Matthias Fuhrland, Jürgen Anke (HTW Dresden),
Timo Burkhardt, HS Mittweida), 2023

Trustnet

Verifiable Credentials

Was ist das?

Ein digitaler verifizierbarer Nachweis (Verifiable Credential) wird von einer Entität (Person, Organisation, Objekt) ausgestellt. Er besteht im Kern aus einem oder mehreren gesicherten Attributen (Inhalt) und einer kryptografischen Signatur. Die Signatur, obwohl eine Abfolge von Zeichenketten, ist nicht zu vergleichen mit einer händischen Unterschrift. Sie ist fälschungssicher, unnachahmlich, unveränderlich und sowohl dem Aussteller als auch dem Dokumenteninhalt sowie optional auch dem Empfänger eindeutig zuzuordnen. Dafür bindet der Herausgeber mit Hilfe des entsprechenden digitalen Schlüsselmaterials seinen eigenen Identifikator sowie optional den Identifikator des Empfängers und einen Hash des Inhalts kryptographisch in die Signatur ein. Der Kernaspekt verifizierbarer Nachweise ist, dass anhand der Signatur die Authentizität von Herausgeberschaft sowie optional von Empfänger und Inhalt der Nachweise orts- und zeitunabhängig in Echtzeit überprüft und belegt werden kann (siehe Abb. 1).

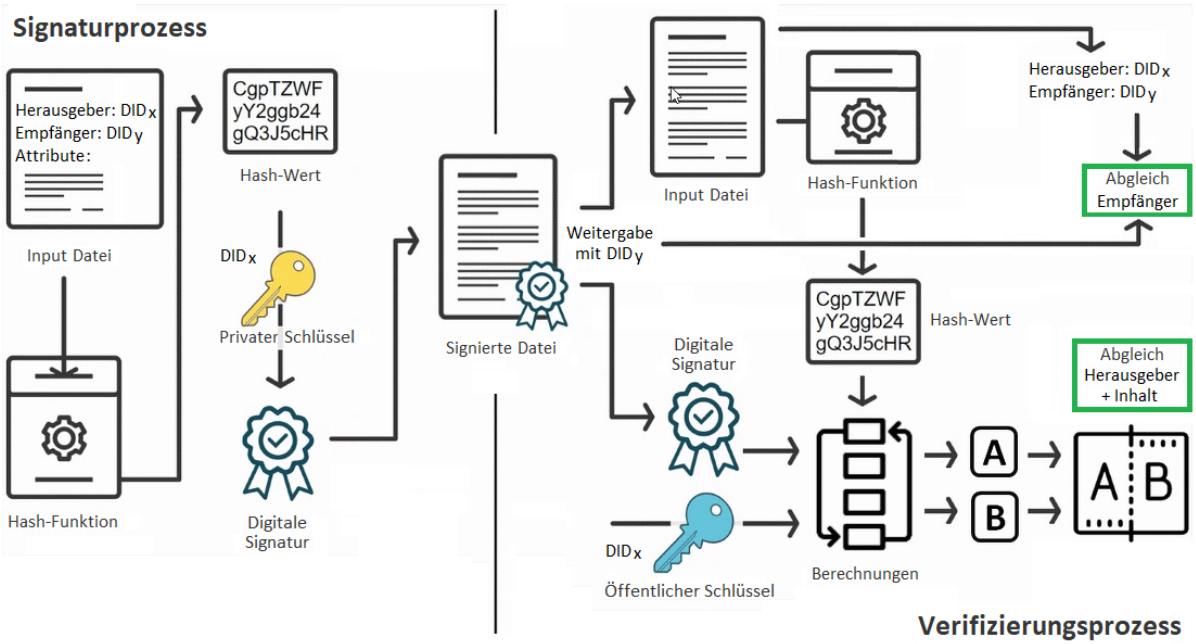

Abb. 1: Signatur- und Verifizierungsprozess bei Verifiable Credentials

Um ein Ökosystem für digitale Nachweise zu begründen (Erstellen, Senden, Empfangen, Überprüfung), braucht es ein digitales Kommunikationssystem. Hierzu wird jedem Akteur ein Identifikator (DID = Decentralized Identifier) zugewiesen, vergleichbar einer Telefonnummer. Dieser Identifikator ermöglicht es, einen exklusiven Kommunikationskanal zum Austausch von Nachweisen zwischen zwei Akteuren einzurichten und ist – wie oben beschrieben - auch Bestandteil des Signaturprozesses von Nachweisen. Verifiable Credentials sind bereits ein internationaler W3C-Standard.

