Validierung digitaler Nachweise mit der Blockchain

Trust as a Service – Vertrauen als Dienstleistung

Viele Prozesse – sowohl im Alltag, als auch in Wirtschaft und Industrie – umfassen die Verarbeitung von personenbezogenen und sensiblen Daten. Hohe Sicherheitsansprüche sind daher Pflicht. Gleichzeitig wollen die Menschen digital leben, ohne die Selbstbestimmung über die Weitergabe ihrer Daten aufgeben zu müssen. Große Daten-Leaks, nicht nur bei Facebook, haben gezeigt, dass die unkontrollierte Speicherung von eigenen Daten in fremder Umgebung alles andere als sicher ist. Mit der Souveränität über die eigenen Daten muss allerdings sichergestellt werden, dass auch die mit ihnen verbundenen Identitäten echt und unverfälscht sind. Die Möglichkeiten für Betrug sind hier enorm und werden aktiv praktiziert. Daher kommen in der digitalen Welt zunehmend Dienste ins Spiel, welche die Vertrauenswürdigkeit garantieren. Dieser „Trust as a Service" scheint in Zukunft unverzichtbar.

Das Zeitalter der digitalen Transformation öffnet ungeahnte Chancen quer durch alle Lebensbereiche. Ein ganz entscheidender Aspekt ist dabei die Optimierung von Prozessen. Im Kleinen betrifft das den persönlichen Alltag, im Großen geht es um hohe Einsparungen.

Papiernachweise leicht zu fälschen

Die Schwachstelle für Nachweise auf einem Papier ist die eigenhändige Unterschrift oder der Stempel. Beide bieten keinen Integritätsschutz, denn sie sind von ihrer Form und Art komplett physikalisch unabhängig von den Informationen, die sie bestätigen und schützen sollen. Der Missbrauch der persönlichen Unterschrift ist deshalb auf mehrere Arten möglich.

Copy and Paste

Um eine Person zu identifizieren, unterschreiben Menschen die Grußkarte sowie den Mietvertrag mit der gleichen eigenhändigen Unterschrift. Das Problem: Mit ein wenig Übung lässt sich diese Unterschrift durch fremde Hand oft so gut kopieren, dass die Fälschung kaum zu erkennen ist. Der Mensch hat somit keine Souveränität über seine persönliche Unterschrift, da jede Person den Schriftzug ohne große Probleme imitieren kann. Um dies zu verhindern, müsste die eigenhändige Unterschrift verdeckt werden, was eine Überprüfung jedoch unmöglich macht.

Zero Knowledge

Ein weiterer wichtiger Punkt ist, dass der Prüfer des Vertrages unter Umständen die echte Unterschrift gar nicht kennt. Soll ein Nachweis von einer Person als unterzeichnet gelten, so kann der Betrüger nach Belieben eine Kombination aus Vor- und Nachnamen kreieren. Webseiten wie https://www.mylivesignature.com/ erlauben dies schon mit wenigen Klicks. Um dies zu verhindern, müsste es eine globale Datenbank geben, die zu jeder Person die dazugehörige persönliche Unterschrift enthält und einen Abgleich ermöglicht. Praktisch gesehen ist

Bild 1: DIPLOMAcompany – Werbung für Betrug [https://www.diplomacompany.com/buy-fake-diplomas.html]

dies weder aus dem Blickwinkel der Umsetzung noch der Sicherheit eine Lösung, um den Missbrauch zu verhindern.

Fake as a Service

Wer sich selbst die Hände nicht schmutzig machen will, kann gefälschte Nachweise auch bequem im Internet bestellen (Bild 1). Allein im Bildungsbereich existieren rund 3.000 Anbieter, bei denen zahlungswillige Möchtegern-Doktoren & Co. akademische Urkunden kaufen können. Mit der Operation Dipsam hat das FBI in den Achtzigern mehrere solche Anbieter in den USA auffliegen lassen. Trotzdem kann unter dem Suchbegriff „buy fake diploma" bei Google unter den sieben Millionen Treffern schnell ein aktueller Anbieter gefunden werden. Europäische Nachweise sind etwa bei DIPLOMAcompany für unter 200 Dollar zu haben.

