Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Eckpunktepapier für Self-sovereign Identities (SSI)

unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT)

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: blockchain@bsi.bund.de
Internet: https://www.bsi.bund.de

Einleitung

Die Digitalisierung von Prozessen in Verwaltung, Industrie und Wirtschaft kann nur gelingen, wenn alle beteiligten Entitäten – seien es natürliche Personen, Verwaltungsstellen, Bauteile, Maschinen oder dergleichen – über eine digitale Identität auf einem ausreichenden Vertrauensniveau identifizierbar sind. Der zunehmende Wunsch nach einer größtmöglichen Datensouveränität rückt dabei das Konzept der selbstverwalteten Identitäten (*Self-sovereign Identities*, SSI) in den Fokus.

Die grundlegende Idee von SSI liegt darin, den Nutzern die Hoheit über ihre Identitätsdaten zu überlassen, in dem Sinne, dass sie ihre Identitätsdaten selbst verwalten und eigenständig entscheiden können, wem sie welche Informationen über ihre Identität offenlegen. Dies unterscheidet SSI von vielen Single-Sign-On-Lösungen oder zentralen Anmeldediensten, bei denen der Nutzer ein – oftmals detailliertes – Profil über seine Identität in einem Nutzerkonto beim ID-Anbieter hinterlegt und anschließend keine Kontrolle mehr darüber hat, welche Daten daraus der Anbieter an Dritte weitergibt oder selbst verwendet.

SSI lässt sich auf unterschiedliche Weise umsetzen. Der oft vorgeschlagene Einsatz eines Distributed Ledgers ist hierbei grundsätzlich möglich, aber keineswegs die einzige Option. So setzt bereits der elektronische Personalausweis mit der eID-Funktion Konzepte für selbstverwaltete Identitäten um, indem er die Möglichkeit bietet, den Zugriff auf die gespeicherten Nutzerattribute diensteabhängig zu steuern.

In seiner Funktion als die Cybersicherheitsbehörde des Bundes befasst sich das BSI seit vielen Jahren aktiv mit der Entwicklung sicherer digitaler Identitäten[1]. Auch die IT-Sicherheit der Blockchain- und Distributed-Ledger-Technologie (DLT) ist unter verschiedenen Gesichtspunkten umfassend analysiert und in diversen Publikationen dargelegt worden[2].

Beide Bereiche bringen Anforderungen an die IT-Sicherheit von Self-sovereign Identities mit sich. Das vorliegende Eckpunktepapier soll eine Übersicht über die wesentlichen Aspekte bieten.

[1] https://www.bsi.bund.de/eID/

[2] Bundesamt für Sicherheit in der Informationstechnik, Blockchain sicher gestalten – Eckpunkte des BSI, Bonn, 2018 und Bundesamt für Sicherheit in der Informationstechnik, Blockchain sicher gestalten. Konzepte, Anforderungen, Bewertungen, Bonn, 2019. Beide erhältlich unter https://www.bsi.bund.de/Blockchain/

Schematische Funktionsweise von SSI

Konkret lässt sich beim SSI-Ansatz (siehe Abbildung 1) ein Nutzer (Identitätsinhaber, *Holder*) beliebige Attribute (*Claims*, z. B. Alter, Schulabschluss, Hersteller eines Bauteils) von der jeweils dafür zuständigen Stelle (Herausgeber, *Issuer*) attestieren. Diese kryptographisch signierten Attribute *((Verifiable) Credentials)* kann der Nutzer selbst z. B. auf einem digitalen Endgerät verwalten und bei Bedarf einem Dritten (Prüfer, *Verifier*) zum Nachweis vorlegen. In der Regel benötigt der Prüfer für die Verifikation zusätzliche Informationen, wie Angaben zu den verwendeten Signaturverfahren und das öffentliche Schlüsselmaterial. Diese Informationen sind in einem allgemein zugänglichen Datenregister hinterlegt und können durch Referenzen in den vorgelegten Credentials abgerufen werden. Manche Lösungsansätze sehen auch ein umfangreicheres Register (*Claims Registry*) vor, auf dem zusätzlich zu dem kryptographischen Material auch Informationen über alle ausgestellten Credentials vermerkt werden. Dabei können sich diese Ansätze darin unterscheiden, ob sie lediglich einen kryptografischen Fingerabdruck zu jedem Credential speichern oder auch Angaben zu den Inhalten selbst.

Die meisten Umsetzungsvorschläge sehen vor, das Register dezentral zu führen und in vielen Fällen in Form einer Blockchain oder eines Distributed Ledgers zu organisieren. Es ist aber wichtig festzuhalten, dass aus technischer Sicht auch andere Strukturen denkbar sind.

