swissdec

Unternehmens-Authentifizierung

Detailspezifikation

Version

Aktuelle Version	Ausgabe 10.05.2019, Version 1.5

Aktuelles Datum:	17.05.2021
Speicher Datum:	01.04.2020
Druck Datum:	17.05.2021
Vorlage:	Richtlinien.docx
Kommentar:	Nachdruck mit Quellenangaben gestattet

Die Detailspezifikation für die Unternehmens-Authentifizierung wurde in Zusammenarbeit mit folgenden Beteiligten erarbeitet:

- Verein Swissdec
- Berner Fachhochschule (Technik und Informatik)
  - Stefan Agosti, Annett Laube, Gerhard Hassenstein, Pascal Mainini, Anton Böhm

Herausgeber

Swissdec
Fluhmattstrasse 1
6004 Luzern
www.swissdec.ch

Inhaltsverzeichnis

1 Einleitung

1.1 Einordnung

Die vom Verein Swissdec betriebene zentrale Informationsplattform für die Standardisierung des elektronischen Datenaustausches ermöglicht bereits heute die vollständig elektronische Übermittlung von Lohndaten im Rahmen des «Lohnstandard-CH (ELM)». Darauf aufbauend und als Erweiterung des Prozesses von der Anmeldung eines Anspruchs bis hin zur Leistungserbringung wird aktuell der «Leistungsstandard-CH (KLE)» entwickelt. Swissdec-zertifizierte Lohnbuchhaltungen und ERP-Systeme vereinfachen damit die Abläufe der Unternehmen, ermöglichen korrekte Deklarationen und verringern den administrativen Aufwand.
Durch die elektronische Abwicklung der Geschäftsprozesse von der Ereignismeldung (Bsp. Unfallmeldung an den Versicherer) bis hin zur Taggeldabrechnung stellen sich zusätzliche Anforderungen an die Identifizierung und die Authentifizierung der teilnehmenden Unternehmen.
In der ersten Phase zur Ausarbeitung der Swissdec Unternehmens-Authentifizierung wurden die Ziele und Anforderungen für ein entsprechendes System erhoben. Auf dieser Basis wurde ein Lösungskonzept ausgearbeitet, welches den Rahmen für die technische Umsetzung einer Authentifizierung der teilnehmenden Unternehmen auf Basis der UID-BFS darstellt. Das Lösungskonzept bildet die Grundlage für die hier vorliegende Detailspezifikation, welche Vorgaben für eine Pilot-Umsetzung des Systems beinhaltet.

1.2 Ziel des Dokuments

Die Detailspezifikation beschreibt in vertiefter Weise die Umsetzung und Ausgestaltung der bereits im Lösungskonzept festgelegten SUA Prozesse zur Registrierung, Erstkonfiguration, Laufzeit, Erneuerung und Sperrung. Die Sicherheits-Anforderungen der Swissdec-Prozesse werden auf der Grundlage der Anforderungen an SUA aus dem Lösungskonzept weiter vertieft und die Umsetzung mittels Swissdec UID-Zertifikaten beschrieben. Ausserdem wird die Ausgestaltung der im Zuge der Prozesse genutzten Credentials (Passwörter, UID-Zertifikate) festgelegt.
Die Detailspezifikation bildet damit die Grundlage für die Umsetzung des Systems im Rahmen einer Pilotierung. Hierbei sollen die Vorgabe und Konzepte aus der Spezifikation umgesetzt und auf ihre Praxistauglichkeit hin überprüft werden. Die Erkenntnisse dieser ersten praktischen Umsetzung sollen nachfolgend wieder in überarbeitete Versionen der Detailspezifikation zurückfliessen.

1.3 Abgrenzung

Die Inhalte der Detailspezifikation konzentrieren sich auf eine erste Umsetzung der Swissdec Unternehmens-Authentifizierung im Rahmen einer Pilotierung. Hierbei wurden die noch im Lösungskonzept vorgesehenen Varianten auf ein Minimum beschränkt. Ausserdem werden die einzelnen Bestandteile der Spezifikation auf ihre technische Umsetzbarkeit hin beschrieben. Dabei basieren die jeweiligen Vorgaben auf den Erkenntnissen aus ähnlichen Kontexten und orientieren sich stark an etablierten Best-Practice-Ansätzen. Gleichwohl kann erst eine praktische Umsetzung allfällige Lücken oder Problemstellungen in der Spezifikation aufzeigen, welche dann in einer nachfolgenden Version beseitigt werden müssen.
Gleich wie im Lösungskonzept beschränkt sich auch die Detailspezifikation der Swissdec Unternehmens-Authentifizierung explizit auf die eindeutige und sichere Authentifizierung von Unternehmen im Rahmen der Kommunikation mit dem Swissdec Distributor bzw. den V&B als Endempfänger. Die hier vorliegende Spezifikation umfasst die Authentifizierungen im Rahmen der automatisierten Maschine zu Maschine (m2m) Kommunikation zwischen ERP-System (Transmitter) und Distributor, sowie im Backend zwischen Distributor und Endempfängersystemen. Andere Anwendungsfälle, welche ebenfalls eine Authentifizierung verlangen (z.B. Zugriff eines Benutzers auf ein Versicherungsportal oder ein Portal von Swissdec) werden in einem separaten Dokument behandelt.
Die fachlichen Geschäftsprozesse z.B. im Rahmen des Lohnstandards-CH (ELM) oder des Leistungsstandards-CH (KLE) werden in dieser Spezifikation nur am Rande betrachtet. Allfällig notwendige Anpassungen bereits bestehender oder noch auszuarbeitender Richtlinien in Hinblick auf die Kompatibilität mit SUA obliegen den jeweils zuständigen Arbeitsgruppen der Swissdec.

1.4 Ziele und Anforderungen

Das Dokument „Swissdec Unternehmens-Authentifizierung – Anforderungserhebung und Lösungskonzept“ (Version 1.1) umfasst die im Rahmen der ersten Phase des Projekts ausgearbeiteten Zielsetzungen und Anforderungen. Diese

wurden für die Detailspezifikation als Basis verwendet und in Kapitel 2 weiter detailliert. Das Kapitel 8 gibt darüber Auskunft inwiefern die einzelnen Anforderungen in der Spezifikation berücksichtigt werden konnten.

1.5 Überblick Swissdec Architektur

Die Swissdec Architektur wird hier kurz vorgestellt, um den Kontext von SUA besser verständlich zu machen.
Die zentrale Datenaustauschplattform, der SwissDec Distributor, dient zur Optimierung und Automatisierung von Prozessen zwischen etwa 200'000 Unternehmen und deren Versicherern & Behörden in der Schweiz. Zurzeit (2018) werden jährlich über 12 Mio. Personendaten mit deren Löhnen zwischen den Teilnehmern verteilt.

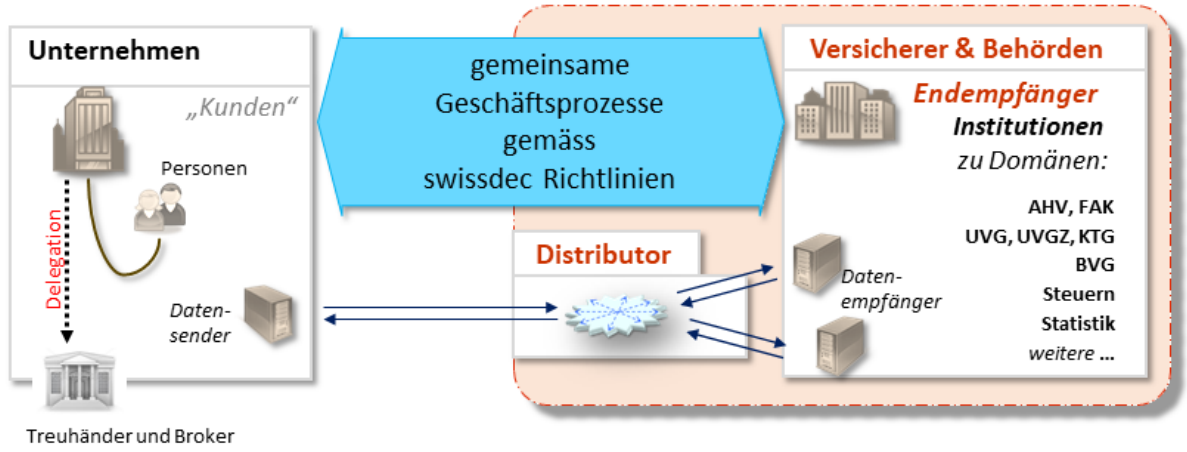

Abbildung 1: Überblick Swissdec Prozesse

Die Prozessteilnehmer sind

- Unternehmen mit ihren ERP-Systemen und deren ERP-Hersteller mittels ‘Transmitter’
- Versicherer & Behörden mit ihren spezialisierten Backend-Systemen mittels ‘Endempfänger’

Die durch den Prozess verbundenen Systeme kommunizieren dabei über m2m-Schnittstellen mittels standardisierter Protokolle.

Die problematische n:m Relation zwischen den Unternehmen und Versicherer & Behörden wird mittels eines zentralen Distributors in eine einfache „n:Distributor:m“ Relation aufgelöst (siehe Abbildung 2). Der Distributor kommuniziert stellvertretend für Versicherer & Behörden mit den Unternehmen und leitet die Daten geprüft und gefiltert an die Endempfänger weiter.
Der Swissdec Distributor agiert gegenüber den Unternehmen als Vertreter der Endempfänger (Versicherer & Behörden).[1] In dieser Funktion geniesst der Distributor das volle Vertrauen der Endempfänger und übernimmt die Abwicklung und die Sicherstellung der Kommunikationsvorgänge in ihrem Namen, gegenüber den ERP-Systemen der Unternehmen. Auf inhaltlicher Ebene trägt der Distributor nur als Vermittler von Nachrichten seinen Teil bei. Für die fachliche Korrektheit der Nachrichten und Geschäftsprozesse sind nur die Systeme der Endempfänger und der Unternehmen zuständig.
Der Einsatz des Swissdec Distributor hat folgende Vorteile:

- Einfachere Entwicklung, Testen und Produktion für Unternehmen, da die ERP-Systeme nur mit dem Distributor kommunizieren,
- Verminderung von Daten- und Prozessredundanz,
- Design-Firewall, d.h. unterschiedliche Versionierungen können auf dem Distributor mittels Transformation überbrückt werden. Der Lifecycle von Versionen erfolgt sanft und smart.
- Dynamische Qualitätssicherung (QS, Plausibilisierung) und Datenfilterung auf dem Distributor
- Keine Datenspeicherung auf dem Distributor, d.h. die Kommunikation zwischen Unternehmen und Versicherern & Behörden verläuft in „Echtzeit“ (7x24).

[1] Die Vertreterrolle des Swissdec Distributors sowie Rollen und Pflichten der Prozessteilnehmer sind in den ABG des Distributors geregelt, siehe https://www.swissdec.ch/de/allgemeine-geschaeftsbedingungen/.

- SW-Hersteller für Transmitter und Endempfänger werden von Swissdec geprüft und zertifiziert, um die hohe Qualität bezüglich der Interoperabilität und Daten und ein ‘plug and play’ der Prozessteilnehmer zu gewährleistet.

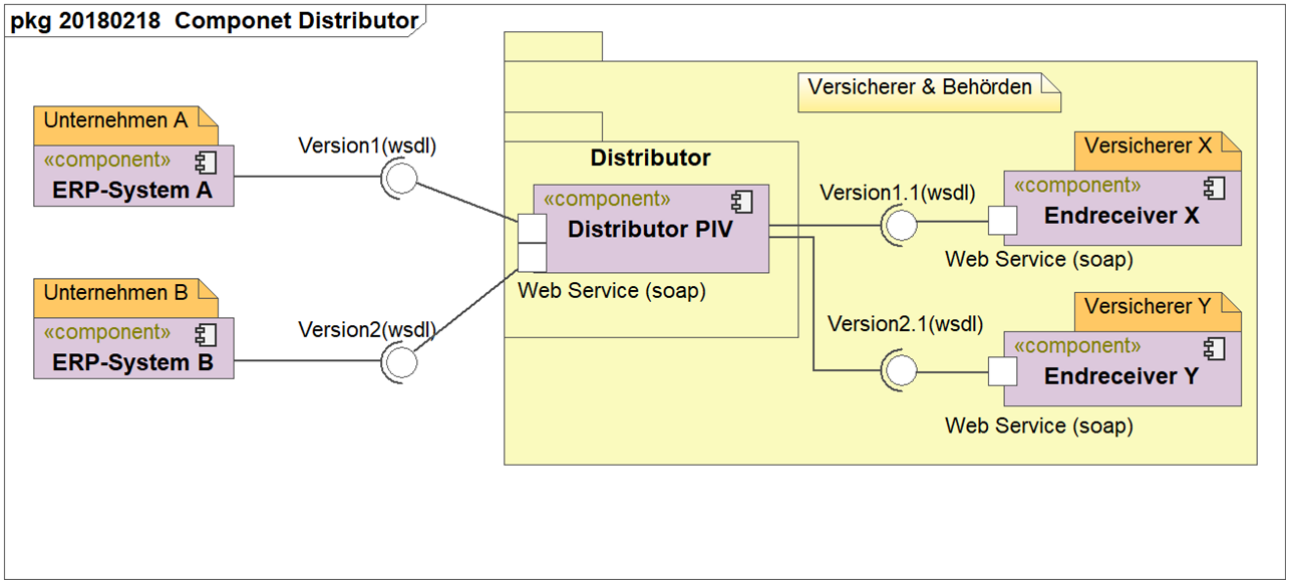

Abbildung 2: Swissdec Kommunikationsbeziehungen

Die technische Architektur basiert auf kaskadierten Web Services, die einen synchronen Aufruf vom Transmitter (ERP-System) über den Distributor zum Endempfänger (Versicherer & Behörden) aufbauen. Damit wird über den Distributor eine „Echtzeit“-Verbindung geführt, die eine zeitkritische Interaktion von Systemen im m2m-Prozess gestatten. Die Web Services sind – zusätzlich zum sicheren Kanal auf Transportebene (SSL/TLS) - durch die standardisierten Sicherheitskonzepte von WSS (Web Services Security; SOAP Message Security: signature+encryption) abgesichert.

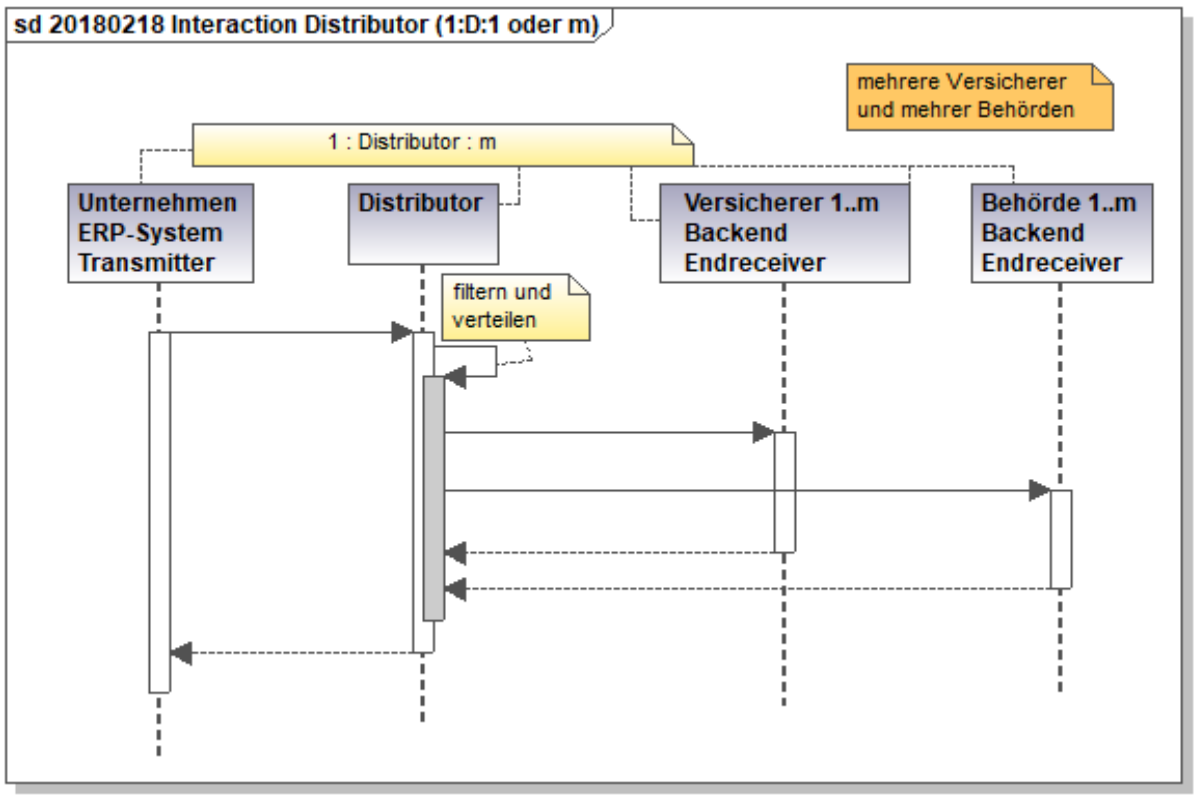

Abbildung 3: Kommunikation 1:Distributor:m

Laufzeitkritische Prozesse werden asynchron abgewickelt, d.h. der Transmitter bekommt nach dem Aufruf sofort wieder die Kontrolle und versucht später mittels Polling seine Antwort abzuholen.

2 Sicherheits-Anforderungen der Swissdec Prozesse

In diesem Abschnitt werden die Sicherheits-Anforderungen an die Swissdec Kommunikation aufgeführt. Es werden die Anforderungen (siehe auch Tabelle 14 Kapitel 8) aus dem Lösungskonzept präzisiert und durch neue Anforderungen, u.a. aus dem parallel entwickelten «Leistungsstandard-CH (KLE)», ergänzt.

2.1 Sicherer Kanal

Die Swissdec Architektur sieht vor, dass alle Kommunikationsverbindungen zwischen ERP-System eines Unternehmens, Swissdec-Distributor und Endempfängersystemen (Versicherungen & Behörden) durch einen sicheren Kanal auf Transportebene (SSL/TLS) geschützt sind. Aus sicherheitstechnischer Sicht macht es durchaus Sinn, wenn für die Verbindung auf Transportebene eine gegenseitige, zertifikatsbasierte Authentifizierung (2-way SSL) vorausgesetzt wird.

- Erweitert Anforderung A-16 (Autorisierung des ERP-Systems).

2.2 Authentifizierung auf Nachrichtenebene

Swissdec benötigt für die Erweiterung seiner Services zusätzlich eine eindeutige Authentifizierung aller beteiligten Stakeholder auf Nachrichtenebene (durch Signieren der übermittelten Daten).

- Erweitert Anforderung A-17 (Authentisierung des Unternehmens) und A-19 (Authentifizierung des Unternehmens)

2.3 Vertraulichkeit auf Nachrichtenebene

Um die übermittelnden Informationen trotz sicherem Kanal zusätzlich gegen weitere Angriffsvektoren schützen zu können, müssen die übertragenen Dateninhalte für den jeweiligen Empfänger verschlüsselt werden.

- Neu erfasste Anforderung A-27 (Vertraulichkeit auf Nachrichtenebene)

2.4 Betriebsumgebung

Die Daten, welche signiert werden müssen, können je nach Prozess recht umfangreich sein, bzw. müssen in zeitlich kurzer Abfolge signiert werden. Dies stellt grosse Anforderungen an die Performance bezüglich Signaturverfahren auf Seiten ERP-System, wie auch auf Seiten Swissdec Distributor dar. Diese Anforderung konnte in der Vergangenheit mit Softzertifikaten zufriedenstellend umgesetzt werden, da die Applikationen jederzeit einen schnellen und einfachen Zugriff auf den Signaturschlüssel haben.

- Erweitert Anforderung A-17 (Authentisierung des Unternehmens)

2.5 Nichtabstreitbarkeit

Über den gesamten Kommunikationsvorgang hinweg, soll der Versand und der Empfang von Daten von allen beteiligten Entitäten nicht in Abrede gestellt werden können. Die Nichtabstreitbarkeit ist eine Voraussetzung für die Verbindlichkeit.
Ziel ist es zu gewährleisten, dass der Versand und der Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es muss dabei unterschieden werden zwischen:

- *Nichtabstreitbarkeit der Herkunft*: Es soll einem Absender einer Nachricht nicht möglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten.
- *Nichtabstreitbarkeit des Erhalts*: Es soll einem Empfänger einer Nachricht nicht möglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten.
- *Beweis einer Kommunikationsverbindung:* Es soll bei zeitkritischen Prozessen einem Sender möglich sein, den Versand einer bestimmten Nachricht nachträglich zu beweisen.

Es muss demnach möglich sein, auch zu einem späteren Zeitpunkt, einen Kommunikationsvorgang wiederherstellen und lückenlos nachvollziehen zu können. Keiner der an einem Datenaustausch beteiligter Sender soll abstreiten können, eine bestimmte Nachricht versandt zu haben. Auf der anderen Seite soll ein Empfänger nicht abstreiten können, eine Nachricht empfangen zu haben.

- Erweitert Anforderung A-20 (Nachvollziehbarkeit)

2.6 Verbindlichkeit

Auf Basis der übermittelten Daten werden Versicherungsleistungen erbracht. Aus diesem Grund ist es wichtig, dass Kommunikationsvorgänge unter dem Gesichtspunkt der Nichtabstreitbarkeit gesichert werden. Dies wird erreicht, in dem alle zu einem Kommunikationsvorgang relevanten Daten und Informationen (inkl. Signatur & Zeitstempel) protokolliert und archiviert werden müssen.

- Erweitert Anforderung A-20 (Nachvollziehbarkeit)

2.7 Registrierung

Die Identifizierung und Registrierung der Unternehmen zwecks Ausstellung von UID-Zertifikaten muss durch Swissdec erfolgen. Dabei kann die Identitätsprüfung eines Unternehmens auf bereits bestehenden Beziehungen mit den antragstellenden Unternehmen basieren. Nur so können Registrierungsprozesse teilautomatisiert, unbürokratisch und dennoch sicher abgewickelt werden.

- Erweitert Anforderung A-09 (Registrierungsstelle), A-10 (Eindeutige Identifikation des Unternehmens), A-11 (Identifikation durch autorisierte Stelle)

3 Swissdec Zertifikate

Zur Umsetzung dieser Anforderungen benötigt Swissdec im Rahmen der Unternehmensauthentifizierung Zertifikate auf unterschiedlichen Ebenen bzw. Anwendungsbereiche.
In Abbildung 4 wird dargestellt, welches System welche Art von Zertifikat benötigt und installiert hat. In den folgenden Kapiteln wird beschrieben wofür jeweils diese Zertifikate eingesetzt werden.

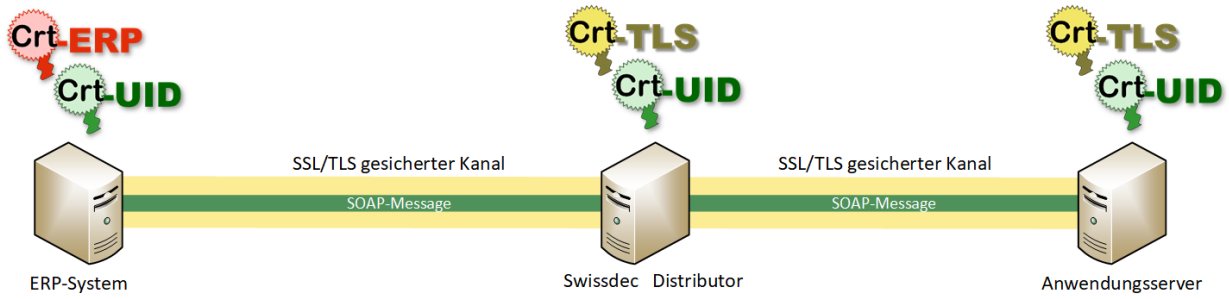

Abbildung 4: Übersicht der Swissdec Zertifikate

3.1 Swissdec UID-Zertifikate

Daten auf SOAP-Ebene werden signiert und verschlüsselt. Dazu werden vom Transmitter, wie auch vom Distributor und den Endempfängersystemen Swissdec UID-Zertifikate verwendet. Inhaltlich haben diese Zertifikate genaue Vorgaben, welche in Kapitel 5.1.5 beschrieben werden.
Da UID-Zertifikate sowohl zum Signieren, wie auch zur Verschlüsselung von SOAP-Nachrichten verwendet werden, würde es sich grundsätzlich empfehlen zwei unterschiedliche Zertifikate pro Anwendung zu verwenden.
Da diese Daten aber nur kurzzeitig für den Transportweg verschlüsselt werden und nicht verschlüsselt abgelegt und zu einem späteren Zeitpunkt dechiffriert werden müssen, entfällt ein Anspruch zur Archivierung von privaten Schlüsseln. Aus diesem Grund, und um das Zertifikatshandling nicht unnötig zu komplizieren, soll bei UID-Zertifikaten auf eine Einschränkung der Anwendung verzichtet werden und ein Zertifikat zum Authentisieren, Signieren und Verschlüsseln eingesetzt werden.
Der Austausch von Daten zwischen den jeweiligen Kommunikationsabschnitten muss jeweils vom Empfänger quittiert werden. Diese Transaktionsquittierung wird ebenfalls mit dem UID-Zertifikat signiert.

