Dieses Dokument wurde in Zusammenarbeit von IBM Deutschland GmbH, esatus AG, Bundesdruckerei GmbH im Rahmen des Projektes "Ökosystem Digitaler Identitäten" erstellt.

Sperrkonzept Basis-ID

I. Technische und prozessuale Ausgestaltung der SSI-Infrastruktur und grundsätzlicher Umgang mit personenbezogenen Daten

Die nachfolgenden Ausführungen fokussieren auf die Darstellung des SSI Gesamtsystems, die beteiligten Hauptakteure und den Umgang mit (personenbezogenen) Daten:

Im Rahmen des SSI Ökosystem sind die Hauptakteure:

1. Der **Holder** als Datensubjekt und Inhaber/Verwalter „seiner" ggf. personenbezogenen Daten in Verifiable Credentials in seiner Wallet – im Regelfall als Smartphone-App –, die betroffene Person.
2. Der **Issuer** als Aussteller von Verifiable Credentials mit Daten, die den Holder betreffen und an ihn an den Holder selbst, ausgegeben werden.
3. Der **Verifier** als Konsument von Daten aus Verifiable Credentials, die er beim Holder anfragt und die dieser in der Wallet zur Übertragung freigeben muss.
4. Das verteilte „**SSI-Netzwerk – verifiable data registry**", das als hochverfügbarer und -performanter, persistenter und unveränderlicher Datenspeicher (Distributed Ledger Indy Ledger) und als Prüfinfrastruktur dient.

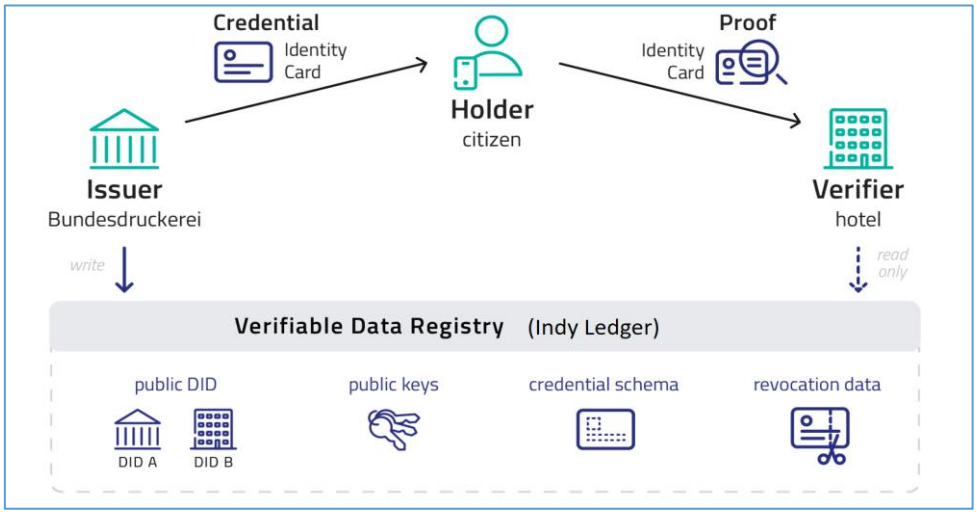

Abbildung 1 Überblick über die SSI Hauptakteure und Infrastruktur

Die innerhalb des SSI-Netzwerks (Verifiable Data Registry Indy Ledger) verarbeiteten Daten sind:

- **Public DIDs**, d. h. Decentralized Identifiers und öffentliche Schlüssel von Organisationen (nicht natürlichen Personen), die als Issuer tätig sind;
- **Datenschemas**, die im Sinne einer Vorlage die möglichen ausstellbaren Attribute in Verifiable Credentials definieren und von einem Public DID Inhaber erstellt werden;
- **Credential Definitions**, die im Sinne einer Instantiierung eines Schemas die konkrete Ausstellung von Verifiable Credentials an Holder ermöglichen und von einem Public DID Inhaber (= Issuer), der ungleich des Schemaerstellers sein kann, erstellt werden;
- **Revocation Registries**, die als kryptografischer Akkumulator die Privatsphäre schützende Invalidierung („Revocation") eines an einen Holder ausgegebenen Verifiable Credentials durch den Issuer ermöglichen und optional pro Credential Definition erstellt werden können.

