Self Sovereign Identity (SSI) - IT-Sicherheitskonzept

„SICHERHEITSDOKUMENTATION – WALLET APP“

Bundeskanzleramt

Datum: 30.12.2021
Version: 0.5 (Arbeitsstand)

Dieses Dokument bezieht sich auf die ab Oktober 2022 neu entwickelte ID Wallet App.

INHALT

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

1 DOKUMENTINFORMATIONEN

1.1 Verteiler

Name	Firma/Abteilung

Tabelle 1: Verteiler

1.2 Versionshistorie

Version	Datum	Bearbeiter/Autor	Grund der Änderung
0.1	15.11.2021	IBM	Erster Draft
0.5	30.12.2021	IBM	Erstellung des Siko's DRAFT

Tabelle 2: Versionshistorie

1.3 Abkürzungsverzeichnis

Abkürzung	Definition
BKAmt	Bundeskanzleramt
BSI	Bundesamt für Sicherheit in der Informationstechnik
VC	Verifiable Credential

Tabelle 3: Abkürzungsverzeichnis

2 DARSTELLUNG DER ANWENDUNG UND DES METHODISCHEN ANSATZES

2.1 Zusammenfassende Beschreibung der Anwendung

Die Bundesrepublik Deutschland wird im Rahmen ihrer Digitalisierungsstrategie ein Ökosystem für Digitale Identitätsnachweise schaffen. Die Grundprämisse hinter diesem neuen Ökosystem ist, dass die Kontrolle digitaler Identitätsnachweise nach dem Ausstellen bei den Nutzer*Innen selbst liegt. Dieses Konzept wird als SSI bezeichnet. Vergleichbar zu haptischen Nachweisen werden Identitätsnachweise als gültig anerkannt, wenn sie nachweislich von einer vertrauenswürdigen Stelle ausgestellt wurden. Die Glaubhaftigkeit von haptischen Nachweisen wird über schwer zu kopierende Materialien und Wasserzeichen sowie Signaturen, Stempel oder Siegel sichergestellt. In der digitalen Welt können digitale Signaturen verwendet werden, um die Authentizität eines Dokuments nachzuweisen. Diese kryptographisch überprüfbaren Zertifikate oder Identitätsnachweise, wie etwa ein digitaler Führerschein, ein digitales Zeugnis oder ein digitales Ticket werden im SSI-Kontext als Verifiable Credentials (VC) bezeichnet. VCs bilden dementsprechend die Grundlage, auf der SSI aufbaut. Sie werden lokal in einer Wallet-App (vergleichbar mit einem Portemonnaie) der Nutzer*Innen gespeichert und können von dort aus auf Nachfrage vorgezeigt und geprüft werden, ohne dass dafür Nutzer*Innen oder Verifizierer mit dem Aussteller oder einer anderen dritten Partei kommunizieren müssen.

Es wird die Distributed Ledger / Blockchain-Technologie für das Netzwerk genutzt, welche die Aufgaben hat, sicherzustellen, dass Einträge unveränderbar sind und die Infrastruktur manipulationssicher bleibt. Der gewählte dezentrale und offene Ansatz verhindert zudem, dass eine einzelne Organisation Kontrolle über das Ökosystem oder die dort verarbeiteten Daten erlangen kann und verhindert ein Vendor-Lock-in. Die Architektur erlaubt es weiterhin Nachweise von der Halter*in an den Prüfer weiterzugeben, ohne dass die Aussteller*in hiervon Kenntnis erlangt.

Es wurde bewusst eine über Blockchain Technologie unterstützte, verteilte Architektur gewählt, um den Single Point of Failure einer zentralen Certificate Authority zu vermeiden und die Abhängigkeit von einer zentralen Instanz auszuschließen.

2.2 Methodik

Das Ziel dieses Dokuments ist die Ermittlung von Sicherheitsanforderungen, die Beurteilung des erreichten Sicherheitsniveaus sowie die Festlegung angemessener Sicherheitsmaßnahmen für die SSI-basierte Wallet-App. Dies geschieht auf der Basis des IT-Grundschutz-Kompendiums (Edition 2021) des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Das Dokument soll IT-Sicherheitsbeauftragte, Fachverantwortliche und Administratoren der Betreiber bei der Erstellung und Erweiterung der betreiberspezifischen IT-Sicherheitskonzepte unterstützen. Dieses IT-Sicherheitskonzept wurde auf der Basis der Vorgaben des BSI, welche in den BSI-Standards 200-1 bis 200-4 beschrieben sind (Stand Februar 2021), erstellt. Die IT-Grundschutz-Vorgehensweise besteht aus den folgenden Elementen:

- **Lösungsbeschreibung und Definition des Informationsverbundes:** Es wird zunächst der Geltungsbereich des Sicherheitskonzepts definiert.
- **Risikobetrachtung anhand der Prozesskette:** Das ID Wallet stellt eine zentrale Komponente im ID-Lifecycle des Identitätssystem dar. Es führt die Identifizierung der Nutzer*in zur Ausstellung der Basis-ID mittels AusweisApp2 SDK durch, hält Basis-ID, sowie weitere Nachweise und führt Verifiable Presentations durch.
- **Strukturanalyse:** Als Grundlage eines jeden IT-Sicherheitskonzepts wird beschrieben, welche Daten mit welchen Systemen aufgrund welcher Prozesse verarbeitet werden.
- **Schutzbedarfsfeststellung:** Hierbei wird ermittelt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.
- **Modellierung:** Für den festgelegten Informationsverbund werden die relevanten Bausteine (Maßnahmensammlungen) aus dem IT-Grundschutz-Kompendium ausgewählt, auf deren Basis im weiteren Verlauf mögliche weitere Sicherheitsmaßnahmen definiert werden.
- **Logging & Monitoring:** Für die Wallet-App wird definiert, wo und wie Sicherheitsrelevante Informationen geloggt werden und wie das entsprechende Monitoring aussieht.
- **Vulnerability-Management & Penetration-Testing:** Beschreibung des Vulnerability-Management Prozesses sowie die Resultate aus dem ersten Penetration-Test.
- **Basis-Sicherheitscheck:** An dieser Stelle wird ein Überblick über das vorhandene Sicherheitsniveau erarbeitet, mithilfe von Interviews und Fragebögen wird der Status quo des Informationsverbunds hinsichtlich des Umsetzungsstatus für jede relevante Maßnahme abgefragt und festgestellt.
- **Ergänzende Sicherheitsanalyse:** Die ergänzende Sicherheitsanalyse stellt sicher, dass die nicht vollständig abgedeckten Risiken (zum Beispiel bei höherem Schutzbedarf) ermittelt werden.
- **Risikoanalyse:** Ziel der Risikoanalyse ist, die vorhandenen Risiken durch eine Risikobehandlung auf ein verträgliches bzw. akzeptables Maß (Restrisiko) zu reduzieren.

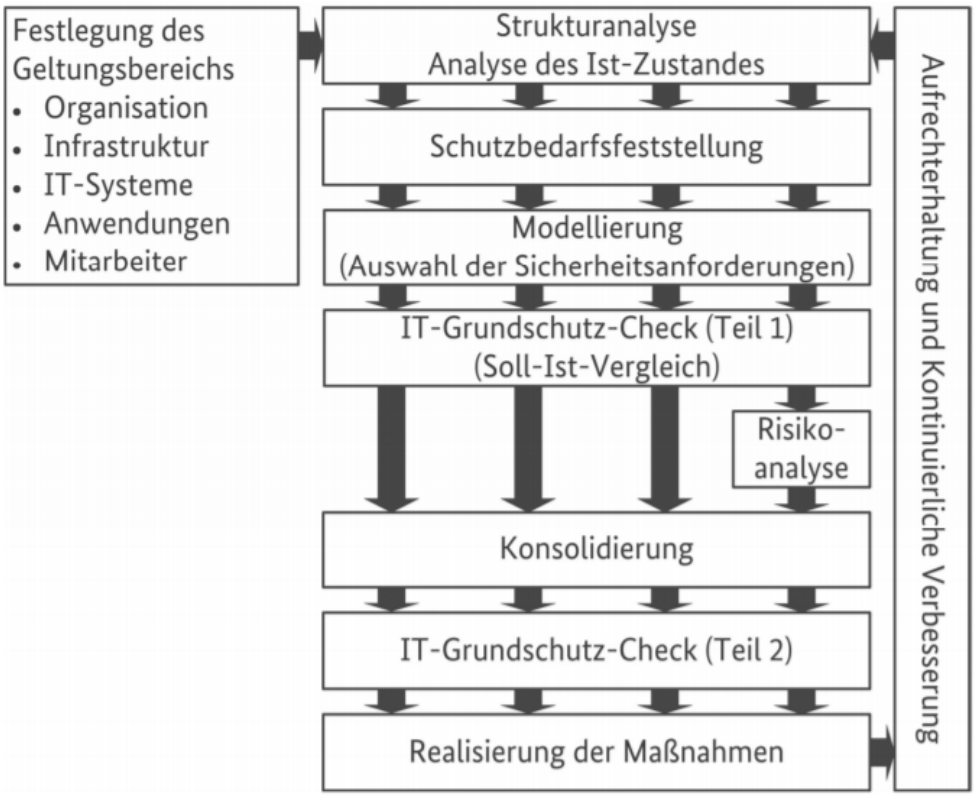

Abbildung 1: IT-Sicherheitskonzeption bei Standard-Absicherung (BSI Standard 200-2)

Das Sicherheitskonzept muss regelmäßig fortgeschrieben und mit dem zuständigen IT-Sicherheitsbeauftragten abgestimmt werden. Die Abbildung 1 veranschaulicht die grundsätzliche Vorgehensweise, die sich in der Struktur dieses Muster-IT-Sicherheitskonzeptes wiederfindet und um eine etwas ausführlichere Darstellung der Lösungsarchitektur erweitert wurde.

2.3 Vorgehensweise

Die Erstellung, Umsetzung und Fortschreibung eines IT-Sicherheitskonzeptes sind verpflichtend. Die IT-Sicherheit ist Teil der Informationssicherheit.

Dieses Dokument muss regelmäßig überprüft und ergänzt sowie mit dem zuständigen IT-Sicherheitsbeauftragten abgestimmt werden.

3 LÖSUNGSBESCHREIBUNG, INFORMATIONSVERBUND UND STRUKTURANALYSE

3.1 Beschreibung der Lösung: Basis-ID

Als erstes wird der folgende Abschnitt den Lebenszyklus der Basis-ID beschreiben, weil dies der primäre Anwendungsfall der Wallet-App ist. Die Bundesdruckerei GmbH (unter Einbindung der Unternehmenstochter D-Trust GmbH) verantwortet die Wahrung der klassischen Schutzziele (Integrität inkl. Authentizität, Vertraulichkeit und Verfügbarkeit inkl. Belastbarkeit) für Daten, Prozesse und Komponenten, die im Zusammenhang mit der Ableitung der Primäridentität auf die Basis-ID stehen.

3.1.1 Enrollment

Die nachfolgende Abbildung gibt einen Überblick darüber, wie für eine Nutzer*in die Basis-ID mittels Online-Ausweisfunktion ausgestellt und übergeben wird. Die folgenden Unterabschnitte beschreiben diesen Prozess im Detail.

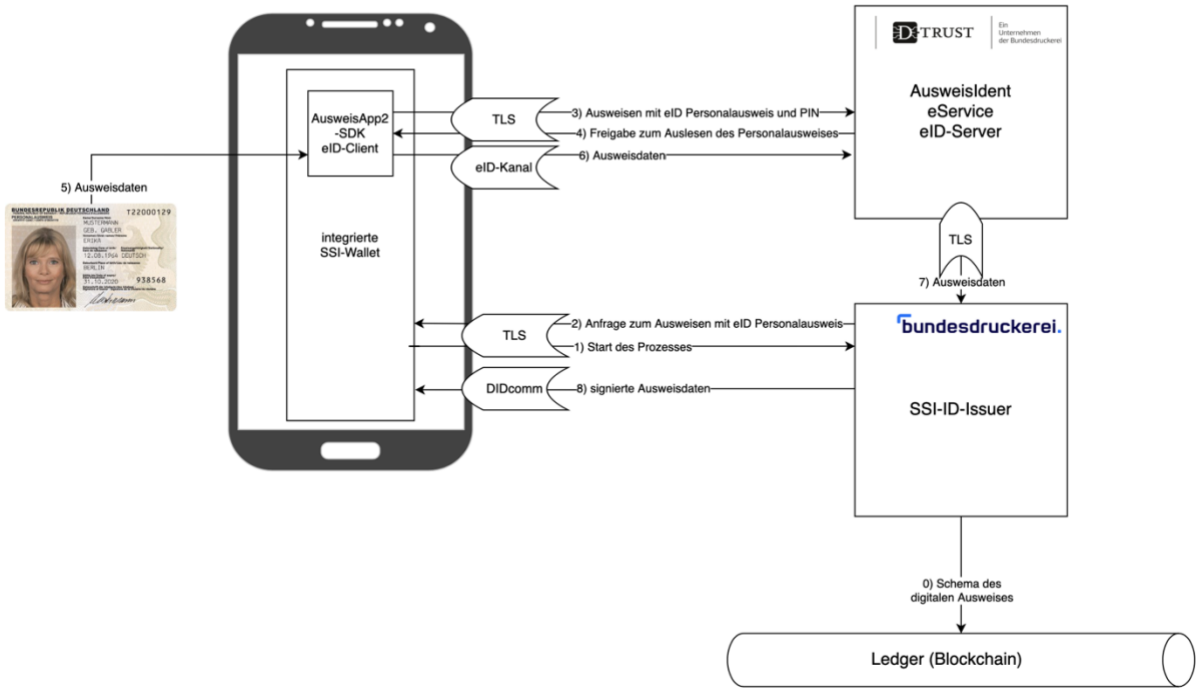

Abbildung 2: Enrollment der Basis-ID

3.1.2 Registrieren

Der Ausstellungsprozess wird im integrierten Flow durch die Nutzer*innen in der Wallet-App initiiert. Diese startet den Prozess mit dem autorisierten Aufruf des Bundesdruckerei-API-Endpunkts (über einen TLS-gesicherten Kanal). Die Wallet authentifiziert sich mittels eines API-Keys. Die Nutzer*in stimmt den Nutzungsbedingungen und der Datenschutzerklärung der Aussteller*in zu.

3.1.3 Identität verifizieren

Die Identifizierung der Nutzer*in erfolgt mittels der eID-Funktion des Personalausweises. Die Issuer-API liefert dafür den Einstiegpunkt (tcTokenUrl) für den eID-Prozess mit. Damit baut das in der Wallet integrierte AusweisApp2-SDK eine Verbindung zum eID-Server auf, prüft die Ausleseberechtigung und holt die Zustimmung der Nutzer*in ein. Dieser autorisiert den Auslesevorgang mit Eingabe seiner eID-PIN in der Wallet-App. Im eID-Kanal werden die angeforderten Identitätsdaten von der eID-Karte (Personalausweis) an den eID-Server übertragen. Der eID-Server antwortet dem integrierten eID-Client nach dem erfolgreichen Auslesen mit der redirectUrl. Diese beinhaltet lediglich den Identifier für die eID-Session, der integrierte eID-Client übergibt die redirectUrl and die Wallet und diese ruft den API-Endpunkt aus redirectUrl auf. Der Ausstellungsdienst fragt die Identitätsdaten beim eID-Server an (über einen TLS-gesicherten Kanal) und der eID-Server gibt die ausgelesenen Identitätsdaten an den Issuer-Service frei. Der Ausstellungsdienst hat jetzt die verifizierten Identitätsdaten der Nutzer*in.

3.1.4 Identität speichern

Der Ausstellungsdienst (SSI-ID-Issuer) speichert keine Nutzer*innendaten, die verifizierten Nutzer*innenattribute werden nur bis zur Ausstellung des Credentials temporär gehalten und danach gelöscht. Es werden lediglich pseudonyme Daten zur Zuordnung für die Sperrung gespeichert (dazu mehr im Abschnitt Sperrung), sowie anonyme Daten für den Lebenszyklus des Credentials.

3.1.5 Ausstellen / Ausliefern

Der Ausstellungsdienst antwortet auf der Wallet nach dem erfolgreichen Durchlauf des eID-Prozesses mit einer DIDComm-Invitation. Diese Einladung beinhaltet die DID, krytografische Schlüssel und Parameter für den Aufbau der Verbindung (DIDComm). Die Wallet empfängt diese und initiiert die DIDComm-Verbindung zur Aussteller*in. Die Aussteller*in kann das Credential mit den verifizierten Nutzer*innenattributen erstellen und kryptografisch signieren und über die erfolgreich aufgebaute Verbindung an die Wallet schicken. Die Nutzer*in nimmt die Anfrage an und die Wallet speichert das Credential ab. Der Ausstellungsdienst generiert ein Sperrkennwort und speichert die Daten für den Lebenszyklus in der internen Sperrdatenbank. Das Sperrkennwort wird über den DIDComm-Kanal sicher übertragen und der Nutzer*in angezeigt.