3.2 SSL/TLS Server Zertifikate

Auf Transportebene kommen beim Distributor und bei den Endempfängern SSL/TLS Server Zertifikate zum Einsatz. Je nach Kommunikationsabschnitt bzw. -richtung kann eine Instanz Server oder Client sein. Es soll an dieser Stelle nicht vorgeschrieben werden, ob dazu zwei unterschiedliche oder nur ein Zertifikat vom Betreiber verwendet werden soll. Als TLS Web-Client Zertifikate sollen für diese Systeme aber die Swissdec UID-Zertifikate zur Authentisierung auf Transportebene eingesetzt werden.
Der Transmitter des ERP-Systems eines Unternehmens hingegen kann nur die Rolle eines Clients einnehmen. Hierfür sollen ausschliesslich die Swissdec UID-Zertifikate als TLS Web-Client eingesetzt werden.
Die TLS Web-Server Zertifikate können von öffentlichen CAs oder von einer firmeninternen CA ausgestellt werden. Wenn Zertifikate einer öffentlichen CA zum Einsatz kommen, so sollte die Anbieterin Mitglied des CAB-Forum[2] und durch Webtrust[3] zertifiziert sein.
Falls die Richtlinien eines Endempfängers erfordern, dass ein Kommunikationspartner zur Authentifizierung nur Zertifikate einer internen PKI haben kann, so kann für diesen Fall ein TLS Web-Client Zertifikat einer firmeninternen CA für den Distributor ausgestellt werden.

3.3 Swissdec ERP-Zertifikate

Die versionsabhängige Prozessfähigkeit eines ERP-Systems wird mit einem anderen Zertifikat ausgewiesen. Diese Zertifikate werden auch auf SOAP-Ebene verwendet, um hiermit Nachrichten zu signieren. Diese Zertifikate sollen

[2] https://cabforum.org

[3] https://webtrust.org

auch künftig von einer Swissdec internen Certification Authority ausgegeben werden. Swissdec unterscheidet dazu zwei interne CA's:

- CA1 welche Zertifikate für den produktiven Einsatz ausstellt.
- CA2 welche Zertifikate für die Entwicklungsumgebung ausstellt.

3.4 Weitere Zertifikate

3.4.1 Registrierung mit Drittzertifikaten

Für die Registrierung können Unternehmen geregelte Zertifikate verwenden, welche für juristische Personen nach Art.7 ZertES von einer akkreditierten CA ausgestellt wurden (siehe Prozess «Registrierung mit geregeltem Zertifikat nach ZertES» in Kap. 6.1.2)

3.4.2 User Zertifikate

In einer späteren Phase wird Swissdec auch Bedarf an Zertifikaten für eine Benutzer-authentifizierung haben. Hier stehen einfache, fortgeschrittene Zertifikate oder geregelte Zertifikate für natürliche Personen zur Auswahl. Welche Art von Zertifikat zum Einsatz kommen wird, ist zum jetzigen Zeitpunkt noch nicht geklärt. Dieser Punkt wird in einem separaten Dokument behandelt.

4 Sicherheit und Vertrauen

Die Sicherheit der Kommunikation und das Vertrauen in die elektronischen Abläufe zwischen Unternehmen (Transmitter), Distributor und Endempfängersystem beruhen auf drei Grundpfeilern.

1. Authentisierter und abgesicherter Transportkanal,
2. Sicherheit und Vertrauen auf Nachrichtenebene (SOAP-Message),
3. Verbindlichkeit der Nachrichtenübermittlung durch Transaktionsquittierung.

4.1 Authentisierter und abgesicherter Transportkanal

Das UID-Zertifikat kommt auf zwei Ebenen zur Anwendung. Wie in Abbildung 5 ersichtlich ist, verwendet das ERP-System dieses Zertifikat, um sich gegenüber dem vorgelagerten Reverse Proxy in einer 2-way SSL/TLS Verbindung zu authentisieren.

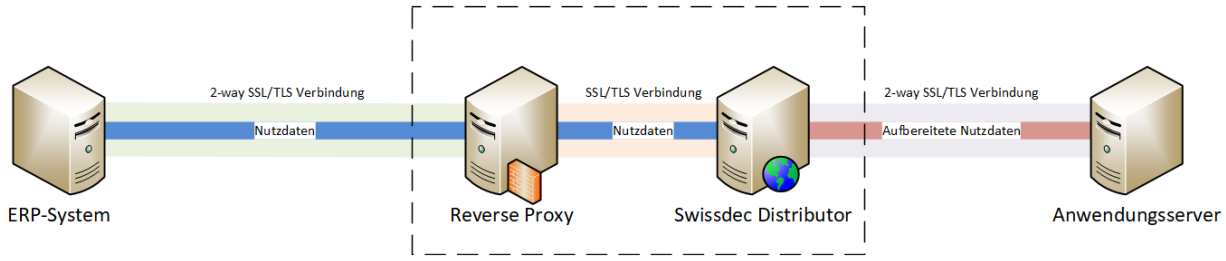

Abbildung 5: SUA Kommunikationsabschnitte

Das dem Swissdec Distributor vorgelagerte Reverse Proxy System, welches aus einer Kaskade von mehreren Komponenten (u.a. SSL/TLS Reverse Proxy und Web Application Firewall) besteht, ist dadurch in der Lage die Authentizität von eintreffenden Paketen bereits auf Transportebene zu prüfen.
Der Transmitter signiert mit seinem UID-Zertifikat den SOAP-Header der Nutzdaten und verschlüsselt diese mit dem UID-Zertifikat des Distributors. Der Reverse Proxy leitet die Nutzdaten unverändert in einer zweiten SSL/TLS Verbindung an den Swissdec Distributor weiter.

Nur wer über ein gültiges UID-Zertifikat verfügt, kann erfolgreich Pakete an den Swissdec Distributor senden. Dies wird vorgelagert vom TLS-Endpunkt geprüft.
Der Distributor wird dadurch entlastet.

Der Reverse Proxy kann die Authentizität einer Nachricht prüfen, kann aber deren Inhalt nicht lesen, da diese für den Distributor verschlüsselt wurden.

Der Distributor prüft die SUA-Signatur der Nutzdaten und kann damit Herkunft und Integrität der Daten verifizieren. In umgekehrter Richtung sendet der Distributor Nutzdaten an das ERP-System ebenfalls signiert und verschlüsselt mit dem UID-Zertifikat.
Der weitere Verlauf der Nachrichten zwischen Distributor und Endempfängersystemen wird ebenfalls auf Transportebene durch SSL/TLS abgesichert. Die vom Distributor aufbereiteten Nutzdaten werden analog zum ersten Kommunikationsabschnitt von ihm signiert und verschlüsselt übertragen.

4.2 Sicherheit und Vertrauen auf Nachrichtenebene (SOAP-Nachricht)

Wie im vorherigen Abschnitt bereits aufgezeigt, wird der SOAP-Header als Teil der Nutzdaten mit dem UID-Zertifikat signiert. Hierbei werden sowohl die Anfragen vom ERP-System an den Distributor (Request) sowie auch die jeweiligen Antworten des Distributors an das ERP-System (Response) signiert. Der Aufbau dieser Nachrichten in Bezug auf Signatur und Verschlüsselung wird in der Folge genauer beschrieben und ist in Abbildung 6 dargestellt.
Betrachtet man eine Nachricht vom ERP-System zum Distributor, so wird in jeder Nachricht im Header ein Zeitstempel (<wsu:Timestamp>) eingefügt. Dieser wird mittels ERP-Zertifikat und auch UID-Zertifikat signiert. Die Signatur mittels ERP-Zertifikat ermöglicht die Verifikation der Prozessfähigkeit des sendenden ERP-Systems. Die ERP-Zertifikat Signatur muss beibehalten werden, da die vom Distributor erhobenen statistischen Auswertungen auf den Informationen aus dem ERP-Zertifikat beruhen.

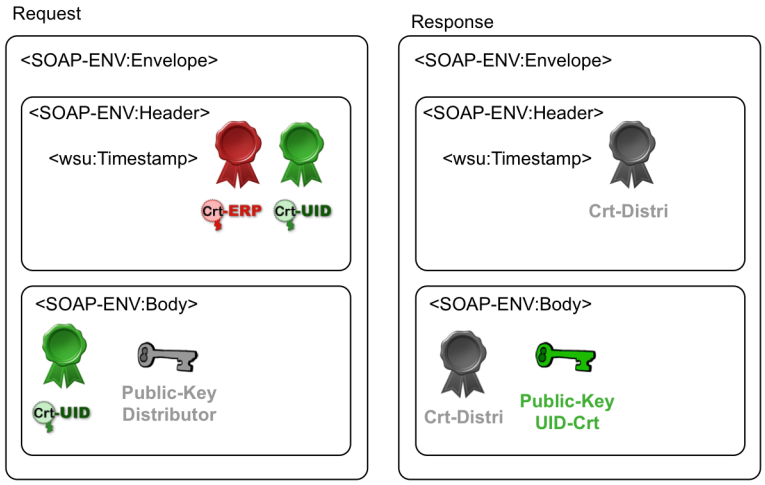

Abbildung 6: Authentisierung mit UID-Zertifikaten

Die Signatur des Zeitstempels mit dem UID-Zertifikat ermöglicht es, bereits im Header einer Nachricht die Herkunft einer Nachricht zu verifizieren. Der Distributor ist damit in der Lage festzustellen, ob es sich dabei um einen legitimierten Absender handelt. Dies ist vor allem daher relevant, da im Gegensatz zum Body, also dem eigentlichen Inhalt der Nachricht, die Informationen im Header nicht verschlüsselt werden. Der Distributor ist also in der Lage, die Signaturen des Zeitstempels zu überprüfen, ohne vorgängig die Nachricht entschlüsseln zu müssen.
Der Body einer Nachricht wird vom Absender ebenfalls mittels UID-Zertifikat signiert, um die Integrität sowie die Authentizität des Inhalts der Nachricht sicherzustellen. Darauffolgend wird der gesamte Body mittels Public-Key des Distributors verschlüsselt um dadurch die Vertraulichkeit gewährleisten zu können.
Die Antwort des Distributors an das ERP-System enthält ebenfalls einen Zeitstempel im Header, welcher mit dem UID-Zertifikat des Distributors signiert wird. Der Body der Nachricht wird mit dem UID-Zertifikat des Distributors signiert, um auch hier die Integrität und Authentizität zu gewährleisten. Verschlüsselt wird der Body daraufhin mit dem Public-Key des UID-Zertifikats des jeweiligen ERP-Systems, welches die Nachricht erhält.
Für jede ausgetauschte Nachricht gilt, dass im Header die verwendeten Zertifikate ohne die Zertifikatskette mitgesendet werden. Dies hat den Vorteil, dass die Zertifikate nicht von den Kommunikationsteilnehmern abgespeichert werden müssen. Aus Sicherheitsgründen muss aber die Zertifikatskette vorab ausgetauscht und zur Verifizierung des Zertifikats gespeichert werden. Eine effiziente Vorprüfung der Nachricht ist mittels der darin bereits enthaltenen Informationen möglich, wodurch Attacken auf den Distributor bereits sehr früh erkannt und abgefangen werden können. Gegenüber dem heutigen Stand (nur ERP-Zertifikat) werden in einer Nachricht dadurch zusätzliche Informationen über den Absender (Inhalt des UID-Zertifikats, siehe Kapitel 5.1) enthalten sein. Diese Informationen sind im unverschlüsselten Teil der Nachricht, sind aber durch den zuvor aufgebauten sicheren Kanal genügend gegen Angriffe geschützt. Die neu hinzukommende Offenlegung der Absenderinformation im Zertifikat stellt damit keine Verschlechterung des Sicherheitsniveaus dar und kann durch die Zugewinne hinsichtlich der Vorprüfung von Nachrichten gerechtfertigt werden.

4.3 Nichtabstreitbarkeit

Über die gesamten Swissdec Nachrichten-Transportwege ist eine Verbindlichkeit im Sinne der Nachvollziehbarkeit des Datenaustausches notwendig (Siehe Anforderung 2.6). Damit soll die Überprüfung einer Übertragung zu einem späteren Zeitpunkt jederzeit ermöglicht werden. Wie in Kapitel 4.1 bereits beschrieben erfolgt die Kommunikation zwischen Unternehmen und Endempfänger über den Distributor. Dieser agiert demzufolge in der Maschinen-zu-Maschinen-Kommunikation als Vermittler. Alle Kommunikationspakete werden über ihn geleitet.
Die in diesem Kapitel zusammengefassten Mechanismen beschreiben auf allgemeiner Ebene das Verhalten der beteiligten Entitäten (Transmitter, Distributor und Endempfänger) um die Verbindlichkeit von übermittelten Daten und Informationen zu einem Swissdec Geschäftsfall einwandfrei gewährleisten zu können.

4.3.1 Voraussetzungen

Es gelten folgende grundlegende Annahmen bzw. Voraussetzungen:

- Im Falle eines Kommunikationsausfalls des Distributors (z.B. bei einem technischen Problem), wird von den Kommunikationspartnern nach einem Timeout ein Sendeversuch abgebrochen, geloggt und zu einem späteren Zeitpunkt wiederholt. Der Betreiber des Distributors informiert die Kommunikationspartner über allfällige Störungen bzw. Ausfälle.

- Ein Ereignis wird immer vom ERP-System eines Unternehmens (Transmitter) angestossen.
- Der Distributor erstellt nach Anstoss eines neuen Ereignisses durch das Unternehmen eine interne ID (Identifikator), mit welchem das Ereignis und der darauffolgende Nachrichtenaustausch zwischen Unternehmen und beteiligten Endempfängern eindeutig identifiziert wird. Der Distributor gibt diese ID an alle teilnehmenden Systeme weiter bzw. in einer Quittierung zurück. Diese ID kann als Fallnummer für eine Supportanfrage bzw. zur Nachvollziehbarkeit einer Transaktion bzw. eines gesamten Geschäftsfalls verwendet werden.
- Alle, an einem Kommunikationsvorgang beteiligten Systeme verfügen über ein Swissdec Unternehmenszertifikat (UID-Zertifikat) und vertrauen dem Herausgeber des Zertifikats (Vertrauensanker).
- Ein Geschäftsfall kann über mehrere Nachrichten vollzogen werden, welche sich über eine unbestimmte Zeitspanne erstrecken können.
- Das ERP-System eines Unternehmens muss den aktuellen Stand eines Geschäftsfalls periodisch abfragen, um damit den Status mit dem Versicherer abzugleichen.
- Bestätigungsnachrichten (Quittierungen) von einem Empfängersystem müssen nach einer maximal zulässigen Zeit beim Sender eintreffen.

4.3.2 Swissdec Nachrichtenschemas

Bevor ein System für die verlässliche Aufbewahrung von Nachrichten zur Nachvollziehbarkeit eines Geschäftsfalls aufgebaut werden kann, muss ein einheitliches Kommunikationsschema unabhängig der abzubildenden Prozesse definiert werden. Das von Swissdec im Lohnstandard (ELM) und im Leistungsstandard (KLE) angedachte bzw. bereits verwendete Kommunikationsschema kann in zwei Phasen aufgeteilt werden.

1. Initialisierung eines Ereignisses.
2. Fachlicher Austausch.

Beide Phasen verfügen dabei über typische Kommunikationsmuster. Die Kommunikationsmuster können folgendermassen zusammengefasst und bezeichnet werden:

Phase 1 - 1:D:n: Das typische Muster bei der Initialisierung eines Ereignisses. Das Unternehmen meldet ein neues Ereignis für ein oder mehrere Endempfängersysteme an (1). Der Distributor empfängt die Meldung und quittiert den Erhalt direkt dem Unternehmen. Der Distributor bereitet die Ereignisdaten auf (2) und verteilt diese je nach Anzahl der Zielsysteme (3). Jedes Zielsystem quittiert ebenfalls den Erhalt direkt beim Distributor. In der Zwischenzeit kann das ERP-System den Status der Verteilung an die Endempfänger beim Distributor abfragen (4). Diese Abfrage kann mehrmals erfolgen [loop 1,n], bis alle Quittierungen eingegangen sind und der Distributor in seiner Statusinformation dem Unternehmen die erfolgreiche Verteilung zurückmelden kann.

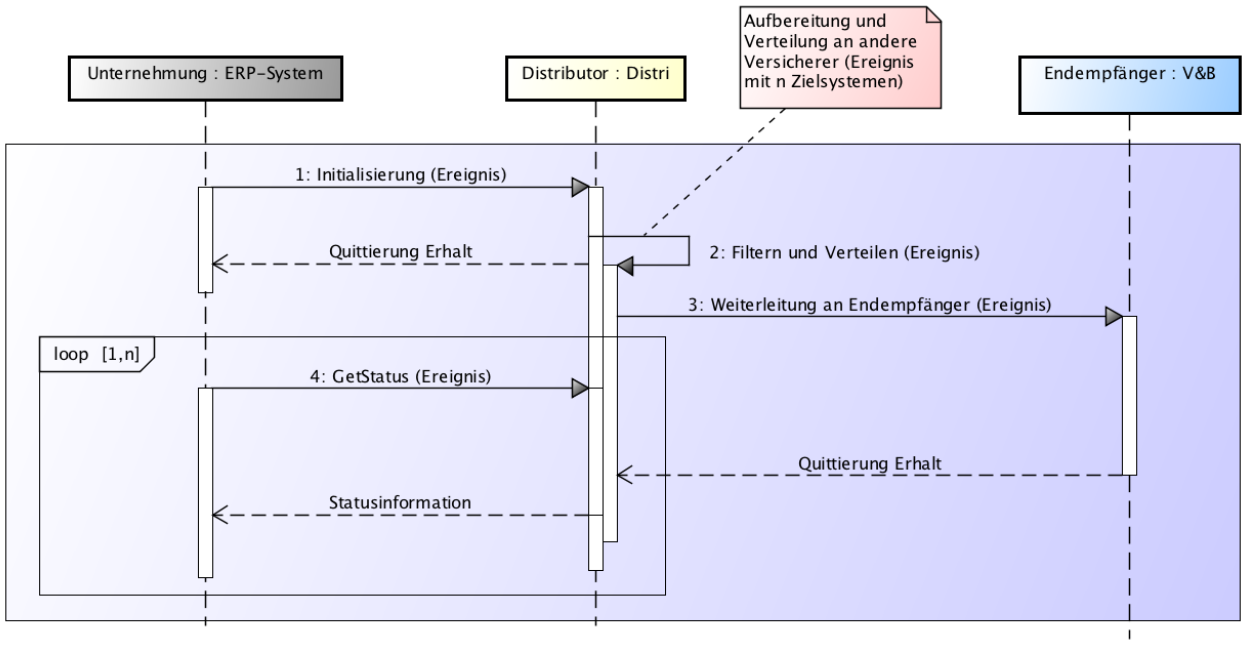

Abbildung 7: Kommunikationsablauf Initialisierung (1:D:n)

Phase 2 - 1:D:1: Je nach gegebenem Standard (Lohnstandard oder Leistungsstandard) und je nach Geschäftsfall kann das ERP-System des Unternehmens bei den einzelnen Endempfängern indirekt über den Distributor nach Status bzw. Resultat einer fachspezifischen Nachricht nachfragen (5). Der Distributor leitet die Anfrage weiter an das adressierte Endempfängersystem (6). Je nach Stand des Prozesses gibt das Empfängersystem eine entsprechende Antwort zurück. Diese Nachricht kann optional eine Bestätigungsaufforderung an das ERP-System des Unternehmens für diese Antwort beinhalten. Wenn eine Bestätigung vom Empfängersystem verlangt ist, antwortet das ERP-System mit einer entsprechenden Bestätigung (7), welche vom Distributor ebenfalls weitergeleitet wird (8). Das Empfängersystem quittiert zum Schluss den Erhalt der Bestätigung. Dieser Nachrichtenfluss kann sich je nach Antwort und Prozessverlauf mehrmals wiederholen [loop 0,n].

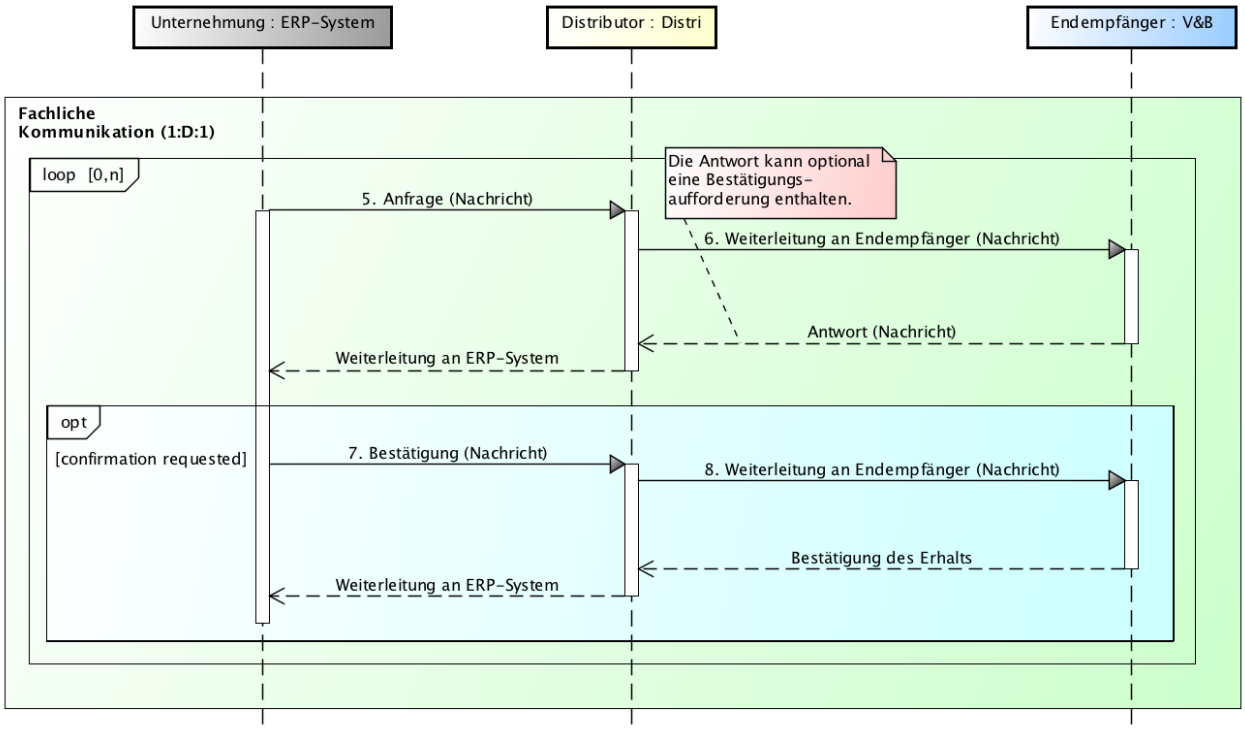

Abbildung 8: Kommunikationsablauf fachlicher Nachrichtenfluss (1:D:1)

Die Anforderungen bezüglich Nichtabstreitbarkeit auf fachlicher Ebene in einem Swissdec Kommunikationsablauf können in der folgenden Tabelle zusammengefasst werden. Es ist dabei zu beachten, dass ein Kommunikationsverkehr immer nur von Unternehmensseite aus angestossen werden kann.