Mehrwert der Verifiable Credentials gegenüber dem Stand der Technik

Angesichts der Tatsache, dass mit signierten PDF-Dokumenten und der eID bereits technische Lösungen für digitale Nachweise und Ausweise natürlicher Personen existieren, stellt sich die berech-

tigte Frage, worin konkret der Mehrwert von Verifiable Credentials liegt. Tabelle 1 stellt hierzu die im Kontext des Trustnets relevanten Eigenschaften vergleichend gegenüber.

Eigenschaft	Signiertes PDF	eID	VC nach W3C
Herausgeberschaft prüfbar	X	X	X
Inhaber prüfbar	-	X	X
Authentizität des Inhalts prüfbar	X	X	X
Portables Datenformat	X	-	X
Austauschprotokoll	-	X	X
Maschinenlesbarer Inhalt	-	X	X
Auslesbarkeit einzelner Attribute (Selective Disclosure)	-	X	X
Skalierbarkeit im Internet	-	-	X
Flexible Abbildung von Sachverhalten	X	-	X
Kompatibilität mit bestehenden Systemen	X	-	In Zukunft
Einfache Zugänglichkeit für Dienstanbieter	X	-	In Zukunft
Identifizierbarkeit von Objekten	-	-	X
Identifizierbarkeit hoheitlicher Entitäten	-	-	X
Identifizierbarkeit juristischer Personen	-	X	X

Tabelle 1: Unterschiede zwischen signiertem PDF, eID und Verifiable Credential nach W3C-Standard

Es ist offenkundig, dass mit Verifiable Credentials als einheitlichem Vertrauensmechanismus die nächste Evolutionsstufe des Internets erreicht werden kann, unabhängig davon, welche zusätzlichen Vertrauensmechanismen für das Trustnet künftig noch entwickelt/genutzt werden.

Mögliche Inhalte einer digitalen Wallet

Digitale Nachweise haben unterschiedliche Lebensdauern. Während sich die Basisidentität einer natürlichen Person nur sehr selten ändert (z.B. bei Umzug), bestehen Ausbildungsnachweise nach

IDs von natürlichen Personen	IDs von juristischen Personen	IDs von Objekten
Identifizierungsdaten: - Daten vom dt. Melderegister (eID / Personalausweis inkl. biometrischer Daten) - Daten zur doppelten Staatsbürgerschaft - ID beim Finanzamt - ID bei der Sozialversicherung	Identifizierungsdaten: - Daten vom Gewerbeamt - Daten vom deutschen Handelsregister - Daten internationaler Register - ID beim Finanzamt - ID bei der Unfallkasse	Identifizierungsdaten: - Daten vom Hersteller/Züchter - Daten zuständiger Melderegister - Daten zuständiger Ämter (z.B. Liegenschaftskataster)
Familiäre ID-Beziehungen - Abstammungsdaten - Elternschaft bei Kindern - Ehe- / eheähnliche Partner	Familiäre ID-Beziehungen - Private Anteilseigner - Verbundene Unternehmen	Eigentumsbeziehungen - Abstammungsdaten - Amtl. Eigentumsnachweise (z.B. Grundbuch-/Patentamt)
Rechtliche ID-Beziehungen - Erziehungsberechtigungen, Vormundschaften - Vertretungsrechte, Vollmachten - gerichtl. Verfügungen - Digitale Erbberechtigung	Rechtliche ID-Beziehungen - Vertretungsrechte (Geschäftsführer, Prokurist) - Vollmachten (z.B. Anwälte, Steuerberater) - Genussrechte, Stimmrechte	Besitz- und Nutzungsrechte - Daten von Vermietern und Verkäufern - Daten von Lizenzgebern - Lieferaufträge
Persönliche Nachweise - Ausbildungsnachweise, Führerscheine - Zertifikate, Arbeitszeugnisse - Bezugsrechte für Sozialleistungen …	Firmen-Nachweise - Zertifizierungen (z.B. nach DIN ISO 9001) - Referenzen anderer Unternehmen/Ministerien - …	Objekt-Nachweise - Zulassungsdaten (z.B. Betriebsgenehmigungen, Fahrzeugscheine) - Zolldaten
Zugehörigkeitsausweise - Mitgliedsausweise, Mitarbeiterausweise - Mitwirkungsnachweise	Unternehmensmitgliedschaften - Branchenverbände, Industrielle Vereine - Kammern	Objektzugehörigkeiten - Produktions-/Liefercharge -
Zugangsrechte zu Objekten - Veranstaltungstickets, Fahrscheine - Zugangsrechte in Gebäuden, Mietbescheinigungen - Softwarelizenzen …	Zugangsrechte zu Objekten - Zugangsrechte in Gebäuden oder auf Grundstücken - Überflugrechte	Zugangsrechte mobiler Objekte (Tiere/Drohnen) - Zugangsrechte in Gebäuden oder auf Grundstücken - Überflugrechte
Eigentumsnachweise - Bankkontodaten - Kaufverträge - Urheberrechte, Herstellungsnachweise	Eigentumsnachweise - Bankkontodaten - Kaufverträge - Urheberrechte, Herstellungsnachweise	
Veränderungsrechte an eigenen Objekten - Behördliche Genehmigungen (z.B. Bau-/ Entsorgungsgenehmigung) …	Veränderungsrechte an eigenen Objekten - Behördliche Genehmigungen (z.B. Baugenehmigung) …	
Veränderungsrechte an fremden Objekten - Erbbaurecht, Nießbrauch, Mietrecht…	Veränderungsrechte an fremden Objekten - Rechte zur baulichen Veränderung (Bauauftrag)	