Die Kanalbindung beim Ausstellen der Basis-ID wird durch folgende Kanäle erreicht (Abbildung 2: Enrollment der Basis-ID). TLS zwischen Ausstellungsdienst (AusweisIdent/eService) und Wallet, und anschließenden Aufbau des eID-Kanals zwischen eID-Dokument und AusweisIdent/eID-Server unter Vermittlung von AusweisApp2/eID-Client. Das Ausstellen der Basis-ID als Verifiable Credential erfolgt im DIDComm-Kanal. Die enge Bindung zwischen Onlineausweisfunktion und Deployment der Credentials wird durch die Integration des AusweisApp2-SDKs in die ID Wallet App auf Softwareebene gewährleistet.

3.1.6 Aktivieren

Sobald die Nutzer*in das Credential annimmt, ist dieses für die Nutzung bereit.

3.1.7 Aktualisieren

Ein mehrmaliges paralleles Ableiten der Basis-ID ist möglich, eine Aktualisierung bzw. Übersicht der Nutzer*in über den Status seiner Ableitungen ist zu einem späteren Zeitpunkt angedacht.

3.1.8 Aussetzten / Sperren

Die Nutzer*in zeigt ihre Autorisierung der Sperrung entweder mittels Personalausweis (über die Restricted ID) oder mittels Sperrkennwort, welches ihr im Registrierungsprozess angezeigt wurde. Das Sperrkennwort wird als Hash ausschließlich intern im Sperrdienst der Aussteller*in für die Basis-ID vorgehalten. Weiter wird der Hash über die Restricted ID (dienst- und kartenspezifisches Kennzeichen/Pseudonym) des Personalausweisinhabers im Sperrdienst der Aussteller*in 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 die Nutzer*in authentifiziert und eine Zuordnung hergestellt.

Die Aussteller*in prüft nun die Autorisierung und löst mittels gespeicherter Sperrliste & Index eine Sperrung aus, indem er den kryptografischen Akkumulator auf dem Ledger anpasst. Genauer: Da die Aussteller*in nach der Ausgabe des Credentials keinen direkten Zugriff mehr hat, gibt es eine anonyme Sperrinformation auf der dezentralen Infrastruktur (Blockchain/Ledger). Diese ist in der Hoheit des Ausstellers. Die Aussteller*in betreibt dafür Sperrlisten (Tails-Files), in jeder Sperrliste werden eine große Anzahl an Credentials referenziert. Hierdurch ergibt sich eine Herdenanonymität.

Der gesamte Zeithorizont zwischen Auslösung der Sperrung und effektiver Umsetzung beträgt ca. 10 Sekunden.

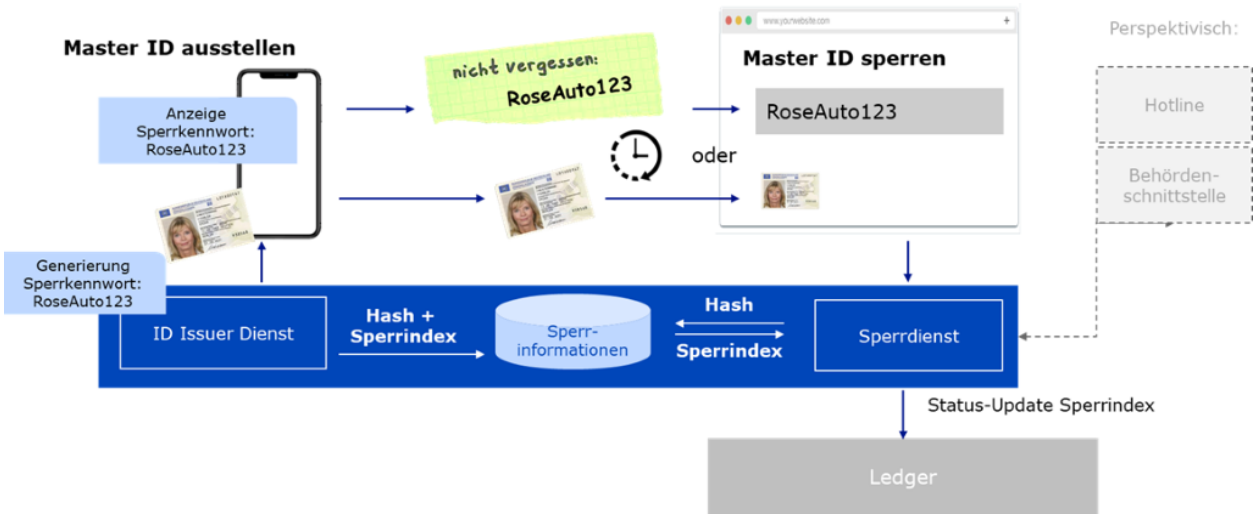

Abbildung 3: Aussetzung / Sperrung der Basis-ID

3.1.9 Reaktivieren

Ein Reaktivieren ist nicht vorgesehen. Es muss ein neues VC generiert werden.

3.1.10 Ersetzen

Ein mehrmaliges paralleles Ableiten ist vorgesehen, ein Ersetzen ist derzeit nicht möglich, bei Sperrung eines abgeleiteten Credentials werden derzeit alle Ableitungen revoziert. Zu einem späteren Zeitpunkt ist die inviduelle Revozierung einzelner Credentials durch die Nutzer*in angedacht.

3.1.11 Löschen

Ein Widerruf kommt der Sperrung eines Credentials gleich, zusätzlich werden alle nut-zer*innenbezogenen (pseudonymen) Daten gelöscht.

3.2 Beschreibung der Lösung: Wallet-App

Dieser Abschnitt gibt einen Überblick über den aktuellen Entwicklungsstand der ID Wallet. Das ID Wallet stellt eine zentrale Komponente im ID-Lifecycle des Identitätssystem dar. Es führt die Identifizierung der Nutzer*in zur Ausstellung der Basis-ID mittels AusweisApp2 SDK durch, hält Basis-ID, sowie weitere Nachweise und führt Verifiable Presentations durch. Das aktuell eingesetzte ID Wallet steht für die zwei Plattformen Android (ab Version >= 7) und iOS (ab Version >= 14) zur Verfügung. In der aktuellen Entwicklungsstufe werden folgende Maßnahmen zur Gewährleistung & Nachprüfung der Integrität und Authentizität des Smartphone OS und der Wallet Applikation implementiert. Diese Maßnahmen erschweren das Installieren der Wallet App auf gerooteten Geräten oder einem Simulator. Darüber hinaus gehende Maßnahmen zur Gewährleistung der Integrität und Authentizität werden in nachfolgenden Entwicklungsiterationen evaluiert. Als erstes wird auf den Prozess der Basis-ID eingegangen, bevor Details der Wallet-App folgen.

3.2.1 Integritätscheck OS und App

Die Aussteller*in der Basis-ID überprüft während des Ausstellungsprozesses, dass keine Manipulation an Betriebssystem und Applikation auf dem Endgerät der Nutzer*in vorgenommen wurde. Dazu werden vom Betriebssystem bereitgestellte Verfahren genutzt. Unter Android wird mittels SafetyNet (https://developer.android.com/training/safetynet) und unter iOS mittels DeviceCheck (https://developer.apple.com/documentation/devicecheck) die Überprüfung durchgeführt. Dabei gibt die Aussteller*in eine sitzungsbezogene challenge (nonce) vor, die zusammen mit Informationen zum mobilen Endgerät vom Attestation Server der Betriebssysteme signiert wird. Die Nutzer*in muss diese signierten Informationen (Attestation) an die Aussteller*in übertragen, bevor die Ausstellung des Credentials erfolgen kann. Die Aussteller*in überprüft dabei insbesondere:

- Integrität/Authentizität mittels Signaturprüfung der Attestation
- Aktualität der Attestation (timestamp)
- Sitzungsbezug (nonce/challenge = Hash der HTTPS Session ID)
- Package Version und Applikation signature key (SafetyNet)
- Ergebnis der Integritätsprüfung (SafetyNet: ctsProfileMatch, basicIntegrity)

3.2.2 App Authentizität mit API Key

Das Ausstellen einer Basis-ID durch die Bundesdruckerei GmbH erfordert die Verwendung eines API Keys für das Kontaktieren des folgenden Bundesdruckerei API-Endpunkt:

- TLS-API Endpunkt zum Initiieren des integrierten Flow der Basis-ID

Der API Key (128 Bit UUID, Wallethersteller- und versionsspezifisch) wird über einen out-of-band Kanal von der Bundesdruckerei GmbH an die esatus AG weitergereicht. Der Prozess ist folgendermaßen definiert:

1. UUID wird in von der Bundesdruckerei in ihrer Deployment Umgebung generiert
2. UUID wird mittels sicherem Transportmedium (verschlüsselte und signierte eMail) an esatus geschickt.

Die esatus AG bindet den erhaltenen API Key als Konstante (X-API-KEY) in den Quellcode der ID Wallet App ein. Um ein unbefugtes Extrahieren zu erschweren, wird der API Key obfuskiert. Die eigentliche Authentisierung ggü. den Endpunkten erfolgt via X-API-Key Feld im HTTP-Header.

3.2.3 Sichere Datenhaltung und kryptographisches Schlüsselmanagement

Die ID Wallet setzt bei der Implementierung der ID-Systemfunktionalitäten auf das Hyperledger Indy SDK und dessen Kryptobibliotheken. Hyperledger Indy ist Open Source und bietet Werkzeuge, Bibliotheken und wiederverwendbare Komponenten für die Verwaltung der selbstbestimmten digitalen Identität. Hierzu gehört die von der ID Wallet verwendete „Indy SDK Default Wallet“ Implementation mit folgenden Schlüsselfunktionen:

- Validator-Interaktion
- Verwaltung von Schlüsseln (siehe Kapitel **Error! Reference source not found.**)
- Verwaltung der Verifiable / Anonymous Credentials

Sämtliche hierbei anfallende Daten, u.a. auch das Link Secret, werden von der Wallet in einer dateibasierten Datenbank (SQLite3) gespeichert, die eine symmetrische und zur Laufzeit transparente Verschlüsselung besitzt (gehärtete Version von SQLCipher[1]). Der zur Verschlüsselung Absicherung (Verschlüsselung und Datenauthentisierung) der Datenbank verwendete symmetrische Schlüssel *key_enc_data* wird folgendermaßen bei jeden Wallet App Start abgeleitet:

- Pin_validation_deriv = PBKDF2(PIN | key_enc_data_salt)
- key_enc_data = SHA256(Pin_validation_deriv | pre_key)

Wobei das zufällig beim initialen Wallet App Start generierte key_enc_data_salt und pre_key Xamarin-eigenen SecureStorage mit Hilfe des hardware-gebundenen, plattformspezifischen symmetrischen Schlüssel *key_hardware* verschlüsselt sicher (verschlüsselt und authentisiert) abgelegt wird.

Die unteren Abbildungen zeigen das hierarchische Schlüsselmodel mit besonderem Augenmerk auf das schützenswerte Authentisierungssecret Link Secret.

[1] https://hyperledger-indy.readthedocs.io/projects/sdk/en/latest/docs/concepts/default-wallet.html?highlight=wallet

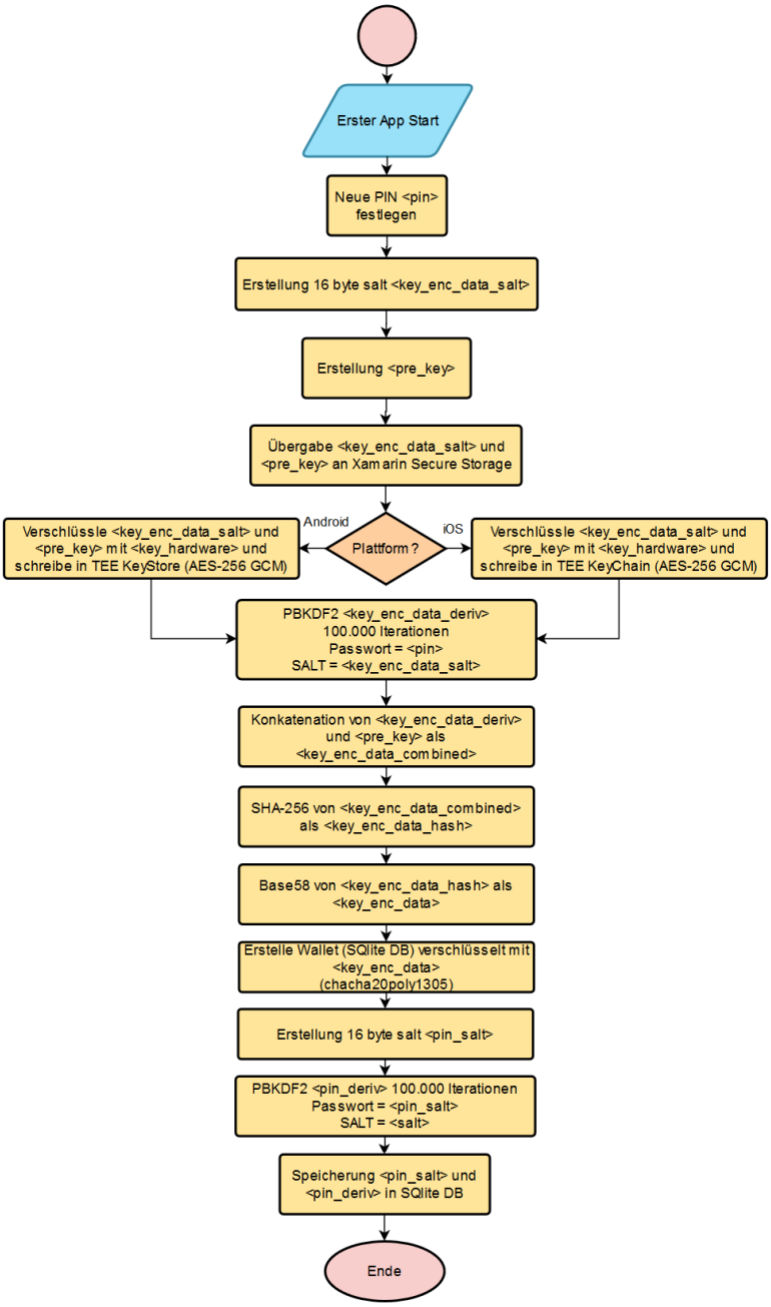

Abbildung 4: Verschlüsselung Link Secret

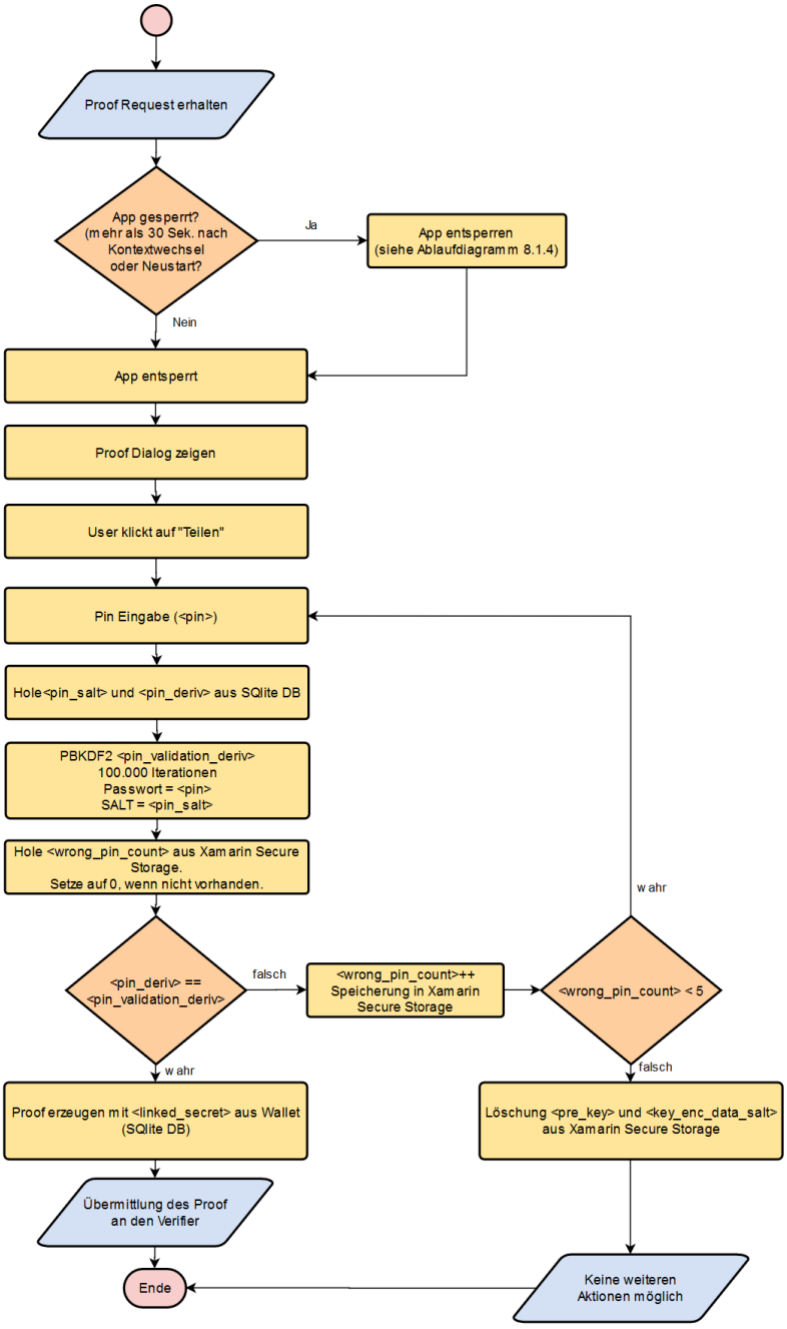

Abbildung 5: Entschlüsselung Link Secret

Für die Benutzung des Link Secrets muss dieses entschlüsselt werden und liegt somit in dieser Zeit im potenziell unsicheren Speicher vor. Um das Kopieren des Link Secrets zu erschweren, müssen noch entsprechende Maßnahmen definiert und umgesetzt werden. Für die definierten Maßnahmen im Pilotbetrieb siehe entsprechendes Systemkonzept.