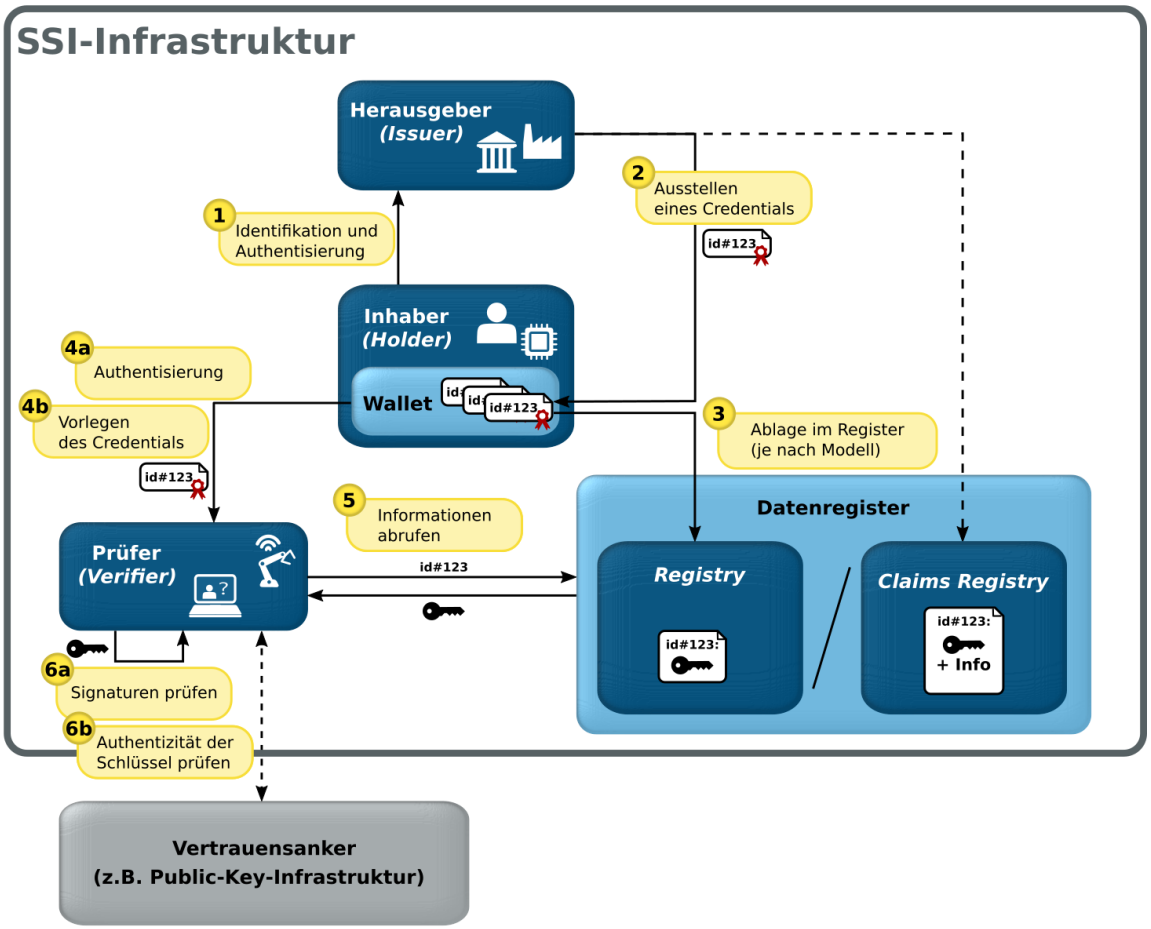

Abbildung 1: Schematische Darstellung von SSI-Abläufen: Nach Identifikation und Authentisierung (1) erhält der Inhaber ein vom Herausgeber ausgestelltes Credential (2) zur eigenen weiteren Verwaltung. Kryptographisches Material und gegebenenfalls zusätzliche Informationen werden im Register abgelegt (3). Nach Authentisierung (4a) und Vorlage des Credentials bei einem Prüfer (4b) ruft dieser die Informationen aus dem Register ab (5), prüft die Signaturen (6a) und verifiziert die Authentizität des Schlüsselmaterials (6b).