	Unternehmen ***(Client)***	**Versicherer & Behörden** ***(Server)***
Nichtabstreitbarkeit der Datenherkunft (Senden)	*Signierte Nachricht*	*Signierte Nachricht*
Nichtabstreitbarkeit des Erhalts	*Fachliche Bestätigung*	*Signierte Bestätigung*

4.3.3 Nichtabstreitbarkeit der Datenherkunft

Zur Gewährleistung der Nichtabstreitbarkeit der Datenherkunft sind folgende Richtlinien zu beachten:

- Jede Nachricht wird von einem Sendersystem (Transmitter, Distributor, Endempfänger) auf SOAP–Ebene mit dem UID-Zertifikat signiert. Damit kann die Herkunft und Integrität einer Nachricht einem Sender einwandfrei zugeordnet werden.

- Jedes Empfängersystem verifiziert die im SOAP-Header enthaltene UID-Signatur und prüft diese anhand der Zertifikatskette bis zum Root-Zertifikat.
- Im Fall einer fehlerhaften Überprüfung der UID-Signatur, muss die erhaltene Nachricht verworfen und eine Fehlermeldung ausgegeben und dem Sender quittiert werden.

4.3.4 Nichtabstreitbarkeit des Empfangs
Zur Gewährleistung der Nichtabstreitbarkeit des Empfangs sind folgende Richtlinien zu beachten:

- Für *Serversysteme* gilt: Eine erfolgreich verifizierte Nachricht wird vom Empfänger (Distributor, Endempfänger) mit einer von ihm signierten Antwortnachricht (Response) bestätigt. Diese Nachricht muss die Signatur der ursprünglich erhaltenen Nachricht des Senders enthalten. Dies kann mit einer Web Service Security *Signature Confirmation* protokolltechnisch umgesetzt werden.
- Für *Clientsysteme* gilt: Wird der Erhalt einer Nachricht von einem ERP-System des Unternehmens bestätigt, so müssen relevante Teile der erhaltenen Nachricht vom ERP-System signiert an den Sender zurückgesendet werden. Diese Bestätigung muss auf fachlicher Ebene erfolgen, da dazu keine protokolltechnische Möglichkeit besteht.
- Der Sender der ursprünglichen Nachricht muss die in der Response enthaltene UID-Signatur verifizieren und anhand der Zertifikatskette bis zum Root-Zertifikat prüfen.
- Im Fall einer fehlerhaften Überprüfung der UID-Signatur, muss die erhaltene Response verworfen und eine Fehlermeldung ausgegeben werden.

4.3.5 *Beweis einer Kommunikationsverbindung:* Damit es bei zeitkritischen Prozessen einem ERP-System möglich ist, den Versand einer bestimmten Nachricht nachträglich zu beweisen, müssen alle Anfragepakete des ERP-Systems an den Distributor von diesem signiert rückbestätigt werden.

4.3.6 Gewährleistung der Nachvollziehbarkeit
Die Nachvollziehbarkeit eines gesamten Swissdec Kommunikationsablaufs (Set von Transaktion zu einem bestimmten Geschäftsfall) kann gewährleistet werden, indem der Distributor als Vermittler alle Verbindungsinformationen (Relationen) speichert. Da der Distributor in der Regel die Daten noch aufbereitet und dadurch zwischen den Kommunikationspartnern inhaltlich transformiert (mapping), bricht er die Signatur des ursprünglichen Senders auf. Deshalb muss er abgehende Pakete ebenfalls selbst signieren.
Die Signatur einer Swissdec-Nachricht beinhaltet im Wesentlichen:

- Einen Hashwert des signierten Inhalts,
- Eine Referenz zum signierten Inhalt im Nachrichtenteil,
- Einen Zeitstempel basierend auf der aktuellen Systemzeit[4],
- Schlüsselinformationen.

Der Distributor muss folgende Informationen zu einem Kommunikationsablauf speichern:

- Geschäftsfallnummer,
- Signatur jeder erhaltenen Nachricht,
- Signatur jeder transformierten und gesendeten Nachricht,
- Die SW-Version des Distributors,
- Kommunikationsmuster (1:D:n, 1:D:1).

Der Distributor persistiert **keine** Nachrichteninhalte. Kommunikationsinhalte werden vom Distributor nur im ‚Arbeitsspeicher' kurzzeitig gehalten. Nachrichteninhalte müssen von den Kommunikationspartnern selbst abgelegt werden. Für diese gelten die folgenden Richtlinien:

- Jeder Sender (Unternehmen oder Versicherer) einer Nachricht speichert vor dem Versand die von ihm signierte Nachricht im Klartext, damit diese zu einem späteren Zeitpunkt wieder gelesen werden können.
- Der Empfänger (Unternehmen oder Versicherer) prüft die Signatur einer empfangenen Nachricht und archiviert diese unverschlüsselt gemäss eigenen Vorgaben.

Wenn die Daten und Informationen zu einem Kommunikationsablauf von allen beteiligten Kommunikationspartnern und die Verbindungsdaten vom Distributor zusammengetragen werden, kann ein Geschäftsfall vollständig rekonstruiert werden. Im Streitfall kann damit ein unbeabsichtigter Fehler oder ein Fehlverhalten nachvollzogen werden.

[4] Es ist zu empfehlen, dass die Swissdec-Teilnehmer über eine gemeinsame Zeitbasis (NTP-Server) verfügen

5 SUA Credentials

Für die Swissdec Unternehmens Authentisierung sollen fortgeschrittene Zertifikate nach eigener Spezifikation eingesetzt werden. Damit entfällt zwar, die in Kapitel 5.1.6 beschriebene, rechtliche Abstützung auf ZertES, aber der Einsatz dieser ‚eigenen' Zertifikate gestaltet sich flexibler und lässt mehr Spielraum zu.

5.1 UID-Zertifikate

5.1.1 Verwendungszweck von UID-Zertifikaten
Da UID-Zertifikate sowohl zum Signieren, wie auch zur Verschlüsselung von SOAP-Nachrichten verwendet werden, empfiehlt sich zwei unterschiedliche Zertifikate (Verschlüsselung und Authentisierung/Signatur getrennt) für diese Anwendungen zu verwenden. Da diese Daten aber nur kurzzeitig für den Transportweg verschlüsselt werden und nicht verschlüsselt abgelegt und zu einem späteren Zeitpunkt dechiffriert werden müssen, entfällt der Anspruch zur Archivierung des privaten Schlüssels.
Aus diesem Grund, und um das Zertifikatshandling (insbesondere für die ERP-Systeme) nicht unnötig zu komplizieren, wird bei UID-Zertifikaten auf eine Einschränkung der Anwendung verzichtet und *ein* Zertifikat zum Authentisieren, Signieren und Verschlüsseln eingesetzt.

5.1.2 Ausgabeformen
Grundsätzlich werden UID-Zertifikate als X.509[5] Softzertifikate von einer dazu beauftragten Certificate Authority (CA) ausgestellt. Diese werden auf die Zielsysteme sicher übertragen und dort automatisch installiert. Wenn dies die Sicherheitsanforderungen einer Unternehmung erfordern, so ist es durchaus möglich das Schlüsselmaterial des UID-Zertifikats auf zertifizierter Hardware des Unternehmens erstellen zu lassen. Am Prozess zur Registrierung bzw. Ausgabe des Zertifikats ändert sich in diesem Fall nichts.

5.1.3 Umgang mit privaten Schlüsseln
Da das Schlüsselpaar zu einem UID-Zertifikat in der sicheren Umgebung des Unternehmens (ERP-System oder spezielle Hardware) erstellt wird, ist kein Backup des privaten Schlüssels möglich, da in diesem Prozess weder Swissdec noch die ausstellende CA je im Besitz des privaten Schlüssels eines UID-Zertifikats sind. Es ist durch die Infrastruktur des Unternehmens sicherzustellen, dass der private Schlüssel in sicherer Umgebung aufbewahrt wird und dass jederzeit autorisierte Applikationen darauf zugreifen können. Im Fall eines Soft-Tokens, muss der private Schlüssel von einem ERP-System lesbar gespeichert werden. Wenn die Sicherheitsanforderungen einer Unternehmung erfordern, dass private Schlüssel nur auf zertifizierter Hardware (Hard-Token, HSM) ausgestellt und gespeichert werden dürfen, so muss sichergestellt werden, dass das ERP-System auf das entsprechende Schlüsselmaterial, welches auf der zertifizierten Hardware abgelegt ist, jederzeit zugreifen kann.

5.1.4 CP/CSP
Für die Swissdec UID-Zertifikate muss die ausgebende Certificate Authority eine Certificate Policy (CP) und ein Certificate Practice Statement (CPS) gemäss den Richtlinien nach RFC 7382[6] erstellen.

5.1.5 Inhalt eines UID-Zertifikats
Unabhängig der Form des Trägers müssen UID-Zertifikate folgende Informationen beinhalten:

Bezeichnung	Beschreibung
Version	Zertifikatsversion (gemäss RFC5280: Version 3)
Serial Number	Eindeutige Identifikation des Zertifikats. Richtet sich nach den Vorgaben der ausgebenden CA.
Certificate Signature Algorithm	Spezifikation des Signaturalgorithmus des Zertifikats, folgt heute üblichen Standards und wird mit der ausgebenden CA abgestimmt. Minimalanforderung: SHA256 with RSA Encryption (Key size 2048 bit)
Issuer	Informationen zum Aussteller des Zertifikats (CA):

[5] Network Working Group, 2008. RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, online: https://www.ietf.org/rfc/rfc5280.txt (03.11.2015).

[6] https://tools.ietf.org/html/rfc7382

		commonName, organizationName, organizationalUnitName, countryName[7]
Validity		Zeitraum der Gültigkeit des Zertifikats: 1 Jahr
Subject		Informationen zum Zertifikatsinhaber (siehe Tabelle 2)
Subject Public Key Info		Informationen zum Schlüssel des Zertifikatsinhabers
	Public Key Algorithm	Public-Key-Algorithmus
	Subject's Public Key	Public Key des Zertifikatinhabers
Extensions:		
	Authority Key Identifier	Identifikation des vom Zertifikatsausstellers genutzten Public Key
	Authority Information Access	URI zu weiteren Informationen des Zertifikatsaustellers: OCSP, CA Issuers
	Certificate Policies	Hinweis (URI) auf weitere Vorgaben (technisch, rechtlich, prozessual), welche zur Verwendung des ausgestellten Zertifikats zu beachten sind. Für die Abklärung der Notwendigkeit und gegebenenfalls die Ausarbeitung solcher Vorgaben wird die Datenschutzverantwortliche der Swissdec hinzugezogen.
	CRL Distribution Points	URI zu einer Certificate Revocation List (CRL) der ausstellenden CA
	Key Usage	Nutzungszweck des im Zertifikat enthaltenen Schlüssels: *keyEncipherment* *digitalSignature*
	Extended Key Usage	*TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)* *Document Signing (1.3.6.1.4.1.311.10.3.12)*
	Subject Key ID	Identifikation eines Zertifikats mit einem spezifischen Public Key
Signature Algorithm		Spezifikation des Signaturalgorithmus des Zertifikats
Signature Value		Signatur des Zertifikats

Tabelle 1: Elemente eines UID-Zertifikats

Die Informationen zum Zertifikatsinhaber werden teilweise automatisiert dem UID-Register des BFS entnommen. Die OrganizationalUnit (OU) kann von der Unternehmung frei vergeben werden. Nachfolgende Tabelle beschreibt die im Zertifikat zum Zertifikatsinhaber enthaltenen Attribute, sowie deren Herkunft.

[7] Optional kann hier zusätzlich die UID-Nummer des Zertifikatausstellers angegeben werden - z.B. UID der Swissdec: Object Identifier (2 5 4 97) = NTRCH-CHE-113.865.903

Abk.	Bezeichnung	Inhalt	Quelle	Prio
CN	commonName	NTRCH-{UID-BFS}@swissdec.ch[8]	BFS UID-Register	MUSS
O	organizationName	<Name> aus dem UID-Register des BFS	BFS UID-Register	MUSS
OU	organizationalUnitName	Untereinheit der Organisation, kann frei gewählt werden und ist kaskadierbar	Benutzereingabe	KANN
L	localityName	Sitz des Unternehmens gemäss UID-Register, <town> aus UID-Register	BFS UID-Register	MUSS
ST	stateOrProvinceName	Kanton des Sitzes des Unternehmens, <locality> aus UID-Register	BFS UID-Register	MUSS
C	countryName	<country> aus UID-Register	BFS UID-Register	MUSS
UID	OID 2.5.4.97	OrganizationIdentifier: UID Nr. nach BFS UID-Register, NTRCH-{UID-BFS}	BFS UID-Register	MUSS
BC	OID 2.5.4.15	Business Category (Private Organization oder Government Entity)[9]	BFS UID-Register	KANN[10]

Tabelle 2: Attribute des Zertifikatinhabers (Subject)

Optional können Adressinformationen der entsprechenden Unternehmung im Subject des UID-Zertifikats abgelegt werden. Diese Adressinformationen können nur zum Zeitpunkt der Ausgabe des Zertifikats geprüft werden. Während der Gültigkeitsdauer des Zertifikats können sich diese Informationen ändern, weshalb sie nicht zwingend vorgeschrieben sind.

Optionale Informationen im Subject:

- OID 2.5.4.9: (streetAdress)
- OID 2.5.4.17: (postalCode)
- OID 1.3.6.1.4.1.311.60.2.1.2: (State) → gleich wie ST
- OID 1.3.6.1.4.1.311.60.2.1.3: (Country) → gleich wie C
- OID 2.5.4.15 (BusinessCategory): Bezeichnet den Typ einer Organisation. Grob kann hier zwischen *PrivateOrganization*, *Business Entity*, *Non-Commercial Entity* oder einer *Government Entity* unterschieden werden.

Eine weitere Option ist die Aufnahme der Informationen über die RA in die Extensions. Dies ist nur sinnvoll, falls die UID-Zertifikate auch ausserhalb des Swissdec-Kontextes eingesetzt werden sollen.

Optionale Informationen für *Certificate Subject Alt Name*:

- Object Identifier (2 5 4 97) = {UID-BFS}
- Object Identifier (2 5 4 13) = BFS-UID of Enterprise

Optionale Informationen für *Certificate Issuer Alt Name*:

- Object Identifier (2 5 4 97) = {UID-BFS}
- Object Identifier (2 5 4 13) = Validator of Enterprise BFS-UID

➔ In Anhang A ist der Aufbau eines UID-Zertifikats als Beispiel aufgeführt.

[8] Entspricht dem *legalperson semantics identifier* nach ETSI-Norm EN 319412-1, Kap. 5.1.

(http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.00_30/en_31941201v010100v.pdf)

[9] Hier könnte man auch den <legal Form> Eintrag aus dem BFS-UID-Register übernehmen.

[10] Nach Absprache mit QuoVadis wird auf die Angabe der Business Category im SUA-Zertifikat verzichtet.

5.1.6 Einsatz geregelter Zertifikate zur Swissdec Unternehmensauthentifizierung

Abklärungen mit dem BAKOM haben ergeben, dass die Totalrevision (ZertES)[11], die Verordnung über die Totalrevision des Bundesgesetzes über die elektronische Signatur (VZertES)[12] und die Anpassungen der Verordnung über elektronische Daten und Informationen (EIDI-V)[13] keine Vereinfachung zur Authentifizierung von Unternehmen für Swissdec bringen. Die ZertES Totalrevision beinhaltet unter anderem die Definition der Formate geregelter Zertifikate für folgende Anwendungen:

1. Elektronische Signatur einer natürlichen Person oder das elektronische Siegel einer UID-Einheit.
2. Elektronische Identifikation einer natürlichen Person oder UID-Einheit.
3. Verschlüsselung elektronischer Daten.

Über die Anwendung der in Punkt 2 und 3 erwähnten Zertifikate enthalten die oben erwähnten Dokumente keine weiteren Angaben. Das TAV zum ZertES[14] verweist in diesem Bereich auf die europäische Norm (EN) ETSI 319 411. Gemäss dieser Norm wäre die Ausgabe eines fortgeschrittenen Zertifikats, welches zur elektronischen Identifikation verwendet wird auch als Soft-Token möglich. Wie in der Stellungnahme von Swissdec vom 28. Juli 2016 zu den Entwürfen von ZertES, VZertES und TAV aufgezeigt wurde, sind die Rahmenbedingungen bei der Verwendung geregelter Zertifikate für die elektronische Identifikation für die Maschine-zu-Maschine Kommunikation unklar. Es ist insbesondere unklar, ob die Ausgabe solcher Zertifikate an ein HW-Token gebunden sind, wie der Registrierungsprozess erfolgen muss und welche Kosten diese Form von Zertifikate nach sich ziehen würden.
Aus diesem Grund verfolgt Swissdec vorerst (unabhängig von der Entwicklung geregelter Zertifikate auf dem Schweizer Markt) den ursprünglich angedachten Ansatz, für die *Swissdec Unternehmens-authentifizierung* fortgeschrittene Zertifikate nach eigener Spezifikation einzusetzen.

5.2 Certificate Signing Request (CSR)

Eine CSP stellt eine standardisierte Schnittstelle (CSR oder CMP[15]) zur Verfügung, um einen Request mit den Angaben zum Subjekt gemäss Vorgaben in der untenstehenden Tabelle 3 von Swissdec automatisiert verarbeiten zu können. Die Struktur des verwendeten elektronischen Zertifikatsantrags ist als PKCS#10[16] standardisiert. Ein CSR muss folgende Angaben zum Inhaber (Subject) und zum Schlüssel beinhalten:

Bezeichnung	Beschreibung
Subject	Informationen zum Zertifikatsinhaber wie commonName (CN), organizationName (O), organizationalUnitName (OU), localityName (L), stateOrProvinceName (ST), countryName (C) sowie die UID des Unternehmens (OID 2.5.4.97) → für detailliertere Informationen siehe Tabelle 2
PublicKey	Öffentlicher Schlüssel des Zertifikatsinhabers (RSA-2048bit-Schlüssel)

Tabelle 3: Attribute eines Certificate Signing Requests (CSR)

5.3 Kryptographische Standards

Es wird davon ausgegangen, dass in allen beteiligten Systemen die heute empfohlenen kryptographischen Algorithmen und Schlüssellängen zur Anwendung kommen. Für die Auswahl der verwendeten kryptographischen Algorithmen ist je nach Kommunikationsabschnitt (vgl. dazu Abbildung 5) ein anderes System zuständig. Demnach muss folgender Grundsatz gelten:

> Alle beteiligten Kommunikationskomponenten (inkl. Transmitter) müssen die für SUA vorgeschriebenen Algorithmen unterstützen.

[11] Totalrevision (ZertES)

[12] Verordnung Totalrevision (VZertES)

[13] Anpassung der Verordnung über elektronische Daten und Informationen (EIDI-V)

[14] TAV: Technische und administrative Vorschriften des BAKOM

[15] CMP (Certificate Management Protocol), IETF RFC 4210

[16] Network Working Group, 2000. RFC2986: PKCS #10: Certification Request Syntax Specification - Version 1.7, online: https://tools.ietf.org/html/rfc2986 (03.11.2015).

Die minimal erlaubten Algorithmen und Schlüssellängen müssen den folgenden Empfehlungen bzw. Richtlinien entsprechen:

- European Telecommunications Standards Institute (ETSI):
  http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf
- Bundesamt für Sicherheit in der Informatik (BSI):
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile

Zusätzlich sollten die Betreiber der Webserverdienste darauf achten, dass die Konfiguration der Webserver den Empfehlungen der Internet Engineering Task Force (IETF) in RFC 7525 entsprechen.

- Recommendations for Secure Use of Transport Layer Security (IETF): https://tools.ietf.org/html/rfc7525 .

5.4 SUA Passwörter

In den nachfolgend beschriebenen SUA-Prozessen werden zwei unterschiedliche Passwörter verwendet. Es handelt sich dabei um das Registrierungspasswort sowie das Sperr-Passwort. Beide werden jeweils in schriftlicher Form per Brief, also auf einem zweiten nicht elektronischen Kanal, vom Distributor bzw. einer V&B dem sich registrierenden Unternehmen zugesendet.

5.4.1 Registrierungspasswort

Der primäre Zweck des Registrierungspasswortes besteht darin, sicherzustellen, dass ein signiertes Zertifikat dem richtigen Empfänger (ERP-System) - und nur diesem - zugeordnet wird. Es dient also der Authentisierung des Unternehmens. Wir unterscheiden folgende Szenarien:

- Szenario 1: ERP-System generiert Keypair (siehe Abschnitt 6.2.1)
  Das Private-/Public-Keypair wird vom ERP generiert und ein Certificate Signing Request (CSR) gemäss PKCS#10 an den Distributor übermittelt.
  Das Passwort dient in diesem Falle lediglich der Authentisierung des ERP gegenüber dem Distributor. Da die Authentisierung online beim Absetzen des CSRs stattfindet, kann ein wirkungsvoller Schutz gegen Bruteforce-Angriffe auf Seite des Distributors (Anzahl Versuche beschränken, Timeouts...) implementiert werden.
- Szenario 2: Hardtoken (siehe Abschnitt 6.2.4)
  Das Keypair mit zugehörigem Zertifikat wird auf einem "Hardtoken" mit zugehöriger PIN dem Unternehmen übergeben. Die Spezifikation delegiert die Details diesbezüglich an die involvierte CA. Der Distributor ist aber nach wie vor als Authentifizierungsinstanz (Registration Authority) in den Prozess einbezogen.

5.4.2 Sperrpasswort

Das Sperrpasswort dient der Authentisierung des Unternehmens für den Fall, dass dieses ein ausgegebenes Zertifikat sperren lassen möchte (siehe Abschnitt 6.6). Das Passwort wird dabei einmal an die Swissdec übermittelt, worauf das Zertifikat gesperrt und bei der Certificate Authority (CA) revoziert wird. Im Anschluss ist ein vollständig neuer Registrationsprozess notwendig.

5.4.3 Anforderungen an die Passwörter

Folgende Anforderungen wurden für die Ausgestaltung der Passwörter berücksichtigt:

ID	Bezeichnung	Beschreibung	Prio
AP-01	Passwortlänge	So kurz wie möglich, so lang wie nötig.	MUSS
AP-02	Benutzer-freundlichkeit	Da die Passwörter schriftlich per Brief übergeben werden, ist auf eine gute Lesbarkeit und leichte Abtippbarkeit zu achten.	MUSS
AP-03	Prüfsumme	Eine Prüfsumme erlaubt die Prüfung auf Korrektheit bereits bei der Eingabe.	MUSS
AP-04	Einzigartigkeit	Eine genügend grosse Entropie garantiert die Einzigartigkeit auch bei einer grossen Anzahl ausgegebener Passwörter.	MUSS
AP-05	Ausgabe	Pro Unternehmen (UID-BFS) existiert zu einem bestimmten Zeitpunkt nur ein gültiges Registrierungspasswort.	MUSS
AP-06	Kennzeichnung	Das Passwort beinhaltet einen frei zu definierenden Bestandteil z.B. zur Kennzeichnung des Ausstellers oder der Version.	MUSS
AP-07	Verschlüsselung	Die Eignung zur Verschlüsselung von Dateiformaten zum Transport von Zertifikaten und zugehörigem Schlüsselmaterial ist gewährleistet.	KANN

Tabelle 4: Anforderungen an die SUA-Passwörter

5.4.4 Ausgestaltung der Passwörter

Der Prozess zur Generierung eines Passwortes umfasst folgende Schritte:

1. Mittels kryptografischen Zufallszahlengenerator (CSPRNG[17]) eingehende Zufallsvariable generieren
2. Abbildung der Zufallsvariable auf reduziertes Zeichenset und Erstellen eines Passwortes der vorgegebenen Länge (12 Zeichen)
3. Ergänzung um Kennzeichen (2 Zeichen)
4. Prüfsummenberechnung nach ISO/IEC 7064, MOD 1271-36 (siehe Codebeispiel) und Ergänzung um Prüfziffer (2 Zeichen)
5. Segmentierung in Viererblöcke (siehe Beispiel)
6. Speicherung in Datenbank mittels Key Derivation Function[18] (KDF)

Folgende zusätzliche strukturelle Vorgaben sind hierzu zu beachten:

Reduziertes Zeichenset	Zahlen: 2345689 Grossbuchstaben: ABCDEFGHJKLMNPQRTUVWXYZ Ausgenommen wurden: 1, 7, 0, O, S
Passwortlänge	12 Zeichen (ohne Prüfziffer und Kennzeichnung)
Kennzeichen	2 Zeichen
Prüfziffer	Berechnung gemäss ISO/IEC 7064, MOD 1271-36 2 Zeichen
Segmentierung	Vier Viererblöcke, insgesamt 16 Zeichen getrennt durch Bindestriche
Key Derivation Function	Argon2[19] (Gewinner des Password-Hashing-Contests[20])

Tabelle 5: Vorgaben zur Struktur der SUA Passwörter

5.4.5 Beispiel eines Passwortes

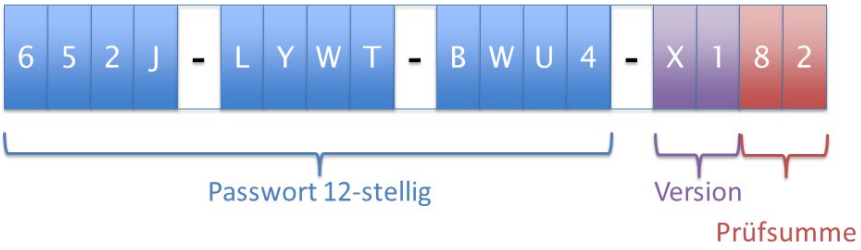

Abbildung 9: Beispiel eines SUA Passwortes

5.4.6 Codebeispiel für die Implementierung

Ein Beispiel für die Implementierung des ISO/IEC 7064, MOD 1271-36 für Java findet man z.B. hier:
https://github.com/danieltwagner/iso7064/blob/master/src/main/java/com/github/danieltwagner/iso7064/Mod1271_36.java

Fremder wiederverwendeter Code muss allerdings einer strengen Kontrolle bezüglich der Korrektheit unterworfen werden. Ebenfalls ist das Copyright zu beachten.