3.2.4 Zugriffskontrolle Wallet

Der Wallet-Zugriff ist aktuell mittels einer 6-stelligen PIN vor unerlaubtem Zugriff geschützt. Diese PIN wird beim ersten Start der Wallet von der Nutzer*in festgelegt und kann nachträglich über den gleichen Prozess und mit vorherig festgelegten PIN geändert werden. Diese PIN muss sowohl beim Start der Wallet App, sowie 30 Sekunden nachdem die App in den Hintergrund verschoben wurde (z.B. beim Kontextwechsel in eine andere App) eingegeben werden. Die PIN-Prüfung findet mittels der oben beschriebenen Schlüsselableitung für die SQLite Datenbank statt. Wird ein falscher PIN eingegeben, schlägt die Entschlüsselung der SQLite Datenbank fehl und die Wallet App kann nicht gestartet werden. Für die Eingabe der PIN durch die Nutzer*in wird eine angepasste Version von XamarinFormsPinView[2] verwendet. Nach 5-maliger Falscheingabe des PINs wird der pre_key gelöscht und die Entschlüsselung der SQLite Datenbank damit unmöglich. Der Fehlbedienungszähler ist in Software umgesetzt. Die folgende Abbildung zeigt den Ablauf der Zugriffskontrolle mit den jeweiligen Merkmalen.

[2] https://github.com/lassana/XamarinFormsPinView

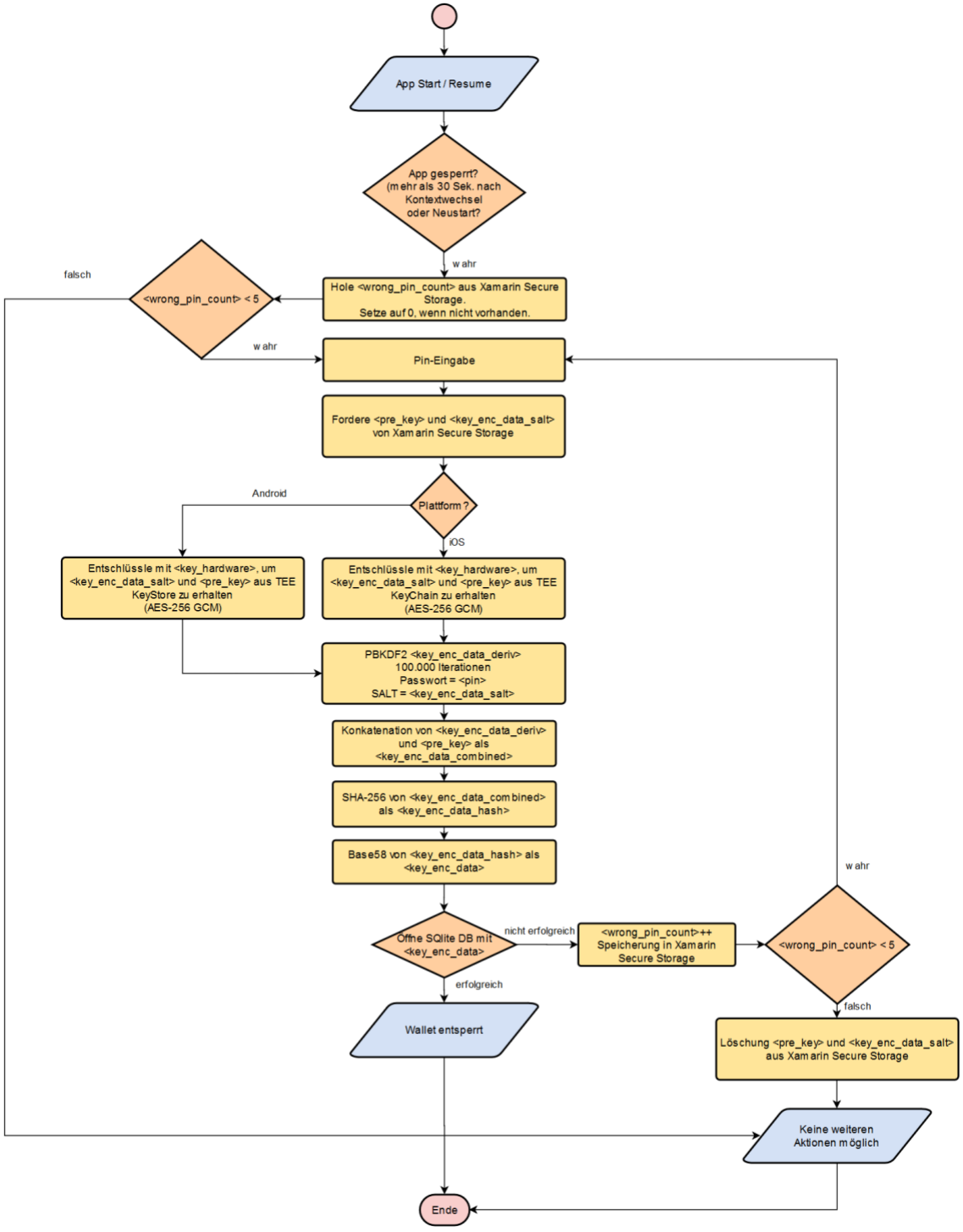

Abbildung 6: Ablauf Zugriffskontrolle

3.2.5 Inhaber-Authentisierung

Die Inhaber-Authentisierung findet über eine Abfrage der gleichen PIN wie beim App Start vor jedem Identity Proof statt. Diese PIN-Abfrage wird über den Programmablauf erzwungen und ist nicht an die Entschlüsselung der SQLite Datenbank bzw. des Link Secrets gebunden.

Um dies zu realisieren, wird die Nutzer-PIN beim initialen Setzen per PBKDF2 und einem zufällig gewähltem Salt abgeleitet und zusammen mit dem Salt in der verschlüsselten SQLite Datenbank gespeichert:

1. Pin_deriv = PBKDF2(PIN | Pin_salt)
2. Speichere Pin_deriv und Pin_salt in SQLiteDB

Dabei ist das Pin_salt ≠ Key_enc_data_salt

Im Rahmen der Inhaber-Authentisierung wird dann die von der Nutzer*in eingegebene PIN erneut abgeleitet und mit dem in der SQLite Datenbank gespeicherten Wert verglichen:

1. DerivedInput = PBKDF2(PIN_INPUT | Pin_salt)
2. DervidedInput =? Pin_deriv

Nach 5-maliger Falscheingabe des PINs wird der pre_key gelöscht und die Entschlüsselung der SQLite Datenbank damit unmöglich. Der Fehlbedienungszähler ist in Software umgesetzt.

3.2.6 Sichere Kanalbündelung beim Ausstellen der Basis-ID

Die Kanalbündelung zwischen Onlineausweisfunktion und Ausstellen der Credentials wird durch die Integration des AusweisApp2 SDKs in die ID Wallet App auf Softwareebene gewährleistet. Der Ausstellungsprozess der Basis-ID wird durch die Wallet initiiert. Sie baut einen TLS-Kanal zum API-Endpunkt der Aussteller*in (SSI Issuer) auf, dieser wird zusätzliche mit Zertifikatspinning (Public Key) geschützt (siehe Kapitel **Error! Reference source not found.**). Der SSI Issuer antwortet mit der sitzungsgebundenen tcTokenUrl, die auf AusweisIdent Service zeigt. Durch diese Anfrage wird der Online Authentisierungsvorgang mittles AusweisIdent Service angestoßen, dieser nimmt im eID-Kontext sowohl die Rolle des eIDServers als auch des eService ein. Die tcTokenUrl wird von der Wallet an das integrierte AusweisApp2-SDK übergeben und antwortet mit dem tcToken, dieses bildet die Startparameter für den eID-Prozess. Anhand des TCToken vermittelt der eID-Client/AusweisApp2-SDK einen sicheren eID-Kanal zwischen dem eID-Dokument und dem eID-Server. Nach Prüfung des Berechtigungszertifikats und Autorisierung des eID-Ausleseprozesses durch die Nutzer*in mittels PIN-Eingabe wird der eID-Kanal aufgebaut und die eID-Attribute im eID-Kanal an den eID-Server übertragen. Anschließend antwortet der eID-Server mit der redirectUrl an den eID-Client/AusweisApp2-SDK, diese wird an die Wallet übergeben und aufgerufen. Die redirectURL zeigt zunächst auf den eService (AusweisIdent) und wird beim Aufruf abschließend an einen sicheren API-Endpunkt (TLS) der Aussteller*in (SSI Issuer) weitergeleitet (es wird ein neuer TLS-Kanal aufgebaut und die Sessions mittels, im volatilen Speicher des Servers abgelegten Session-Cookies gematcht). Der eService der Aussteller*in

(AusweisIdent) holt nun die eID-Daten vom eID-Server ab. Der SSI Issuer holt die Ausweisdaten vom eService mittels AusweisIdent-Schnittstellen (OpenID Connect) ab. Dabei stellt AusweisIdent die Rolle des OpenID Provider dar und der SSI Issuer ist in der Rolle der Relying Party. Die Aussteller*in antwortet der Wallet nun über den gesicherten API-Endpunkt (TLS) mit der DIDComm-Invitation, diese wird vom SSI-Agenten der Aussteller*in generiert. Eine DIDComm-Invitation kann nicht mehrfach benutzt werden. Die Wallet kann mittels dieser DIDComm-Invitation nun einen sicheren DIDComm-Kanal zum SSI-Agenten der Aussteller*in Aufbauen. Über diesen DIDComm-Kanal wird nun das Credential mit den eID-Atttributen ausgestellt.

Zusammenfassend wird die Kanalbündelung erreicht, indem die Wallet zwei TLS-Kanäle mit der Aussteller*in aufbaut (verbunden über eine Session ID) und über diese TLS-Kanäle sowohl der eID-Kanal als auch der DIDComm-Kanal initiiert und von der integrierten Wallet verwaltet werden.

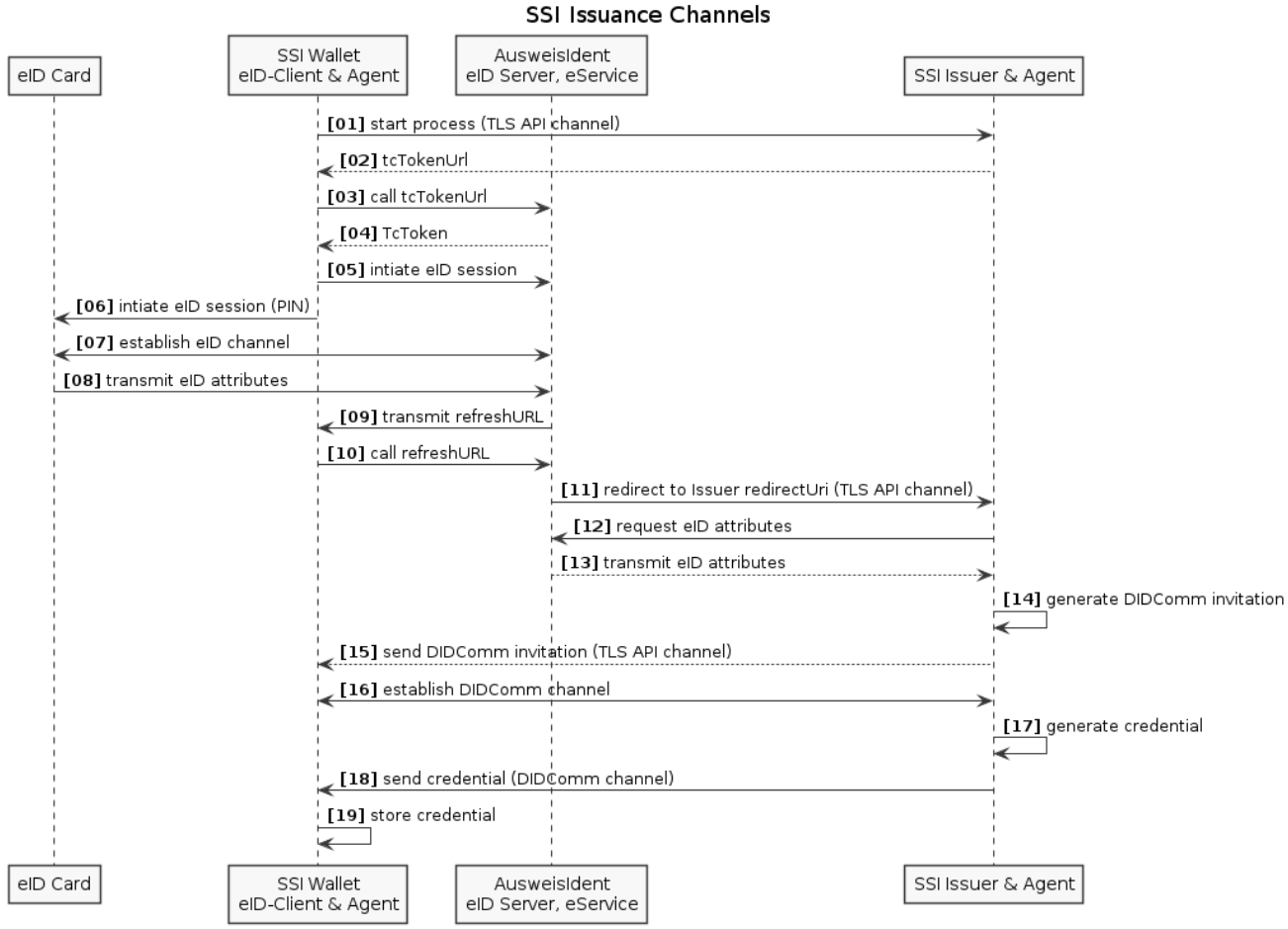

Abbildung 7: Sichere Kanalbündelung beim Ausstellen der Basis-ID

3.3 Risikobetrachtung anhand der Prozesskette

Der Prozess des Prüfens der Informationen aus der eID und das entsprechende Ausstellen des MasterID VCs durch die Bundesdruckerei genügt aufgrund der Erfahrungen der Bundesdruckerei und der Integration des Services in die bestehenden Kompetenzen der Bundesdruckerei hohen Sicherheitsanforderungen; dabei wird eine bestehende kryptographische Vertrauenskette (eID) auf eine neue Vertrauenskette (Credential Definition der MasterID in der Blockchain und Signatur durch die Bundesdruckerei) übertragen. Die Wallet-App selbst kann keine gültige Änderung des VCs erstellen, da sie den privaten Schlüssel der Bundesdruckerei nicht kennt. Als das schwächste Glied in der Kette ist das jeweilige Smartphone der Nutzer*in zu betrachten. Um die Widerstandsfähigkeit eines mobilen Endgerätes einschätzen zu können, müssen detaillierte Informationen zu den Sicherheits- und Privatsphärenmechanismen (in Hardware und Software) des Endgeräts vorliegen. Bekannte Schwachstellen einer Sicherheitskomponenten fließen zusätzlich in eine Einschätzung zur Widerstandsfähigkeit ein. Um die Sicherheit der ID-Lösung auf dem mobilen Endgerät während der kompletten Nutzungsdauer sicherzustellen, müssen die gesammelten Geräte- und Schwachstelleninformationen kontinuierlich aktualisiert und gesichtet werden. Im sehr heterogenen Android Ökosystem sind die benötigten Informationen nicht, wie z.B. bei Apple iOS, an einem zentralen Anlaufpunkt abrufbar. Hier müssen u.a. Herstellerwebseiten, Blogs, Zertifizierungsportale, sowie Schwachstellendatenbanken ausgewertet und in einer zentralen Datenbank aufbereitet zur Verfügung gestellt werden.