Validierungsservice

Bei der Realisierung eines Validierungsservices müssen mehrere Punkte beachtet werden, da Sicherheit, Automatisierung durch Digitalisierung, Datenschutz und Souveränität gleichermaßen berücksichtigt werden sollen. Forschungen am Institut für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen haben im Frühjahr 2018 ergeben, dass mithilfe der Blockchain-Technologie die nötigen Kriterien berücksichtigt und umgesetzt werden können.

Sicherungsschicht

Als Vorlage diente die Transportschichtsicherheit (TLS/SSL) der TCP/IP-Protokollarchitektur.[1] Die Einführung einer neuen, unabhängigen TLS/SSL-Schicht erlaubt die uneingeschränkte Nutzung sowohl der Möglichkeiten auf der darüber liegenden Anwendungsebene als auch der Funktionen

Bild 2: TLS im TCP/IP-Protokollstapel

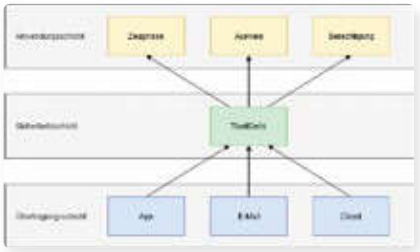


Bild 3: Absicherung über einheitliche Sicherheitsschicht

aller darunter liegenden Kommunikationsebenen (Bild 2).

Diese Schicht wird auch bei der Validierung von Nachweisen eingesetzt und bietet, wie in Bild 3 zu sehen, die gleichen Vorteile wie TLS/SSL. Sie garantiert die Unversehrtheit der übertragenden Daten, die von der Anwendungsschicht mithilfe der Übertragungsschicht transportiert werden. Ein generalisierter Ansatz ermöglicht den Einsatz der gleichen Sicherheitstechnologie und sorgt für ein einheitliches IT-Sicherheitslevel bei unterschiedlichen Anwendungsfällen.

Unsichere Kommunikationssysteme können genutzt werden, da die Daten vor der Anzeige auf ihre Integrität – auf Veränderung während der Übertragung – überprüft werden. Der Ablauf ist in Bild 4 dargestellt. So lassen sich alle üblichen Kommunikationsmethoden, wie der Versand von E-Mails, wo keine Integritätschecks im Protokoll selbst implementiert sind, dennoch gesichert nutzen. Ebenfalls kann eine günstige Infrastruktur, wie eine externe Cloud, genutzt werden, um den Transport zwischen zwei Systemen sicher zu realisieren. Somit wird die Übertragungsschicht gesichert, ohne die direkte Kommunikation zwischen Sender und Empfänger ändern oder einschränken zu müssen. Eine Manipulation der Daten in den Endsystemen innerhalb der Anwendung wird allerdings nicht erkannt.

Bild 4: Sichere Übertragung von Informationen

Blockchain-Technologie als Vertrauensservice

Als Basis für einen Vertrauensservice hat das Institut die Blockchain-Technologie gewählt.[2] Sie verspricht dank Dezentralisierung und Verkettung aller Informationen, die in Transaktionen eingefügt sind, einen hohen Manipulationsschutz.