[17] https://en.wikipedia.org/wiki/Cryptographically_secure_pseudorandom_number_generator

[18] https://en.wikipedia.org/wiki/Key_derivation_function

[19] https://password-hashing.net/argon2-specs.pdf

[20] https://password-hashing.net/

6 SUA Prozesse

Der Gesamtprozessablauf im Hinblick auf die Authentifizierung von Unternehmen umfasst vier Phasen: Registrierung, Konfiguration, Betrieb sowie Erneuerung und Sperrung (des Zertifikats).
Untenstehende Abbildung 10 zeigt die beiden Hauptstränge des Prozesses mit den jeweiligen wichtigsten Bestandteilen über alle vier Phasen auf. In den nachfolgenden Kapiteln wird detailliert auf die einzelnen Schritte der Prozesse eingegangen.

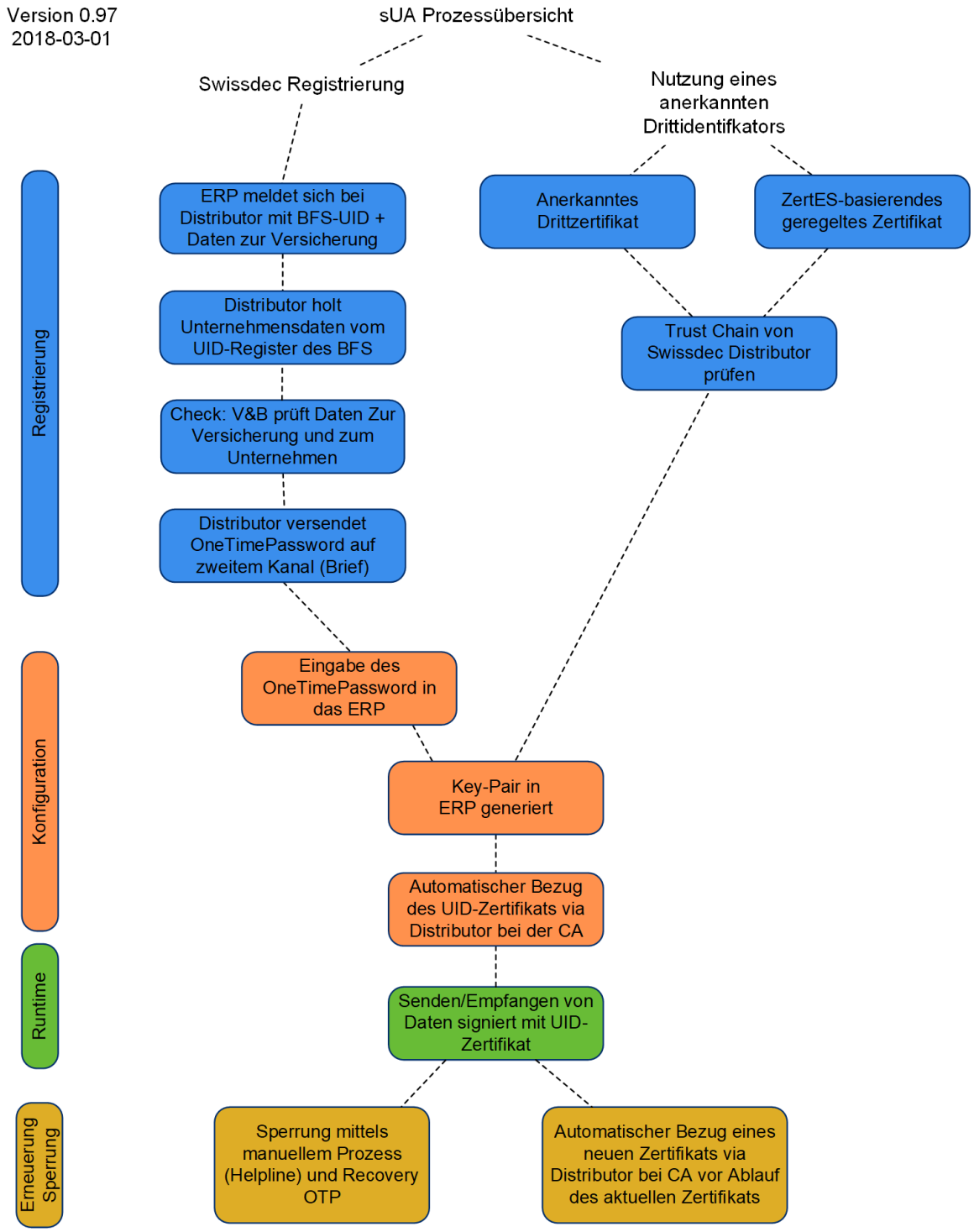

Abbildung 10: Gesamtprozess Swissdec Unternehmens-Authentifizierung in vier Phasen

6.1 Registrierungsprozess

Für die Registrierung sind zwei grundsätzliche Möglichkeiten vorgesehen (siehe Abbildung 10). Auf der einen Seite beinhaltet dies eine Registrierung bei Swissdec und auf der anderen Seite eine vereinfachte Registrierung mit Hilfe eines Dritt-Identifikators, wie einem ZertES-basierenden (geregelten) Zertifikat.
Aktuell ist davon auszugehen, dass die direkte Registrierung bei Swissdec der übliche Weg sein wird, wie Firmen zukünftig Geschäftsprozesse auf der Basis der Swissdec Unternehmens-Authentifizierung abwickeln können. Mit zunehmender Verbreitung von Unternehmenszertifikaten, welche nach den Vorgaben des ZertES ausgestellt wurden, lässt sich der Registrierungsprozess wesentlich vereinfachen.

6.1.1 Swissdec Registrierung

Grundlage einer Registrierung ist eine bestehende Vertragsbeziehung mit einer Versicherung. Dabei wird davon ausgegangen, dass die Versicherung bei Vertragsabschluss das Unternehmen überprüft und jederzeit aktuelle UID-Daten (UID-Nummer, Name des Unternehmens laut Handelsregister, …) in ihren Stammdaten-Systemen führt.
Unternehmen ohne bestehende Vertragsbeziehung müssen den Weg über die direkte Registrierung mit Hilfe eines geregelten Zertifikats (siehe Kapitel 6.1.2) nehmen.
Auch Treuhänder, die später zur Laufzeit Daten der von ihnen verwalteten Unternehmen mit ihrem UID-Zertifikat signieren werden, müssen den normalen Registrierungs- und Konfigurationsprozess durchlaufen. Es wird davon ausgegangen, dass Treuhänder auch Unternehmen mit Vertragsbeziehungen zu den V&B sind, auf deren Grundlage eine Registrierung möglich ist.
Für die Registrierung bei der Swissdec sind prinzipiell zwei Varianten möglich, welche sich im Wesentlichen darin unterscheiden, ob die Versicherungen und Behörden mit den Unternehmen in Kontakt treten oder dies an die Swissdec delegieren. Abschnitt 6.1.1.1 beschreibt den bevorzugten Prozessablauf, in welchem die für die Registrierung notwendigen Informationen vom Distributor der Swissdec an die Unternehmen versendet werden. Im nachfolgenden Abschnitt 6.1.1.2 wird der mögliche Registrierungsprozess mittels Kontaktaufnahme durch die Versicherungen und Behörden kurz beschrieben.
In beiden Fällen werden die Informationen zur Erstkonfiguration, die aus dem Registrierungsprozess resultieren, per zweitem, nicht elektronischem Kanal an die Unternehmen geschickt. An diesen Kanal werden die folgenden Anforderungen gestellt:

ID	Bezeichnung	Beschreibung	Prio
AB-01	Überprüfung der Adresse	Der Adresse (Email-Adresse, SMS-Nummer, PostAdresse) muss der Versicherung, bei der sich das Unternehmen registriert, bekannt sein und von der Versicherung überprüft worden sein.	MUSS
AB-02	Sicherheit	Es muss sichergestellt werden, dass die Informationen den Adressaten erreichen und nicht in fremde Hände geraten können.	MUSS
AB-03	Übergebbarkeit	Die übermittelten Informationen müssen an die zuständige Person (Kontaktperson) weitergegeben werden.	MUSS
AB-04	Ablegbarkeit	Die übermittelten Informationen sollten einfach zu speichern und abzulegen sein.	KANN
AB-05	Dauer	Die übermittelten Informationen müssen in vernünftiger Zeit den Adressaten erreichen.	MUSS
AB-06	Inhalt	Die Informationen müssen selbsterklärend sein, um die Folgeaktionen auszulösen (Weitergabe an Kontaktperson).	MUSS
AB-07	Nachvollziehbarkeit	Es muss es möglich sein, den Aufenthaltsort, Sende-Status und Abgabe beim Adressanten der verschickten Informationen zu ermitteln.	MUSS
AB-08	Kosten	Die Kosten sollten angemessen sein.	KANN

Tabelle 6: Anforderungen an den nicht elektronischen Kanal

In der Tabelle 7 wird die Erfüllung der Anforderung durch die verschiedenen Medien aufgezeigt.

ID	Bezeichnung	Email	SMS	Brief
AB-01	Überprüfung der Adresse	Evtl. bekannt	Evtl. bekannt	Postadresse der Geschäftsleitung des Unternehmens ist bekannt (Teil der Geschäftsbeziehung)
AB-02	Sicherheit	Empfang relativ sicher (evtl. Empfangsbestätigung notwendig)	Empfang nicht sicher	Durch ein Post-Unternehmen garantiert; u.U. muss Einschreiben verwendet werden.
AB-03	Übergebbarkeit	Kann einfach weitergeleitet (an Email-Adresse der Kontaktperson)	Kann einfach weitergeleitet, aber Kenntnis SMS-Nummer notwendig	Persönliche Übergabe oder durch Hauspost im Unternehmen
AB-04	Ablegbarkeit	Email-Archivierung /Ausdrucken	Nicht einfach	Direkt möglich
AB-05	Dauer	Sehr schnell	Im Normalfall sehr schnell	Je nach Versandart (1 Tag bis 1 Woche)

AB-06	Inhalt	Erfüllt	zu kurz	erfüllt
AB-07	Nachvollziehbar-keit	Schwierig nachzuvollziehen, nur Empfangsbestätigung	Nicht möglich	mit A-Post-Plus oder Einschreiben möglich
AB-08	Kosten	Keine Kosten	Geringe Kosten	Je, nach Versandart

Tabelle 7: Erfüllung der Anforderungen an den nicht elektronischen Kanal durch die verschiedenen Medien

Wie aus Tabelle 7 ersichtlich, erfüllt der Brief-Kanal die gestellten Anforderungen zurzeit am besten, wobei die Kriterien Sicherheit, Kosten und Dauer gegeneinander abgewogen werden müssen. Im Weiteren wird deshalb ein eingeschriebener Brief (oder A-Post-Plus-Brief) als zweiter, nicht elektronischer Kanal referenziert.
Der Registrierungsprozess wird sowohl als BPMN-Diagramm als auch als Sequenzdiagramm dargestellt. Die beiden Sichten konzentrieren sich dabei einerseits auf den konkreten Prozessablauf und andererseits auf die darin stattfindenden Kommunikationsbeziehungen.

6.1.1.1 Distributor versendet Brief an Unternehmen

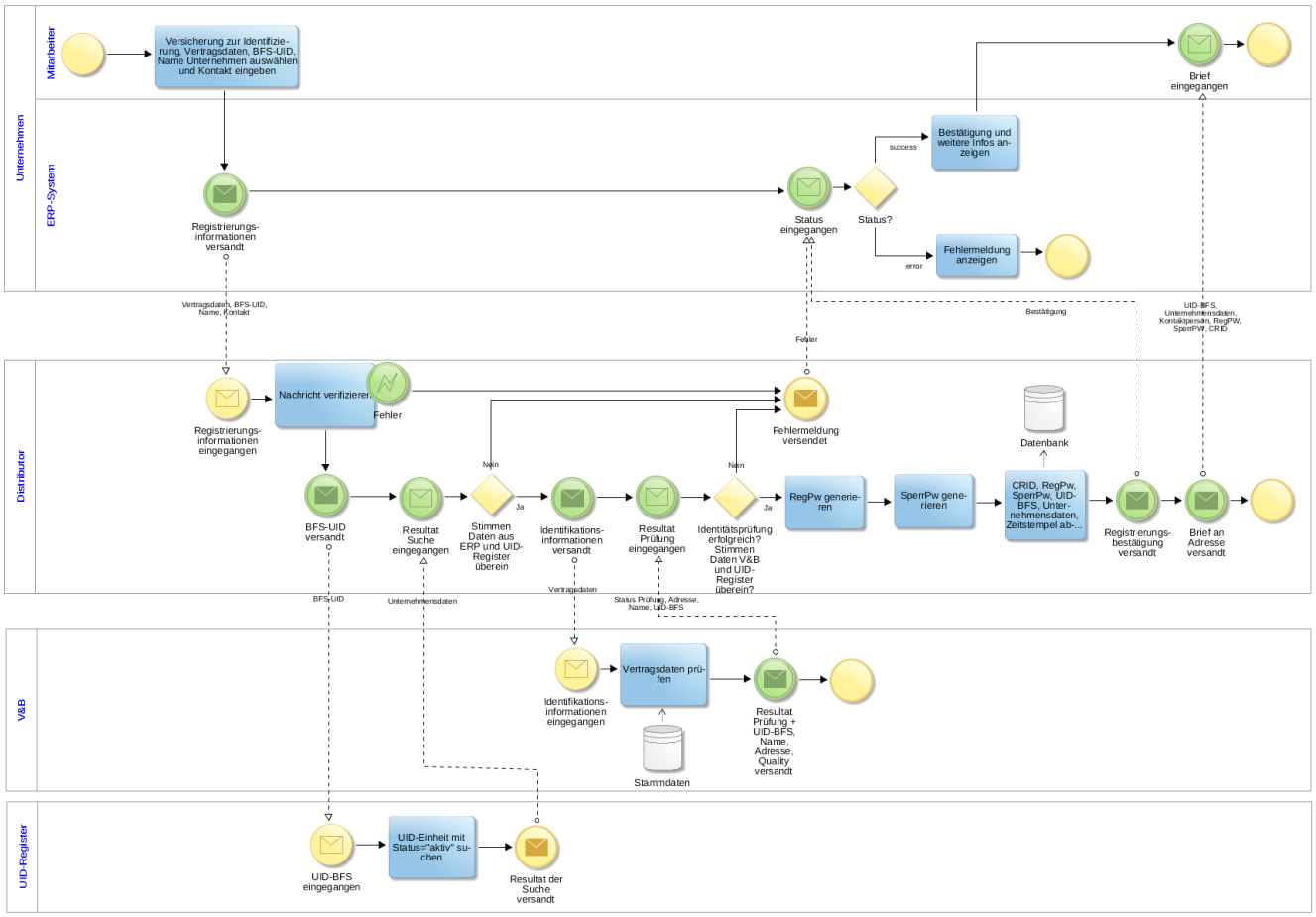

Abbildung 11: Registrierungsprozess

Möchte sich ein Unternehmen für die Swissdec Unternehmens-Authentifizierung registrieren, so wählt ein zuständiger Mitarbeiter des Unternehmens im ERP-System eine Versicherung aus, welche für die Identifikation der Unternehmen genutzt werden soll. Die zur Registrierung notwendigen Informationen (Vertragsinformationen IData, BFS-UID, Name des Unternehmens) werden grösstenteils durch das ERP-System automatisiert bereitgestellt und an den Distributor gesendet. Zusätzlich muss eine verantwortliche Kontaktperson mit ausreichend identifizierenden Angaben, wie Name, E-Mail, Telefon/Mobilnummer, Funktion/Abteilung, ausgewählt oder eingegeben werden.
Der Distributor verifiziert die erhaltene Nachricht. Er stellt auch sicher, dass nur eine begrenzte Anzahl aktiver Registrierungs-Anfragen (z.B. maximal 5)[21] für eine BFS-UID möglich sind. Dem ERP-System wird das Ergebnis der

[21] Ein Unternehmen kann mehrere aktiven Registrierungs-Anfragen haben, z.B. für mehrere ERP-Systeme. Durch die Limitierung der Anzahl der Anfragen soll verhindert werden, dass neue Anfragen abgesetzt werden können, bevor die aktiven abgeschlossen werden konnten (das

Verifikation durch das Senden einer generierten *CertificateRequestID* (CRID), die das ERP-System und den Request eindeutig identifiziert, mitgeteilt.
Wurde die Nachricht erfolgreich vom Distributor verifiziert, werden die Informationen zum Unternehmen aus dem UID-Register des BFS angefragt. Mit Hilfe der BFS-UID wird ein «aktiver» Datensatz zum Unternehmen gesucht. Dieser wird mit den erhaltenen Daten des Unternehmens (Name lt. Handelsregister) abgeglichen.
Im nächsten Schritt werden die Angaben zum Vertrag vom Distributor an die zuvor ausgewählte V&B weitergeleitet. Die V&B prüft mit Hilfe ihrer Stammdaten die vom Unternehmen gesendeten Daten (Vertragsdaten) auf Gültigkeit und Übereinstimmung. Das Resultat der Prüfung wird zusammen mit den aus den Stammdaten entnommenen UID, Namen des Unternehmens und Adressinformationen (Geschäftsleitung) an den Distributor zurückgesendet.
Ist das von V&B zurückgesendete Prüfungsergebnis negativ, so wird dies vom Distributor dem ERP-System des Unternehmens signalisiert, welches dem Benutzer eine entsprechende Fehlermeldung ausgibt. Der Benutzer muss sich nun direkt mit V&B in Verbindung setzen, um Versicherungs- und Unternehmensdaten abzugleichen.
Der Distributor schliesst nun die Identitätsprüfung durch einen Abgleich der von V&B erhaltenen Daten mit denen aus dem UID-Register ab. Neben der UID-Nummer und dem Namen des Unternehmens können auch die Adressdaten abgeglichen werden (automatisch oder auch manuell).
Im Falle einer positiven Identitätsprüfung generiert der Distributor ein Registrierungspasswort und ein Sperrpasswort. Beide Passwörter werden zusammen mit der UID-BFS, den Angaben aus dem UID-Register des BFS, der CRID und einem Zeitstempel abgespeichert. Das Registrierungspasswort wird für die später folgende Konfiguration benötigt, hat aber eine zeitlich beschränkte Gültigkeit von 30 Tagen. Der Distributor sendet eine Bestätigung der erfolgreichen Identifizierung des Unternehmens an das ERP-System, welches dies dem Benutzer anzeigt. Diese Bestätigung enthält u.a. auch die Daten zum Unternehmen aus dem UID-Register des BFS, die für die Erstellung des UID-Zertifikats verwendet werden.
Der Distributor, oder eine hierfür von der Swissdec beauftragte Drittpartei, erstellt einen Brief (Einschreiben oder A-Post-Plus) an die von V&B bereitgestellten Adresse (Geschäftsleitung), welcher neben zusätzlichen Informationen (z.B. zum Konfigurationsprozess) das Registrierungspasswort, das Sperrpasswort, die CRID, die UID-BFS, die Angaben zum Unternehmen aus dem UID-Register des BFS und die verantwortliche Kontaktperson des Unternehmens enthält. Die Informationen werden so auf einem zweiten, nicht elektronischen Kanal der verantwortlichen Person eines Unternehmens zugestellt, was die Qualität der Identifizierung zusätzlich anhebt. Dies entspricht nach gängigen Authentisierungsstandards wie (eIDAS Verordnung der EU, eCH-0170v2, NIST SP 800-63 und ISO 29115) einer hohen Stufe zur Verifikation eines Empfängers bei der Übergabe eines Authentifizierungsmittels. Wenn von der Drittpartei unterstützt, kann auch der Status des versendeten Briefes (z.B. in Vorbereitung, versandt, angekommen) vom Distributor an das Unternehmen übermittelt werden.
Der gesamte Registrierungs-Prozess ist verbindlich und es werden die Konzepte aus Kapitel 2 noch zusätzlich angewendet.
Um einen reibungslosen Ablauf der Registrierung und anschliessenden Konfiguration (siehe Kap. 6.2) zu gewährleisten, soll es möglich sein die beiden Prozesse im Testmodus durchzuführen. Im **Testmodus** werden keine Briefe verschickt und kein Zertifikat ausgestellt. Die Abfrage der UID-Registers und Überprüfung durch eine V&B finden wie bei einer echten Registrierung statt. So können die Fälle, dass die Angaben im UID-Register nicht aktuell waren und zunächst korrigiert werden müssen, einfach abgehandelt werden.

Verschicken des Briefes kann ja 1-2 Tag dauern). Grund der Limitierung sind die Vermeidung von unnötigen Anfragen an das UID-Register des BFS sowie das unnötige Versenden von Briefen, das unerwünschte Kosten verursachen könnte.