Konsequenterweise bedeutet dies für den Umgang mit personenbezogen Daten:

- Der Holder / die betroffene Person hält „seine" personenbezogenen Daten selbst in seiner Wallet und nutzt und kontrolliert die Datenflüsse explizit selbstbestimmt. Seine Daten sind ausschließlich auf seinem Endgerät gespeichert.
- Es erfolgt keine Verarbeitung und Speicherung von personenbezogenen Daten auf dem SSI-Netzwerk (Distributed Ledger).
- Issuer und Verifier verarbeiten und speichern/löschen ggf. personenbezogene Daten in ihren internen Systemen und erfüllen die Anforderungen der DSGVO in eigener Verantwortung.

Die Bundesdruckerei (bdr) verarbeitet als Aussteller der Basis-ID personenbezogene Daten im Ausstellprozess unter Beachtung der DSGVO. Im Folgenden betrachten wir aber insbesondere den Sperrprozess.

II. Beschreibung des Sperrprozesses von Credentials mit Hyperledger Indy[1]

Für den Rückruf (Sperrprozess) von Verifiable Credentials (VC) kommen bei SSI sogenannte kryptographische Akkumulatoren, die auf dem Distributed-Ledger-Netzwerk gespeichert werden, in Verbindung mit Zero-Knowledge-Proofs zum Einsatz. Damit ist es möglich, dass der Besitzer eines VCs einen Beweis erstellt, dass das eigene VC nicht widerrufen ist, ohne dass der Verifizierer dadurch Rückschlüsse auf das VC selbst (etwa in Form einer Wiedererkennung desselben VCs oder Ermitteln von weiteren Informationen durch Nachfragen beim Aussteller) ziehen kann.

Die nachfolgenden Unterpunkte erläutern die beteiligten Komponenten des Sperrprozesses, deren Funktionen und damit die Ableitung für die Sperrung der Basis ID. Damit verbunden wird auf etwaige Fehlinterpretationen eingegangen im Rahmen der bisherigen BfDI Kommunikation.

1. *Der kryptographische Akkumulator ist vereinfacht ein Ergebnis einer Multiplikation unterschiedlicher Faktoren.*

Der Aussteller stellt dafür gemeinsam mit der Credential Definition auch eine sogenannte Revocation Registry auf dem Ledger aus, diese beinhaltet den kryptografischen Akkumulator und die URL zum Tails-File. Die Revocation Registry hat eine fest definierte Größe. Der Aussteller generiert einen privaten Schlüssel des Akkumulators und alle statischen Einträge des Tails Files. Daraus berechnet er den initialen öffentlichen Akkumulatorwert des Revocation Registry, unabhängig davon, ob ihr ein VC zugeordnet ist, oder nicht. Der Aussteller speichert den initialen Akkumulatorstand auf dem Ledger. Dieser Vorgang findet einmalig beim Erstellen der Credential Definition statt.

2. *Das Tails-File beinhaltet Faktoren zur Errechnung des Akkumulators, von denen jeder einem Credential zugeordnet ist. Dieses liegt nicht auf dem Ledger.*

Das Tails-File selbst beinhaltet keine sensitiven Daten, wird vom Aussteller gehostet und nur von den Holdern (einmalig) abgefragt. Jedes Credential wird einer bestimmten Revocation Registry sowie einem bestimmten Index des Tails-Files zugeordnet. Dieser Index zusammen mit einer "Witness" und dem Hidden-Attribut (eigener Faktor) wird dem Holder beim Ausstellen des Credentials übermittelt. Die Witness ist dabei das mathematischen Produkt der anderen Faktoren, welche multipliziert mit dem eigenen Faktor den Akkumulatorwert ergeben.

[1] https://hyperledger-indy.readthedocs.io/projects/hipe/en/latest/text/0011-cred-revocation/README.html