Des Weiteren ist die Nutzer*in-Authentisierung auf der Wallet-App mit dem 6-stelligen PIN ungenügend. Eine App, welche Zugriffe auf besonders schützenswerte Daten gewährt, benötigt mindestens ein zwei Faktoren-Authentisierung. Entweder mittels einer transaction authentication number (TAN) oder einer entsprechenden Authenticator-App wie z.B. Google Authenticator.

3.4 Datenfelder

Die folgenden Datenfelder werden bearbeitet:

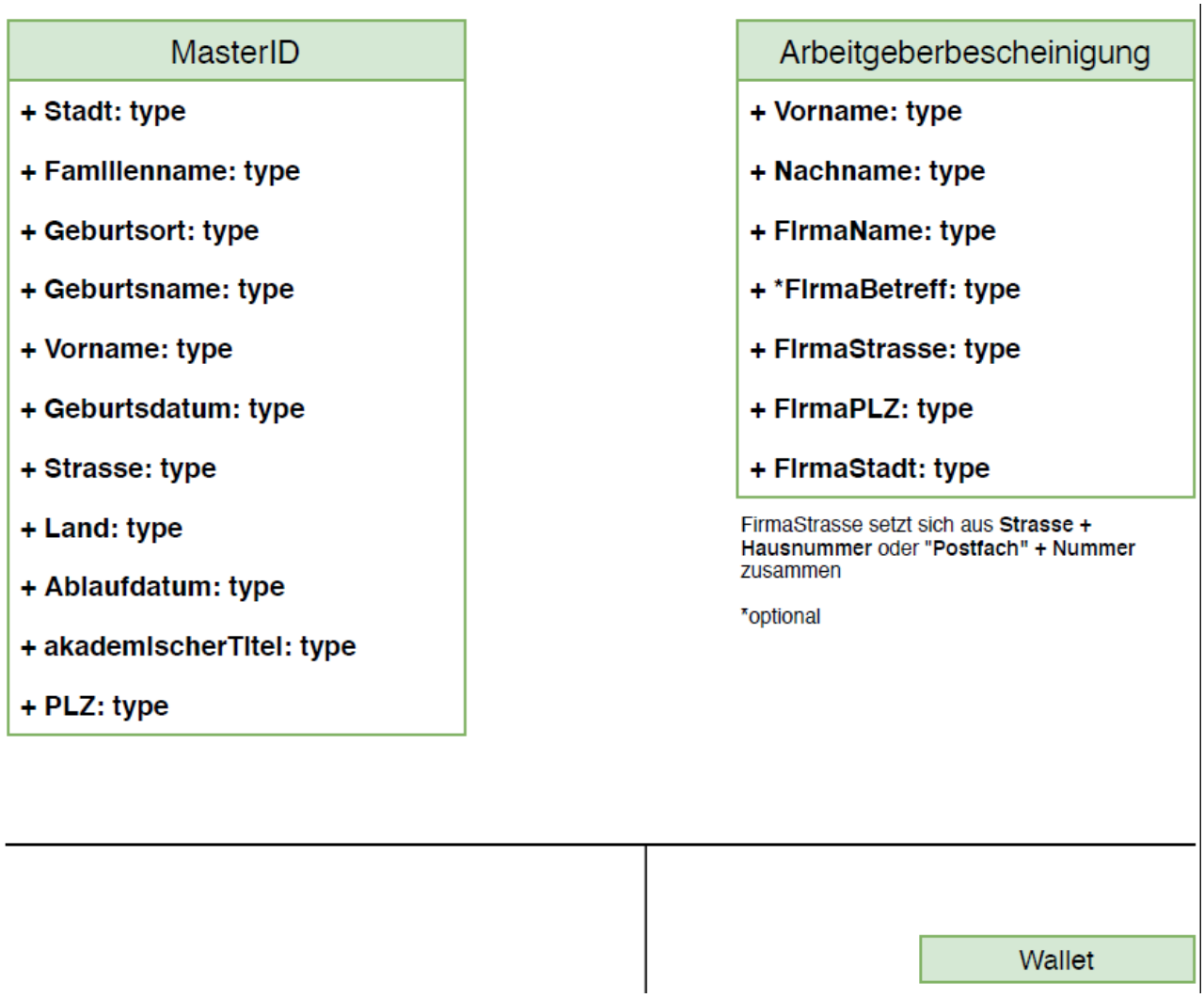

Abbildung 8: Datenfelder

3.5 Informationsverb., Netzplan und Kommunikationsverbindungen

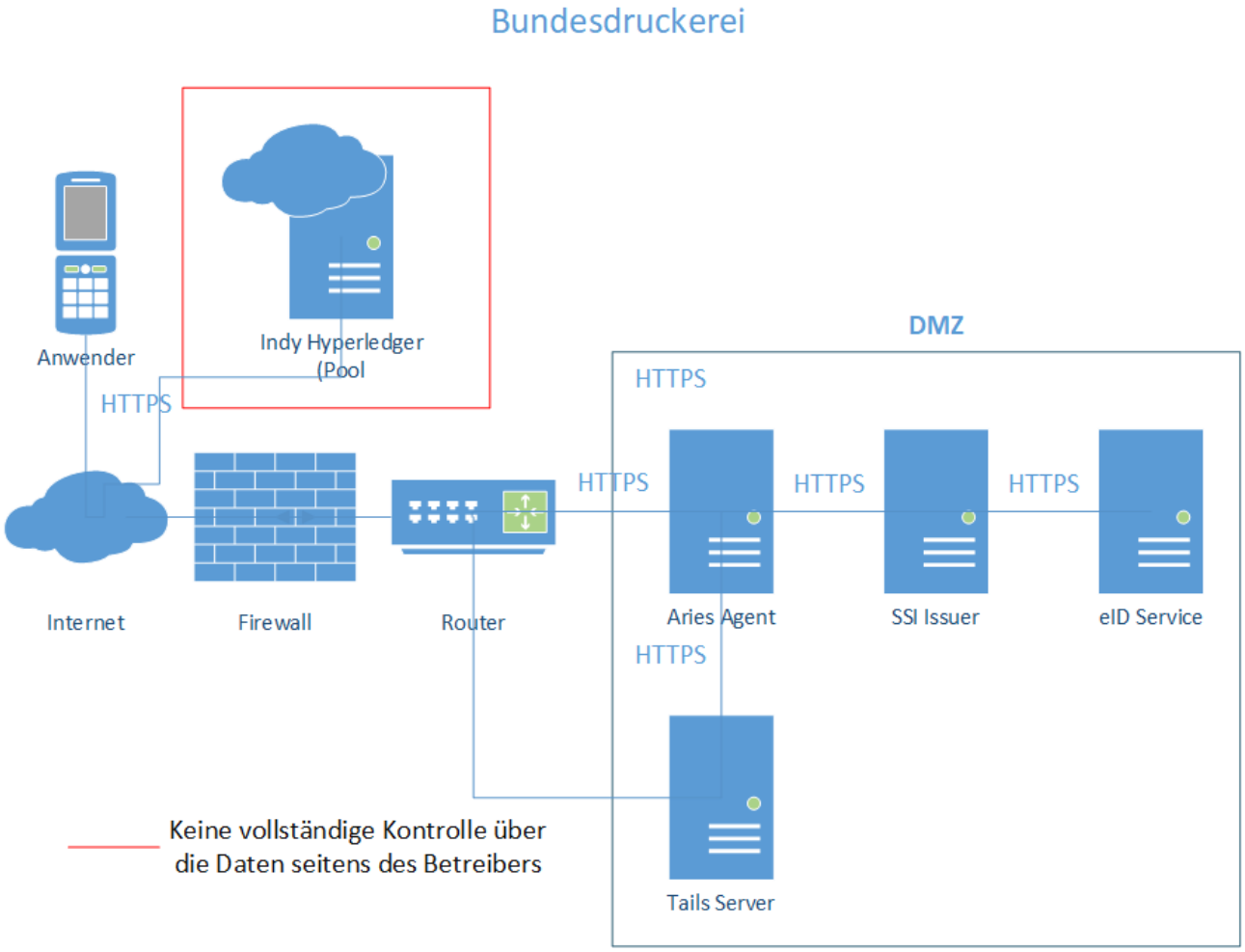

Abbildung 9: Bundesdruckerei

3.6 Wesentliche IT-Anwendungen und IT-Systeme

Die Komponenten des Gesamtsystems laufen derzeit in Kubernetes Clustern bzw. werden als virtuelle Maschine betrieben. Die verschiedenen Komponenten werden auf Ubuntu (Linux) Servern installiert und konfiguriert. Die Endnutzer*innen der Anwendung nutzen eine Smartphone-App für SSI-Interaktionen, die esatus Wallet. Seitens der Bundesdruckerei wird neben einem eID-Service zur Erstellung von MasterID Credentials ein weiterer Aries Agent betrieben, um die Credentials auszustellen. Zudem betreiben die Bundesdruckerei, esatus sowie IBM einen Knoten des unternehmensübergreifenden Indy Blockchain-Netzwerkes. Auf den Mobilgeräten (iOS und Android) der Testnutzer*Innen kommt die von esatus entwickelte ID-Wallet App zum Einsatz.

Übersicht:

Komponente	**Technologie**	**Zweck**
Server Basis	Ubuntu Server, Docker	Hostsystem der Infrastruktur für alle untenstehenden Komponenten
Web-Frontend Company	Angular	Benutzeroberfläche für Angestellte im Arbeitgeber-Unternehmen für die Ausstellung von CompanyIDs an die Arbeitnehmer*Innen der Arbeitgeber-Unternehmen
Hyperledger Indy Netzwerk	Hyperledger Indy	Infrastruktur zum Speichern und öffentlichen Auslesen von Schemas, Credential Definitions und Revocation Registries
Tails-Server	bcgov / indy-tails-server	Infrastruktur zum Download der Tails-Files durch die Wallet-Apps beim Ausstell-Vorgang von VCs durch Arbeitgeber-Unternehmen und Bundesdruckerei
Aries Agent (ACA-PY)	Python	Client-Funktionen für die Blockchain, Kommunikation mit den Wallets der Nutzer*Innen, Ausstellen (Arbeitgeber-Unternehmen, Bundesdruckerei) und Prüfen von VCs

Mobiltelefon	esatus SSI Wallet	Speichern von kryptographischen Schlüsseln und VCs, Kommunikation mit den Agents und dem Hotel-Controller auf Seite der Nutzer*Innen Die App ist über eine PIN, gespeichert im gesicherten Speicher des Smartphones (sowohl iOS (Secure Enclave) als auch Android (Secure storage)), geschützt. Diese PIN entsperrt die App und gewährt anschließend den Zugriff auf weitere Elemente des sicheren Speichers. Bei der Generierung des Wallet wird der „master key“ mittels der Indy-SDK Methode „indy_generate_wallet_key“ erzeugt. Die „key derivation method“ des Wallet kann angepasst werden und ist per default „ARAGON2I_MOD“; Die für den Nutzer optionale biometrische Überprüfung erfolgt durch die von den Systemen bereitgestellten Funktionen, heißt die App selbst verwaltet keine biometrischen Daten.
eID Service	Bereits BSI-Konformität[3]	Prüfen der auf dem Personalausweis aktivierten eID durch die Bundesdruckerei
SSI Issuer	Bereits BSI-Konformität	Ausstellen eines MasterID VCs auf Basis der aus der eID stammenden, verifizierten Daten durch die Bundesdruckerei

Tabelle 4: IT-Systeme und Anwendungen

[3] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03130/tr-03130.html

4 SCHUTZBEDARFSFESTSTELLUNG

Zweck der Schutzbedarfsfeststellung ist es, zu ermitteln, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich hierfür eine Einteilung in die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“. Grundsätzlich ist bei den Assets, die durch eine Kern-Absicherung geschützt werden sollen, von einem Schutzbedarf der Kategorien „hoch“ und „sehr hoch“ auszugehen. Trotzdem muss der Schutzbedarf dieser wenigen, besonders geschäftskritischen Assets dediziert eingeschätzt werden.

4.1 Datenklassen

Die folgenden Datenklassen wurden definiert. Der Schutzbedarf wird anhand der Definitionen des BSI Standards 100-2 in Stufen normal, hoch und sehr hoch bewertet.

Datenklasse	**Enthaltene Daten**	**Schutzbedarf Integrität**	**Schutzbedarf Verfügbarkeit**	**Schutzbedarf Vertraulichkeit**
Credential Templates				
MasterID (Master ID)	• Private ID (Link Secret) • Credential ID (Revocation) • Policy ID • Public Key • Stadt • Familienname • Geburtsort • Geburtsname • Vorname • Geburtsdatum • Straße • Land, • Ablaufdatum • akademischer Titel • PLZ	hoch	normal	hoch
Arbeitgeber- Credential (Corporate ID)	• Vorname • Nachname • Firma Name • Firma Land • Firma Straße • Firma PLZ	normal	normal	normal

	• Firma Stadt			
Öffentliche Daten (auf der Blockchain bzw. dem Tails-Server)				
Corporate ID Schema	• Name • Version • eine Liste mit Attributsnamen	normal	normal	normal
Corporate ID Credential Definition	• Schema ID (das DID eines Credential Schemas) • Issuer DID (die DID eines Schema Credential Ausstellers)	hoch	normal	normal
Revocation Registry	• ID (Registry ID) • revocDefType (Registry Typ) • tag (einzigartige beschreibende ID der Registry), credDefId (Credential Definition ID), • issuanceType: (Default oder OnDemand) • maxCredNum (maximale Anzahl der Credentials, die die Registry bedienen kann) • tailsHash (Hash der Tails) • tailsLocation (Ort des Tail Files) • publicKeys (ursa formatierte Public Keys) • ver (Version des Revocation Registry Definition json) • revoc_reg_entry_json (Revocation Registry Eintrag der den initialen Status der Revocation Registry beinhaltet) • prevAccum (vorheriger Accumulator Wert) • accum (derzeitiger Accumulator Wert) • issued (ein Array von ausgestellten Indizes) 3. revoked (Array von revoked Indizes)	hoch	normal	normal
Tails-File	• Liste mit randomisierten Zahlen (aktuell: 1.000)	normal	normal	normal

SSI-Daten im Rahmen der Ausstellung der CompanyID				
Employee	• Id (einzigartige ID des Angestellten) • firstName • familyName • companyName • companySubject • companyAddressStreet • companyAddressZipCode • companyAddressCity	normal	normal	normal
Connection Invitation	• recipientKeys (öffentliche Schlüssel, die mit der Einladung verbunden sind, der private Schlüssel befindet sich beim Einladenden / Ersteller der Verbindungs-Einladung) • @type (Typ der didcomm Nachricht) • imageUrl (URL der Grafik die das einladende Unternehmen repräsentiert) • @id (einzigartige ID der Verbindungseinladung) • Label (label für das einladende Unternehmen) • serviceEndpoint (Host Name oder IP-Addresse des company-agents)	normal	normal	normal
Connection	• Accept (kontrolliert die automatische Annahme von Verbindungen, ist hier auf „auto“ gesetzt) • alias (ein Label für die Verbindung, im Projekt wir hier die „employee id“ genutzt) • connection_id (einzigartige ID der Verbindung) • created_at (Zeitstempel des Aufbaus der Verbindung) • initiator (definiert wer die Verbindung aufgebaut hat, hier immer „self“) • invitation_key (der Empfänger Key der Einladung die zum Verbindungsaufbau führte) • invitation_mode (kontrolliert wie oft die	normal	normal	normal

	Verbindungseinladung genutzt werden kann, hier immer auf „once“ (einmal) gesetzt) • my_did (die DID des DID Dokuments welches mit der lokalen Seite der Verbindung zusammen hängt) • state (Status der Verbindung wie sie im Aries DID Exchange Protocol definiert ist) • their_did (die DID des DID Dokuments welches mit der Remote Seite der Verbindung zusammen hängt) • their_label (ein Label dass die einladende Partei definiert, hier bspw. auf „esatus Wallet“ gesetzt) • updated_at (Zeitstempel des letzten Updates)			
Credential Exchange Record Issue Credential	• Der „credential exchange record“ ist ein temporärer Eintrag, der erstellt wird, wenn einem Angestellten ein Credential angeboten wird. Akzeptiert dieser das Credential, so wird der Eintrag gelöscht.	hoch	normal	hoch
Issued Credential	• cred_rev_id (die Credential Revocation ID) • rev_reg_id (die ID der Credential Revocation Registry) • employee_id (die ID des Angestellten dem das Credential zugeordnet ist)	normal	normal	normal

Tabelle 5: Datenklassen

4.2 Verarbeitete Daten je Komponente, Schutzbedarfsermittlung

In diesem Abschnitt wurden die Datenklassen den Komponenten zugeordnet, sowie deren Schutzbedarf hinsichtlich Integrität, Verfügbarkeit und Vertraulichkeit bewertet.