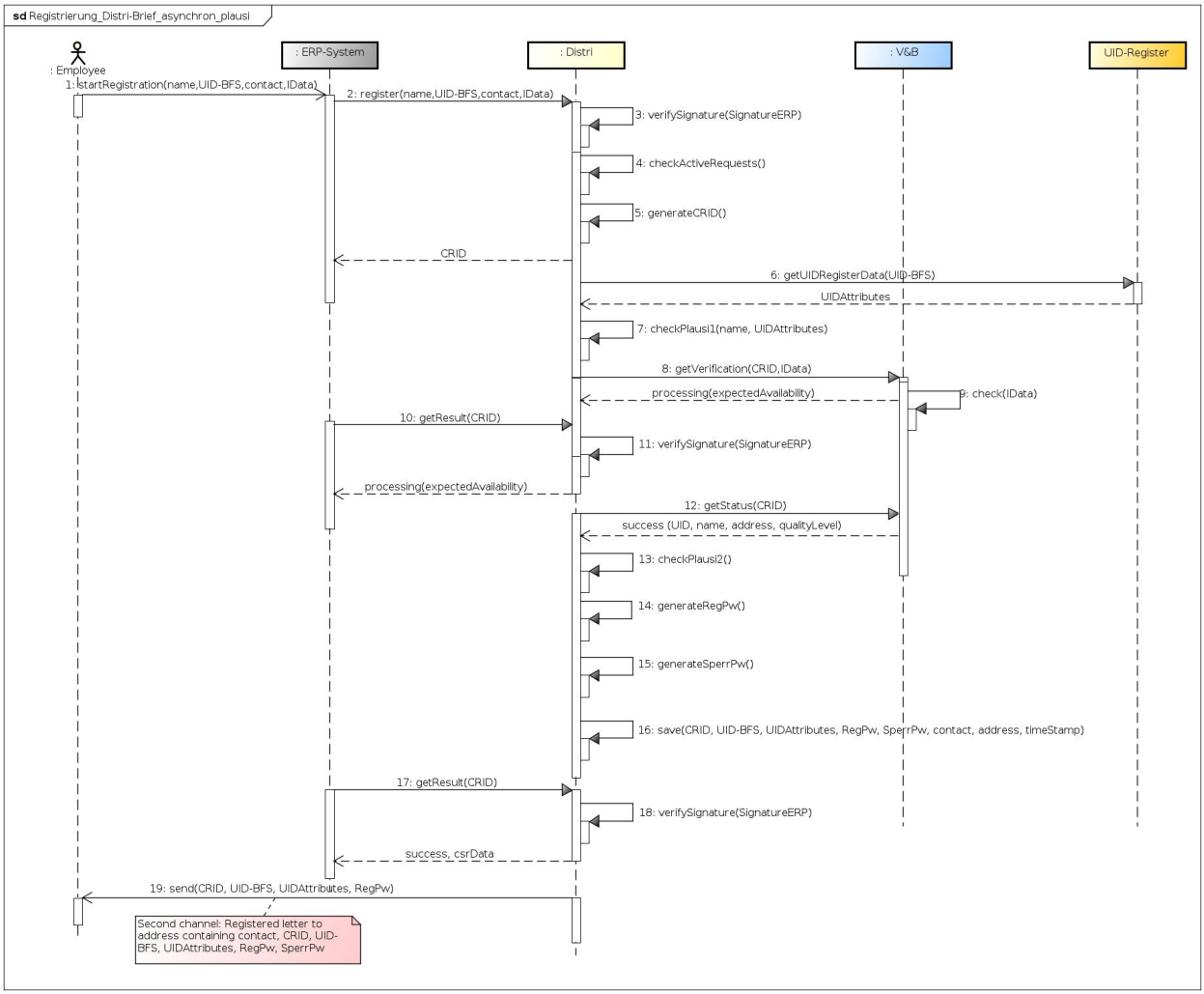

Abbildung 12: Sequenzdiagramm Registrierungsprozess

Die Kommunikation zwischen dem ERP und dem Distributor ist generell asynchron, d.h. das Ergebnis des (synchronen) register-Aufruf, der die CRID zurückgibt, wird mit Hilfe von wiederholten (synchronen) getResult-Abfragen abgeholt. Die Kommunikation zwischen BFD-UID-Register und der V&B-Systeme erfolgt synchron.

Tabelle 8 : Beschreibung der Einzelschritte im Registrierungsprozess

Nr.	Beschreibung
1	**startRegistration(name, UID-BFS, contact, IData)**: Der Benutzer wählt den Namen (name) laut Handelsregister und die UID-BFS seines Unternehmens sowie eine dazugehörige im ERP-System hinterlegte Versicherungsbeziehung zur Identifikation des Unternehmens aus. Die notwendigen Informationen zur Versicherung werden dem ERP-System entnommen. Zusätzlich gibt der Benutzer eine Kontaktperson mit identifizierenden Informationen ein. IData: Versicherungsdaten (insurance data), Informationen zur Vertragsbeziehung. Müssen folgende Attribute enthalten: • Versicherernummer / InsuranceID Identifikation, um den Endempfänger zu identifizieren, • Kundennummer / CustomerIdentity, • Vertragsnummer/Subnummer / ContractIdentity. contact: Identifizierende Informationen zur verantwortlichen Person. Sollte folgende Attribute enthalten: • Vollständiger Name • E-Mail

	• Telefon/Mobilnummer • Abteilung/Funktion
2	**register(name, UID-BFS, contact, IData):** Das ERP-System sendet die Angaben zur Versicherung, zum Unternehmen (UID-BFS), zum Treuhänder und die Kontaktdaten an den Distributor.
3	**verifySignature(SignatureERP):** Der Distributor prüft die Signatur der Nachricht auf ihre Gültigkeit sowie die Kompatibilität zur Version des SUA-Standards.
4	**checkActiveRequests():** Der Distributor stellt sicher, dass die maximale Anzahl von Registrierungs-Anfrage für eine BFS-UID nicht überschritten wurde. Falls eine Überschreitung erkannt wird, wird der Registrierungs-Prozess abgebrochen und das ERP erhält bei der nächsten getResult()-Anfrage den Status error zurück.
5	**generateCRID():** Der Distributor generiert eine CRID (CertificatRequestID) für den Geschäftsfall, die den Registrierungsprozess des ERP-Systems eindeutig identifiziert.
<--	Der Distributor sendet dem ERP-System eine Bestätigung des Nachrichteneingangs: CRID: Generierte ID des Geschäftsfalls, um das Resultat der Identitätsprüfung abzuholen. Identifiziert das ERP-System und den zugehörigen Request.
6	**getUIDRegisterData(UID-BFS):** Der Distributor sendet einen synchronen Request mit der UID-BFS des Unternehmens an das UID-Register des BFS.
<--	Der Distributor erhält als Response die zur Prüfung des CSR nötigen Attribute (UIDAttributes) des Unternehmens. Diese umfassen folgende Attribute[22] [23]: • Name: <root>/eCH-0108:organisation/eCH-0098:organisationIdentification/eCH-0097:organisationName • Land: <root>/eCH-0108:organisation/eCH-0098:contact/eCH-0046:address[eCH-0046:otherAddressCategory/text()='main']/eCH-0046:postalAddress/eCH-0010:addressInformation/eCH-0010:country • Stadt: <root>/eCH-0108:organisation/eCH-0098:contact/eCH-0046:address[eCH-0046:otherAddressCategory/text()='main']/eCH-0046:postalAddress/eCH-0010:addressInformation/eCH-0010:town • Lokalität (Kanton)[24]: <root>/eCH-0108:organisation/eCH-0098:contact/eCH-0046:address[eCH-0046:otherAddressCategory/text()='main']/eCH-0046:postalAddress/eCH-0010:addressInformation/eCH-0010:locality • BusinessCategory (Rechtsform)[25]: <root>/eCH-0108:organisation/eCH-0098:organisationIdentification/eCH-097:legalForm • PublicStatus[26]: <root>/eCH-0108:uidregInformation/eCH-0108:uidregPublicStatus Die abgefragte UID-BFS muss in diesem Fall als „Aktiv“ gekennzeichnet sein, da ansonsten nicht davon ausgegangen werden kann, dass die Attribute aktuell bzw. korrekt sind.

[22] Gemäss: Bundesamt für Statistik BFS, 2015. UID-Register – Webservice Schnittstelle 3.0. Online: https://www.bfs.admin.ch/bfs/de/home/register/unternehmensregister/unternehmens-identifikationsnummer/uid-register/uid-schnittstellen.assetdetail.1760903.html (20.02.2018).

[23] Die der Schnittstelle des BFS-UID-Registers zugrundeliegenden eCH-Standards wurden Q1/2018 aktualisiert, eine Änderung der Schnittstelle ist daraufhin nicht auszuschliessen.

[24] Lokalität ist eine optionale Information im UID-Register des BFS.

[25] Rechtsform ist eine optionale Information im UID-Register des BFS. Es wird eine zweistellige (01, 02, 03) oder vierstellige Nomenklatur nach eCH-0097 (https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0097&documentVersion=4.0) verwendet, die dann beim Übertragen ins Zertifikat entsprechend umgewandelt werden muss.

[26] **PublicStatus** gibt Auskunft darüber, ob die im UID-Register enthaltenen Daten eines Unternehmens öffentlich auf dem Internet zugänglich gemacht werden dürfen. Siehe auch Kapitel 9.6.

	UID-Status: <root>/eCH-0108:uidregInformation/eCH-0108:uidregStatusEnterpriseDetail
7	**checkPlausi1(name,UIDAttributes):** Der Distributor überprüft die Daten aus dem BFS-UID-Register und gleicht diese mit den Angaben des Unternehmens aus Schritt 2 ab. Stimmen die Angaben nicht überein wird die Registrierung mit einer Fehlermeldung abgebrochen.
8	**getVerification(CRID, IData):** Der Distributor sendet die CRID und die Angaben zur Vertragsbeziehung an die zuvor ausgewählte V&B.
9	**check(IData):** Die V&B nimmt auf der Grundlage ihrer Stammdaten die Prüfung der Vertragsbeziehung des Unternehmens vor. Dieser Vergleich kann automatisiert oder manuell durch einen Mitarbeiter ausgeführt werden. Wird eine vollständige Übereinstimmung der beiden Datensätze festgestellt, so liegt eine positive Identitätsprüfung vor. Stimmen die gesendeten Daten nicht mit den Stammdaten der V&B überein, so kann die Identität des Unternehmens nicht bestätigt werden.
<--	**processing(expectedAvailability):** Die V&B bestätigt, dass die Verarbeitung begonnen hat und teilt dem Distributor eine zu erwartende Zeitspanne mit, nach welcher die Verarbeitung abgeschlossen sein sollte.
10	**getResult(CRID):** Das ERP-System erfragt nach dem Erhalt der Bestätigung (CRID) beim Distributor den Status der aktuellen Verarbeitung. Hierzu sendet das ERP-System die entsprechende CRID in einem mit dem ERP-Zertifikat signierten Request an den Distributor.
11	**verifySignature(SignatureERP):** Siehe 3
<--	**processing(expectedAvailability):** Der Distributor antwortet dem ERP-System, dass die Verarbeitung noch läuft und teilt die geschätzte Zeitspanne mit, nach welcher die Verarbeitung abgeschlossen sein sollte.
12	**getStatus(DID):** Nach Ablauf der von der V&B festgelegten Zeitspanne erfragt der Distributor den Status der aktuellen Verarbeitung mittels entsprechendem Request..
<--	**success(BFS_UID, name, address, qualityLevel, contact):** Das Resultat der Prüfung wird vom Versicherer an den Distributor zurückgesendet. Die Response enthält im Positivfall folgende Elemente: • success: Identität erfolgreich bestätigt, • BFS-UID: Die UID-Nummer des Unternehmens aus den Stammdaten von V&B, • name: Name des Unternehmens, • address: Adressangaben des Kundenunternehmens mit Name des Unternehmens (Geschäftsleitung), Postfach, Strasse, Hausnummer, Postleitzahl, Ort, • qualityLevel: Qualität der Überprüfung der Daten (z.B. 0 – automatisch, 10 – manuell, 100 – entspr. ZertES), • contact: Kontaktperson bei V&B, die die Überprüfung vorgenommen hat und im Supportfall zu kontaktieren ist. Im negativen Fall wird ein Fehler gesendet: • error: Fehler bei der Identitätsprüfung In diesem Fall werden die nachfolgenden Schritte auf dem Distributor nicht ausgeführt.
13	**checkPlausi2():** Der Distributor gleicht nun die Angaben von V&B mit den zuvor erhaltenen Daten aus dem UID-Register ab. Dabei werden die UID-Nummern, die Namen des Unternehmens und Adressangaben automatisch (z.B. mittels unscharfer Methoden aus dem Bereich der KI) oder auch manuell abgeglichen. Stimmen die Daten aus den beiden Quellen überein, ist die Registrierung erfolgreich und kann mit den nächsten Schritten fortgesetzt werden.

14	**generateRegPw():** Bei einer positiven Identitätsprüfung (success) generiert der Distributor ein Registrierungspasswort (RegPw) gemäss den entsprechenden Vorgaben (siehe Abschnitt 5.4).
15	**generateSperrPw():** Zusätzlich generiert der Distributor ein Sperrpasswort (SperrPw) gemäss den Vorgaben aus Abschnitt 5.4. Dieses wird im Sperrungsprozess verwendet (siehe Abschnitt 6.6)
16	**save(CRID, UID-BFS, UIDAttributes, RegPw, SperrPw, contact, address, timeStamp):** Der Distributor speichert RegPw und SperrPw zusammen mit der UID-BFS, den Angaben zum Unternehmen aus des UID-Register (UIDAttributes), der CRID, den Kontaktdaten (contact), die Adressangaben (address) und einem Zeitstempel (timeStamp) ab. Die zeitliche Gültigkeit eines RegPw ist auf maximal 30 Tage beschränkt.
17	**getResult(CRID):** Nach Ablauf der vorgegebenen Zeitspanne (expectedAvailability) erfragt das ERP-System beim Distributor den Status der aktuellen Verarbeitung. Hierzu sendet das ERP-System den entsprechenden CRID in einem mit dem ERP-Zertifikat signierten Request an den Distributor.
18	**verifySignature(SignatureERP):** Siehe 3
<--	Liegt dem Distributor das Resultat der Identitätsprüfung vor, so wird dem ERP-System das Resultat (success | error) als Response gesendet. Zusammen mit dem Resultat success werden die bestätigte UID-BFS und die notwendigen Informationen, die zum Erstellen eines CSR (SubjektInformation) benötigt werden, mitgeschickt.
19	**send(CRID, UID-BFS, UIDAttributes, RegPw, SperrPw):** Wurde die Identität der Unternehmung erfolgreich geprüft (success) sendet der Distributor, bzw. eine von der Swissdec damit beauftragte Drittpartei einen Brief (zweiter, nicht elektronischer Kanal) an die Geschäftsleitung des Unternehmens (address) mit Angaben der erhaltenen Kontaktperson (contact). Hierfür werden übermittelten Kontaktinformationen aus dem ERP und Adressdaten aus dem Kundenstamm von V&B genutzt. Der Brief enthält mindestens folgende Informationen, die zur Konfiguration benötigt werden: • CRID zur Identifikation des spezifischen Registrierungsprozesses. • UID-BFS und UIDAttributes des sich registrierenden Unternehmens, • RegPw zur Konfiguration, • SperrRW zum Sperren des UID-Zertifikats, • Gültigkeit des RegPW.

Im Fall einer positiven Identitätsprüfung durch V&B erhält der zuständige Mitarbeiter nach erfolgreichem Abschluss der Registrierung die Informationen zum Unternehmen, die dem UID-Register des BFS entnommen wurden (elektronisch als Antwort auf eine getResult()-Abfrage bzw. im Brief).

6.1.1.2 V&B versendet Brief an Unternehmen

Der Prozess verläuft grundsätzlich analog zum Registrierungsprozess, in welchem der Distributor den Brief an die Unternehmen versendet.

Wurde die vom ERP-System an den Distributor gesendeten Registrierungsinformationen erfolgreich durch den Distributor verifiziert, wird von diesem das Registrierungs- und das Sperrpasswort generiert. Im Unterschied zum vorherigen Ablauf werden nun zusammen mit den für die Identifikation des Unternehmens relevanten Informationen (Versicherungsprofil, UID-BFS) nun zusätzlich die Passwörter an die V&B gesendet.

Die V&B prüft mit Hilfe ihrer Stammdaten die vom Unternehmen gesendeten Registrierungsinformationen auf Gültigkeit und Übereinstimmung. Das Resultat der Identitätsprüfung wird zurückgesendet.

Im Falle einer positiven Identitätsprüfung versendet die V&B einen Brief (Einschreiben oder A-Post-Plus) an die Geschäftsleitung des Unternehmens mit Angaben zur Kontaktperson (contact), welcher neben zusätzlichen Informationen (z.B. zum Konfigurationsprozess) das Registrierungspasswort, dessen Gültigkeit, das Sperrpasswort, die CRID und die UID-BFS enthält.

Dieser Registrierungsprozess ist zwar möglich, im Moment aber ausgeschlossen. Denkbar ist aber eine Initialisierung der Registrierung der Unternehmen durch die V&B, allerdings mit einem Rundschreiben (Massenversand), das nur noch die Anleitung für die Registrierung aus Kapitel 6.1.1.1 enthält.

6.1.2 Registrierung mit geregeltem Zertifikat nach ZertES

Die detaillierte Beschreibung des Registrierungsprozesses mit geregelten ZertES-Zertifikaten wurde in ein separates Dokument «Swissdec Unternehmens-Authentifizierung - Detailspezifikation - Ergänzung Registrierung mit ZertES» [1] ausgelagert.

6.1.3 Vor- und Nachteile der unterschiedlichen Registrierungsprozesse

Tabelle 9 : Vor- und Nachteile der einzelnen Varianten des Registrierungsprozesses

Prozess	Vorteile	Nachteile
Distributor versendet Brief	• Zentraler und einheitlich ausgestalteter Versand der Briefe durch Swissdec • Informationen müssen nicht der V&B weitergegeben werden. • Optional: Keine Übermittlung von Adressinformationen von Kunden nötig[27]	• Kontaktinformationen zu Kunden werden an den Distributor und ggf. eine Drittpartei übermittelt • Kein direkter Kundenkontakt V&B zu Kunden
V&B versendet Brief	• Direkter Kontakt V&B zu Kunden • Vertrauensverhältnis Kunde – Anbieter	• V&B muss Prozess zum Verschicken der Briefe etablieren • Viele unterschiedliche Organisationen sind direkt im Registrierungsprozess involviert • Schreiben mit RegPw kann in der sonstigen Versicherungs-korrespondenz verloren gehen
Registrierung mit ZertES-Zertifikat	• Registrierung und Konfiguration in einem Schritt möglich (kein Brief notwendig) • Registrierung für Unternehmen ohne Vertragsbeziehung mit V&B • Identifikation der Unternehmen entspricht den ZertES-Vorgaben • ZertES-akkreditierte Registration Authority • Nutzung der bereits vorhandenen Zertifikatsinfrastruktur • Keine Beteiligung der V&B nötig	• Aufwand zum Erhalt eines ZertES-basierten Zertifikats für Unternehmen sehr hoch • Verbreitung der ZertES-basierten Zertifikate eher gering und beschränkt auf Grossfirmen

6.2 Registrierung von Treuhändern

Ein Treuhänder muss sich nur für ein sUA-Zertifikat registrieren, wenn er in Stellvertretung für ein Unternehmen Daten an V&B schicken möchte und dies nicht direkt vom ERP des Unternehmens aus macht (in diesem Fall werden alle Nachrichten mit sUA-Zertifikat des Unternehmens signiert). Die Stellvertretung wird in diesem Fall organisatorisch vom Unternehmen geregelt und es bedarf keiner schriftlichen Vollmacht, die bei der Versicherung hinterlegt wird.

Hat der Treuhänder ein eigenes ERP-System, in dem er die Daten der von ihm verwalteten Unternehmen pflegt (verschiedene Mandanten), benötigt er ein sUA-Zertifikat.

Bei der Registrierung von Treuhändern müssen 2 Fälle unterschieden werden.

a) Der Treuhänder hat, wie andere Unternehmen auch bereits eine Vertragsbeziehung zu einer registrierenden Versicherung oder Behörde (V&B), auf deren Grundlage eine sUA-Registrierung durchgeführt werden kann. Dann durchläuft er den normalen Registrierungsprozess (siehe Kapitel 6.1.1).

[27] Die Adressinformationen werden nicht durch die V&B zur Verfügung gestellt, sondern werden gemäss dem alternativen Schritt 9 in Tabelle 8 direkt beim UID-BFS-Register bezogen und für den Versand des Briefes verwendet.

b) Der Treuhänder hat keine direkte Beziehung zu V&B, auf deren Grundlage eine sUA-Registrierung durchgeführt werden kann. In diesem Fall kann die Vertragsbeziehung eines von ihm verwalteten Unternehmen zur Registrierung verwendet werden. Dazu muss er in seinem ERP einen Registrierungsprozess starten und bei diesem zusätzlich zu den Vertrags-Angaben des Unternehmens, seine Angaben (Name des Treuhänders, UID, Kontaktinformation, ...) als sog. Delegate angeben. Die registrierende V&B prüft die Angaben von Unternehmen und Treuhänder sowie das Vorliegen einer Vollmacht. Im Unterschied zum normalen Registrierungsprozess, wird nun der Brief mit dem Registrierungspasswort zum Treuhänder geschickt, der dann auch sein Treuhänder-UID-Zertifikat konfiguriert, in seinem ERP hinterlegt und damit alle Nachrichten mit seinem sUA-Zertifikat signiert, die er im Namen der von ihm verwalteten Unternehmen verschickt.

6.3 Erstkonfigurationsprozess

6.3.1 Erstkonfiguration mit vorgängiger Registrierung

Der Erstkonfigurationsprozess startet im ERP mit der Auswahl eines Registrierungsvorganges (Eingabe von CRID und UID-BFS) für eine zuvor durchgeführte Registrierung (noch laufend oder erfolgreich abgeschlossen). Das ERP zeigt die SubjectInformationen für das UID-Zertifikat, die in der Registrierungsbestätigung enthalten war, dem zuständigen Mitarbeiter an.

Der zuständige Mitarbeiter prüft diese Informationen. Wurde der gewählte Registrierungsvorganges bereits abgeschlossen und hat der zuständige Mitarbeiter bereits den Brief mit dem Registrierungspasswort erhalten, kann die Konfiguration fortgesetzt werden.

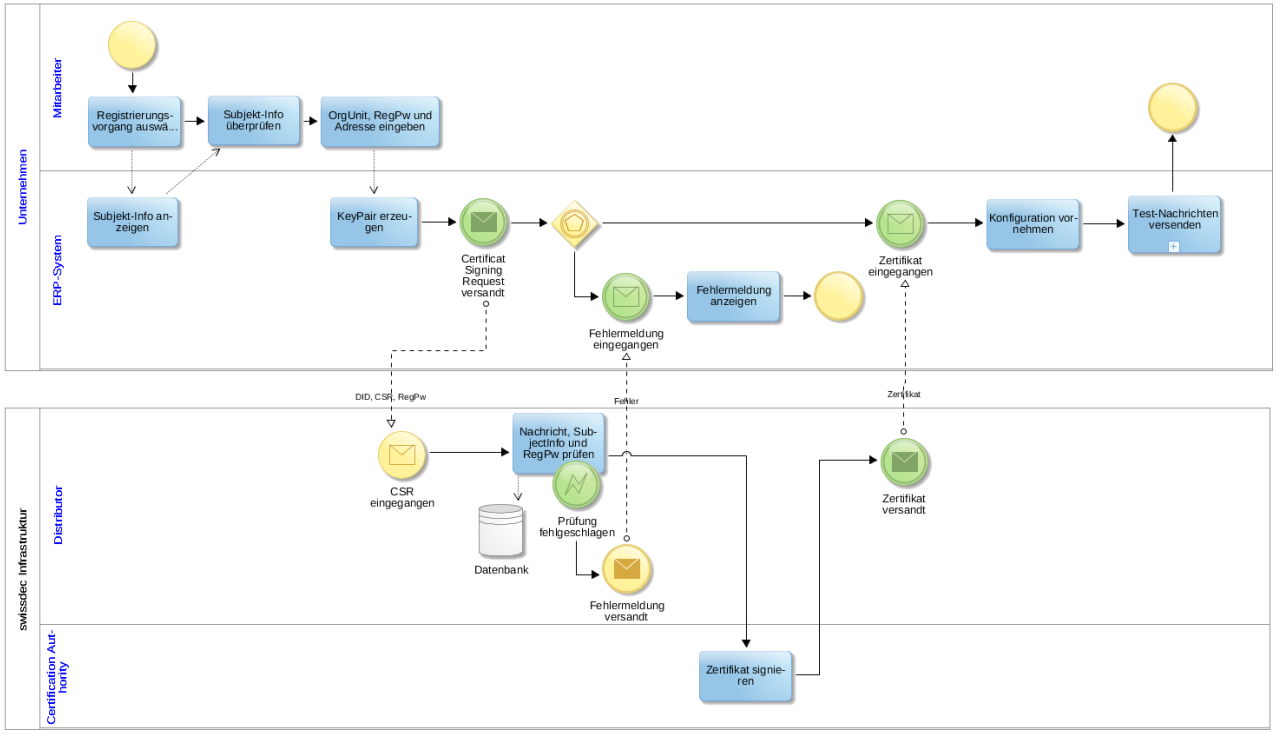

Abbildung 13: Erstkonfigurationsprozess

Im nächsten Schritt muss der zuständige Mitarbeiter das erhaltene Registrierungspasswort angeben. Zusätzlich kann er die Angaben zum Unternehmen für das UID-Zertifikat durch die Angabe einer Untereinheit (siehe auch Tabelle 2) ergänzen.

Das ERP-System erzeugt dann das KeyPair und sendet anschliessend einen Certificate Signing Request (CSR) zusammen mit dem Registrierungspasswort, der CRID und UID-BFS an den Distributor.