Wahl der Technologie und allgemeine Sicherheitsanforderungen

Ein tragfähiges Konzept für Self-sovereign Identities muss die Anforderungen der verschiedenen Akteure gleichermaßen berücksichtigen. Beispielsweise stehen für den Identitätsinhaber die Verfügbarkeit eines angebotenen Dienstes, der Schutz sensibler Daten und gegebenenfalls die Portabilität und Interoperabilität der Credentials im Vordergrund. Für den Prüfer ist die Authentizität der vorgelegten Credentials und ihre sichere Bindung an die zu authentisierende Person oder Entität entscheidend. Zur Wahl der passenden Technologie und zur besseren Einschätzung von Aufwand und Grenzen geplanter SSI-Projekte sind folgende Punkte zu beachten:

- **Self-sovereign Identities müssen nicht zwingend auf einem DLT-basierten Register beruhen.** Die Dezentralität und hohe Verfügbarkeit eines Distributed Ledgers werden zwar oft als Vorteil genannt, sind aber kein Alleinstellungsmerkmal dieser Technologie. Auch andere Systeme, wie beispielsweise verteilte Datenbanken oder Verzeichnisdienste, können für das Datenregister in Betracht kommen. Soll das Register nur zur Verwaltung der Vertrauensanker und nicht als umfassende Claims Registry genutzt werden, kann je nach Anwendungsfall bereits der elektronische Personalausweis eine mögliche Alternative bieten. Der Auswahl der passenden Technologie sollte stets eine sorgfältige Feststellung des Schutzbedarfes der verwendeten Daten und die Erstellung eines umfassenden Anforderungskatalogs vorausgehen.
- **Die Verwendung eines Distributed Ledgers erhöht die Komplexität des Gesamtsystems um Protokolle und Verfahren, für die es bislang keine belastbaren Sicherheitsaussagen gibt.** Die Distributed-Ledger-Technologie ist nach wie vor geprägt von einer Vielzahl an Einzellösungen, fehlenden Standards und einem Mangel an etablierten Sicherheitsempfehlungen. Sicherheitsempfehlungen fehlen insbesondere in vielen Fällen, in denen neuartige Funktionen durch wenig untersuchte Protokolle und kryptographische Verfahren umgesetzt werden sollen (z. B. für Konsens und Widerruf). Das entstehende Sicherheitsrisiko ist sorgfältig abzuwägen. Auch Standardisierungsprozesse im Bereich DLT sind noch nicht abgeschlossen. Dadurch wird die Planungssicherheit speziell für das Design interoperabler SSI-Systeme und -Anwendungen erschwert.
- **Die Sicherheit des Gesamtsystems ist über alle Ebenen sicherzustellen.** Alle Sicherheitsaussagen müssen in dem Maße, wie dies für den Schutzbedarf der verknüpften Anwendungen adäquat ist, durch Penetrationstests, Zertifizierungen von Komponenten oder ähnliche Maßnahmen unterlegt sein. Dies umfasst die kryptographische Absicherung der Nachrichten genauso wie die Authentisierung der Teilnehmer an ihrem Endgerät zur Ausübung ihrer Rollen durch Verfügung über ihr Schlüsselmaterial. Die einschlägigen Technischen Richtlinien des BSI[3] bieten umfassende Leitlinien zur sicheren Umsetzung dieser und weiterer Teilaspekte. Die getroffenen Maßnahmen müssen die Sicherheit der verarbeiteten Daten über den gesamten Zeitraum, in dem Schutzbedarf besteht, gewährleisten. Dazu muss ein Konzept zur Kryptoagilität existieren, das erlaubt, die Maßnahmen bei Bedarf, also z. B. vor Ablauf ihrer Eignung, zu ersetzen. Dem Schlüsselmanagement kommt ebenfalls eine wichtige Rolle zu. Da der Verlust privater Schlüssel erfahrungsgemäß nicht in jedem Fall zu verhindern ist, darf er nicht zum unwiederbringlichen Verlust von Credentials führen. Ein Mechanismus für Schlüsselaustausch oder -wiederherstellung – zusammen mit einem klar definierten Rechtemanagement zur Autorisierung solcher Maßnahmen – ist vonnöten. Es ist aber zu bedenken, dass das angestrebte Sicherheitsniveau hohe Hürden an die praktische Umsetzung solcher Mechanismen stellen kann.
- **Auch bei der Verwendung von Self-sovereign Identities hat die Datensouveränität praktische Grenzen.** Das skizzierte Modell verhindert nicht, dass der Prüfer Kenntnis über die Daten des

3 insbesondere TR-02102 („Kryptographische Verfahren: Empfehlungen und Schlüssellängen“) und TR-03107 („Elektronische Identitäten und Vertrauensdienste im E-Government“); erhältlich unter https://www.bsi.bund.de/TR/