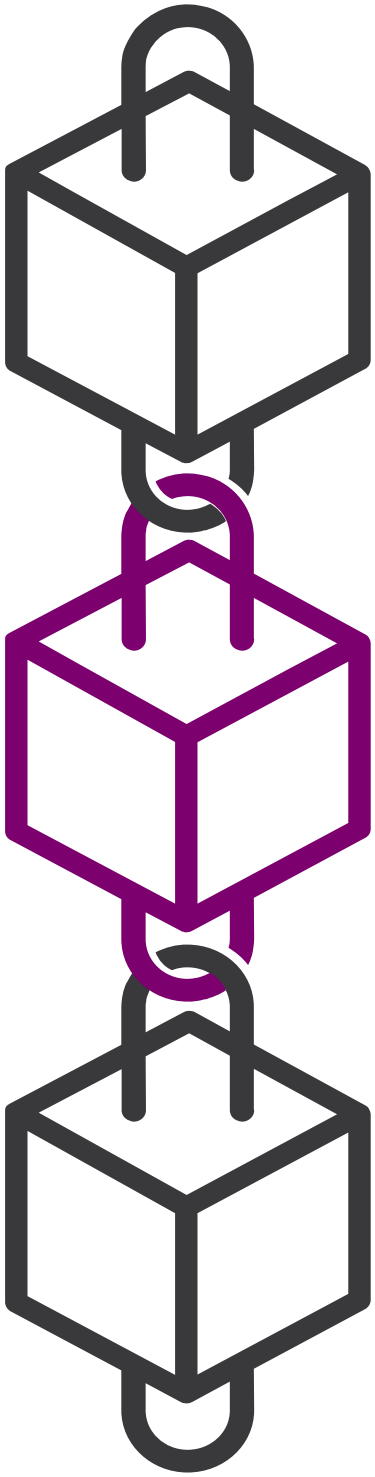
Eine zentrale Lösung hat zwar den Vorteil einer vereinfachten Systemwartung, bringt jedoch auf der Negativ-Seite den „Single Point of Failure" mit sich. Ist der zentrale Server für die Überprüfung nicht erreichbar, so ist der gesamte Dienst nicht funktionsfähig. Ein vielleicht noch größeres Problem entsteht hier bei Manipulation. Es gibt kein weiteres System, mit welchem die Daten verglichen werden können. Alles, was zentral abgelegt ist, wird als gültig interpretiert. Bei einem dezentralen Ansatz gibt es keinen Server, der an oberster Stelle steht, sondern mehrere gleichberechtigte Server. Diese werden von verschiedenen Parteien betrieben, die unabhängig voneinander sind. Im Falle von Zeugnissen wären das zum Beispiel die Hochschulen selbst. Sie haben in den meisten Fällen eine eigene IT-Infrastruktur und sind damit unabhängig von Regierungen oder großen Rechenzentren, die von Anbietern wie Microsoft, Amazon oder Google betrieben werden. Änderungen an der Blockchain bei einem Server würden durch den

Abgleich der anderen Server auffallen und könnten korrigiert werden.

Ein weiterer Punkt ist die Protokollierung des Lebenszyklus eines Nachweises. Ein Nachweis kann drei Zustände haben: er existiert nicht, er wurde ausgestellt oder er wurde wiederrufen. Diese Zustände werden durch Transaktionen in der Blockchain repräsentiert. Möchte ein Prüfer den Zustand eines Nachweises ermitteln, so muss er die komplette Blockchain nach den Einträgen durchsuchen. Danach kennt er den aktuellen Zustand des Nachweises. Die Transaktionen werden in Blöcken zusammengefasst, die mit kryptografischen Verfahren verkettet werden. Somit ist es nicht möglich, einen fremden Nachweis in die chronologische Reihenfolge einzufügen oder den Widerruf zu löschen.

Bei der Untersuchung der möglichen Blockchain-Lösungen stellte sich heraus, dass keine der öffentlich zugänglichen Bockchain-Technologien für die Validierung von Zeugnissen besonders geeignet war. Viele Blockchain-Technologien sind für die Verwendung von Kryptowährungen ausgelegt, da dies der erste und bekannteste Anwendungsfall war, der mit einer Blockchain realisiert werden konnte. Jeder Beteiligte kann die Transaktionen der Blockchain unabhängig überprüfen und somit feststellen, ob die Verteilung der Beträge konsistent ist. Die Blockchain soll jedoch nicht die Ein- und Auszahlungen von Konten protokollieren, sondern Informationen für die Validierung von Nachweisen persistent speichern.

Ein weiterer Punkt sind die verwendeten Konsensmechanismen, um die Einträge zu speichern. Die bekanntesten Blockchains setzen hier auf den „Proof-of-Work"-Algorithmus. Dabei müssen die beteiligten Rechnersysteme ein komplexes Mathematikrätsel lösen, das viele Rechenressourcen benötigt. Hat ein Rechner das Rätsel gelöst, so teilt er sein Ergebnis den anderen Teilnehmern mit. Diese können das Ergebnis mit wenig Aufwand prüfen. Dies ist notwendig, da jeder dem Netzwerk beitreten und die Kette der Blockchain erweitern darf. Diese Art von Blockchain wird „public permissionless" genannt.



