ein öffentlicher Schlüssel für den Prüfvorgang.



Signieren mit dem privaten Schlüssel

Eine Signatur wird erzeugt, indem die ausstellende Entität den digitalen Nachweis verschlüsselt. Hierzu nutzt sie ihren privaten Schlüssel. Eine Signatur erstellen kann also nur, wer Zugang zum privaten Schlüssel hat.

Prüfen mit dem öffentlichen Schlüssel

Um die Integrität des Nachweises zu prüfen, wird die Signatur entschlüsselt. Dies mit dem öffentlichen Schlüssel der ausstellenden Entität. Das Ergebnis dieses Vorgangs ist der ursprüngliche Nachweis. Eine mögliche Veränderung des Nachweises würde bei einem Abgleich sichtbar werden. Prüfen kann entsprechend, wer Zugang zum öffentlichen Schlüssel hat.

Einsatz von Hashwerten

In der Praxis wird statt des Nachweises nur ein sogenannter Hashwert des Nachweises signiert, der kleiner (Datenmenge) ist als der Nachweis selbst. Der Prüfvorgang ergibt entsprechend auch nur den Hashwert anstelle des ursprünglichen Nachweises. Aus dem Hashwert kann der ursprüngliche Nachweis nicht rekonstruiert werden. Das ist jedoch kein Problem:

- Der Hashwert kann jedoch jederzeit neu berechnet werden.
- Wurde der Nachweis verändert, verändert sich auch der Hashwert.

Exkurs: Rechtliche Perspektive / Qualifizierte Signatur

Der Signaturbegriff wird in verschiedenen Fachkontexten verwendet. Zum einen, wie im oben beschriebenen technischen Kontext, verwendet. Im juristischen Kontext ist dies die elektronische Signatur:

Maßgeblich ist hier die eIDAS Verordnung. Bei dieser handelt es sich um einen europaweit gültigen Rechtsrahmen für elektronische Signaturen. Dies ermöglicht eine schnelle Verbreitung der Anwendungsmöglichkeiten von elektronischen Signaturen. Innerhalb der Verordnung werden drei Grundtypen unterschieden: Einfach, Fortgeschritten, Qualifiziert.

Einfache elektronische Signatur

Daten, welche Rückschlüsse auf die Authentizität der oder des Signierenden ermöglichen, werden elektronisch mit einem Dokument verbunden. Ein entsprechendes Beispiel ist die

gewöhnliche E-Mail-Signatur, die mit dem eigenen Namen unterzeichnet wird, ein Bild einer Unterschrift oder das händische Unterzeichnen auf einem Touchpad. Es sind weder überprüfbare Aussagen über die Identität der oder des Signierenden noch über die Integrität der Daten möglich. Hierbei handelt es sich um die Form mit der schwächsten rechtlichen Wirkung.

Fortgeschrittene elektronische Signatur (FES)

Die Identität der oder des Signierenden wird geprüft, um die Authentizität zu bestätigen. Mittels kryptographischer Verfahren wird die Integrität der Dokumenteninhalte sichergestellt. Hierzu wird ein Drittanbieter benötigt, der dem Signierenden nach Identifizierung ein kryptographisches Schlüsselpaar ausstellt. Als Beispiel lässt sich hier das Verschlüsselungsverfahren PGP aufführen. Hierdurch kann die Identität der oder des Signierenden durch Dritte nachvollzogen werden. Sie bietet mehr Sicherheit, da eine eindeutige Zuordnung und Identifizierung des Signierenden erforderlich ist und eine Manipulation der Daten erkennbar wird.

Qualifizierte elektronische Signatur (QES)

Im Unterschied zur FES wird bei der QES ein staatlich geprüfter Anbieter genutzt. Aufgrund dieser zusätzlichen Sicherheit erfolgt eine Gleichstellung der QES mit der herkömmlichen handschriftlichen Unterschrift gemäß §126a BGB und die Zuteilung eines erhöhten Beweiswert.

	Einfache Signatur	**Fortgeschrittene Signatur (FES)**	**Qualifizierte elektronische Signatur (QES)**
Wirkung	Nur Bestätigung eines Vorgangs; Vertragsschluss dennoch möglich Kein besonderes Vertrauen und Sicherheit	Schutz vor Manipulation, dient dem Identitätsnachweis Höheres Vertrauen und Sicherheit aufgrund von Prüfung der Integrität und Authentizität	Erfüllung der Schriftform; Gleichzusetzen mit einer handschriftlichen Unterschrift Erhöhtes Vertrauen und Sicherheit aufgrund von staatlicher Prüfung der Integrität und Authentizität

	Einfache Signatur	Fortgeschrittene Signatur (FES)	Qualifizierte elektronische Signatur (QES)
Entstehung und technische Grundlage	Keine besonderen Voraussetzungen	Unterschiedliche kryptographische Verfahren z.B. PKI	Herausgabe erfolgt durch einen geprüften Dritten Dienstleister (Vertrauensdiensteanbieter) nach einem rechtlich geprüften und festgelegten Verfahren mit einer Signaturerstellungseinheit, Nutzung eines elektronischen Zertifikats
Identifikation	Nein	Ja ohne rechtliche Vorgaben	Ja mit rechtlichen Vorgaben (2FA)
Kontext der Nutzung	Internet, interne Kommunikation	Kommunikation	Verträge mit Schriftformerfordernis
Rechtliche Grundlage und Rechts-wirkung	Art. 3 Nr. 10 eIDAS; Art. 25 eIDAS Freie richterliche Beweiswürdigung	Art. 3 Nr. 11 eIDAS; Art. 25 eIDAS Freie richterliche Beweiswürdigung	Art. 3 Nr. 12 eIDAS; Anhang I eIDAS; §126a BGB Art. 25 eIDAS Beweiskraft privater Urkunden: Urkunde, die von einer Privatperson ausgestellt wurde und deren Echtheit durch Unterzeichnung des Ausstellers festgestellt werden kann (Testament, ...).
Beispiel	E-Mail-Signatur	PGP	Vertragsschluss
Vorteile	Keine gesonderten Vorteile und somit nur für einfache oder interne Prozesse geeignet	Ein Vertrauen in den signierten Datensatz kann durch die eindeutige Identifizierung des Absenders gewährleistet werden	Verkürzung des Prozesses zum Vertragsschluss beim Schriftformerfordernis aufgrund des rechtssicheren Versendens auf elektronischem Weg anstatt des langsameren Postwegs