Tabelle 2: Bandbreite möglicher Inhalte einer digitalen Wallet

Ausstellung ein Leben lang. Eine mittlere Lebensdauer haben Nachweise über Arbeitgeber, Kitaplätze, Mietbescheinigungen usw.. Bisherige ID-Dienste beschränken sich oft auf die Basisidentität natürlicher Personen, die vor allem in selten genutzten Verwaltungsprozessen zum Einsatz kommt und durch die eID-Prozesse stark gesichert wird. Die Grundlage für Alltagsrelevanz und regelmäßige Nutzung von ID-Diensten entsteht jedoch vor allem durch kurzlebige Nachweise, die häufig genutzt werden, z.B. Tickets, Reservierungen und Kundenkarten für Mobilität, Kultur und Freizeit, aber auch durch eine hohe Bandbreite der digital nutzbaren Credentials. Ohne Anspruch auf Vollständigkeit soll Tabelle 2 die Bandbreite möglicher Inhalte einer digitalen Wallet aufzeigen. Dabei kann man nach ihrem Inhalt bzw. Art der Daten prinzipiell verschiedene Arten von Verifiable Credentials klassifizieren:

1. Ausweis-Credential => *Beleg für Identifizierungsdaten*
    a. Ausweis/Siegel einer hoheitlichen Entität
    b. Ausweis einer juristischen Person
    c. Ausweis einer natürlichen Person
    d. Ausweis eines (autonomen) Objekts
2. Nachweis-Credential => *Beleg für Rechte und/oder Beziehungen*
    a. Temporäre/anlassbezogene Rechte (z.B. Event-Ticket, Lastschriftmandat)
    b. Befristete Rechte (z.B. Monatskarte)
    c. Dauerhafte Rechte (z.B. Ausbildungsnachweis)
    d. Entziehbare Rechte (z.B. Führerschein, Zugangsrechte, Nutzungsrechte)
    e. Nachweise familiärer Beziehungen
    f. Nachweise rechtlicher Beziehungen
    g. Zugehörigkeitsnachweise (Mitarbeiter- oder Mitgliedsausweis)
    h. Eigentumsbeziehungen
3. Bild-Credential => *Beleg für Aussehen*
    a. Biometriedaten (Passbild, Fingerabdruck, Irisscan, Handvenenscan)
    b. Objektfotos
    c. Konstruktionsdaten (CAD-Daten, BIM-Daten …)
4. Wert-Credential => *Beleg für Wertversprechen*
    a. Digitaler Geldschein (ausgestellt durch die Notenbank) => Prove of Authority
    b. Digitaler Scheck (ausgestellt durch einen Kontoinhaber)
    c. Digitaler Gutschein (ausgestellt durch Unternehmen)
    d. Digitale Rabattmarke

Die Entwicklung des Trustnets wird vermutlich weitere Arten von Verifiable Credentials hervorbringen. Allein anhand der Bandbreite personen- und unternehmensbezogener Daten, die in staatlichen Registern vorgehalten werden, wird klar, wie groß das Anwendungspotential von Nachweis-Credentials im Kontext der Verwaltungsdigitalisierung ist. Biometriedaten in Form von Bildcredentials haben insbesondere bei Prozessen mit Prüfung personengebundener Rechte ihre Bedeutung, aber auch bei der anonymisierten Altersprüfung. Digitale Geldscheine könnten einen Teil des Zahlungsverkehrs von den Hausbanken entkoppeln und dadurch die Systemrelevanz von Banken senken. Die strukturierte Herausgabe hoheitlicher Nachweise von der Kommune an den Bürger in Form von Verifiable Credentials könnte der Schlüssel sein, um nicht nur in puncto Ausweisdokumente, sondern auch in Bezug auf die Nachweisdokumente staatliche Vertrauensanker breitenwirksam zu digitalisieren.