© depositphotos.com/RichTphot

Für ein effizientes Geschäftsmodell ist allerdings eine „Private-permissioned"-Blockchain von Vorteil.[3] Hierbei ist das Netzwerk nicht jedem zugänglich, und nur ausgewählte Personen/Organisationen dürfen ihm beitreten. Somit können Leserechte reguliert und gebührenpflichtig realisiert werden. Zudem existiert ein Rechtesystem, nachdem nicht jeder Teilnehmer Transaktionen oder Blöcke erstellen darf. Mit dieser Variation lassen sich mehrere Use Cases realisieren oder verschiedene Geschäftsmodelle innerhalb eines Cases abbilden. Die Aussteller können somit eindeutig identifiziert werden. Durch die Abspeicherung der Prüfsummen mit Signatur kann jedoch kein Rückschluss gezogen werden, welcher Nachweis signiert wurde.

Asymmetrische Unterschriften

Die bekannte eigenhändige Unterschrift – mit Vor- und Nachnamen – kann als symmetrische Unterschrift bezeichnet werden. Für das Signieren und das Überprüfen der eigenhändigen Unterschrift wird das gleiche Abbild genutzt. Typische minimale Abweichungen sind auf die Motorik des Menschen zurückzuführen und können durch Nervosität, Müdigkeit oder andere Faktoren beeinflusst werden. Diese geringe Variation ist der Grund, warum nicht exakt geprüft werden kann und eine gewisse Abweichung akzeptiert werden muss. Die persönliche Unterschrift kann auch als statisch angesehen werden, da sie unabhängig von den Informationen ist, die mit ihr akzeptiert werden. Eine Kopie durch eine andere Person kann also leicht durchgeführt werden, wenn diese einmal die eigenhändige Unterschrift zu sehen bekommt. Sollte dies nicht der Fall sein, kann die Person die Unterschrift in gewisser Weise erraten, da sie den Vornamen und Nachnamen beinhaltet und dem Prüfer keine persönliche Unterschrift für einen Vergleich vorliegt.

Eine asymmetrische, digitale Unterschrift, beziehungsweise digitale Signatur, besteht aus zwei verschiedenen Komponenten. Die eine wird zum Signieren verwendet, die andere zum Validieren. Dieses Verfahren wird auch bei der asymmetrischen Verschlüsselung genutzt. Eine Person, allgemein Entity, erzeugt ein digitales Schlüsselpaar und publiziert ihren öffentlichen Schlüssel. Nachrichten können mit diesem öffentlichen Schlüssel verschlüsselt werden und anschließend nur vom Besitzer des geheimen Schlüssels entschlüsselt werden. Die beiden Schlüssel können auch für das Signaturverfahren genutzt werden. Der geheime Schlüssel wird für die Signierung einer Nachricht verwendet. Die Signatur kann dann mit dem öffentlichen Schlüssel validiert werden. Das Ergebnis ist für jede Nachricht unterschiedlich, da es abhängig vom Inhalt der Nachricht ist. Tabelle 1 zeigt deutlich, das kleinste Veränderungen an der Nachricht die Signatur deutlich sichtbar verändern.

	Original	Verändert
Nachricht	Hello World	Hallo World
Signatur	fGSxSqHvmIIO+r5BIFlucexN ...	JgvpbsAeTxDC3vIWWsdqGL ...

Tabelle 1: Abhängigkeit zur Nachricht bei Signatur

Prüfsummen/Hashwerte

Bei der Verschlüsselung gibt es eine Funktion zum Verschlüsseln und Entschlüsseln. Der Klartext ist am Ende wieder lesbar. Prüfsummen oder Hashwerte werden jedoch mit einer Einwegfunktion berechnet, deren Ergebnis nicht zurückgerechnet werden kann. Dies ist im Falle einer Integritätsprüfung auch nicht relevant, da nicht der Klartext, sondern die Prüfsummen verglichen werden. Das Verfahren berechnet dafür aus einem beliebigen Input eine Bitfolge. Die Länge der Bitfolge ist dabei abhängig von der verwendeten Einwegfunktion und nicht von der Größe der des Inputs. Die Verwendung des SHA-256 Algorithmus erzeugt zum Beispiel immer eine Ausgabe von 512 Bits. Zudem gilt der Algorithmus als kollisionsfrei, sodass praktisch gesehen zwei unterschiedliche Inputs nicht die gleichen Prüfsummen/Hashwerte generieren können.