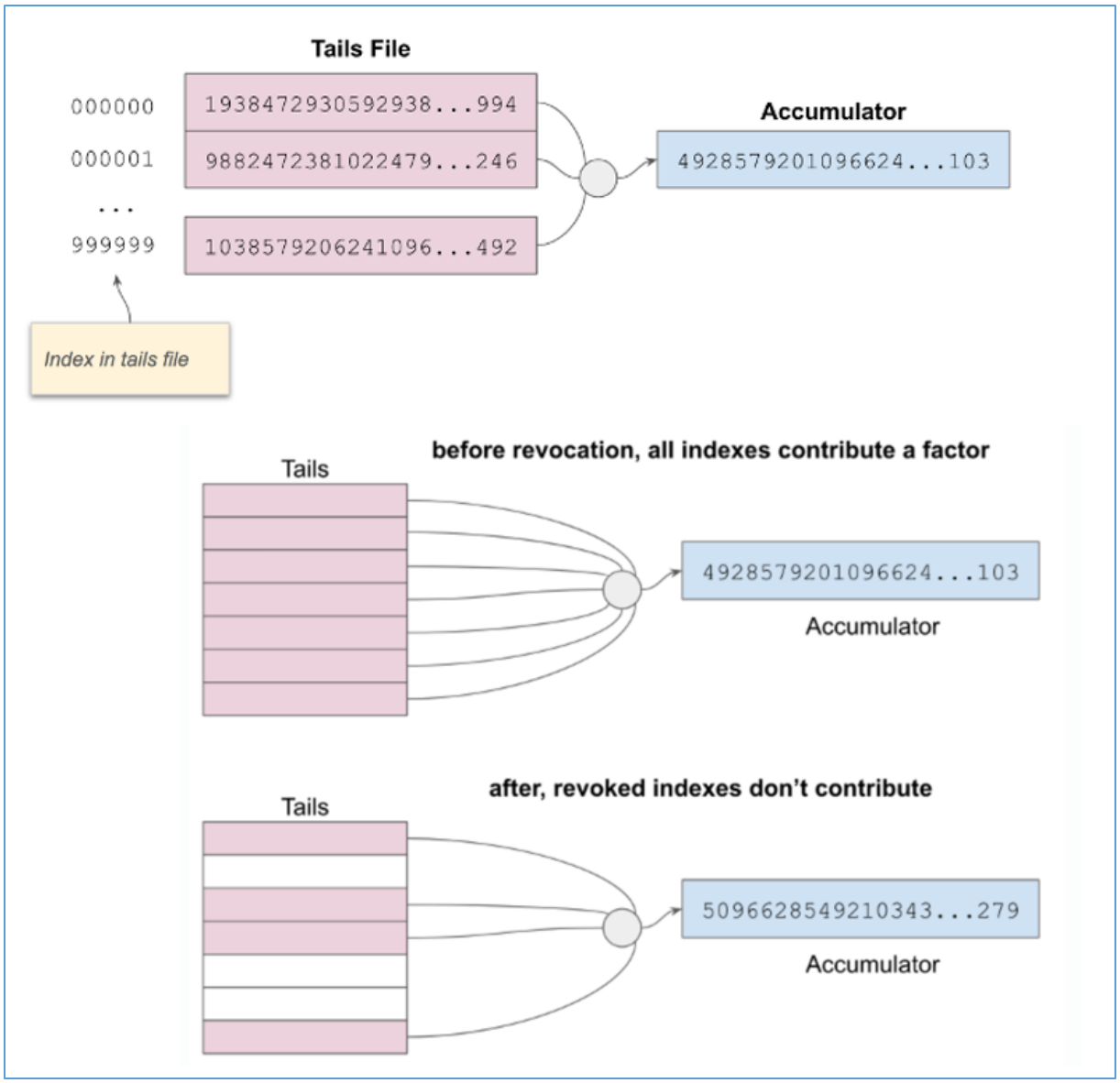

Abbildung 2 Kryptografischer Akkumulator und Tailes File

Mittels dieser Revozierungsinformationen (eigener Faktor und Witness) im Credential und des Akkumulatorwertes kann der Holder beim Presentation Proof beweisen, dass sein VC Teil des Akkumulators ist und somit nicht revoziert wurde. Dabei nutzt er nur den Akkumulatorwert. Er muss nicht seinen eigenen Faktor übermitteln oder andere Daten, die seinem Credential zuordenbar wären.

Hat sich der Stand des Akkumulators zum initialen Stand der Ausstellung geändert, so muss die Holder Wallet die Witness-Delta-Indizes vom Ledger abfragen. Diese sind gespeichert in den Revocation Entrys. Damit ist der Holder in der Lage, mit Hilfe des neu ermittelten Witness-Wertes multipliziert mit dem eigenen Faktor weiter die Nicht-Revozierung seines Credentials auf Grundlage des aktuellen Akkumulatorwertes zu beweisen.

Zusammenfassende Beschreibung des Sperrprozesses der Basis-ID:
Für die Sperrung der Basis-ID ist ein Sperrdienst etabliert, der online für Nutzer erreichbar ist. Der Nutzer zeigt seine Autorisierung der Sperrung entweder mittels Personalausweis (über die Restricted ID) oder mittels Sperrkennwort, welches ihm im Registrierungsprozess angezeigt und übermittelt wurde.