Der Distributor prüft die erhaltene Nachricht auf deren Gültigkeit (Signatur ERP-Zertifikat) sowie Vollständigkeit (notwendige Informationen zur Zertifikatserstellung) bzw. Konformität (Struktur des CSR) und verifiziert das mitgelieferte Registrierungspasswort in Kombination mit der Registrierungsnummer. Die im CSR enthaltene SubjectInformationen wird mit den bei der Registrierung gespeicherten Unternehmensdaten abgeglichen. Ein

Misserfolg dieser Prüfungen wird unmittelbar dem ERP-System mittels entsprechender Fehlermeldung mitgeteilt und der Prozess abgebrochen.
Hat der Distributor einen gültigen CSR erhalten, so wird dieser direkt an die Certification Authority (CA) gesendet, welche das Zertifikat automatisiert signiert und an den Distributor zurücksendet.
Der Distributor sendet das signierte Zertifikat an das ERP-System, welches von diesem integriert wird.
Sobald das erhaltene UID-Zertifikat ins ERP-System integriert wurde, kann dessen korrekte Funktionsweise mit Hilfe von CheckInteroperability-Nachrichten überprüft werden. Nach einem erfolgreichen Test wird das verwendete Registrierungspasswort ungültig gemacht.

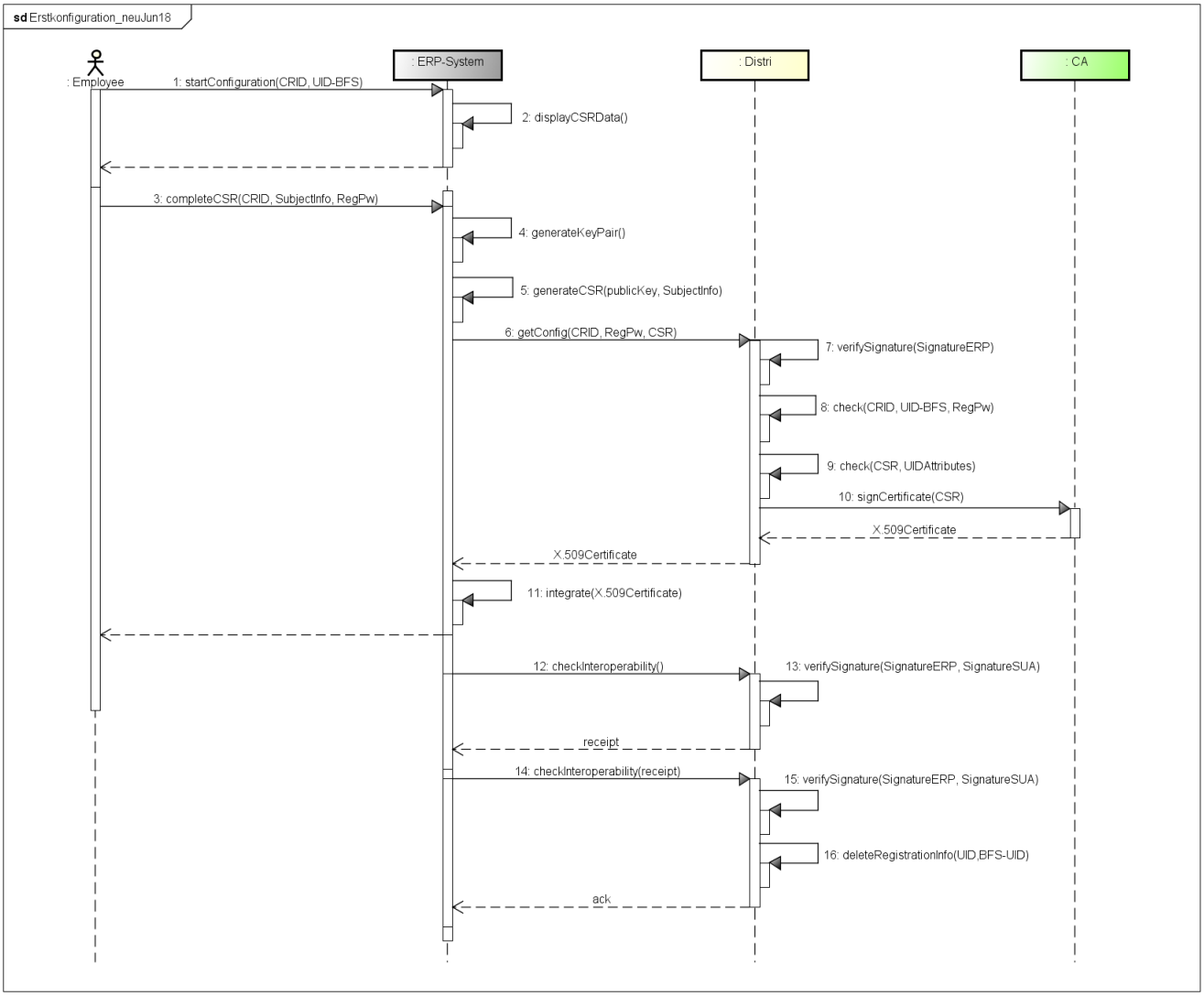

Abbildung 14: Sequenzdiagramm Erstkonfigurationsprozess

Tabelle 10: Beschreibung der Einzelschritte im Erstkonfigurationsprozess

Nr.	Beschreibung
1	**startConfiguration(CRID, UID-BFS):** Der Konfigurationsprozess wird direkt im ERP-System angestossen. Ein verantwortlicher Mitarbeiter wählt im ERP-System die CRID und die UID-BFS, für die eine erfolgte Registrierung vorliegt.
2	**displayCSRData():** Das ERP-System zeigt die erhaltenen Informationen zum CSR dem Benutzer an.
<--	Das ERP zeigt den erhaltenen Status dem Benutzer an.
3	**completeCSR(CRID, SubjectInfo, RegPw):** Der Benutzer übergibt die komplettierten SubjectInformation (die Daten kommen aus dem UID-Register

	des BFS und nur die Untereinheit der Organisation kann ergänzt werden, siehe auch Tabelle 2) zusammen mit dem RegPw.
4	**generateKeyPair():** Das ERP-System generiert das Schlüsselpaar (Private und Public Key) gemäss den Vorgaben aus Abschnitt 5.3.
5	**generateCSR(publicKey, SubjectInfo):** Das ERP-System erstellt einen CSR (Certificate Signing Request) gemäss den Vorgaben in Tabelle 3.
6	**getConfig(CRID, RegPw, CSR):** Das ERP-System sendet einen Request an den Distributor. Dieser enthält die CRID, den CSR und das RegPw.
7	**verifySignature(SignatureERP):** Der Distributor prüft die Signatur der Nachricht auf ihre Gültigkeit sowie die Kompatibilität zur Version des SUA-Standards.
8	**check(CRID, UID-BFS, RegPw):** Der Distributor überprüft die Gültigkeit des RegPw in Kombination mit der entsprechenden UID-BFS und der CRID mittels der Daten aus der Datenbank.
9	**check(CSR, UIDAttribute):** Der vom ERP-System erstellte CSR wird auf seine strukturelle Übereinstimmung mit den Vorgaben des SUA-Standards (Abschnitt 5.1.6) überprüft. Ausserdem werden die darin enthaltenen SubjectInformation mit den Informationen aus der Datenbank des Distributors verglichen. Wird eine Abweichung von den Vorgaben oder ein Unterschied zu den beim Distributor abgelegten Informationen festgestellt, erhält das ERP-System eine entsprechende Fehlermeldung.
10	**signCertificate(CSR):** Der CSR wird vom Distributor an die CA gesendet. Die konkrete Ausgestaltung dieser Schnittstelle und der übermittelten Daten muss mit der gewählten CA abgestimmt werden.
<--	Die CA antwortet mit dem signierten X.509 Zertifikat.
<--	Der Distributor sendet als Response dem ERP-System das signierte Zertifikat (X.509Certificate) als Base64-kodiertes Zertifikat (PEM).
11	**integrate(X.509Certificate):** Das ERP-System integriert das X.509 Zertifikat.
12	**checkInteroperability():** Nachdem das Zertifikat erfolgreich vom ERP-System integriert wurden, schickt dieses eine eine checkInteroperability-Message an den Distributor geschickt.
13	**verifySignature(SignatureERP, SignatureSUA):** Der Distributor prüft die Signaturen der Nachricht. Diese muss gemäss der Spezifikation zur Signatur und Verschlüsselung mittels ERP-Zertifikat und UID-Zertifikat korrekt signiert sein.
<--	Hat der Distributor die Nachricht erfolgreich überprüft, sendet er dem ERP-System eine entsprechende Quittung (receipt).
14	**checkInteroperability(receipt):** Damit der Distributor überprüfen kann, dass das ERP-System neben dem Senden auch in der Lage ist zu empfangen, sendet dieses die erhaltene Quittung (receipt) in einer zweiten Nachricht zurück an den Distributor.
15	**verifySignature(SignatureERP, SignatureSUA):** siehe Schritt 13.
16	**deleteRegistrationInfo(CRID, UID-BFS, RegPw):** Wurde die zweite Testnachricht erfolgreich verifiziert, werden alle Informationen zum Registrierungsvorgang (u.a. RegPw) vom Distributor aus der Datenbank gelöscht.
<--	**ack:** Der Distributor bestätigt den Erhalt der zweiten Testnachricht gegenüber dem ERP-System.

6.3.2 Option: Distributor generiert Schlüsselpaar und Zertifikat

Während der Ausarbeitung der vorliegenden Detailspezifikation wurde eine Option ausgearbeitet, welche es zulassen würde, dass der Distributor zentral das Schlüsselmaterial generiert und das UID- Zertifikat erstellt, wenn das ERP aus technischen Gründen nicht dazu in der Lage ist. Das UID-Zertifikat würde dann auf elektronischem Wege an das ERP-System gesendet und dort lediglich integriert. Weitere Details finden sich im entsprechenden Zusatzdokument „Swissdec Unternehmens-Authentifizierung – Detailspezifikation Distributor generiert Schlüsselpaar und Zertifikat".
Das Schlüsselmaterial und speziell der private Schlüssel werden ausserhalb des zu dessen Nutzung vorgesehenen Systems generiert, was bezüglich der Sicherheit mit wesentlichen Nachteilen verbunden ist:

- Das Schlüsselmaterial muss in elektronischer Form übertragen werden.
- Das Schlüsselmaterial sowie das Zertifikat müssen in einem geeigneten Containerformat gespeichert und vor unberechtigtem Zugriff geschützt werden.
- Das Registrierungspasswort wird neben der Authentifizierung im Rahmen des Konfigurationspasswortes zusätzlich zur Verschlüsselung der Container-Datei verwendet, was zusätzliche Anforderung an dessen Ausgestaltung mit sich bringt.
- Das Handling und die Zwischenspeicherung der Container-Datei birgt zusätzliche Sicherheitsrisiken, welche sowohl durch technische aber auch organisatorische Vorgaben gemindert werden müssen.

Ausserdem unterstützen die in der grossen Mehrheit der ERP-Systeme verwendeten Standard-Frameworks das Generieren eines Schlüsselpaars sowie das Erstellen eines entsprechenden CSR. Dies macht die Implementierung auf Seiten der EPR-Systeme relativ einfach. Zusätzlich kann dies durch die Bereitstellung von entsprechenden Code-Samples unterstützt werden.

6.3.3 Option: Konfiguration mit automatischer Registrierung (Massenversand)

Ausserdem wurde die Option einer automatischen Registrierung mit Hilfe eines Massenversands von Registrierungsbriefen durch die V&B ausgearbeitet und geprüft. Die entsprechenden Ergebnisse finden sich im separaten Dokument „Swissdec Unternehmens-Authentifizierung – Detailspezifikation Massenversand".
Aus den folgenden Gründen wurde diese Option als ungeeignet eingestuft und damit nicht mehr weiterverfolgt:

- Aus Sicherheitsgründen muss der Anstoss für die Teilnahme an der Swissdec Unternehmens-Authentifizierung und damit für die Zustellung eines Registrierungspasswortes immer von einem Unternehmen und damit einem ERP-System ausgehen. Damit kann davon ausgegangen werden, dass die notwendige Information und Sensibilisierung für den Ablauf des Registrierungs- und Konfigurationsprozesses bei den verantwortlichen Personen im Unternehmen vorhanden ist.
- Sofern ein Unternehmen sich nicht aus eigenem Antrieb heraus für die SUA registriert, ist nicht abzuschätzen, wann ein versendetes Registrierungspasswort tatsächlich genutzt wird. Daher müsste die Gültigkeit eines auf diese Weise versendeten RegPw länger ausgelegt werden, was wiederum das Risiko eines Missbrauches erhöht.
- Werden Registrierungspasswörter über einen Massenversand durch die V&B versendet, ist nicht auszuschliessen, dass ein und dasselbe Unternehmen mehrere gültige Briefe mit unterschiedlichen Registrierungspasswörtern erhält. Gemäss Abschnitt 5.4 existiert aber zu einem spezifischen Zeitpunkt nur ein gültiges Registrierungspasswort pro Unternehmen bzw. UID-BFS.

6.3.4 Option: Konfiguration mit Hard-Token

Da die Erstellung des Schlüsselpaares für das UID-Zertifikat immer auf Seiten des Unternehmens erfolgt, wird das Swissdec Zertifikat als Soft-Token in der sicheren Umgebung des ERP-Systems abgespeichert oder auf einer zertifizierten Hardwarekomponente (Crypto-Token oder HSM) erstellt und abgelegt. In beiden Fällen unterscheidet sich der Registrierungsprozess aus Sicht Swissdec und ausstellende CA aber nicht grundlegend.
Für die Ausstellung, die Revozierung und Erneuerung eines Swissdec UID-Zertifikats ist die Certificate Authority verantwortlich. Im Fall eines Hard-Tokens ist die konkrete Ausgestaltung und technische Umsetzung mit der verantwortlichen CA abzuklären. Unabhängig der Form des Tokens nimmt Swissdec die Rolle der Registration Authority ein, in dem die unterschiedlichen Varianten des Registrierungsprozesses gemäss Abschnitt 6.1 vorgängig durchgeführt werden müssen.
Aufgrund des erhöhten Sicherheitsniveaus beim Einsatz eines Hard-Tokens ist es möglich, die Gültigkeit des darin verankerten Zertifikats zu verlängern. Ist beim Soft-Zertifikat eine dreimalige automatische Erneuerung für ein Jahr vorgesehen, so soll dies beim Einsatz eines Hard-Tokens max. drei Jahre genutzt werden können. Nach Ablauf der drei Jahren, ist aber auch beim Hard-Token eine erneute Überprüfung der Identität des Unternehmens mittels Neu-Registrierung notwendig.
Der Konfiguration-Prozess ist damit sehr ähnlich, wie in Kapitel 6.2.1, nur das die CA das Hard-Token an das Unternehmen versendet. Das Unternehmen muss dieses dann für eine ERP-System verfügbar machen. Zum Testen der korrekten Konfiguration des ERP-Systems können die in Kapitel 6.2.1 Tabelle 10 Schritte 12-16 beschriebenen

checkInteroperability-Nachrichten verwendet werden. Mit dem Austausch dieser Nachrichten wird der Prozess beendet und damit auch sichergestellt, dass das Hard-Token korrekt installiert wurde.
Dieser Prozess funktioniert auch für Token in HSM-Modulen, wobei es in der Verantwortung der Unternehmen liegt, sicherzustellen, dass das ERP-System Zugriff auf das Schlüsselmaterial hat.
Die Vor- und Nachteile dieser Variante sind in Tabelle 11 aufgeführt.

Tabelle 11: Vor- und Nachteile von Hardtoken

Vorteile	Nachteile
• Zertifikat und damit Keys werden auf einem sicheren Hardware Device gelagert • Zwei-Faktor-Authentifizierung (Token plus PIN) • Ausgabe und Management des Hard-Tokens liegt ausschliesslich bei der CA	• ERP-Systeme müssen den Hard-Token unterstützen (physische Schnittstelle, ERP in der Cloud) • PIN Handling: pro Zertifikatsnutzung eingeben oder Zwischenspeicherung (Caching)

6.4 Laufzeitprozesse am Beispiel Leistungsstandard-CH (KLE)

Die Verwendung des UID-Zertifikats wird beispielhaft an den Laufzeitprozessen des Leistungsstandards-CH (KLE) gezeigt.

6.4.1 Ereignismeldung

Ein Ereignis (Incident) wird von dem Unternehmen einer zuständigen Versicherung & Behörde mitgeteilt. Hierzu dient die Ereignismeldung direkt im ERP-System. Es ist möglich, in einer Ereignismeldung direkt mehrere Versicherungen & Behörden zu adressieren und diesen die jeweils erforderlichen Informationen zukommen zu lassen.
Das nachfolgende Sequenzdiagramm zeigt den Ablauf einer Ereignismeldung nach dem Leistungsstandard-CH. Sowohl in der Darstellung, als auch in der nachfolgenden Beschreibung, wird explizit ein Fokus auf die im Kontext der Swissdec Unternehmens-Authentifizierung relevanten Punkte gelegt. Die fachlich spezifischen Informationen des Prozesses finden sich in der entsprechenden Dokumentation zum Leistungsstandard-CH.

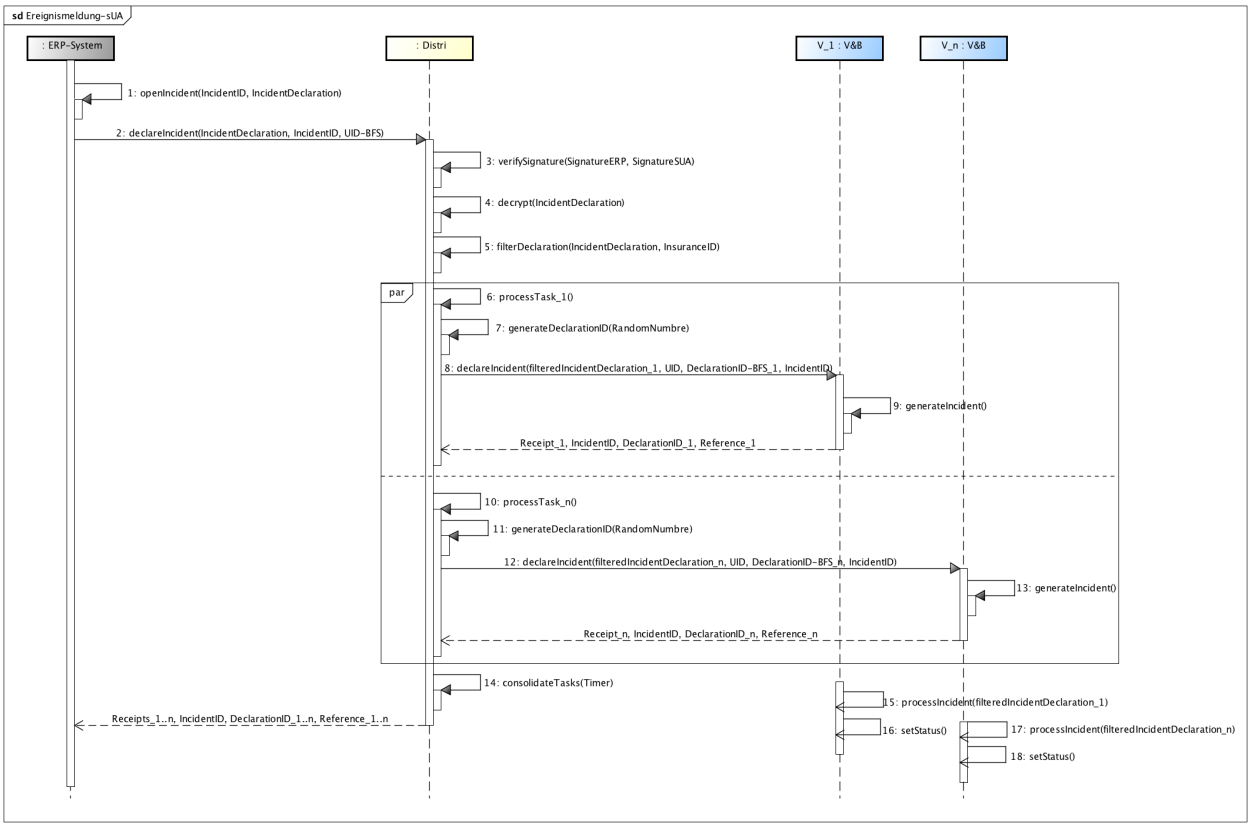

Abbildung 15: Ereignismeldung Leistungsstandard-CH (KLE) mit SUA

Tabelle 12: Beschreibung der Einzelschritte für die Ereignismeldung im Leistungsstandard-CH mit SUA

Nr.	Beschreibung
1	**openIncident(IncidentID, IncidentDeclaration):** Im ERP-System wird ein neues Ereignis angelegt und eine entsprechende Identifikationsnummer (IncidentID) vergeben. Die für die V&B relevanten Informationen werden in einer IncidentDeclaration erfasst.
2	**declareIncident(IncidentDeclaration, IncidentID, UID-BFS):** Ist die IncidentDeclaration vollständig erfasst, kann diese via Distributor an die jeweils adressierten Versicherer oder Behörden gesendet werden. Zusätzlich werden die IncidentID und die UID-BFS übermittelt.
3	**verifySignature(SignatureERP, SignatureSUA):** Der Distributor prüft die Signaturen der Nachricht. Diese muss gemäss der Spezifikation zur Signatur und Verschlüsselung mittels ERP-Zertifikat und UID-Zertifikat korrekt signiert sein.
4	**decrypt(IncidentDeclaration):** Der Distributor entschlüsselt den Inhalt der gesendeten Nachricht.
5	**filterDeclaration(IncidentDeclaration, InsuranceID):** Um Redundanz in der Kommunikation zu vermeiden, werden die jeweiligen Daten nur einmal in der IncidentDeclaration gesendet. Der Distributor bereitet die gesendeten Daten für jeden Empfänger individuell auf, so dass nur die für den Empfänger relevanten Teile der Nachricht an diesen weitergeleitet werden. Die InsuranceID identifiziert dabei die einzelnen Endempfänger der gesendeten IncidentDeclaration.
6 / 10	**processTask():** Vom Distributor wird für jede weiterzuleitende Nachricht ein separater Task gestartet. Hierbei ist die Anzahl der Tasks abhängig von der Anzahl in der IncidentDeclaration erfassten Endempfänger.
7 / 11	**generateDeclarationID(RandomNumber):** Der Distributor generiert für jede zu versendende Nachricht eine individuelle und im Kontext der Swissdec Geschäftsprozesse eindeutige Identifikationsnummer, eine DeclarationID.
8 / 12	**declareIncident(filteredIncidentDeclaration_1..n, UID-BFS, DeclarationID_1..n, IncidentID):** Die pro Endempfänger zusammengestellten Informationen (filteredIncidentDeclaration) werden zusammen mit der UID-BFS der Unternehmen der entsprechenden DeclarationID sowie der IncidentID an den Endempfänger gesendet. Die Nachricht wird vom Distributor signiert und mit dem Public Key des Endempfängers verschlüsselt.
10 / 13	**generateIncident():** Der Versicherer oder die Behörde verarbeiten die erhaltene Nachricht.
<--	Als Antwort wird ein Receipt, das die IncidentID, die DeclarationID sowie eine Reference enthält, zurückgegeben. • Reference: Fallnummer der Versicherung oder Behörde.

Nr.	Beschreibung
14	**consolidateTasks(Timer):** Sofern mit einer IncidentDeclaration mehrere Tasks durch den Distributor erstellt worden sind, fasst dieser die einzelnen Antworten der beteiligten Endempfänger zusammen. Hierbei müssen die einzelnen Antworten innerhalb eines vorgegebenen Zeitfensters (Timer) beim Distributor eintreffen. Treffen die Antworten nicht im vorgegebenen Zeitraum beim Distributor ein, so wird der Prozess abgebrochen und eine Fehlermeldung an das ERP-System gesendet. Die Ereignismeldung muss in diesem Fall noch einmal gesendet werden.
<--	Der Distributor sendet alle erhaltenen Receipts, IncidentID, DeclarationIDs und References zurück an das ERP-System. Dadurch wird der erfolgreiche Abschluss der Ereignismeldung bestätigt. Die Meldung wird vom Distributor signiert und mit dem Public Key des ERP-Systems (UID-Zertifikat) verschlüsselt.
15 / 17	**processIncident(filteredIncidentDeclaration):** Unabhängig von der Ereignismeldung wird der jeweils beim Endempfänger eröffnete Incident weiterverarbeitet.
16 / 18	**setStatus():** Im weiteren Verlauf der Bearbeitung des Incident kann die Versicherung oder Behörde jeweils einen der vorgegebenen Status setzen. Dieser wird im Rahmen eines Kommunikationsaufrufs durch das ERP-System des Unternehmens, diesem jeweils mitgeteilt.