Komponente	**Verarbeitete Daten**	**Schutzbedarf Integrität**	**Schutzbedarf Verfügbarkeit**	**Schutzbedarf Vertraulichkeit**
Blockchain-Knoten (Indy Node)	*Speicherung:* DIDs der Nodes, Bundesdruckerei, Arbeitgeber, Corporate ID Schema, Corporate ID Credential Definitions, Revokation Registries	hoch	hoch	normal
Aries Agent (ACA-PY) Unternehmen	*Erstellung, Zwischenverarbeitung, Durchleitung:* Arbeitgeber-Credential, Corporate ID Schema, Corporate ID Credential Definition, Revocation Registry, Tails File, Connection Invitation, Connection, Credential Exchange Record, Corporate ID, Issued Credential	hoch	normal	hoch
Tails Server	*Speicherung:* Tails Files	gering	normal	normal
Company-Controller	*Zwischenverarbeitung, Durchleitung:* Arbeitgeber-Credential, Employee, Connection Invitation, Issued Credential	normal	normal	normal
Web-Frontend Company	*Verarbeitung:* Einwilligung zur Teilnahme am Piloten, Mitarbeiter Firmendetails, Ausstellung Arbeitgeber-	normal	normal	normal

	Credential, Proof Request, Proof Presentation			
MongoDB Company	*Speicherung:* Einwilligung zur Teilnahme am Piloten, Arbeitgeber-Credential	normal	normal	normal
ID-Wallet App (signierte Daten)	*Verarbeitung, Speicherung:* MasterID, Arbeitgeber-Credential, DID Document, Tails File, Connection Invitation, Connection, Credential Exchange Record, Corporate ID, Proof RequestPresentation Exchange Record	normal	normal	hoch

Tabelle 6: Schutzbedarf Daten je Komponente

Die Tabelle *Gesamtüberblick Schnittstellen* enthält eine Auflistung der wesentlichen Verbindungen. Nachstehend werden diese Verbindungen beschrieben.

Verbindung	Beschreibung
eID Ausstellung	Der Anwender initiiert die Ausstellung seiner MasterID via AusweisApp2. Die App baut eine Verbindung zum eID-Service der Bundesdruckerei auf, nach Verifizierung [tbd] baut dieser eine Verbindung zum SSI-Issuer auf zwecks Ausstellung der Master ID. Der SSI-Issuer baut eine Verbindung zur AusweisApp2 zwecks Übermittlung der signierten MasterID auf. Die Wallet erstellt ein Schlüsselpaar mit privater DID und speichert die MasterID ab. Die Kommunikation läuft über das Internet (Kommunikation Wallet mit Blockchain-Knoten, Tails-Server und Company-Agent) sowie das LAN der Bundesdruckerei, innerhalb der DMZ. Die Verbindung zwischen dem Mobiltelefon und der Bundesdruckerei ist bidirektional, die Verbindung wird nach Ausstellung der MasterID getrennt.
Ausstellung Arbeitgeber-Credential	Schnittstellen: S2, S3 und gegebenenfalls S6 Nach Erhalt einer E-Mail initiieren die Testnutzer*Innen (Mitarbeiter*Innen) die Ausstellung des Arbeitgeber Credentials mittels eines QR Code Scans. Nachfolgend baut das Mobiltelefon eine Verbindung zum Unternehmensnetzwerk auf und lädt das Credential herunter, dieses wird dann zusammen mit der dazugehörigen DID in der Wallet gespeichert.

	Besitzt ein Unternehmen keinen eigenen Hyperledger Indy Node, so wird seitens der Unternehmens Aries Agents noch eine Verbindung zu zwei Hyperledger Indy Node aufgebaut, um die DID auch dort zwecks späterer Verifizierung der Authentizität zu speichern. Die Kommunikation läuft hier über das Internet, sowie das LAN des Unternehmens. Die Verbindung Mobiltelefon – Unternehmensnetzwerk verlässt die DMZ nicht. Der Aries Agent baut intern noch eine Verbindung zum Company Controller auf, der sich im Intranet des Unternehmens befindet. Die Verbindung zwischen Mobiltelefon und Unternehmensnetzwerk ist bidirektional, endet jedoch nach Übertragung des Credentials. Die eventuell aufgebaute Verbindung zu einem Hyperledger Node ist ebenfalls bidirektional, wird aber nach Übertragung der DID ebenfalls beendet.
Hyperledger Nodes Synchronisierung	Jeder Blockchain-Knoten repliziert neue Ledger-Einträge mit den anderen Blockchain-Knoten. Die Verbindungen sind bidirektional. Die Node-Betreiber haben keinen vollständigen Einfluss auf die Daten, die in das Ledger geschrieben werden. Die Kommunikation findet hier über das Internet statt.

Tabelle 7: Kommunikationsverbindungen

5 MODELLIERUNG NACH IT-GRUNDSCHUTZ

Zur Ergänzung der Sicherheitskonzepte der Organisationen, die Teile der neuen Infrastruktur betreiben werden, werden diejenigen Anforderungen des Grundschutzes identifiziert, denen ggf. neue, spezifische Maßnahmen gegenübergestellt werden müssen.

5.1 Auswahl der relevanten IT-Grundschutz-Bausteine

Im Rahmen dieses Sicherheitskonzepts werden folgende Bausteine betrachtet:

Sicherheitsmanagement
ISMS.1 Sicherheitsmanagement

Betrieb
OPS.2.1 Outsourcing für Kunden
OPS.2.2 Cloud-Nutzung
OPS.3.1 Outsourcing für Dienstleister

Konzeption und Vorgehensweise
CON.2 Datenschutz
CON.3 Datensicherungskonzept
CON.10 Entwicklung von Webanwendungen

Anwendungen
APP.1.4 Mobile Anwendung (Apps)
APP.3.1 Webanwendungen
APP.3.2 Webserver
APP.4.3 Relationale Datenbanksysteme
APP.5.3 Allgemeiner E-Mail-Client und -Server
APP.6 Allgemeine Software
APP.7 Entwicklung von Individualsoftware

IT-Systeme
SYS.1.1 Allgemeiner Server
SYS.1.2.2 Windows Server 2012
SYS.1.3 Server unter Linux und Unix
SYS.1.5 Virtualisierung
SYS.1.6 Kubernetes (CD)
SYS.3.2.1 Allgemeine Smartphones und Tablets
SYS.3.2.2 Mobile Device Management (MDM)
SYS.3.2.3 iOS (for Enterprise)
SYS.3.2.4 Android
SYS.3.3 Mobiltelefon

Netze und Kommunikation
NET.3.1 Router und Switches
NET.3.2 Firewall
NET.3.3 VPN

Die folgenden Bausteine werden **nicht** betrachtet, da sie entweder keinen Bezug zum Projekt haben, beziehungsweise davon ausgegangen wird, dass die Anforderungen der Bausteine bereits ausreichend durch geeignete Maßnahmen erfüllt werden:

Organisation und Personal
ORP.1 Organisation
ORP.2 Personal
ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
ORP.4 Identitäts- und Berechtigungsmanagement
ORP.5 Compliance Management (Anforderungsmanagement)

Konzeption und Vorgehensweise
CON.1 Kryptokonzept
CON.3 Datensicherungskonzept
CON.4 Auswahl und Einsatz von Standardsoftware
CON.5 Entwicklung und Einsatz von Individualsoftware
CON.6 Löschen und Vernichten
CON.7 Informationssicherheit auf Auslandsreisen
CON.8 Software-Entwicklung
CON.9 Informationsaustausch

Betrieb
OPS.1.1.2 Ordnungsgemäße IT-Administration
OPS.1.1.3 Patch- und Änderungsmanagement
OPS.1.1.4 Schutz vor Schadprogrammen
OPS.1.1.5 Protokollierung
OPS.1.1.6 Software-Tests und -Freigaben
OPS.1.2.2 Archivierung
OPS.1.2.4 Telearbeit
OPS.1.2.5 Fernwartung
OPS.2.1 Outsourcing für Kunden
OPS.2.2 Cloud-Nutzung
OPS.3.1 Outsourcing für Dienstleister

Detektion und Reaktion
DER.1 Detektion von sicherheitsrelevanten Ereignissen
DER.2.1 Behandlung von Sicherheitsvorfällen
DER.2.2 Vorsorge für die IT-Forensik
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
DER.3.1 Audits und Revisionen
DER.3.2 Revision auf Basis des Leitfadens IS-Revision
DER.4 Notfallmanagement

Anwendungen
APP.1.1 Office-Produkte
APP.1.2 Web-Browser
APP.2.1 Allgemeiner Verzeichnisdienst
APP.2.2 Active Directory
APP.2.3 OpenLDAP
APP.3.3 Fileserver
APP.3.4 Samba
APP.3.6 DNS-Server

APP.4.2 SAP-ERP-System
APP.4.6 SAP ABAP-Programmierung
APP.5.1 Allgemeine Groupware
APP.5.2 Microsoft Exchange und Outlook

IT-Systeme
SYS.1.7 IBM Z-System
SYS.1.8 Speicherlösungen
SYS.2.1 Allgemeiner Client
SYS.2.2.2 Clients unter Windows 8.1
SYS.2.2.3 Clients unter Windows 10
SYS.2.3 Clients unter Linux und Unix
SYS.2.4 Clients unter macOS
SYS.3.1 Laptops
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
SYS.4.3 Eingebettete Systeme
SYS.4.4 Allgemeines IoT-Gerät
SYS.4.5 Wechseldatenträger

Industrielle IT
IND.1 Prozessleit- und Automatisierungstechnik
IND.2.1 Allgemeine ICS-Komponente
IND.2.2 Speicherprogrammierbare Steuerung (SPS)
IND.2.3 Sensoren und Aktoren
IND.2.4 Maschine
IND.2.7 Safety Instrumented Systems

Netze und Kommunikation
NET.1.1 Netzarchitektur und -design
NET.1.2 Netzmanagement
NET.2.1 WLAN-Betrieb
NET.2.2 WLAN-Nutzung
NET.4.1 TK-Anlagen
NET.4.2 VoIP
NET.4.3 Faxgeräte und Faxserver

Infrastruktur
INF.1 Allgemeines Gebäude
INF.2 Rechenzentrum sowie Serverraum
INF.5 Raum sowie Schrank für technische Infrastruktur
INF.6 Datenträgerarchiv
INF.7 Büroarbeitsplatz
INF.8 Häuslicher Arbeitsplatz
INF.9 Mobiler Arbeitsplatz
INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum
INF.11 Allgemeines Fahrzeug
INF.12 Verkabelung

6 ANFORDERUNGEN - EMPFEHLUNGEN

Die folgenden Anforderungen sollten von allen beteiligten Unternehmen besonders und gesondert nochmals auf ihren Erfüllungsgrad hin überprüft werden. Details zu den einzelnen Anforderungen sind im entsprechenden Excel „BSI-Grundschutz-Check_SSI_Wallet App“ dokumentiert.

6.1 Sicherheitsmanagement

ISMS.1 Sicherheitsmanagement

ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen (B)

Im Rahmen des Sicherheitsprozesses MÜSSEN für die gesamte Informationsverarbeitung ausführliche und angemessene Sicherheitsmaßnahmen festgelegt werden. Alle Sicherheitsmaßnahmen SOLLTEN systematisch in Sicherheitskonzepten dokumentiert werden. Die Sicherheitsmaßnahmen SOLLTEN regelmäßig aktualisiert werden.

(alle SSI Komponenten)

ISMS.1.A10 Erstellung eines Sicherheitskonzepts (S)

Für den festgelegten Geltungsbereich (Informationsverbund) SOLLTE ein angemessenes Sicherheitskonzept als das zentrale Dokument im Sicherheitsprozess erstellt werden. Es SOLLTE entschieden werden, ob das Sicherheitskonzept aus einem oder aus mehreren Teilkonzepten bestehen soll, die sukzessive erstellt werden, um zunächst in ausgewählten Bereichen das erforderliche Sicherheitsniveau herzustellen.

Im Sicherheitskonzept MÜSSEN aus den Sicherheitszielen der Institution, dem identifizierten Schutzbedarf und der Risikobewertung konkrete Sicherheitsmaßnahmen passend zum betrachteten Informationsverbund abgeleitet werden. Sicherheitsprozess und Sicherheitskonzept MÜSSEN die individuell geltenden Vorschriften und Regelungen berücksichtigen.

Die im Sicherheitskonzept vorgesehenen Maßnahmen MÜSSEN zeitnah in die Praxis umgesetzt werden.
Dies MUSS geplant und die Umsetzung MUSS kontrolliert werden.

(alle SSI Komponenten)

ISMS.1.A16 Erstellung von zielgruppengerechten Sicherheitsrichtlinien (H)

Neben den allgemeinen SOLLTE es auch zielgruppenorientierte Sicherheitsrichtlinien geben, die jeweils bedarfsgerecht die relevanten Sicherheitsthemen abbilden.

(alle SSI Komponenten)

6.2 Betrieb

OPS.2.1 Outsourcing für Kunden

OPS.2.1.A2 Rechtzeitige Beteiligung der Personalvertretung [Zentrale Verwaltung] (S)

Die Personalvertretung SOLLTE rechtzeitig über ein Outsourcing-Vorhaben informiert werden. Die Personalvertretung SOLLTE schon in der Angebotsphase beteiligt werden. Je nach Outsourcing- Vorhaben SOLLTEN die gesetzlichen Mitwirkungsrechte beachtet werden.

(Relevanz: MongoDB – Arbeitgeber)

OPS.2.1.A3 Auswahl eines geeigneten Outsourcing-Dienstleisters (S)

Für die Auswahl des Outsourcing-Dienstleisters SOLLTE ein Anforderungsprofil mit den Sicherheitsanforderungen an das Outsourcing-Vorhaben erstellt werden. Außerdem SOLLTEN Bewertungskriterien für den Outsourcing-Dienstleister und dessen Personal vorliegen. Diese SOLLTEN auf dem Anforderungsprofil basieren.

(Relevanz: jegliche Komponente, jedoch im Besonderen bei Komponenten, die Personendaten verarbeiten, im Hinblick auf Datenschutz und den Ort der Speicherung, MongoDB, Controller, Aries Agent)

OPS.2.1.A6 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben[Fachverantwortliche] (S)

Der Outsourcing-Kunde SOLLTE für jedes Outsourcing-Vorhaben ein Sicherheitskonzept basierend aufden zugehörigen Sicherheitsanforderungen erstellen. Ebenso SOLLTE jeder Outsourcing-Dienstleister ein individuelles Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben vorlegen. Beide Sicherheitskonzepte SOLLTEN miteinander abgestimmt werden. Das Sicherheitskonzept des Outsourcing-Dienstleisters und dessen Umsetzung SOLLTEN zu einem gesamten Sicherheitskonzept zusammengeführt werden. Der Outsourcing-Kunde oder unabhängige Dritte SOLLTEN regelmäßig überprüfen, ob das Sicherheitskonzept wirkt.