Die Reduzierung auf 512 Bits sowie die Unmöglichkeit einer Rückwärtsrechnung erlauben es, die Prüfsumme und deren Signatur persistent in einer Blockchain zu speichern. Diese Prüfsummen können auf den Endgeräten direkt berechnet werden, sodass sensible Informationen nicht über das Internet auf fremde Systeme übertragen werden müssen. Anschließend müssen alle Transaktionen in der Blockchain gesucht werden, welche die Prüfsumme enthalten und folglich den Lebenszyklus eines Nachweises protokollieren. Für eine schnelle Durchsuchung können die Prüfsummen in einer separaten Datenbank für die schnelle Suche indexiert werden.

Use Cases

Nachweise von Dokumenten werden in allen Branchen seit mehreren Jahrhunderten ausgestellt. Sie dokumentierten eine Eigenschaft zu einem bestimmten Zeitpunkt und schreiben diese optional einer Person zu. Ein großes Potenzial steckt in der Digitalisierung, da durch sie viel besser skaliert werden kann und Prozesse unabhängiger von menschlichen Aktionen werden.

Bildung – Hochschulzeugnisse

Laut dem Bundesverband deutscher Unternehmer ist jedes zehnte Zeugnis im Bildungsbereich in Deutschland frisiert. Das französische Florian Mantione Institut geht sogar davon aus, dass in Frankreich jeder dritte Bewerber sein Zeugnis manipuliert. Möchte ein Personalverantwortlicher das Zeugnis prüfen, so muss er sich mit dem Aussteller, zum Beispiel den Hochschulen, in Verbindung setzen. Bei allein 500 Hochschulen in Deutschland und den rechtlichen Vorschriften, die für die Einhaltung der Datenschutzgrundverordnung notwendig sind, dauert es mehrere Stunden oder sogar Tage, um ein Zeugnis manuell zu prüfen. Dieser Aufwand und die damit verbundenen hohen Kosten sind nachvollziehbare Gründe, warum Personaler heute oft auf eine Prüfung verzichten. Sie setzen die Firma einem vermeidbaren Risiko aus, da bei einem Vorfall der Ruf der Firma irreparabel geschädigt werden kann. Dieser Schaden kann auf allen Ebenen passieren und ist unabhängig von der Position im Unternehmen.

Ein effizienteres Verfahren für die Überprüfung von Hochschulzeugnissen ist in Bild 5 zu sehen. In diesem Beispiel stellt die Hochschule dem Absolventen ein digitales Zeugnis aus, mit dem dieser sich bei einem Arbeitgeber bewerben kann. Zusätzlich zur Ausgabe des digitalen Zeugnisses wird eine originale Prüfsumme des digitalen Zeugnisses mithilfe einer Einwegfunktion berechnet. Die Prüfsumme wird dann von der Hochschule digital signiert. Die digitale Signatur erlaubt eine eindeutige Zuordnung zum digitalen Zeugnis und die Möglichkeit, die Echtheit zu überprüfen. Die originale Prüfsumme und digitale Signatur werden in eine Transaktion geschrieben und in die manipulationssichere Blockchain gespeichert.

Der Absolvent entscheidet eigenständig, wem er sein digitales Zeugnis gibt. Bei Erhalt des digitalen Zeugnisses berechnet das Validierungssystem des Prüfers die aktuelle Prüfsumme, um diese mit der originale Prüfsumme vergleichen zu können. Zwei identische digitale Zeugnisse erzeugen immer die gleiche Prüfsumme. Auf der Basis dieser Eigenschaft kann mit der aktuellen Prüfsumme die Blockchain durchsucht werden. Bei einer positiven Rückmeldung erhält das Validierungssystem des Prüfers die Signatur, mit dessen Hilfe der Herausgeber identifiziert und verifiziert werden kann.