6.4.2 Polling

Ist eine Ereignismeldung erfolgt, wird für den weiteren Verlauf der Verarbeitung des Incidents eine Eins-zu-Eins-Kommunikation zwischen dem ERP-System des Unternehmens und dem jeweiligen Endempfänger (V&B) etabliert. Obwohl weiterhin jegliche Kommunikation über den Distributor verläuft, wird jeweils nur ein spezifischer Endempfänger durch das ERP-System adressiert. Wie im Leistungsstandard-CH (KLE) festgehalten wird hierzu ein Polling-Verfahren[28] angewendet. Der Distributor agiert dabei als sogenannter Security Endpoint gegenüber den verschiedenen V&B. Er authentifiziert jede von einem Unternehmen versendete Nachricht mit Hilfe der Signatur des UID-Zertifikats und ist gegenüber den Unternehmen für die Verschlüsselung der von den V&B gesendeten Antwortmeldungen verantwortlich.

[28] Die Kommunikationsstruktur von Swissdec beruht auf einer doppelten Client-Server-Kommunikation (ERP -> Distributor und Distributor -> V&B). Eine Konsequenz daraus ist, dass V&B keinen Nachrichtenaustausch initiieren kann. Damit trotzdem Nachrichten von V&B das ERP erreichen können, pollt dieses (und auch der Distributor) in regelmässigen Abständen die V&B-Systeme.

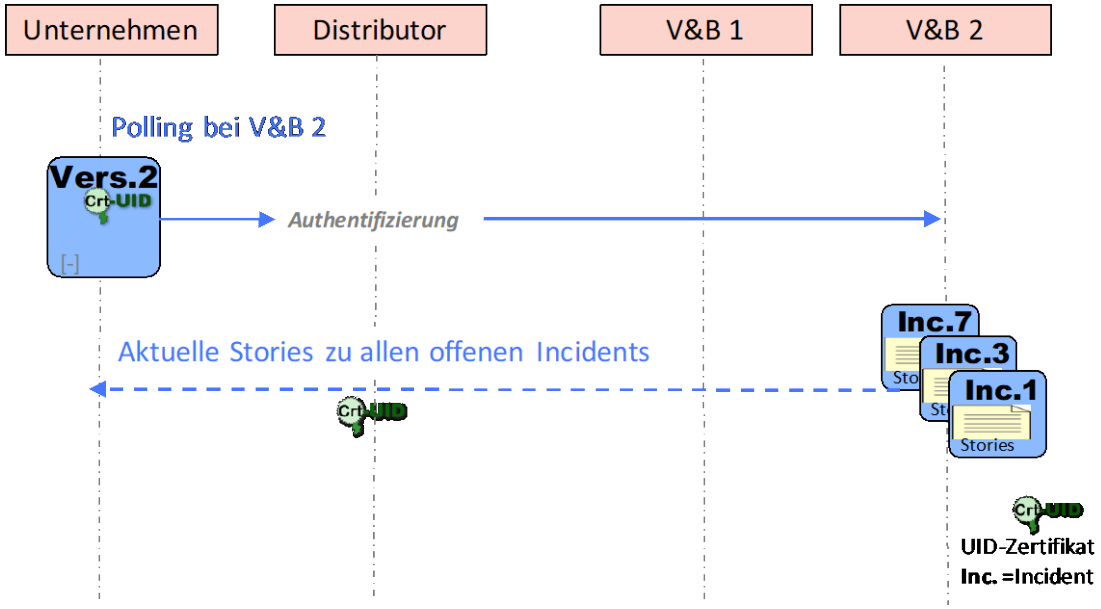

Abbildung 16: Polling Verfahren (schematisch)

Durch die Verwendung der Swissdec Unternehmens-Authentifizierung ist garantiert, dass in der Kommunikation zwischen ERP-System und V&B die Unternehmen als Absender jederzeit eindeutig identifizierbar sind und dadurch die Kommunikation möglichst effizient ausgestaltet werden kann. Es ist dadurch möglich, dass als Antwort (Response) auf einen Aufruf durch das ERP-System (Request), Daten zu verschiedenen bei einem Endempfänger aktiven Incidents an das ERP-System gesendet werden können. In diesem können dann die jeweiligen Informationen oder Anforderungen im Kontext des entsprechenden Incidents direkt bearbeitet werden.

6.4.3 Stellvertretung

Gemäss den im Rahmen des Lösungskonzeptes zur Swissdec Unternehmens-Authentifizierung festgelegten Anforderungen muss eine Stellvertretung eines Unternehmens z.B. durch einen Treuhänder möglich sein (A-13). Ebenfalls wurde bereits im Lösungskonzept in Anforderung 14 (A-14) festgelegt, dass die Verifizierung der Gültigkeit einer solchen Stellvertretung im Rahmen der Kommunikation zwischen ERP-System und Endempfänger den V&B obliegt.
Demnach hat dies keinerlei Auswirkung auf die oben beschriebenen Registrierungs- und Erstkonfigurationsprozesse. Ein Stellvertreter registriert sich unter seiner eigenen UID-BFS gemäss dem vorgesehenen Prozess und kann nach der Konfiguration im Name eines anderen Unternehmens Daten via Distributor an einen V&B senden. Dieser muss anhand des Inhalts und des Absenders der enthaltenen Daten prüfen, ob eine legitime Stellvertretung vorliegt und damit eine Weiterverarbeitung der Daten stattfindet kann.

6.5 Erneuerung

Der Erneuerungsprozess für die UID-Zertifikate (nur Soft-Token) verläuft analog zum Erstkonfigurationsprozess (Abschnitt 6.2.1). Lediglich folgende Punkte sind davon abweichend:

- Der Prozess muss nicht mittels Eingabe eines Registrierungspasswortes angestossen werden, sondern wird automatisch ausgelöst, sobald die Gültigkeitsdauer des aktuell verwendeten UID-Zertifikats weniger als 30 Tage beträgt. Hierbei wird der Prozess so oft vom ERP-System angestossen, bis ein neues gültiges Zertifikat ausgestellt und integriert wurde.
- Das initial erhaltene Sperrpasswort bleibt auch nach der Erneuerung des UID-Zertifikats weiterhin gültig, so dass vom Distributor kein weiterer Brief mit einem Sperrpasswort versendet wird.
- Für die gesamte Kommunikation im Rahmen des Erneuerungsprozesses wird noch das gültige Schlüsselmaterial (UID-Zertifikat) verwendet. Erst nach Abschluss der Konfiguration mit dem neuen erstellten Zertifikat wird eine entsprechende Testnachricht mit diesem versendet, welches ab diesem Zeitpunkt weiter genutzt wird.
- Um sicherzustellen, dass sich die Angaben zum Unternehmen (Name, Land, Stadt), die auch im UID-Zertifikat verankert sind, nicht verändert haben, fragt der Distributor auch des UID-Register des BFS mit der BFS-UID des Unternehmens an. Stimmen die Angaben im UID-Register nicht mit den Angaben im alten UID-

Zertifikat überein, wird die Erneuerung mit einer Fehlermeldung abgebrochen und es muss ein erneuter Registrierungsprozess (siehe Kapitel 6.1) angestossen werden.

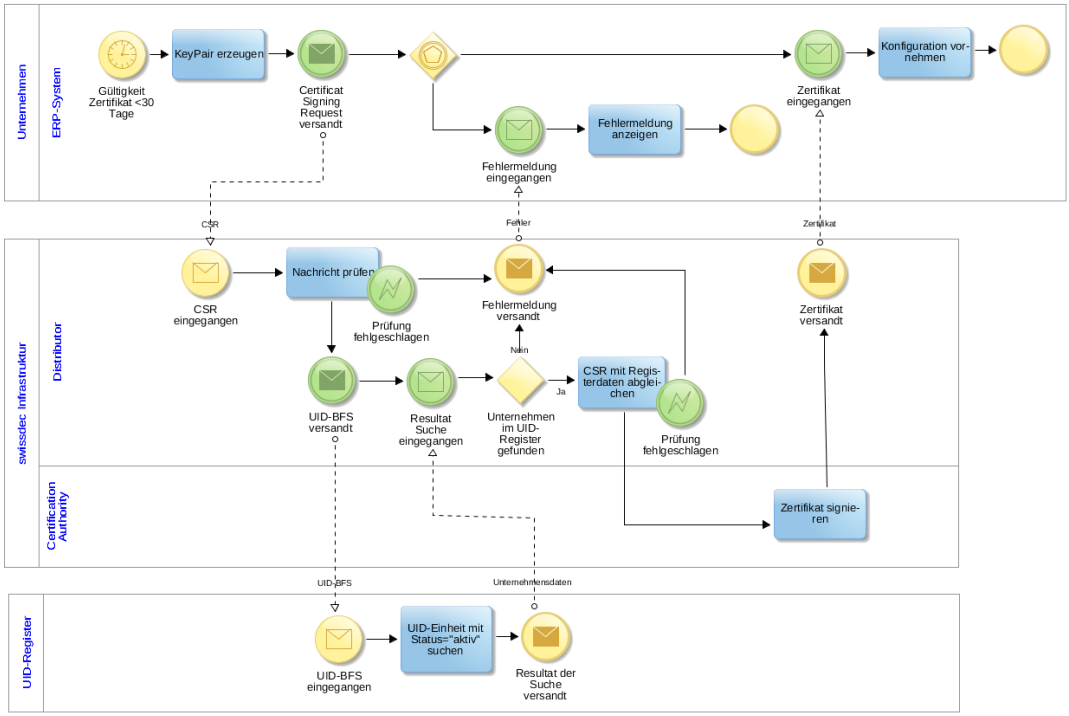

Abbildung 17: Erneuerungsprozess

Da es sich um einen automatisierten Prozess handelt, ist es notwendig, dass regelmässig eine Überprüfung der Aktualität und Authentizität des Unternehmens stattfindet. Daher ist die automatische Erneuerung eines UID-Zertifikats auf eine dreimalige Erneuerung beschränkt. Nachdem das ERP-System drei Mal ein neues Zertifikat automatisch bezogen hat, wird das Unternehmen aufgefordert den Registrierungsprozess von neuem zu starten und seine Identität von eine V&B mittels einer aktuellen Vertragsbeziehung bestätigen zu lassen.

Bei einem Wechsel des SUA-Zertifikates kann es zu Problemen bei langlaufenden Prozessen, z.B. beim Leistungsstandard (KLE) kommen. Durch einen turnusgemässen Zertifikatswechsel kann es dazu kommen, dass Ergebnisse zu einer Ereignismeldung mit neuerem Schlüsselmaterial verschlüsselt werden müssen, als die ursprünglich erste Meldung verlangte. Der Distributor muss damit entsprechend umgehen können.

6.6 Sperrung

Im Falle eines befürchteten oder erfolgten Missbrauchs eines UID-Zertifikats ist eine Sperrung möglich. Hierfür wird das Sperrpasswort verwendet, welches dem Unternehmen im Rahmen des Registrierungsprozesses per Brief zugestellt wurde.
Die Sperrung eines UID-Zertifikats erfolgt in der Regel durch den Inhaber selbst. In Ausnahmefällen kann auch Swissdec eine Sperrung vornehmen, wenn vor Ablauf des regulären Gültigkeitszeitraumes ein Unternehmen vom Swissdec Funktionsangebot ausgeschlossen werden muss. Die Sperrung erfolgt in zwei Phasen. In einer ersten Phase autorisiert sich ein Mitarbeiter eines Unternehmens gegenüber Swissdec, um die Sperrung eines UID-Zertifikats anzustossen. Swissdec sperrt nach erfolgter Prüfung des Antrags unverzüglich das UID-Zertifikat auf dem Distributor. Erst in einer zweiten Phase wird der Sperrungsantrag an die zuständige CA weitergeleitet.
Da jede authentifizierte Swissdec-Funktion mit der Sperrung auf dem Distributor sofort unterbunden wird, ist eine Statusprüfung (‚Certificate Revocation List' oder ‚Online Certificate Status Protocol') durch die Teilnehmer nicht notwendig.

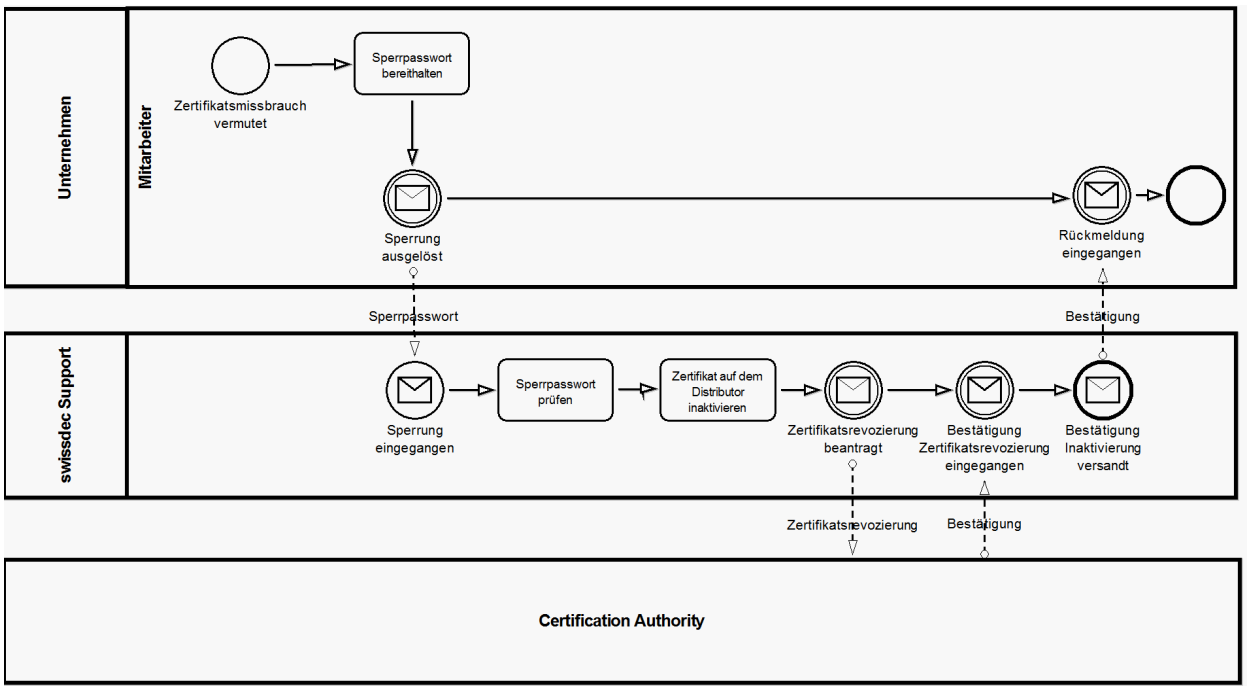

Abbildung 18: Sperrprozess

Ein berechtigter Mitarbeiter des Unternehmens löst die Sperrung aus, indem er den Swissdec Support kontaktiert und dort das Sperrpasswort zur Identifikation angibt. Der Support überprüft das Sperrpasswort und bietet dem Unternehmen Unterstützung. Sofern tatsächlich von einem Missbrauch des Zertifikats ausgegangen werden muss, inaktiviert/sperrt der Support das entsprechende Zertifikat direkt auf dem Distributor und veranlasst die Revozierung des Zertifikats bei der CA. Dem Mitarbeiter des Unternehmens wird bestätigt, dass das betroffene Zertifikat revoziert wurde.
Sofern dem betroffenen Unternehmen das Sperrpasswort nicht mehr vorliegt, oder dieses nicht zugänglich ist, muss die Legitimität des Mitarbeiters zunächst geklärt werden. Hierfür wird individuell mit Hilfe einer fachspezifischen Selbstauskunft und der Hinzunahme einer V&B geprüft, ob die anrufende Person im Namen des betroffenen Unternehmens das Zertifikat sperren darf oder nicht.
Es ist zu beachten, dass die Sperrung eines Zertifikates nicht mehr rückgängig gemacht werden kann. Damit ein Unternehmen, nach durchgeführter Sperrung, wieder mit dem Distributor kommunizieren kann, ist eine neue Registrierung (gemäss Abschnitt 6.1) notwendig.

6.7 Fehler- und Exception-Handling

In den unter Kapitel 6 beschriebenen SUA Prozess wurde in den Sequenzdiagrammen jeweils das Hauptaugenmerk auf den Positivfall eines bestimmten Prozessablaufes gelegt. Die korrespondierenden BPMN-Prozessdarstellungen weisen bestimmte Fehlerfälle aus, wenn diese aus dem Prozessablauf heraus entstehen, nicht aber technische Problematiken wiederspiegeln. An dieser Stelle soll kurz auf das grundsätzliche Fehler- und Exception Handling im Kontext der SUA Prozesse eingegangen werden.
Jeder Prozessschritt und jeder Kommunikationsverlauf können potenziell fehlerbehaftet sein oder zu einem nicht intendierten Ergebnis bzw. Zustand führen. Tritt ein solches Verhalten ein, so sind alle beteiligten Kommunikationsteilnehmer der SUA Unternehmens-Authentifizierung gehalten, dem Absender eines Request eine Exception zurückzugeben. Diese beinhaltet die entsprechende Information zum aufgetretenen Fehler und kann durch den anderen Kommunikationspartner angemessen abgefangen und behandelt werden.

7 Dynamische Bestandteile der Spezifikation

Verschiedene Elemente der SUA Credentials (Kapitel 5) und der SUA Prozesse (Kapitel 6) wurden in der Spezifikation festgelegt, haben aber grundsätzlich einen dynamischen Charakter. Nachfolgende Tabelle 13 gibt einen Überblick über diese Elemente, den Kontext, in welchem sie Verwendung finden sowie ihre aktuelle festgelegte Ausprägung. Da sich die jeweils festgelegte Ausprägung auf dem aktuellen Kenntnisstand beruht, ist es angebracht, diese im Rahmen der auf die Spezifikation nachgelagerten Pilotierung sowie auch einer späteren Implementierung zu überprüfen. Auf der Grundlage neuer Erkenntnisse aus der Umsetzung und Nutzung der Swissdec Unternehmens-Authentifizierung können diese dann regelmässig angepasst werden.

Tabelle 13: Dynamische Elemente in der Spezifikation

Kontext	Element	Ausprägung
UID-Zertifikat	Zertifikat Crypto-Algorithmus	SHA256 with RSA Encryption
	Schlüssellänge (key size)	2048 bit
	Gültigkeitszeitraum des Zertifikats	1 Jahr Mit HardToken: 3 Jahre
Registrierungspasswort	Passwortlänge	12 Zeichen + 2 Zeichen für Kennzeichen + 2 Zeichen Prüfziffer
	Gültigkeitszeitraum des RegPw	Maximal 30 Tage
Sperrpasswort	Passwortlänge	12 Zeichen + 2 Zeichen für Kennzeichen + 2 Zeichen Prüfziffer
	Gültigkeitszeitraum des SperrPw	unbegrenzt
Erneuerungsprozess	Zeitraum vor Ablauf des Zertifikats, ab welchem das ERP-System mit der Erneuerung startet.	30 Tage
	Anzahl möglicher automatischer Erneuerungen	3
Registrierungsprozess	Anzahl aktiver Registrierungs-Anfragen	5
Registrierungsprozess	Zweiter, nicht elektronsicher Kanal	Eingeschriebener Brief/ A-Post Plus

8 Übereinstimmung mit den Anforderungen aus dem Lösungskonzept

Im Rahmen des Lösungskonzeptes zur Swissdec Unternehmens-Authentifizierung wurden Anforderungen an dessen Ausgestaltung formuliert. Die vorliegende Detailspezifikation hat sich an den formulierten Anforderungen orientiert und diese bei der konkreten Ausarbeitung weitestgehend berücksichtigt.
Nachfolgende Tabelle 14 gibt noch einmal einen Überblick über die im Lösungskonzept festgehaltenen Anforderungen. Die letzte Spalte gibt an, inwiefern die einzelnen Anforderungen in der Detailspezifikation umgesetzt wurden. Ein „✓“ bedeutet vollständige Umsetzung der Anforderung, „(✓)“ eine teilweise oder nicht explizite Berücksichtigung der Anforderung und „x“ weist darauf hin, dass die entsprechende Anforderung im Rahmen der Detailspezifikation nicht berücksichtigt werden konnte.

Tabelle 14: SUA-Lösungskonzept - Anforderungen

ID	Bezeichnung	Beschreibung	Prio	
A-01	Ausstellung UID-Zertifikat	Ist ein Unternehmen eindeutig identifiziert, stellt eine CA Zertifikate auf der Basis der Unternehmensidentifikationsnummer (UID) aus.	MUSS	✓
A-02	Ausstellung Hersteller-zertifikat	Der Distributor prüft die Geschäftsprozessfähigkeit eines ERP-Systems mittels eines für den ERP-Hersteller spezifischen Zertifikats.	MUSS	✓
A-03	Certification Authority (CA)	Um die Vertrauenswürdigkeit der verwendeten Zertifikate zu gewährleisten, garantiert die Certification Authority (CA) eine den Geschäftsprozessen angemessene Qualität ihrer Zertifikate und Prozesse.	MUSS	✓
A-04	Zuordnung UID Zertifikat	Ein UID-Zertifikat beinhaltet nur eine UID.	MUSS	✓
A-05	Zertifikate pro UID	Einer UID können mehrere Zertifikate zugeordnet werden. (Zertifikatserneuerung, mehrere ERP-Instanzen)	MUSS	✓
A-06	UID-Zertifikats-laufzeit	Wird von der CA ein UID-Zertifikat ausgestellt, ist dieses für einen beschränkten Zeitraum (min. 1 Jahr) gültig.	MUSS	✓
A-07	UID-Zertifikats-erneuerung	Ist das Ende der Zertifikatslaufzeit erreicht, bezieht das ERP-System automatisch ein neues Zertifikat bei der CA.	MUSS	✓
A-08	UID-Zertifikat revozieren	Im Falle eines Missbrauchs von Zertifikaten werden diese durch die CA unmittelbar revoziert.	MUSS	✓
A-09	Registrierungs-stelle	Unternehmen registrieren sich bei einer von Swissdec autorisierten Stelle.	MUSS	✓
A-10	Eindeutige Identifikation des Unternehmens	Will sich ein Unternehmen registrieren, identifiziert die von Swissdec autorisierte Stelle dieses eindeutig, gemäss einem vorgegebenen Prozess.	MUSS	✓
A-11	Identifikation durch autorisierte Stelle	Ein Unternehmen wird mittels fachspezifischer Selbstauskunft oder einem zweiten sicheren Kanal von der von Swissdec autorisierten Stelle identifiziert.	MUSS	✓
A-12	Identifikation durch Third Party	Ein Unternehmen wird durch eine vertrauenswürdige Drittpartei (Trusted Third Party) identifiziert.	KANN	✓
A-13	Stellvertretung (z.B. Treuhänder)	Der Stellvertreter muss sich registrieren und gegenüber dem Distributor mit seiner eigenen UID authentisieren können.	MUSS	✓
A-14	Stellvertretung verifizieren	Die Versicherung oder Behörde verifiziert, als Endempfänger einer Nachricht, eine allfällige Stellvertretung.	MUSS	✓
A-15	Automatische Konfiguration des ERP-Systems	Nach erfolgreich abgeschlossenem Registrierungsprozess bezieht das ERP-System das UID-Zertifikat (optional mit privatem Schlüssel) sowie weitere Konfigurationsinformationen automatisch vom Distributor und/oder der CA und ist innerhalb von Minuten einsatzbereit.	MUSS	✓
A-16	Autorisierung des ERP-Systems	Wird eine Nachricht vom ERP-System versendet, muss es sich beim Distributor für die Swissdec Geschäftsprozesse autorisieren.	MUSS	✓
A-17	Authentisierung des Unternehmens	Wird eine Nachricht vom ERP-System versendet, signiert es diese mit dem UID-Zertifikat.	MUSS	✓
A-18	Verifizierung des ERP-Systems	Trifft eine Nachricht ein, prüft der Distributor die Autorisierung des ERP-Systems und die Swissdec Geschäftsprozesse.	MUSS	✓
A-19	Authentifizierung des Unternehmens	Trifft eine Nachricht ein, prüft der Distributor die Signaturen, verarbeitet die Informationen und leitet die Identitätsinformation den Empfängern weiter.	MUSS	✓
A-20	Nachvollzieh-barkeit	Der Nachrichtenfluss muss durch das Unternehmen/ERP-System, Distributor sowie Versicherer & Behörden in angemessener Weise nachvollziehbar sein.	MUSS	✓
A-21	Benutzer-freundlichkeit	Sowohl die Inbetriebnahme als auch die Verwendung des Systems sind benutzerfreundlich ausgestaltet.	MUSS	(✓)
A-22	Einfache Inbetriebnahme	Die Konfiguration eines ERP-Systems bedarf keiner Hinzunahme eines technischen Spezialisten.	MUSS	✓
A-23	Schnelle Inbetriebnahme	Besteht bereits eine Beziehung zwischen Unternehmung und einer Versicherung oder Behörde, lässt sich der Registrierungsprozess inklusive Konfiguration des ERP-Systems in höchstens 10 Minuten durchführen.	MUSS	✓

A-24	Browser-Portal-Zugriff	Aus dem ERP-System ist ein Browserzugriff auf ein (V&B-)Portal möglich.	MUSS	(✓)
A-25	Plausibilisierung der Nachrichten	Erhält der Distributor eine Nachricht, so prüft dieser ob die im Zertifikats-UID mit der in der Nachricht	MUSS	✓
A-26	Verwendete Zertifikats-infrastruktur	Die verwendete Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate basiert auf dem RFC-5280 X.509 (aktuell Version 3).	MUSS	✓
A-27	Vertraulichkeit auf Nachrichtenebene	Um die übermittelnden Informationen trotz sicherem Kanal zusätzlich gegen weitere Angriffsvektoren schützen zu können, müssen die übertragenen Dateninhalte für den jeweiligen Empfänger verschlüsselt werden.	MUSS	✓

Es ist zu erkennen, dass alle im Lösungskonzept festgehaltenen Anforderungen im Rahmen der Detailspezifikation berücksichtigt wurden. Gleichwohl haben verschiedene Anforderungen nur teilweise oder nicht explizit in der Detailspezifikation Eingang gefunden:

- A-21 Benutzerfreundlichkeit:
  Die Benutzerfreundlichkeit wurde im Rahmen der Ausarbeitung und Spezifizierung der SUA Prozesse berücksichtigt. Beispielsweise wurde bei der Ausgestaltung der Passwörter darauf geachtet, dass diese einfach einzugeben sind und eine Falscheingabe durch den Benutzer direkt vom ERP-System erkannt werden kann (Prüfziffer). Gewisse Bestandteile, gerade auf Seiten der ERP-Systeme und der Ausgestaltung des User Interfaces, bedürfen im Rahmen der Erstellung der Anforderung an eine Zertifizierung einer weiterführenden Spezifikation bzw. einer Umsetzung in Zusammenarbeit mit den entsprechenden ERP-Herstellern. Hierbei muss gesondert noch einmal der Punkt Benutzerfreundlichkeit berücksichtigt und miteinbezogen werden.
- A-24 Browser-Portal-Zugriff:
  Die Möglichkeit des Zugriffs auf Web-Portale von bestimmten V&B über einen Browser-Aufruf direkt im ERP-System ist im Lohnstandard-CH (ELM)[29] vorgesehen und wird bereits entsprechend unterstützt. In der SUA Detailspezifikation wurden keine weiteren Vorgaben hierzu gemacht. Es bleibt aktuell noch offen, ob zukünftig SUA auch für die Authentisierung von Web-Portalen der V&B genutzt werden kann bzw. soll.