(Relevanz: betrifft jegliche Komponente, die abgegeben werden soll)

OPS.2.1.A11 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb (S)

Es SOLLTE ein Betriebskonzept für das Outsourcing-Vorhaben erstellt werden, das auch die Sicherheitsaspekte berücksichtigt. Die Sicherheitskonzepte der Outsourcing-Partner SOLLTEN regelmäßig daraufhin überprüft werden, ob sie aktuell und zueinander konsistent sind. Der Status dervereinbarten Sicherheitsmaßnahmen SOLLTE regelmäßig kontrolliert werden. Zwischen den Outsourcing-Partnern SOLLTE regelmäßig kommuniziert werden. Vorschläge zu Änderungen und Verbesserungen SOLLTEN regelmäßig besprochen und abgestimmt werden.

Die Outsourcing-Partner SOLLTEN regelmäßig gemeinsame Übungen und Tests durchführen, um das Sicherheitsniveau aufrechtzuerhalten. Informationen über Sicherheitsrisiken und wie damit umgegangen wird, SOLLTEN regelmäßig zwischen den Outsourcing-Partnern ausgetauscht werden. Es SOLLTE ein Prozess festgelegt werden, der den Informationsfluss bei Sicherheitsvorfällen sicherstellt, welche die jeweiligen Vertragspartner betreffen.

(Relevanz: betrifft den Betrieb jeder abgegebenen Komponente)

OPS.2.1.A16 Sicherheitsüberprüfung von Mitarbeitern (H)

Mit externen Outsourcing-Dienstleistern SOLLTE vertraglich vereinbart werden, dass die Vertrauenswürdigkeit des eingesetzten Personals geeignet überprüft wird. Dazu SOLLTEN gemeinsamKriterien festgelegt werden.

(Relevanz: bei Betrieb von Komponenten, die personenbezogene Daten verarbeiten, wie MongoDB, Controller, Aries Agent)

OPS.2.2 Cloud-Nutzung

OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung [Fachverantwortliche, Institutionsleitung, Datenschutzbeauftragter] (B)

Eine Strategie für die Cloud-Nutzung MUSS erstellt werden. Darin MÜSSEN Ziele, Chancen und Risiken definiert werden, die die Institution mit der Cloud-Nutzung verbindet. Zudem MÜSSEN die rechtlichen und organisatorischen Rahmenbedingungen sowie die technischen Anforderungen untersucht werden, die sich aus der Nutzung von Cloud-Diensten ergeben. Die Ergebnisse dieser Untersuchung MÜSSEN in einer Machbarkeitsstudie dokumentiert werden.

Es MUSS festgelegt werden, welche Dienste in welchem Bereitstellungsmodell zukünftig von einem Cloud-Diensteanbieter bezogen werden sollen. Zudem MUSS sichergestellt werden, dass bereits in der

Planungsphase zur Cloud-Nutzung alle grundlegenden technischen und organisatorischen Sicherheitsaspekte ausreichend berücksichtigt werden.

Für den geplanten Cloud-Dienst SOLLTE eine grobe individuelle Sicherheitsanalyse durchgeführt werden. Diese SOLLTE wiederholt werden, wenn sich technische und organisatorische Rahmenbedingungen wesentlich verändern. Für größere Cloud-Projekte SOLLTE zudem eine Roadmap erarbeitet werden, die festlegt, wann und wie ein Cloud-Dienst eingeführt wird.

(Relevanz: alle SSI Komponenten)

OPS.2.2.A2 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung[Fachverantwortliche] (B)

Auf Basis der Strategie für die Cloud-Nutzung MUSS eine Sicherheitsrichtlinie für die Cloud-Nutzung erstellt werden. Sie MUSS konkrete Sicherheitsvorgaben beinhalten, mit denen sich Cloud-Dienste innerhalb der Institution umsetzen lassen. Außerdem MÜSSEN darin spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter sowie das festgelegte Schutzniveau für Cloud-Dienste hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert werden. Wenn Cloud-Dienste internationaler Anbieter genutzt werden, MÜSSEN die speziellen länderspezifischen Anforderungen und gesetzlichen Bestimmungen berücksichtigt werden.

(Relevanz: alle SSI Komponenten)

OPS.2.2.A7 Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung (S)

Auf Grundlage der identifizierten Sicherheitsanforderungen (siehe OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*) SOLLTE durch den Cloud-Kunden ein Sicherheitskonzept für die Nutzung von Cloud-Diensten erstellt werden.

(Relevanz: alle SSI Komponenten, Erweiterung bestehender Sicherheitskonzepte)

OPS.2.2.A8 Sorgfältige Auswahl eines Cloud-Diensteanbieters [Institutionsleitung](S)

Basierend auf der Service-Definition für den Cloud-Dienst SOLLTE durch den Cloud-Kunden ein detailliertes Anforderungsprofil für einen Cloud-Diensteanbieter erstellt werden. Eine Leistungsbeschreibung und ein Lastenheft SOLLTEN erstellt werden. Für die Bewertung eines Cloud-Diensteanbieters SOLLTEN auch ergänzende Informationsquellen herangezogen werden. Ebenso SOLLTEN verfügbare Service-Beschreibungen des Cloud-Diensteanbieters sorgfältig geprüft und hinterfragt werden.

(Relevanz: bei Betrieb von Komponenten, die personenbezogene Daten verarbeiten, wie MongoDB, Controller, Aries Agent)

OPS.2.2.A12 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb (S)

Alle für die eingesetzten Cloud-Dienste erstellten Dokumentationen und Richtlinien SOLLTEN durch den Cloud-Kunden regelmäßig aktualisiert werden. Der Cloud-Kunde SOLLTE außerdem periodisch kontrollieren, ob der Cloud-Diensteanbieter die vertraglich zugesicherten Leistungen erbringt. Auch SOLLTEN sich der Cloud-Diensteanbieter und der Cloud-Kunde nach Möglichkeit regelmäßig abstimmen. Ebenso SOLLTE geplant und geübt werden, wie auf Systemausfälle zu reagieren ist.

(Relevanz: alle SSI Komponenten)

OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung (S)

Der Cloud-Kunde SOLLTE sich vom Cloud-Diensteanbieter regelmäßig nachweisen lassen, dass die vereinbarten Sicherheitsanforderungen erfüllt sind. Der Nachweis SOLLTE auf einem international anerkannten Regelwerk basieren (z. B. IT-Grundschutz, ISO/IEC 27001, Anforderungskatalog Cloud Computing (C5), Cloud Controls Matrix der Cloud Security Alliance). Der Cloud-Kunde SOLLTE prüfen, ob der Geltungsbereich und Schutzbedarf die genutzten Cloud-Dienste erfasst.

Nutzt ein Cloud-Diensteanbieter Subunternehmer, um die Cloud-Dienste zu erbringen, SOLLTE er dem Cloud-Kunden regelmäßig nachweisen, dass diese die notwendigen Audits durchführen.

(Relevanz: alles SSI Komponenten)

OPS.2.2.A17 Einsatz von Verschlüsselung bei Cloud-Nutzung (H)

Wenn Daten durch einen Cloud-Diensteanbieter verschlüsselt werden, SOLLTE vertraglich geregelt werden, welche Verschlüsselungsmechanismen und welche Schlüssellängen eingesetzt werden dürfen. Wenn eigene Verschlüsselungsmechanismen genutzt werden, SOLLTE ein geeignetes Schlüsselmanagement sichergestellt sein. Bei der Verschlüsselung SOLLTEN die eventuellen Besonderheiten des gewählten Cloud-Service-Modells berücksichtigt werden.

(Relevanz: alle SSI Komponenten, auch eine Prüfung hinsichtlich einer Störung der Komponenten)

OPS.2.2.A19 Sicherheitsüberprüfung von Mitarbeitern [Personalabteilung] (H)

Mit externen Cloud-Diensteanbietern SOLLTE vertraglich vereinbart werden, dass in geeigneter Weise überprüft wird, ob das eingesetzte Personal qualifiziert und vertrauenswürdig ist. Dazu SOLLTEN gemeinsam Kriterien festgelegt werden.

(Relevanz: Aries Agent, Controller, MongoDB)

OPS.3.1 Outsourcing für Dienstleister

OPS.3.1.A3 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben (S)

Der Outsourcing-Dienstleister SOLLTE für seine Dienstleistungen ein Sicherheitskonzept besitzen. Für individuelle Outsourcing-Vorhaben SOLLTE er außerdem spezifische Sicherheitskonzepte erstellen, dieauf den Sicherheitsanforderungen des Outsourcing-Kunden basieren. Zwischen Outsourcing-Dienstleister und Outsourcing-Kunden SOLLTEN gemeinsame Sicherheitsziele erarbeitet werden. Es SOLLTE außerdem eine gemeinsame Klassifikation für alle schutzbedürftigen Informationen erstellt werden. Es SOLLTE regelmäßig überprüft werden, ob das Sicherheitskonzept auch umgesetzt wird.

(Relevanz: alle SSI Komponenten)

OPS.3.1.A5 Regelungen für den Einsatz des Personals des Outsourcing Dienstleisters [Personalabteilung] (S)

Mitarbeiter des Outsourcing-Dienstleisters SOLLTEN geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit des Outsourcing-Kunden unterrichtet werden. Soweit es gefordert ist, SOLLTEN die Mitarbeiter des Outsourcing-Dienstleisters nach Vorgaben des Kunden überprüft werden, z. B. durch ein Führungszeugnis. Die Mitarbeiter des Outsourcing Dienstleisters SOLLTEN schriftlich dazu verpflichtet werden, einschlägige Gesetze, Vorschriften, Vertraulichkeitsvereinbarungen und interne Regelungen einzuhalten. Es SOLLTE Vertretungsregelungen in allen Bereichen geben.

(Relevanz: Aries Agent, Controller, MongoDB)

OPS.3.1.A7 Erstellung eines Mandantentrennungskonzeptes durch denOutsourcing-Dienstleister (S)

Durch ein geeignetes Mandantentrennungskonzept SOLLTE sichergestellt werden, dass Anwendungs-und Datenkontexte verschiedener Outsourcing-Kunden sauber getrennt sind. Das Mandantentrennungskonzept SOLLTE durch den Outsourcing-Dienstleister erstellt und dem Outsourcing-Kunden zur Verfügung gestellt werden. Das Mandantentrennungskonzept SOLLTE für den Schutzbedarf des Outsourcing-Kunden angemessene Sicherheit bieten. Die benötigten Mechanismen zur Mandantentrennung beim Outsourcing-Dienstleister SOLLTEN ausreichend umgesetzt sein.

(Relevanz: alle SSI Komponenten)

OPS.3.1.A10 Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb (S)

Die Sicherheitskonzepte der Outsourcing-Partner SOLLTEN regelmäßig daraufhin überprüft werden,ob sie noch aktuell und zueinander konsistent sind. Der Status der vereinbarten Sicherheitsmaßnahmen SOLLTE regelmäßig kontrolliert werden. Die Outsourcing-Partner SOLLTEN angemessen kooperieren. Hierüber hinaus SOLLTEN sie sich regelmäßig zu Änderungen und Verbesserungen abstimmen.

Die Outsourcing-Partner SOLLTEN regelmäßig gemeinsame Übungen und Tests durchführen. Informationen über Sicherheitsrisiken und wie damit umgegangen wird SOLLTEN regelmäßig zwischen den Outsourcing-Partnern ausgetauscht werden. Es SOLLTE ein Prozess festgelegt werden, der den Informationsfluss bei Sicherheitsvorfällen sicherstellt, welche die jeweiligen Vertragspartner betreffen.

(Relevanz: alle SSI Komponenten)

OPS.3.1.A11 Zutritts-, Zugangs- und Zugriffskontrolle [Zentrale Verwaltung] (S)

Zutritts-, Zugangs- und Zugriffsberechtigungen SOLLTEN geregelt sein, sowohl für das Personal des Outsourcing-Dienstleisters als auch für die Mitarbeiter der Outsourcing-Kunden. Es SOLLTE ebenfalls geregelt sein, welche Berechtigungen Auditoren und andere Prüfer erhalten. Es SOLLTEN immer nur so iele Rechte vergeben werden, wie für die Wahrnehmung einer Aufgabe nötig ist. Es SOLLTE ein geregeltes Verfahren für die Vergabe, die Verwaltung und den Entzug von Berechtigungen geben.

(Relevanz: alle SSI Komponenten)

OPS.3.1.A12 Änderungsmanagement [Institution] (S)

Es SOLLTE Richtlinien für Änderungen an IT-Komponenten, Software oder Konfigurationsdaten geben. Bei Änderungen SOLLTEN auch Sicherheitsaspekte berücksichtigt werden. Alle Änderungen SOLLTEN geplant, getestet, genehmigt und dokumentiert werden. Auf welche Weise und in welchem Umfang die Änderungen dokumentiert werden, SOLLTE mit dem Outsourcing-Kunden abgestimmt werden. Die Dokumentation SOLLTE dem Outsourcing-Kunden zur Verfügung gestellt werden. Es SOLLTEN Rückfall-Lösungen erarbeitet werden, bevor Änderungen durchgeführt werden. Bei größeren, sicherheitsrelevanten Änderungen SOLLTE das Informationssicherheitsmanagement der auslagernden Institution schon im Vorfeld beteiligt werden.

(Relevanz: alle SSI Komponenten)

OPS.3.1.A16 Sicherheitsüberprüfung von Mitarbeitern [Personalabteilung] (H)

Die Vertrauenswürdigkeit von neuen Mitarbeitern und externem Personal beim Outsourcing-Dienstleister SOLLTE durch geeignete Nachweise überprüft werden. Hierzu SOLLTEN gemeinsam mit dem Outsourcing-Kunden vertraglich Kriterien vereinbart werden.

(Relevanz: alle SSI Komponenten)

6.3 Konzeption und Vorgehensweise

CON.2 Datenschutz

CON.2.A1 Umsetzung Standard-Datenschutzmodell (B)

Die gesetzlichen Bestimmungen zum Datenschutz (DSGVO, BDSG und LDSG) MÜSSEN eingehalten werden. Wird die SDM-Methodik nicht berücksichtigt, die Maßnahmen also nicht auf der Basis der Gewährleistungsziele systematisiert und mit dem Referenzmaßnahmen-Katalog des SDM abgeglichen, SOLLTE dies begründet und dokumentiert werden.

(Relevanz: Aries Agent, Controller, MongoDB)

CON.3 Datensicherungskonzept

CON.3.A1 Erhebung der Einflussfaktoren für Datensicherungen[Fachverantwortliche, IT-Betrieb] (B)

Der IT-Betrieb MUSS für jedes IT-System und darauf ausgeführten Anwendungen die Rahmenbedingungen für die Datensicherung erheben. Dazu MUSS der IT-Betrieb die Fachverantwortlichen für die Anwendungen und die Zuständigen für die jeweiligen IT-Systeme befragen. Der IT-Betrieb MUSS mindestens die nachfolgenden Rahmenbedingungen berücksichtigen:

- Speichervolumen,
- Änderungsvolumen,
- Änderungszeitpunkte,
- Verfügbarkeitsanforderungen,
- Integritätsbedarf sowie
- rechtliche Anforderungen.

Die Ergebnisse MÜSSEN nachvollziehbar und auf geeignete Weise festgehalten werden. NeueAnforderungen MÜSSEN zeitnah berücksichtigt werden.

(Relevanz: alle SSI Komponenten)

CON.3.A6 Entwicklung eines Datensicherungskonzepts [Fachverantwortliche, IT-Betrieb] (S)

Der IT-Betrieb SOLLTE ein Datensicherungskonzept auf Basis des Minimaldatensicherungskonzepts erstellen. Dieses SOLLTE mindestens die nachfolgenden Punkte umfassen:

- Definitionen zu wesentlichen Aspekten der Datensicherung (z. B. zu differenzierende Datenarten),
- Gefährdungslage,
- Einflussfaktoren je IT-Systeme,
- Datensicherungsplan je IT-Systeme sowie
- relevante Ergebnisse des Notfallmanagements/BCM, insbesondere die Recovery Point Objective (RPO) je IT-System.

Der IT-Betrieb SOLLTE das Datensicherungskonzept mit den jeweiligen Fachverantwortlichen derbetreffenden Anwendungen abstimmen.

Die Mitarbeiter SOLLTEN über den Teil des Datensicherungskonzepts unterrichtet werden, der sie betrifft. Regelmäßig SOLLTE kontrolliert werden, ob das Datensicherungskonzept korrekt umgesetztwird.

CON.3.A13 Einsatz kryptografischer Verfahren bei der Datensicherung [IT-Betrieb](H)

Um die Vertraulichkeit und Integrität der gesicherten Daten zu gewährleisten, SOLLTE der IT-Betrieb alle Datensicherungen verschlüsseln. Es SOLLTE sichergestellt werden, dass sich die verschlüsselten Daten auch nach längerer Zeit wieder einspielen lassen. Verwendete kryptografische Schlüssel SOLLTEN mit einer getrennten Datensicherung geschützt werden.