Identitätsinhabers nach der Überprüfung behält oder gar an Dritte weiterleitet. Dadurch kann der Identitätsinhaber die Souveränität über seine Daten verlieren. Werden zur Verwaltung der Credentials Anwendungen eingesetzt, die nicht lokal auf dem eigenen Endgerät, sondern von einem externen Dienst betrieben werden, begibt sich der Nutzer in eine Abhängigkeit von dem betreffenden Dienst und auch von dessen Verfügbarkeit. Auch dies bedeutet für den Identitätsinhaber eine Einschränkung seiner Datensouveränität. Außerdem muss bedacht werden, dass die Nutzung der meisten Dienste die Bereitstellung gewisser Identitätsdaten voraussetzt. Dass sich ein Nutzer bewusst gegen deren Preisgabe entscheiden kann, stärkt zwar seine Datensouveränität, wird aber auch bei SSI dazu führen, dass ihm ein solcher Dienst dann verwehrt bleibt.

Authentisierung und Vertrauen

Eine Identitätsverwaltung kann ihren Zweck nur erfüllen, wenn sie die Authentizität der Credentials sicherstellen kann. Kryptographischen Signaturen kommt in diesem Zusammenhang eine große Rolle zu, sie reichen alleine aber nicht aus. Es bedarf zudem sicherer Übertragungskanäle und Authentisierungsfaktoren, um die digitalen Identitäten verlässlich an reale Identitäten zu binden.

- **Die Identität und Authentizität aller teilnehmenden Parteien ist auf angemessenem Sicherheitsniveau zu verifizieren.** Damit sich der Prüfer auf die Validität der vorgelegten Credentials und auch deren berechtigte Nutzung verlassen kann, müssen Credentials einen Authentizitätsnachweis beinhalten und gegen Zugriff und Nutzung durch einen Angreifer geschützt sein. Man spricht in diesem Fall auch von *Verifiable Credentials*. Der Prüfer muss sich von der Authentizität des Herausgebers überzeugen und zudem darauf vertrauen, dass dieser seinerseits eine Prüfung der Identität des Inhabers und der Korrektheit der Claims vorgenommen hat. Genauso muss sich auch der Identitätsinhaber von der Authentizität des Prüfers überzeugen, um eine unabsichtliche Weitergabe von Daten an Unberechtigte zu verhindern. Auf technischer Ebene müssen die gegenseitigen Authentisierungen an einen sicheren Übertragungskanal gebunden und das zugrundeliegende Vertrauensmodell klar definiert sein. Dabei muss auch dem Umstand Rechnung getragen werden, dass verschiedene Diensteanbieter oder verschiedene Jurisdiktionen unterschiedliche Anforderungen an das Vertrauensniveau der Identitätsprüfung und der Authentisierung der Identitätsinhaber haben können.
- **Die Eignung eines Distributed Ledgers zur Herstellung von Vertrauen in die Akteure ist nicht ausreichend untersucht.** Es gibt Ideen, das Vertrauen in die Herausgeber der Credentials durch ein Web Of Trust herzustellen. Dabei wird die Vertrauenswürdigkeit Einzelner durch andere attestiert und dies auf dem Ledger protokolliert. Bei einem solchen Ansatz ist sicherzustellen, dass die Reputation eines Herausgebers nicht durch einen Akteur oder eine kleine Gruppe von Akteuren unverhältnismäßig stark beeinflusst werden kann, etwa indem ein Akteur viele Identitäten annimmt, um überproportional oft für die Vertrauenswürdigkeit eines speziellen Herausgebers zu votieren (*Sybil-Angriff*). Sollte das verwendete DLT-Modell über ein Anreizsystem verfügen, z. B. zur Erhebung von Transaktionsgebühren oder einer Vergütung für die Ausstellung von Credentials, dürfen keine Fehlanreize entstehen. Verzichten nämlich Herausgeber – etwa aus Gründen der Gewinnmaximierung – auf eine Identitätsprüfung der Identitätsinhaber, werden Sicherheit und Verlässlichkeit des gesamten Systems unterminiert. Das komplexe Zusammenspiel zwischen dezentralem Vertrauen, monetären Anreizen und Konsensbildung auf dem Ledger ist noch nicht in dem Maße untersucht, als dass es eine Grundlage für belastbare Sicherheitsaussagen bieten würde.
- **Der Einsatz zentraler Instanzen als Vertrauensanker steht nicht notwendigerweise im Widerspruch zum Konzept selbstverwalteter digitaler Identitäten.** Die Distributed-Ledger-Technologie ist nach derzeitigem Forschungsstand und aktuellen Empfehlungen nicht in der Lage, eigenständig ausreichendes Vertrauen zu schaffen, das für alle Anwendungen eine Authentisierung auf angemessenem Niveau gewährleistet. Zusätzliche Maßnahmen, wie eine Public-Key-Infrastruktur (PKI), müssen insbesondere dann hinzugezogen werden, wenn Anwendungen ein erhöhtes Sicherheitsniveau erreichen sollen, also beispielsweise eine eIDAS-konforme Authentisierung verlangen. Die Einbeziehung einer zentral geführten PKI kann hier einen sicheren Vertrauensanker für die Authentisierung schaffen. Da dadurch die Ablage und Verwaltung der Credentials nicht unmittelbar beeinflusst werden, können diese weiterhin unter der Selbstverwaltung der Nutzer bleiben.