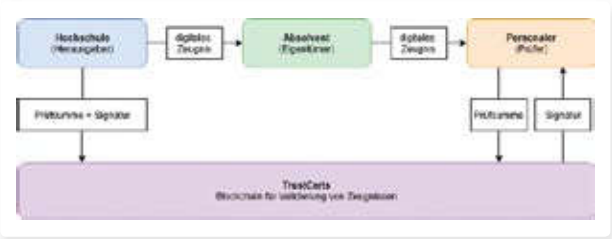


Bild 5: Signierung und Validierung eines digitalen Zeugnisses

E-Government – Nachweise

Nicht nur Firmen und Hochschulen können von der Digitalisierung profitieren, sondern auch die Städte und Gemeinden. Viele Informationen sind heute schon über die Webseiten abrufbar und ersparen den Besuch beim Rathaus oder an anderen zentralen Stellen in der Stadt. Genehmigungen müssen allerdings weiterhin vor Ort beantragt und ausgestellt werden. Menschliche Prozesse können deutlich schlechter und nur in einem gewissen Maße skaliert werden. Öffnungszeiten schränken die Erreichbarkeit ein und die Anzahl der Schalter die Menge an Bürgern, die gleichzeitig bedient werden können. Deswegen kann sich der Prozess zur Beschaffung eines Nachweises, wie Parkausweis oder Meldebescheinigung, über Tage oder Wochen hinziehen, da sowohl ein freier Termin bei der Stadt als auch beim Bürger gefunden werden muss.

Ein digitaler Dienst setzt dagegen keinen gemeinsamen Termin voraus. Möchte der Bürger einen Nachweis beantragen, so muss er sich der Stadt gegenüber authentifizieren. Ist dies geschehen, kann die Stadt den beantragten Nachweis ausstellen. Beide Schritte können durch digitale Prozesse realisiert werden. Die Identifizierung geschieht über ein zuvor registriertes Online-Konto, das einmalig durch die physische Anwesenheit beim Rathaus oder mithilfe des neuen Personalausweises erbracht wird. Ist die anfallende Gebühr in Echtzeit überwiesen, zum Beispiel mit PayPal, kann ein Server der Stadt automatisch eine Genehmigung oder einen Nachweis digital generieren. Dieser wird dann signiert und anschließend digital sicher und vertrauenswürdig zugestellt. Der komplette Prozess von Identifizierung/Authentifizierung bis zum Erhalt des Nachweises ist in wenigen Minuten abgeschlossen und ist jederzeit durchführbar, da keine menschlichen Ressourcen seitens der Stadt benötigt werden und der Prozess komplett automatisiert ist.

Fazit

„Trust as a Service" ist heute ohne Weiteres über IT-Infrastrukturen realisierbar. Für die gebotene Sicherheit erweisen sich moderne Blockchain-Technologien als entscheidender Faktor. Die dazu benötigten Verfahren haben sich in anderen Anwendungsfällen bereits über Jahre bewährt und schaffen in ihrer Kombination ein neues Level des Vertrauens. So lassen sich nicht nur interne, sondern auch externe Prozesse in den Bereichen Wirtschaft, Industrie oder Internet of Things sicher umsetzen. ■

Literatur

[1] *J. Meng, N. Pohlmann: „Sicherheit zwischen Klick und Webseite. TLS/SSL: Eine Frage der Implementierung", IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT GmbH, Ausgabe 2/2019*

[2] *N. Pohlmann: „Blockchain-Technologie unter der Lupe – Sicherheit und Vertrauenswürdigkeit kryptografisch verketteter Datenblöcke", IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT GmbH, Ausgabe 5/2018*

[3] *N. Pohlmann: Lehrbuch „Cyber-Sicherheit", Springer Vieweg Verlag, Wiesbaden 2019 ISBN 978-3-658-25397-4*

MIRKO MOLLIK,
Mitarbeiter im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen. Er beschäftigt sich unter anderem mit der Blockchain-Technologie und der Zeugnis-Validierung.

NORBERT POHLMANN,
Informatikprofessor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.