(Relevanz: alle SSI Komponenten)

CON.10.A16 Mehr- Faktor- Authentisierung (S)

Die Entwickler SOLLTEN eine Mehr-Faktor-Authentisierung implementieren.

(Relevanz: alle SSI Komponenten)

6.4 Anwendungen

APP.1.4 Mobile Anwendung (Apps)

Der gesamte Baustein sollte seitens der Projektentwickler betrachtet werden.

APP.3.1 Webanwendungen

Der gesamte Baustein sollte seitens der Projektentwickler betrachtet werden.

APP.3.2 Webserver

Der gesamte Baustein sollte seitens der Projektentwickler betrachtet werden.

APP.4.3 Relationale Datenbanksysteme

Der gesamte Baustein sollte seitens der Projektentwickler analog betrachtet werden.

APP.5.2 Microsoft Exchange und Outlook

Dieser Baustein ist nur zu betrachten bei Einsatz der betreffenden Software.

(Relevanz: Versand der QR Codes, Möglichkeit der Löschung, Fälschung, etc.)

APP.5.2.A3 Berechtigungsmanagement und Zugriffsrechte (B)

Zusätzlich zum allgemeinen Berechtigungskonzept MUSS die Institution ein Berichtigungskonzept für die Systeme der Exchange-Infrastruktur erstellen, geeignet dokumentieren und anwenden.

Der IT-Betrieb MUSS serverseitige Benutzerprofile für einen rechnerunabhängigen Zugriff der Benutzer*Innen auf Exchange-Daten verwenden. Er MUSS die Standard-NTFS-Berechtigungen für das Exchange-Verzeichnis so anpassen, dass nur autorisierte Administratoren und Systemkonten auf die Daten in diesem Verzeichnis zugreifen können.

(Relevanz: siehe oben)

APP.5.2.A9 Sichere Konfiguration von Exchange-Servern (S)

Der IT-Betrieb SOLLTE Exchange-Server entsprechend den Vorgaben aus der Sicherheitsrichtlinie installieren und konfigurieren. Konnektoren SOLLTEN sicher konfiguriert werden. Der IT-Betrieb SOLLTE die Protokollierung des Exchange-Systems aktivieren. Für vorhandene benutzerspezifische Anpassungen SOLLTE ein entsprechendes Konzept erstellt werden.

Bei der Verwendung von funktionalen Erweiterungen SOLLTE sichergestellt sein, dass die definierten Anforderungen an die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit weiterhin erfüllt sind.

(Relevanz: siehe oben)

APP.5.2.A11 Absicherung der Kommunikation zwischen Exchange-Systemen (S)

Der IT-Betrieb SOLLTE nachvollziehbar entscheiden, mit welchen Schutzmechanismen die Kommunikation zwischen Exchange-Systemen abgesichert wird. Insbesondere SOLLTE der IT-Betrieb festlegen, wie die Kommunikation zu folgenden Schnittstellen abgesichert wird:

- Administrationsschnittstellen,
- Client-Server-Kommunikation,
- vorhandene Web-based-Distributed-Authoring-and-Versioning-(WebDAV)-Schnittstellen,
- Server-Server-Kommunikation und
- Public-Key-Infrastruktur, auf der die E-Mail-Verschlüsselung von Outlook basiert.

(Relevanz: siehe oben)

APP.5.3 Allgemeiner E-Mail-Client und -Server

APP.5.3.A2 Sicherer Betrieb von E-Mail-Servern (B)

Der IT-Betrieb MUSS Schutzmechanismen gegen Denial-of-Service (DoS)-Attacken ergreifen. Für den E-Mail-Empfang sowie den Zugriff von E-Mail-Clients über öffentliche Datennetze MÜSSEN E-Mail-Server eine sichere Transportverschlüsselung anbieten. Versenden E-Mails-Server von sich aus E-Mails, SOLLTEN sie dafür ebenfalls eine sichere Transportverschlüsselung nutzen.

Die Institution MUSS alle erlaubten E-Mail-Protokolle und Dienste festlegen. Außerdem MUSS der IT-Betrieb den E-Mail-Server so einstellen, dass er nicht als Spam-Relay missbraucht werden kann.

Werden Nachrichten auf einem E-Mail-Server gespeichert, MUSS der IT-Betrieb eine geeignete Größenbeschränkung für das serverseitige Postfach einrichten und dokumentieren.

APP.5.3.A6 Festlegung einer Sicherheitsrichtlinie für E-Mail (S)

Die Institution SOLLTE eine Sicherheitsrichtlinie für die Nutzung von E-Mails erstellen und regelmäßig aktualisieren. Die Institution SOLLTE alle Benutzer*Innen und Administrator*Innen über neue oder veränderte Sicherheitsvorgaben für E-Mail-Anwendungen informieren. Die E-Mail-Sicherheitsrichtlinie SOLLTE konform zu den geltenden übergeordneten Sicherheitsrichtlinien der Institution sein. Die Institution SOLLTE prüfen, ob die Sicherheitsrichtlinie korrekt angewendet wird.

Die E-Mail-Sicherheitsrichtlinie für Benutzer*Innen SOLLTE vorgeben,

- wie sich die Kommunikation absichern lässt,
- welche Benutzerzugriffsrechte es gibt,
- wie E-Mails auf gefälschte Absender überprüft werden,
- wie sich übermittelte Informationen absichern lassen,
- wie die Integrität von E-Mails überprüft werden soll,
- welche offenen E-Mail-Verteiler verwendet werden dürfen,
- ob E-Mails privat genutzt werden dürfen,

- wie mit E-Mails und Postfächern ausscheidender Mitarbeiter umgegangen werden soll,
- ob und wie Webmail-Dienste genutzt werden dürfen,
- wer für Gruppenpostfächer zuständig ist,
- wie mit Datei-Anhängen umgegangen werden soll und
- wie E-Mails im HTML-Format vom Benutzer*Innen behandelt werden sollen.

Die E-Mail-Sicherheitsrichtlinie SOLLTE ergänzend für Administratoren die Einstellungsoptionen der E-Mail-Anwendungen beinhalten, außerdem die Vorgaben für mögliche Zugriffe von anderen Servern auf einen E-Mail-Server. Auch Angaben zu berechtigten Zugriffspunkten, von denen aus auf einen E- Mail-Server zugegriffen werden darf, SOLLTEN in der Richtlinie enthalten sein.

Die E-Mail-Sicherheitsrichtlinie SOLLTE den Umgang mit Newsgroups und Mailinglisten regeln.

(Relevanz: Versand der QR Codes, Möglichkeit der Löschung, Fälschung, etc.)

APP.5.3.A9 Erweiterte Sicherheitsmaßnahmen auf dem E-Mail-Server (S)

Die E-Mail-Server einer Institution SOLLTEN eingehende E-Mails mittels des Sender Policy Frameworks (SPF) und mit Hilfe von Domain Keys überprüfen. Die Institution SOLLTE selbst Domain Keys und SPF einsetzen, um von ihr versendete E-Mails zu authentisieren.

Wird SPF verwendet, SOLLTE eindeutig vorgegeben werden, wie mit E-Mails verfahren werden soll. Der Softfail-Parameter („~“) SOLLTE nur zu Testzwecken verwendet werden.

Die Institution SOLLTE Domain-based Message Authentication, Reporting and Conformance (DMARC) nutzen, um festzulegen, wie von ihr versendete E-Mails durch den empfangenden E-Mail-Server überprüft werden sollen. DMARC-Reporte SOLLTEN regelmäßig ausgewertet werden. Die Institution SOLLTE festlegen, ob DMARC-Reporte über empfangene E-Mails an andere Institutionen versendet werden.

Die Institution SOLLTE die E-Mail-Kommunikation über DANE und MTA-STS absichern.

(Relevanz: Versand der QR Codes, Möglichkeit der Löschung, Fälschung, etc.)

APP.6 Allgemeine Software

Der gesamte Baustein sollte seitens jedes Projektteilnehmers betrachtet werden.

APP.7 Entwicklung von Individualsoftware

Der gesamte Baustein sollte seitens der Projektentwickler betrachtet werden.

6.5 IT-Systeme

SYS.1.1 Allgemeiner Server

SYS.1.1.A1 Geeignete Aufstellung (B)

Server MÜSSEN an Orten betrieben werden, zu denen nur berechtigte Personen Zutritt haben. Server MÜSSEN daher in Rechenzentren, Rechnerräumen oder abschließbaren Serverschränken aufgestellt beziehungsweise eingebaut werden (siehe hierzu die entsprechenden Bausteine der Schicht INF Infrastruktur). Server DÜRFEN NICHT als Arbeitsplatzrechner genutzt werden. Als Arbeitsplatz genutzte IT-Systeme DÜRFEN NICHT als Server genutzt werden.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A2 Benutzerauthentifizierung an Servern (B)

Für die Anmeldung von Benutzern und Diensten am Server MÜSSEN Authentisierungsverfahren eingesetzt werden, die dem Schutzbedarf der Server angemessen sind. Dies SOLLTE in besonderem Maße für administrative Zugänge berücksichtigt werden. Soweit möglich, SOLLTE dabei auf zentrale, netzbasierte Authentisierungsdienste zurückgegriffen werden.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A6 Deaktivierung nicht benötigter Dienste (B)

Alle nicht benötigten Dienste und Anwendungen MÜSSEN deaktiviert oder deinstalliert werden, vor allem Netzdienste. Auch alle nicht benötigten Funktionen in der Firmware MÜSSEN deaktiviert werden. Auf Servern SOLLTE der Speicherplatz für die einzelnen Benutzer, aber auch für Anwendungen, geeignet beschränkt werden. Die getroffenen Entscheidungen SOLLTEN so dokumentiert werden, dass nachvollzogen werden kann, welche Konfiguration und Softwareausstattung für die Server gewählt wurden.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A10 Protokollierung (B)

Generell MÜSSEN alle sicherheitsrelevanten Systemereignisse protokolliert werden, dazu gehören mindestens:

- Systemstarts und Reboots,
- erfolgreiche und erfolglose Anmeldungen am System (Betriebssystem und Anwendungssoftware),

- fehlgeschlagene Berechtigungsprüfungen,
- blockierte Datenströme (Verstöße gegen ACLs oder Firewallregeln),
- Einrichtung oder Änderungen von Benutzern, Gruppen und Berechtigungen,
- sicherheitsrelevante Fehlermeldungen (z. B. Hardwaredefekte, Überschreitung von Kapazitätsgrenzen) sowie
- Warnmeldungen von Sicherheitssystemen (z. B. Virenschutz).

(Relevanz: alle SSI Komponenten)

SYS.1.1.A11 Festlegung einer Sicherheitsrichtlinie für Server (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an Server in einer separaten Sicherheitsrichtlinie konkretisiert werden. Diese Richtlinie SOLLTE allen Administratoren und anderen Personen, die an der Beschaffung und dem Betrieb der Server beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A12 Planung des Server-Einsatzes (S)

Jedes Server-System SOLLTE geeignet geplant werden. Dabei SOLLTEN mindestens folgende Punkte berücksichtigt werden:

- Auswahl der Hardwareplattform, des Betriebssystems und der Anwendungssoftware,
- Dimensionierung der Hardware (Leistung, Speicher, Bandbreite etc.),
- Art und Anzahl der Kommunikationsschnittstellen,
- Leistungsaufnahme, Wärmelast, Platzbedarf und Bauform,
- Realisierung administrativer Zugänge (siehe SYS.1.1.A5 *Schutz der Administrationsschnittstellen*),
- Zugriffe von Benutzern,
- Realisierung der Protokollierung (siehe SYS.1.1.A10 *Protokollierung*),
- Realisierung der Systemaktualisierung (siehe SYS.1.1.A7 *Updates und Patches für Betriebssystem und Anwendungen*) sowie
- Einbindung ins System- und Netzmanagement, in die Datensicherung und die Schutzsysteme (Virenschutz, IDS etc.).

Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A16 Sichere Grundkonfiguration von Servern (S)

Die Grundeinstellungen von Servern SOLLTEN überprüft und falls erforderlich entsprechend den Vorgaben der Sicherheitsrichtlinie angepasst werden. Erst nachdem die Installation und die Konfiguration abgeschlossen sind, SOLLTE der Server mit dem Internet verbunden werden.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A19 Einrichtung lokaler Paketfilter (S)

Vorhandene lokale Paketfilter SOLLTEN über ein Regelwerk so ausgestaltet werden, dass die eingehende und ausgehende Kommunikation auf die erforderlichen Kommunikationspartner, Kommunikationsprotokolle bzw. Ports und Schnittstellen beschränkt wird. Die Identität von Remote-Systemen und die Integrität der Verbindungen mit diesen SOLLTE kryptografisch abgesichert sein.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A23 Systemüberwachung und Monitoring von Servern (S)

Das Server-System SOLLTE in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden. Hierbei SOLLTEN der Systemzustand und die Funktionsfähigkeit des Systems und der darauf betriebenen Dienste laufend überwacht werden. Fehlerzustände sowie die Überschreitung definierter Grenzwerte SOLLTEN hierüber an das Betriebspersonal meldet werden.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A24 Sicherheitsprüfungen für Server (S)

Server SOLLTEN regelmäßigen Sicherheitstests unterzogen werden, die überprüfen, ob alle Sicherheitsvorgaben eingehalten werden und ggf. vorhandene Schwachstellen identifizieren. Diese Sicherheitsprüfungen SOLLTEN insbesondere auf Servern mit externen Schnittstellen durchgeführt werden. Um mittelbare Angriffe über infizierte Systeme im eigenen Netz zu vermeiden, SOLLTEN jedoch auch interne Server in festgelegten Zyklen entsprechend überprüft werden. Es SOLLTE geprüft werden, ob die Sicherheitsprüfungen automatisiert, z. B. mittels geeigneter Skripte, realisiert werden können.

Je nach installierter Komponente sollten auch die Anforderungen bei erhöhtem Schutzbedarf betrachtet werden.

(Relevanz: alle SSI Komponenten)

SYS.1.1.A27 Hostbasierte Angriffserkennung (H)

Hostbasierte Angriffserkennungssysteme (Host-based Intrusion Detection Systems, IDS bzw. Intrusion Prevention Systems, IPS) SOLLTEN eingesetzt werden, um das Systemverhalten auf Anomalien und Missbrauch hin zu überwachen. Die eingesetzten IDS/IPS-Mechanismen SOLLTEN geeignet ausgewählt, konfiguriert und ausführlich getestet werden. Im Falle einer Angriffserkennung SOLLTE das Betriebspersonal in geeigneter Weise alarmiert

werden. Über Betriebssystem-Mechanismen oder geeignete Zusatzprodukte SOLLTEN Veränderungen an Systemdateien und Konfigurationseinstellungen überprüft, eingeschränkt und gemeldet werden.

(Relevanz: alle SSI Komponenten)

SYS.1.2.2 Windows Server 2016 (CD)

Dieser Baustein ist nur zu betrachten bei Einsatz von Hyper-V für den Betrieb von Docker Images, dann jedoch vollständig.

(Relevanz: alle SSI Komponenten)

SYS.1.3 Server unter Linux und Unix

Der gesamte Baustein sollte seitens der Projektentwickler betrachtet werden.

(Relevanz: alle SSI Komponenten)

SYS.1.5 Virtualisierung

Der gesamte Baustein sollte seitens der Projektentwickler und Testteilnehmer betrachtet werden.

(Relevanz: alle SSI Komponenten)

SYS.1.6 Kubernetes (CD)

Der gesamte Baustein sollte seitens der Projektentwickler, aber auch der Testteilnehmer bei Nutzung von Kubernetes betrachtet werden.

(Relevanz: alle SSI Komponenten)

SYS.3.2.1 Allgemeine Smartphones und Tablets

Der gesamte Baustein sollte (nochmals) betrachtet werden bei Einsatz von betrieblichen Smartphones oder Tablets für den Testbetrieb.

(Relevanz: ID-Wallet)

SYS.3.2.2 Mobile Device Management (MDM)

Bei Einsatz dienstlicher Geräte in Verbindung mit MDM sollten die Anforderungen bei erhöhtem Schutzbedarf geprüft werden.

(Relevanz: ID-Wallet)

SYS.3.2.3 iOS (for Enterprise)

Bei Einsatz dienstlicher Geräte mit iOS sollten insbesondere die Anforderungen bei erhöhtem Schutzbedarf geprüft werden.