Datenregister und Wallets

Die Credentials, die beim Nutzer verbleiben, sollen dezentral verwaltet werden. Hierfür werden in der Regel dedizierte Hard- oder Softwareprodukte zum Einsatz kommen. Häufig wird für ein solches Produkt der Begriff *Wallet* aus dem DLT-Kontext verwendet, aber auch der Chip auf dem elektronischen Personalausweis würde hierunter fallen.

Daten im Wallet, aber auch im öffentlichen Datenregister müssen vor missbräuchlicher Verwendung geschützt werden. Insbesondere sind die folgenden Punkte zu berücksichtigen:

- **Ein sicheres Management der Credentials ist über ihre gesamte Lebensdauer zu gewährleisten.** Die Entwicklung von Wallets sollte nach Security-by-Design-Maßgaben erfolgen. Dabei muss etwa die Bindung der Identität an ihren Inhaber mit technischen Maßnahmen sichergestellt werden. Es muss gewährleistet sein, dass nur der Identitätsinhaber die Credentials verwenden kann. Insbesondere darf er die auf ihn ausgestellten Credentials nicht auf eine andere Person übertragen können. Auch darf es Dritten ohne das ausdrückliche Zutun des Identitätsinhabers nicht möglich sein, eine Verlinkung zwischen mehreren Credentials desselben Identitätsinhabers zu erkennen. Ferner muss es ein klares Konzept und die technischen Möglichkeiten zum Widerruf von Credentials geben. Dabei ist zu berücksichtigen, dass eine solche grundsätzlich in unterschiedlichen Situationen durch unterschiedliche Parteien nötig werden kann, z. B. wenn ein Herausgeber eine erteilte Erlaubnis wieder entziehen muss, wenn ein Identitätsinhaber Missbrauch seiner Daten befürchtet oder wenn das Vertrauen Dritter in die ordnungsgemäße Ausstellung durch den Herausgeber verletzt ist.
- **Es ist sorgfältig zu prüfen, ob die Distributed-Ledger-Technologie die geeignete Wahl für die Umsetzung des Datenregisters ist, insbesondere wenn dieses auch die ausgestellten Credentials umfassen soll.** Die Protokollierung aller ausgestellten Credentials kann gegebenenfalls deren Widerruf organisatorisch vereinfachen, da über den jeweils aktuellsten Stand Buch geführt wird. Ob allerdings die intrinsischen Eigenschaften eines Distributed Ledgers für die Claims Registry von Vorteil sind, ist im Einzelnen sorgfältig abzuwägen. So ist z. B. die Löschung von Daten aus einem Ledger technisch nicht vorgesehen, aber die dauerhafte Aufbewahrung längst abgelaufener Informationen ist inhaltlich meist überflüssig und erzeugt große Datenmengen. Manipulationen der gespeicherten Claims im Register werden bereits auffallen, wenn der Prüfer Informationen im Register nicht vorfindet oder die anschließende Prüfung der Herausgebersignatur fehlschlägt. Für die reine Detektierbarkeit von Manipulationen bringt eine DLT-Lösung daher keinen weiteren Vorteil. Falls die Credentials bereits mit Zeitstempeln versehen sind, ist auch eine lineare chronologische Speicherung der Daten nicht vonnöten. In jedem Fall ist technisch sicherzustellen, dass durch die Transparenz des Registers keine Rückschlüsse auf sensible Inhalte der Credentials und auch keine Verlinkungsangriffe ermöglicht werden. Letztere haben zum Ziel, mehrere Attribute zu verknüpfen und einem Nutzer zuzuordnen. Dadurch könnten möglicherweise anwendungsübergreifende Nutzerprofile erstellt werden, und der eingangs genannte SSI-Gedanke, Identitätsdaten nur kontrolliert und diensteabhängig offenzulegen, wäre ausgehebelt.