Das Sperrkennwort wird als Hash ausschließlich intern im Sperrdienst des Ausstellers für die Basis-ID vorgehalten. Des Weiteren wird der Hash über die Restricted ID (dienst- und kartenspezifisches Kennzeichen/Pseudonym) des Personalausweisinhabers im Sperrdienst des Ausstellers für die Basis-ID vorgehalten. Damit verknüpft sind Sperrinformationen für das konkret ausgegebenen Basis-ID Credential. Bei einer Sperranfrage wird erneut mittels Hash über das Sperrkennwort bzw. die Restricted ID der Nutzer authentifiziert und eine Zuordnung hergestellt. Der Aussteller der BasisID hat keine identifizierenden Merkmale über den Nutzer gespeichert, womit auch keine Reproduzierbarkeit auf seine Identität möglich ist.

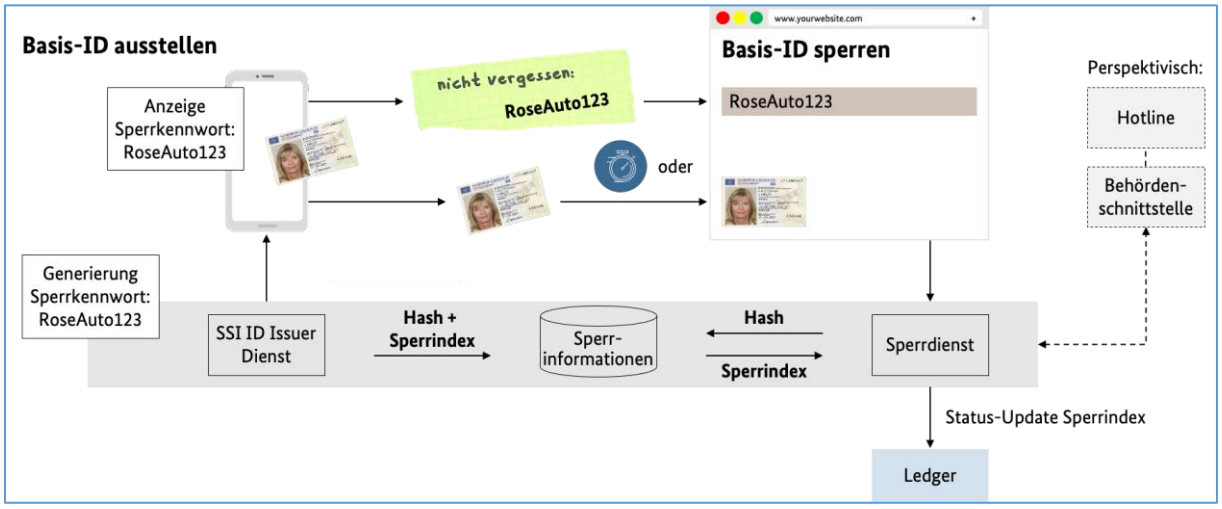

Abbildung 3 Sperrung der Basis-ID

Die dr hält als Aussteller keine Liste aller Bürgerinnen und Bürger vor, die eine Basis-ID nutzen, um Sperrungen durchzusetzen. Die technische Umsetzung erfolgt folgendermaßen:

- Bei Authorisierung des Nutzers mittels Sperrkennwort wird nur das Sperrkennwort verwendet und keine zusätzlichen Attribute. Zur Durchsetzung der Sperrung wird der Hash des Sperrkennwortes für die ausgestellten Basis-IDs in der Sperrdatenbank der BDR gespeichert. Das Sperrkennwort ist zufällig generiert und enthält keine Personeninformationen. Das Sperrkennwort ist 13 Zeichen lang (64bit) mit Base36 encodiert.
- Zur Durchsetzung der Sperrung bei Authorisierung mittels Personalausweis wird der Hash der restrictedID für die ausgestellten Basis-IDs in der Sperrdatenbank der bdr gespeichert. Der Restricted Identifier (restrictedID) berechnet sich aus dem Chip des Personalausweises auf Basis eines öffentlichen Schlüssels, der im Berechtigungszertifikat des Online-Dienstanbieters hinterlegt ist und einem geheimen Schlüssel der auf dem Personalausweis gespeichert ist[2].
- Der Aussteller (bdr) löst nach erfolgreicher Authentisierung mittels der gespeicherten Sperrliste & Index eine Sperrung aus, indem er den kryptografischen Akkumulator auf dem Ledger anpasst.

[2] BSI TR – 03110 Teil 2: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Technische-Richtlinien/technische-richtlinien_node.html

Schlussfolgerungen aus der Beschreibung:
Grundsätzlich verfügt nur der Aussteller über die Rechte zur Änderung des Akkumulatorstands und somit auch zur Ausführung der Sperrung. Für eine Sperrung eines VC benötigt der Aussteller also die RevocationRegistryID (die auf ein Tails File verweist) und einen Index. Welche Daten der Aussteller dazu speichert, obliegt jedoch dem Aussteller selbst. Dieser kann ein Mapping zwischen ausgegebenen VC (mit entsprechenden Daten) zu den Sperrinformationen in seiner internen Datenbank speichern. Im Fall der Basis-ID speichert der Aussteller jedoch keine personenbezogenen Daten zur Identifizierung, sondern lediglich ein anonymes, „autorisierendes" Merkmal.