(Relevanz: ID-Wallet)

SYS.3.2.4 Android

Bei Einsatz dienstlicher Geräte mit Android sollten insbesondere die Anforderungen bei erhöhtem Schutzbedarf geprüft werden.

(Relevanz: ID-Wallet)

SYS.3.3 Mobiltelefon

Auch hier sollten bei Einsatz von dienstlichen Geräten insbesondere die Anforderungen bei erhöhtem Schutzbedarf geprüft werden.

(Relevanz: ID-Wallet)

6.6 Netze und Kommunikation

NET.3.1 Router und Switches

NET.3.1.A5 Schutz vor Fragmentierungsangriffen (B)

Am Router und Layer-3-Switch MÜSSEN Schutzmechanismen aktiviert sein, um IPv4- sowie IPv6Fragmentierungsangriffe abzuwehren.

(Relevanz: alle SSI Komponenten)

NET.3.1.A7 Protokollierung bei Routern und Switches (B)

Ein Router oder Switch MUSS so konfiguriert werden, dass er unter anderem folgende Ereignisse protokolliert:

- Konfigurationsänderungen (möglichst automatisch)
- Reboot
- Systemfehler
- Statusänderungen pro Interface, System und Netzsegment sowie
- Login-Fehler

(Relevanz: alle SSI Komponenten)

NET.3.1.A9 Betriebsdokumentationen (B)

Die wichtigsten betrieblichen Aufgaben eines Routers oder Switches MÜSSEN geeignet dokumentiert werden. Es SOLLTEN alle Konfigurationsänderungen sowie sicherheitsrelevante Aufgaben dokumentiert werden. Die Dokumentation SOLLTE vor unbefugten Zugriffen geschützt werden.

(Relevanz: alle SSI Komponenten)

NET.3.1.A10 Erstellung einer Sicherheitsrichtlinie (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTE eine spezifische Sicherheitsrichtlinie erstellt werden. In der Sicherheitsrichtlinie SOLLTEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie Router und Switches sicher betrieben werden können. Die Richtlinie SOLLTE allen Administratoren bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den festgelegten Anforderungen abgewichen, SOLLTE das mit dem ISB abgestimmt und dokumentiert werden. Es SOLLTE regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse SOLLTEN geeignet dokumentiert werden.

(Relevanz: alle SSI Komponenten, bestehende Sicherheitskonzepte)

NET.3.1.A12 Erstellung einer Konfigurations-Checkliste für Router und Switches (S)

Es SOLLTE eine Konfigurations-Checkliste erstellt werden, anhand derer die wichtigsten sicherheitsrelevanten Einstellungen auf Routern und Switches geprüft werden können. Da die sichere Konfiguration stark vom Einsatzzweck abhängt, SOLLTEN die unterschiedlichen Anforderungen der Geräte in der Konfigurations-Checkliste berücksichtigt werden.

(Relevanz: alle SSI Komponenten)

NET.3.1.A13 Administration über ein gesondertes Managementnetz (S)

Router und Switches SOLLTEN ausschließlich über ein separates Managementnetz (Out-of-BandManagement) administriert werden. Eine eventuell vorhandene Administrationsschnittstelle über das eigentliche Datennetz (In-Band) SOLLTE deaktiviert werden. Die verfügbaren Sicherheitsmechanismen der eingesetzten Managementprotokolle zur Authentisierung, Integritätssicherung und Verschlüsselung SOLLTEN aktiviert werden. Alle unsicheren Managementprotokolle SOLLTEN deaktiviert werden.

(Relevanz: alle SSI Komponenten)

NET.3.1.A18 Einrichtung von Access Control Lists (S)

Der Zugriff auf Router und Switches SOLLTE mithilfe von Access Control Lists (ACLs) definiert werden. In der ACL SOLLTE anhand der Sicherheitsrichtlinie der Institution festgelegt werden, über welche ITSysteme oder Netze mit welcher Methode auf einen Router oder Switch zugegriffen werden darf. Für den Fall, dass keine spezifischen Regeln existieren, SOLLTE generell der restriktivere Whitelist-Ansatz bevorzugt werden.

(Relevanz: alle SSI Komponenten)

NET.3.1.A21 Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur (S)

Router und Switches SOLLTEN an ein zentrales Identitäts- und Berechtigungsmanagement angebunden werden (siehe ORP.4 *Identitäts- und Berechtigungsmanagement)*.

(Relevanz: alle SSI Komponenten)

NET.3.1.A23 Revision und Penetrationstests (S)

Router und Switches SOLLTEN regelmäßig auf bekannte Sicherheitsprobleme hin überprüft werden. Auch SOLLTEN regelmäßig Revisionen durchgeführt werden. Dabei SOLLTE unter anderem geprüft werden, ob der Ist-Zustand der festgelegten sicheren Grundkonfiguration entspricht. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden.

Abweichungen SOLLTE nachgegangen werden.

Sowie sämtliche Anforderungen bei Installation und Betrieb von Komponenten mit erhöhtem Schutzbedarf.

(Relevanz: alle SSI Komponenten)

NET.3.1.A24 Einsatz von Netzzugangskontrollen (H)

Eine Port-based Access Control SOLLTE nach IEEE 802.1x auf Basis von EAP-TLS implementiert werden. Es SOLLTE KEINE Implementierung nach den Standards IEEE 802.1x-2001 und IEEE 802.1x2004 erfolgen.

(Relevanz: alle SSI Komponenten)

NET.3.2 Firewall

NET.3.2.A1 Erstellung einer Sicherheitsrichtlinie (B)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie erstellt werden. In dieser MÜSSEN nachvollziehbar Anforderungen und Vorgaben

beschrieben sein, wie Firewalls sicher betrieben werden können. Die Richtlinie MUSS allen im Bereich Firewalls zuständigen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

(Relevanz: alle SSI Komponenten, Erweiterung bestehender Sicherheitsrichtlinien)

NET.3.2.A2 Festlegen der Firewall-Regeln (B)

Die gesamte Kommunikation zwischen den beteiligten Netzen MUSS über die Firewall geleitet werden. Es MUSS sichergestellt sein, dass von außen keine unerlaubten Verbindungen in das geschützte Netz aufgebaut werden können. Ebenso DÜRFEN KEINE unerlaubten Verbindungen aus dem geschützten Netz heraus aufgebaut werden.

Für die Firewall MÜSSEN eindeutige Regeln definiert werden, die festlegen, welche Kommunikationsverbindungen und Datenströme zugelassen werden. Alle anderen Verbindungen MÜSSEN durch die Firewall unterbunden werden (Whitelist-Ansatz). Die Kommunikationsbeziehungen mit angeschlossenen Dienst-Servern, die über die Firewall geführt werden, MÜSSEN in den Regeln berücksichtigt sein.

Es MÜSSEN Verantwortliche benannt werden, die Filterregeln entwerfen, umsetzen und testen. Zudem MUSS geklärt werden, wer Filterregeln verändern darf. Die getroffenen Entscheidungen sowie die relevanten Informationen und Entscheidungsgründe MÜSSEN dokumentiert werden.

(Relevanz: alle SSI Komponenten)

NET.3.2.A3 Einrichten geeigneter Filterregeln am Paketfilter (B)

Basierend auf den Firewall-Regeln aus NET.3.2.A2 *Festlegen der Firewall-Regeln* MÜSSEN geeignete Filterregeln für den Paketfilter definiert und eingerichtet werden.

Ein Paketfilter MUSS so eingestellt sein, dass er alle ungültigen TCP-Flag-Kombinationen verwirft. Grundsätzlich MUSS immer zustandsbehaftet gefiltert werden. Auch für die verbindungslosen Protokolle UDP und ICMP MÜSSEN zustandsbehaftete Filterregeln konfiguriert werden. Die Firewall MUSS die Protokolle ICMP und ICMPv6 restriktiv filtern.

(Relevanz: alle SSI Komponenten)

NET.3.2.A4 Sichere Konfiguration der Firewall (B)

Bevor eine Firewall eingesetzt wird, MUSS sie sicher konfiguriert werden. Alle Konfigurationsänderungen MÜSSEN nachvollziehbar dokumentiert sein. Die Integrität der Konfigurationsdateien MUSS geeignet geschützt werden. Bevor Zugangspasswörter abgespeichert werden, MÜSSEN sie mithilfe eines zeitgemäßen kryptografischen Verfahrens abgesichert werden (siehe CON.1 *Kryptokonzept*). Eine Firewall MUSS so konfiguriert sein, dass ausschließlich zwingend erforderliche Dienste verfügbar sind. Wenn funktionale Erweiterungen benutzt werden, MÜSSEN die Sicherheitsrichtlinien der Institution weiterhin erfüllt sein. Auch MUSS begründet und dokumentiert werden, warum solche Erweiterungen eingesetzt werden. Nicht benötigte (Auskunfts-)Dienste sowie nicht benötigte funktionale Erweiterungen MÜSSEN deaktiviert oder ganz deinstalliert werden.

Informationen über den internen Konfigurations- und Betriebszustand MÜSSEN nach außen bestmöglich verborgen werden.

(Relevanz: alle SSI Komponenten)

NET.3.2.A9 Protokollierung (B)

Die Firewall MUSS so konfiguriert werden, dass sie mindestens folgende sicherheitsrelevante Ereignisse protokolliert:

- abgewiesene Netzverbindungen (Quell- und Ziel-IP-Adressen, Quell- und Zielport oder ICMP/ICMPv6-Typ, Datum, Uhrzeit)
- fehlgeschlagene Zugriffe auf System-Ressourcen aufgrund fehlerhafter Authentisierungen, mangelnder Berechtigung oder nicht vorhandener Ressourcen
- Fehlermeldungen der Firewall-Dienste
- allgemeine Systemfehlermeldungen und
- Konfigurationsänderungen (möglichst automatisch). Werden Sicherheitsproxies eingesetzt, MÜSSEN Sicherheitsverletzungen und Verstöße gegen AccessControl-Listen (ACLs oder auch kurz Access-Listen) in geeigneter Weise protokolliert werden. Hierbei MÜSSEN mindestens die Art der Protokollverletzung bzw. des ACL-Verstoßes, Quell- und Ziel-IPAdresse, Quell- und Zielport, Dienst, Datum und Zeit sowie, falls erforderlich, die Verbindungsdauer protokolliert werden. Wenn sich ein Benutzer am Sicherheitsproxy authentisiert, MÜSSEN auch Authentisierungsdaten oder ausschließlich die Information über eine fehlgeschlagene Authentisierung protokolliert werden.

(Relevanz: alle SSI Komponenten)

NET.3.2.A14 Betriebsdokumentationen (B)

Die betrieblichen Aufgaben einer Firewall MÜSSEN nachvollziehbar dokumentiert werden. Es MÜSSEN alle Konfigurationsänderungen sowie sicherheitsrelevanten Aufgaben dokumentiert werden, insbesondere Änderungen an den Systemdiensten und dem Regelwerk der Firewall. Die Dokumentation MUSS vor unbefugten Zugriffen geschützt werden.

(Relevanz: alle SSI Komponenten)

NET.3.2.A16 Aufbau einer „P-A-P“-Struktur (S)

Eine „Paketfilter – Application-Level-Gateway – Paketfilter“ (P-A-P)-Struktur SOLLTE eingesetzt werden. Sie MUSS aus mehreren Komponenten mit jeweils dafür geeigneter Hard- und Softwarebestehen. Für die wichtigsten verwendeten Protokolle SOLLTEN Sicherheitsproxies auf Anwendungsschicht vorhanden sein. Für andere Dienste SOLLTEN zumindest generische Sicherheitsproxies für TCP und UDP genutzt werden. Die Sicherheitsproxies SOLLTEN zudem innerhalb einer abgesicherten Laufzeitumgebung des Betriebssystems ablaufen.

(Relevanz: alle SSI Komponenten)

NET.3.2.A23 Systemüberwachung und -Auswertung (S)

Firewalls SOLLTEN in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden. Es SOLLTE ständig überwacht werden, ob die Firewall selbst sowie die darauf betriebenen Dienste korrekt funktionieren. Bei Fehlern oder wenn Grenzwerte überschritten werden SOLLTE das Betriebspersonal alarmiert werden. Zudem SOLLTEN automatische Alarmmeldungen generiert werden, die bei festgelegten Ereignissen ausgelöst werden. Protokolldaten oder Statusmeldungen SOLLTEN NUR über sichere Kommunikationswege übertragen werden.

(Relevanz: alle SSI Komponenten)

NET.3.2.A24 Revision und Penetrationstests (S)

Die Firewall-Struktur SOLLTE regelmäßig auf bekannte Sicherheitsprobleme hin überprüft werden. Es SOLLTEN regelmäßige Penetrationstests und Revisionen durchgeführt werden.

Sowie sämtliche Anforderungen bei Installation und Betrieb von Komponenten mit erhöhtem Schutzbedarf.

(Relevanz: alle SSI Komponenten)

NET.3.3 VPN

NET.3.3.A1 Planung des VPN-Einsatzes (B)

Die Einführung eines VPN von Unternehmen MUSS sorgfältig geplant werden. Dabei MÜSSEN die Verantwortlichkeiten für den VPN-Betrieb festgelegt werden. Es MÜSSEN für das VPN zudem Benutzergruppen und deren Berechtigungen geplant werden. Ebenso MUSS definiert werden, wie erteilte, geänderte oder entzogene Zugriffsberechtigungen zu dokumentieren sind.

Damit wäre eine Austellung einer CompanyID nur im virtuellen privaten Netzwerk möglich, in welchem das mobile Telefon des AN eine VPN Verbindung ins Unternehmensnetz aufbaut.

(Relevanz: alle SSI Komponenten)

NET.3.3.A4 Sichere Konfiguration eines VPN (B)

Für alle VPN-Komponenten MUSS eine sichere Konfiguration festgelegt werden. Diese SOLLTE geeignet dokumentiert werden. Auch MUSS der zuständige Administrator regelmäßig kontrollieren, ob die Konfiguration noch sicher ist und sie eventuell für alle IT-Systeme anpassen.

(Relevanz: alle SSI Komponenten)

NET.3.3.A6 Durchführung einer VPN-Anforderungsanalyse (S)

Eine Anforderungsanalyse SOLLTE durchgeführt werden, um für das jeweilige VPN die Einsatzszenarien zu bestimmen und daraus Anforderungen an die benötigten Hard- und Software- Komponenten ableiten zu können. In der Anforderungsanalyse SOLLTEN folgende Punkte betrachtet werden:

- Geschäftsprozesse beziehungsweise Fachaufgaben,
- Zugriffswege,
- Identifikations- und Authentisierungsverfahren,
- Benutzer*Innen und deren Berechtigungnen
- Zuständigkeiten, sowie
- Meldewege.

(Relevanz: alle SSI Komponenten)

NET.3.3.A8 Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung (S)

Eine Sicherheitsrichtlinie zur VPN-Nutzung SOLLTE erstellt werden. Diese SOLLTE allen Mitarbeitern bekannt gegeben werden. Die in der Sicherheitsrichtlinie beschriebenen Sicherheitsmaßnahmen SOLLTEN im Rahmen von Schulungen erläutert werden. Wird einem Mitarbeiter ein VPN-Zugang eingerichtet, SOLLTE ihm ein Merkblatt mit den wichtigsten VPN-Sicherheitsmechanismen ausgehändigt werden. Alle VPN-Benutzer SOLLTEN verpflichtet werden, die Sicherheitsrichtlinien einzuhalten.

(Relevanz: alle SSI Komponenten)

NET.3.3.A12 Benutzer- und Zugriffsverwaltung bei Fernzugriff-VPNs (S)

Für Fernzugriff-VPNs SOLLTE eine zentrale und konsistente Benutzer- und Zugriffsverwaltung gewährleistet werden.

(Relevanz: alle SSI-Komponenten)

7 RISIKOANALYSE

Eine Risikoanalyse im Kontext der Informationssicherheit hat die Aufgabe, relevante Gefährdungen für den Informationsverbund zu identifizieren und die daraus möglicherweise resultierenden Risiken abzuschätzen. Das Ziel ist es, die Risiken durch angemessene Gegenmaßnahmen auf ein akzeptables Maß zu reduzieren, die Restrisiken transparent zu machen und dadurch das Gesamtrisiko systematisch zu steuern.

Folgende Komponenten bzw. Entscheidungen müssen realisiert werden, bevor eine Risikoanalyse gestartet werden kann:

- Definitiver Architektur Entscheid
- Betreiber Organisation
- Definition der Geschäftsprozesse

Eine abschließende Risikoanalyse, die die Maßnahmen des Betreibers erfasst, muss nach der Umsetzung und dem Aufsetzen der Komponenten bei den Betreibern erfolgen.