III. Der Akkumulatorstand (Sperrinformation) als anonymes Datum

Weil die Sperrinformation für sich, d.h., auf der dezentralen Infrastruktur und ohne Verknüpfung mit der BasisID, keine Identifizierung einer natürlichen Person ermöglicht, und auch einer natürlichen Person nicht zuordnenbar ist, handelt es sich um ein anonymes Datum.

Zwar gilt einerseits: Wenn die Sperrinformation zu einer Basis ID passt, handelt es sich um eine individuelle Sperrinformation. Andererseits: Ohne Weitere Informationen, die auf dem Ledger nicht vorhanden sind, lässt sich diese Sperrinformation nicht zuordnen.

Die DSGVO definiert den Begriff anonym/Anonymisierung nicht legal. Mit Hilfe des Erwägungsgrundes 26 sowie der Begriffsdefinition des personenbezogenen Datums in Art. 4 Nr. 1 DSGVO lässt sich ein unionales Begriffsverständnis ermitteln, vgl. *Meyer*, Landesrechtliche Legaldefinitionen der „Anonymisierung" im Anwendungsbereich der DSGVO, ZD 2021, 669, 671:

„Erwägungsgrund 26 DSGVO beschreibt das Ergebnis einer Anonymisierung: Personenbezogene Daten werden so verändert, „dass die betroffene Person nicht oder nicht mehr identifiziert werden kann". Damit fehlt es an einem der Elemente der Legaldefinition des personenbezogenen Datums in Art. 4 Nr. 1 DSGVO. Zentral für das Anonymisierungsverständnis der DSGVO ist, dass eine Identifizierbarkeit nur vorliegt bei einer Verfügbarkeit von Identifizierungsmitteln, die „nach allgemeinem Ermessen wahrscheinlich genutzt werden". Damit entscheidet sich die DSGVO gegen eine absolute Anonymisierung. Es reicht aus, wenn die betroffene Person zwar theoretisch reidentifiziert werden könnte, die dazu erforderlichen Mittel aber höchst wahrscheinlich nicht genutzt werden (faktische Anonymisierung).

Dieses Wahrscheinlichkeitskriterium unterscheidet die faktische Anonymisierung von der in Art. 4 Nr. 5 DSGVO definierten Pseudonymisierung. Eine Pseudonymisierung bewirkt zwar, dass die betroffene Person nicht mehr identifiziert ist. Es existiert jedoch eine Zuordnungsregel (gesondert aufbewahrte zusätzliche Informationen i.S.d. Art. 4 Nr. 5 DSGVO), die die Person reidentifiziert, und deren (zukünftige) Anwendung hinreichend realistisch oder gar erwünscht erscheint. Realistisch ist die Anwendung insbesondere dann, wenn die Zuordnungsregel bei demjenigen Verantwortlichen verbleibt, der auch den pseudonymisierten Datenbestand besitzt."

Gemäß des BfDI – Positionspapiers zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche – gilt zudem Folgendes:

„Eine absolute Anonymisierung derart, dass die Wiederherstellung des Personenbezugs für niemanden möglich ist, dürfte häufig nicht möglich sein und ist im Regelfall datenschutzrechtlich auch nicht gefordert. Ausreichend ist in der Regel, dass der Personenbezug derart aufgehoben wird, dass eine Re-Identifizierung praktisch nicht durchführbar ist, weil der Personenbezug nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden kann." (S. 4)

Thesen und Schlussfolgerungen:

1. Der Aussteller der Basis-ID (bdr) kann anhand des Akkumulators und des Index vom Tails-file keine Person identifizieren.
   a. Er verfügt weder über personenidentifizierende Informationen, noch über legale Mittel zur Erlangung von personenidentifizierenden Zusatzinformationen bei einem Dritten.
   b. Daneben gibt es keine denkbaren Szenarien einer Re-Identifizierung, da sie mathematisch nicht (ohne Zusatzinfo in Form des Vorlegens des Personalausweises oder des Sperrkennwortes durch den Betroffenen selbst) möglich ist.
2. Gleichzeitig sind die Persönlichkeitsrechte der Betroffenen keinen Gefahren ausgesetzt, da anhand des Hash-Werts keine Profilbildung o.ä. erfolgen kann.