[29] Swissdec (2015). Richtlinien, online: http://www.Swissdec.ch/de/releases-und-updates/richtlinien/ (02.12.2015).

9 Offene Punkte

In der vorliegenden Detailspezifikation konnten einzelne Punkte noch nicht abschliessend festgelegt werden. Diese sollten aber in einer späteren Überarbeitung oder in der Ausarbeitung weiterer zertifizierungsrelevanter Dokumente noch einmal aufgenommen und gegebenenfalls auf der Basis des Informationsstandes neu beurteilt bzw. genauer spezifiziert werden.

9.1 Prozesse und Vorgaben zur Certificate Authority (CA)

Es ist davon auszugehen, dass zur Umsetzung der Swissdec Unternehmens-Authentifizierung die Zusammenarbeit mit einer akkreditierten Certificate Authority gesucht wird. Es soll in diesem Zusammenhang abgeklärt werden, ob einfachere CA-Anbieter wie z.B. Let's Encrypt[30] Dienste in ähnlicher Qualität anbieten können. Im Rahmen des entsprechenden Auswahlverfahrens sollten die hier dargelegten Vorgaben zu den Prozessen und der Ausgestaltung der Zertifikatsinfrastruktur berücksichtigt werden. Gleichwohl müssen die Details in den konkreten Abläufen der Zertifikatserstellung und auch der Ausgestaltung des Zertifikates mit dem ausgewählten Anbieter der CA abgeglichen und gegebenenfalls angepasst werden.
Ein Detail, das abgeklärt werden muss, ist die Verwendung der Business Category (BC), die der Rechtform aus dem BFS-UID-Registers entspricht. So werden im BFS-UID-Register die Zahlenwerte nach eCH-0097[31] verwendet, während in den EV-Guidelines[32] des CabForums nur 4 Werte verwendet werden.

9.2 TLS Client-Authentisierung

Wie in diesem Dokument beschrieben, wird die Authentifizierung des Absenders beim Aufbau eines sicheren Kanals mit einem TLS Client Zertifikat überprüft. Dies soll mittels UID-Zertifikat erfolgen. Hierzu müssen im Rahmen der Pilotierung noch Abklärungen getroffen, wie dies durch die bestehenden Standardframeworks unterstützt wird und ob einfache Code-Samples für die wichtigsten Plattformen bereitgestellt werden können. Ausserdem muss der Infrastruktur-Provider der Swissdec miteinbezogen werden, um in einem weiteren Schritt festlegen zu können, wie der Übergang zwischen der aktuell verwendeten einseitigen TLS-Authentisierung zu einer zertifikatsbasierten TLS Client-Authentisierung gemacht werden kann.

9.3 SUA-Prozesse und Benutzerführung in den unterschiedlichen ERP-Systemen

In der Ausgestaltung der Prozesse und Sicherheitselemente wurde so weit möglich auf die Benutzerfreundlichkeit sowohl bei der Einrichtung als auch im Betrieb geachtet. Gleichwohl muss hinsichtlich einer konkreten Implementierung der SUA Prozesse auf Seiten der ERP-Systeme mit den entsprechenden Herstellern das Gespräch gesucht und gegebenenfalls gewisse Vorgaben gemacht werden, wie Abläufe und damit die Benutzerführung auf möglichst einheitliche Weise in den Systemen abgebildet werden können.

9.4 Postanbindung

Im Registrierungsprozess wird davon ausgegangen, dass die Identität der Unternehmung so geprüft wird, dass ein Brief (Einschreiben oder A-Post-Plus) über einen zweiten, nicht elektronischen Kanal an eine verantwortliche Person im Unternehmen gesendet wird. Dieser Brief sollte persönlich übergeben werden. Die Rahmenbedingungen, Prozesse und Kosten für diese Art der Übergabe eines solchen Briefes müssen noch mit den zuständigen Stellen bei der Post abgeklärt werden.
Alternativ wäre sicherlich auch ein eingeschriebener Brief mit persönlicher Kontaktinformation aber OHNE persönliche Aushändigung ausreichend um die Kette der Unternehmensregistrierung mit einer genügend hohen Vertrauensstufe abzuschliessen.
Wie könnte die Anbindung eines solchen Services bei der Post aussehen? Gibt es einen bestehenden Service bei der Post, über welchen der Distributor den Versand eines eingeschriebenen Briefs mit den notwendigen Daten in Auftrag geben kann?

[30] https://letsencrypt.org/

[31] https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0097&documentVersion=4.0

[32] https://cabforum.org/wp-content/uploads/CA-Browser-Forum-EV-Guidelines-v1.6.8.pdf Kapitel 9.2.4, Seite 11

9.5 Registrierung von Unternehmen ohne Vertragsbeziehung mit V&B

Eine Registrierung für SUA kann im Moment nur auf Grundlage einer bestehenden Vertragsbeziehung mit einer Versicherung oder mit Hilfe eines geregelten Zertifikats erfolgen. Für den Fall, dass weitere Prozesse, z.B. Quellensteuer, auf SUA umgestellt werden sollen, müssen weitere Registrierungsmöglichkeiten, z.B. aufgrund einer bestehenden Beziehung mit einer Steuerbehörde, geprüft werden.

9.6 Abfrage BFS UID-Register

Die Einträge im UID-Register können für die Öffentlichkeit, aber nicht für die Verwaltung gesperrt sein (siehe eCH-0108 - Datenstandard Unternehmensregister, Kap. 4.2.2.2). Hier sollte mit dem BFS abgeklärt werden, ob Swissdec als Verwaltung (z.B. in Stellvertretung für das Bundesamt für Statistik) auftreten kann, um vollständigen Zugriff auf die Registerdaten zu bekommen.
Als Alternative kann zum Abgleich der Daten während der Registrierung (siehe Kap. 6.1.1) vom Unternehmen auch ein schriftlicher Auszug aus dem UID-Register vorgelegt werden.

9.7 Zertifikats-Erneuerung während langlaufender Prozesse

Zertifikats-Wechsel können zu Problemen bei langlaufenden Prozessen, z.B. beim Leistungsstandard (KLE) führen. Bei der Überprüfung von Signaturen dürfte das Problem weniger auftreten, wenn zu jeder signierten Nachricht das SUA-Zertifikat mitgeliefert wird. Somit kann der Adressat sein Schlüsselmaterial aktualisieren. Bei der Verschlüsselung von Nachrichten ist die Gefahr grösser, wenn der Absender nicht in der Lage ist das zu verwendende Schlüsselmaterial zu aktualisieren, und eine Antwort noch mit ‘veralteten’ Schlüsseln verschlüsselt. In Abhängigkeit der betroffenen Prozesse müssen Massnahmen definiert werden, um mit diesen Problemen umgehen zu können, z.B. indem definiert wird, dass bei jedem Polling-Versuch auch das Zertifikat mitgesandt wird.

10 Abbildungsverzeichnis

11 Tabellenverzeichnis

12 Glossar

Bundesamt für Statistik (BFS)
Statistisches Amt der Schweiz mit Sitz in Neuenburg.

Certification Authority (CA)
Eine Organisation, die digitale Zertifikate herausgibt. Ein digitales Zertifikat dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen.[33]

Certificate Chain
Dient zur Verifizierung eines digitalen Zertifikats, wobei die ausgebende CA als den Vertrauensanker für die Verifizierung der Zertifikatshierarchie bildet. Dadurch ist es möglich die Glaubwürdigkeit des Zertifikatsherausgebers zu prüfen.[34]

Certificate Signing Request (CSR)
Standardisiertes Format zum Anfordern eines digitalen Zertifikats. Der CSR enthält den öffentlichen Schlüssel eines Schlüsselpaares und muss von der Registrierungsstelle auf Authentizität geprüft werden.[35]

Credentials
Ein Berechtigungsnachweis (englisch: credentials) ist ein Instrumentarium, das einem System die Identität eines anderen Systems oder eines Benutzers bestätigen soll. Voraussetzung ist eine im System bekannte Identität. Der Nachweis geschieht meist nach Benennen der Identität in Form einer Benutzerkennung in Verbindung mit einem Authentifizierungsmerkmal.[36]

Declaration-ID
Diese Identitätsnummer wird bereits vom heutigen System verwendet und gehört zu einem bestimmten Geschäftsfall. Der Transmitter sendet in seinem Initial-Request keine Declaration-ID mit. Erst der Distributor fügt in seinen Meldungen dann eine Declaration-ID ein, um damit Rückfragen an den Support zu erleichtern.

EIDI-V
Verordnung des EFD über elektronische Daten und Informationen.

ERP-System
Ein ERP-System ist eine komplexe oder eine Vielzahl von miteinander kommunizierender Anwendungssoftware bzw. IT-Systemen, die zur Unterstützung der Ressourcenplanung des gesamten Unternehmens eingesetzt werden.[37]

OCSP
Das **Online Certificate Status Protocol** (**OCSP**) ist ein Protokoll, das es ermöglicht, den Status von X.509-Zertifikaten bei einem Validierungsdienst abzufragen. Siehe auch RFC 6960.

Privacy Enhanced Mail (PEM) - Dateiformat
Häufig verwendetes Dateiformat zur Speicherung von Schlüsselmaterial und X.509 Zertifikaten auf Basis einer Base64 Encodierung.[38]

Fachliche Quittierung
Diese Form der Quittierung erfolgt auf der inhaltlichen bzw. fachlichen Ebene zwischen Sender und Empfänger. Eine fachliche Quittierung ist abhängig vom gegebenen Prozess und kann sich über einen längeren Zeitraum erstrecken.

Registrierungspasswort (RegPw)
Der primäre Zweck des Registrierungspasswortes besteht darin, sicherzustellen, dass ein signiertes Zertifikat, allenfalls mit zugehörigem Private-/Public-Keypair dem richtigen Empfänger (ERP-System) - und nur diesen – zugeordnet wird. Es dient also der Authentisierung des Unternehmens.

Requests for Comments (RFC)
Die Requests for Comments (kurz RFC; zu Deutsch: Bitte um Kommentare) sind eine Reihe von technischen und organisatorischen Dokumenten des RFC-Editors zum Internet (ursprünglich Arpanet), die am 7. April 1969 begonnen wurden.[39]

RSA

[33] http://de.wikipedia.org/wiki/Zertifizierungsstelle

[34] http://en.wikipedia.org/wiki/Chain_of_trust

[35] http://de.wikipedia.org/wiki/Certificate_Signing_Request

[36] https://de.wikipedia.org/wiki/Berechtigungsnachweis_(Identifikationstechnik)

[37] https://de.wikipedia.org/wiki/Enterprise-Resource-Planning

[38] https://en.wikipedia.org/wiki/Privacy-enhanced_Electronic_Mail

[39] https://de.wikipedia.org/wiki/Request_for_Comments

RSA (Rivest, Shamir und Adleman) ist ein asymmetrisches kryptographisches Verfahren, das sowohl zur Verschlüsselung als auch zur digitalen Signatur verwendet werden kann.[40]

SHA256
SHA-2 (von englisch: secure hash algorithm, sicherer Hash-Algorithmus) ist der Oberbegriff für die vier kryptographischen Hashfunktionen SHA-224, SHA-256, SHA-384 und SHA-512, die 2001 vom US-amerikanischen NIST als Nachfolger von SHA-1 standardisiert wurden.[41]

SOAP
SOAP (ursprünglich für Simple Object Access Protocol) ist ein Netzwerkprotokoll, mit dessen Hilfe Daten zwischen Systemen ausgetauscht und Remote Procedure Calls durchgeführt werden können. SOAP ist ein industrieller Standard des World Wide Web Consortiums (W3C).[42]

Sicherheit auf Transportebene (Sicherer Kanal)
Die Sicherheit auf Transportebene beinhaltet die Übertragung der Daten in einem sicheren TLS (HTTPS) Kanal. Sender- und Empfängersystem haben sich authentisiert und einen Sitzungsschlüssel vereinbart, mit welchem die zu übertragenden Daten authentisiert und verschlüsselt werden.

Sicherheit auf Nachrichtenebene
Dies betrifft die zusätzliche Authentisierung und Verschlüsselung der Nutzdaten in einem sicheren Kanal. Im Fall von Swissdec werden SOAP Nachrichten mit Web Service Security abgesichert.

Sperrpasswort (SperrPw)
Das Sperrpasswort dient der Authentisierung des Unternehmens für den Fall, dass dieses ein ausgegebenes Zertifikat sperren lassen möchte.

Subject Information
In einem X.509 Zertifikat enthaltene Informationen zur Organisation, für welche das Zertifikat ausgegeben wurde.

Swissdec Unternehmens-Authentifizierung (SUA)
Prozesse und technische Voraussetzung zur eindeutigen Identifizierung von Unternehmen im Zuge der Swissdec Geschäftsprozesse.

Transaktionsquittierung
Bei dieser Form der Quittierung wird nur die Übertragung einer Nachricht bestätigt. Die Form der Nachricht (Syntax, Signatur, Semantik, usw.) wird dabei vom Empfängersystem geprüft und fliesst in die Quittierung ein. Die Prüfung des Inhalts der Nachricht ist Teil der fachlichen Quittierung. Eine Transaktionsquittierung muss demnach in einem bestimmen Zeitraum erfolgen. Ist dies nicht der Fall, kann der Sender die Auslieferung einer Nachricht als nicht erfolgreich taxieren und diese erneut senden.

Transmitter
Der Transmitter ist die Schnittstelle zwischen dem ERP-System und Swissdec. Das ERP System bereitet die zu sendenden Daten auf und übergibt diese der Transmitter Komponente, welche die Daten Swissdec-Konform über einen sicheren Kanal an den Distributor sendet. Der Transmitter validiert dabei die XML Deklarationen des ERP-Systems zu einem bestimmten Prozess anhand des offiziellen Swissdec XSD Validierungsschemas. Die Daten werden dann sicher (signiert und verschlüsselt) vom Transmitter über den sicheren Kanal (HTTPS) übertragen. Der Transmitter ist auch für das gesamte Error-Handling, für den Empfang der Antworten vom Distributor und für die Prüfung der Transaktionsquittierung zuständig. Der Transmitter übernimmt zudem die Archivierung und das Logging der Nachrichten.

Transport Layer Security (TLS) / Secure Sockets Layer (SSL)
Transport Layer Security (TLS, deutsch: Transportschichtsicherheit), weitläufiger bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL), ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.[43]

Unternehmens-Identifikationsnummer (UID-BFS)
Wird seit Januar 2011 durch das Bundesamt für Statistik (BFS) für jedes in der Schweiz wirtschaftlich aktive Unternehmen als eindeutige Identifikation für alle Behördenkontakte ausgegeben.[44]

UID-BFS-Register

[40] https://de.wikipedia.org/wiki/RSA-Kryptosystem

[41] https://de.wikipedia.org/wiki/SHA-2

[42] https://de.wikipedia.org/wiki/SOAP

[43] https://de.wikipedia.org/wiki/Transport_Layer_Security

[44] http://de.wikipedia.org/wiki/Unternehmens-Identifikationsnummer

Öffentliches Register des Bundes, in welchem alle wirtschaftlich aktiven Unternehmen mit einer eindeutigen Identifikation verzeichnet sind. Diese ist zu erreichen über: https://www.uid.admin.ch

Uniform Resource Identifier (URI)
Ein Uniform Resource Identifier (Abk. URI, englisch für einheitlicher Bezeichner für Ressourcen) ist ein Identifikator und besteht aus einer Zeichenfolge, die zur Identifizierung einer abstrakten oder physischen Ressource dient.[45]

V&B
Versicherungen und Behörden sind die Stelle, welche im Zuge der Swissdec Geschäftsprozesse Daten und Informationen von den Unternehmen übermittelt erhalten.

Versicherungsprofil (VProfil)
Informationen zur Vertragsbeziehungen zwischen einem Unternehmen und einer Versicherung.

VZertES
Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23.11.2016

WS-Security (WSS)
Web Services Security (WS-Security, WSS) ist im Wesentlichen eine Erweiterung zu SOAP, um Sicherheitsaspekte für Webservices einzubringen.

X.509 Zertifikat
Standard für eine Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate spezifiziert im RFC-5280.

ZertES
Bundesgesetz über die elektronische Signatur vom 18.3.2016 (Stand 1.1.2017)

[45] https://de.wikipedia.org/wiki/Uniform_Resource_Identifier

13 Referenzen

[1] A. Laube, G. Hassenstein und A. Böhm, «Swissdec Unternehmens-Authentifizierung - Detailspezifikation - Ergänzung Registrierung mit ZertES,» 2019.

14 Versionskontrolle

Version	Datum	Beschreibung	Autor
1.0	20.07.18	Version 1.0 der DetailSpezifikation	Annett Laube
1.1	08.11.18	Aktualisierung/Anpassung WSDL	Annett Laube
1.2	31.01.19	Auslagerung RegKonf ZertES	Annett Laube
1.3	04.04.19	Beschreibung Registrierung Treuhänder	Annett Laube
1.4	26.04.19	Anpassung SUA-Zert, Formattierung	Annett Laube
1.5	10.05.19	Anpassung Inhalt SUA-Zert, CSR-Anforderung und Zertifikatsbeispiel im Anhang	Gerhard Hassenstein

Anhang A

Beispiel eines UID-Zertifikats:

Certificate:
- Version:
  - Version 3
- Serial Number:
  - 00:01:02:03
- Certificate Signature Algorithm:
  - PKCS #1 SHA-256 With RSA Encryption
- Issuer:
  - CN = Swissdec Root Certificate Authority
  - OU = Digital Certificate Services
  - O = Swissdec
  - C = CH
- Validity:
  - Not Before:
    - 13.10.18, 09:58:30 (13.10.18, 07:58:30 GMT)
  - Not After:
    - 13.10.19, 09:58:30 (13.10.19, 07:58:30 GMT)
- Subject:
  - **CN = NTRCH-CHE-123.456.789@swissdec.ch**
  - **OU = Finanzabteilung**
  - **O = Huggentobler AG**
  - **L = Langnau**
  - **ST = Bern**
  - **C = CH**
  - **Object Identifier (2 5 4 97) = NTRCH-CHE-123.456.789**
- Subject Public Key Info:
  - Subject Public Key Algorithm:
    - PKCS #1 RSA Encryption
  - Subject's Public Key:
    - Modulus (2048 bits):
    - c7 67 67 1f ca e4 10 28 12 e8 64 95 38 4e 74 01
    - 11 f3 96 70 24 1a c8 bd 82 02 6c 7a 4b 10 87 60
    - 4a 18 f8 af ea 46 ea 86 bd 6a 20 b0 da 77 76 e6
    - d2 9d f2 7f bf 2a 15 f3 e4 36 e6 80 38 66 97 b4
    - df 33 f1 56 c0 82 a5 63 d4 22 0f ea 86 36 40 67
    - e6 c9 f3 5b 43 1e 56 cc 94 cd 1d 53 88 5b 9b 5e
    - 2f b0 3f 85 6c cc 16 df 7c fd 59 f7 f2 7a af 36
    - b5 6f 7b 73 b7 22 48 ef 49 45 0f 35 ad 24 f0 c4
    - 93 b9 a7 cf 7b 2d 77 cb b3 29 bf dd 02 53 d0 3a
    - f2 38 d1 2d e1 b5 f2 e5 dd 06 16 e5 49 b3 c0 0d
    - 2e 41 68 b2 f4 f9 01 40 57 79 f7 e7 ea e6 1c 15
    - c7 74 ca 4c 47 87 b1 f8 7e 4c 0b dc 5a ec 5a f1
    - 87 d7 cf 8f cb b4 53 50 a6 4b 9d 3c 3a 5c a1 11
    - cf b1 1e 23 0d 6c 0b 04 d2 d9 d5 83 14 0a 4c d0
    - a6 a4 90 2d 65 36 2e c7 fd 8d 0f 7b d2 3f bf 37
    - 57 d9 9a a2 db 1a 99 2d be a0 e2 27 7e 73 1e 3d
    - Exponent (24 bits):
    - 65537
- Extensions:
  - Certificate Authority Key Identifier:
    - Not Critical
    - Size: 20 Bytes / 160 Bits
    - 37 41 ec 21 1c a9 3e d7 aa 9c 19 96 d0 72 df ed 45 04 d1 15
  - Authority Information Access:

Not Critical
OCSP: URI: https://ocsp.swissdec.ch/sua-issuer
CA Issuers: URI: https://ca.swissdec.ch/sua-issuer.crt
Certificate Policies:
Not Critical
2.16.756.1.83.23.0:
Certification Practice Statement pointer:
https://www.swissdec.ch/cps
CRL Distribution Points:
Not Critical
URI: https://crl.swissdec.ch/sua-issuer.crl
Certificate Key Usage:
Critical
keyEncipherment
digitalSignature
Extended Key Usage:
TLS Web Client Authentication
Document Signing
Certificate Subject Key ID:
Not Critical
Size: 20 Bytes / 160 Bits
64 a8 a2 ab c9 ee 2f 89 47 2c 56 f3 bd 4f c8 26 23 26 23 f7
Certificate Signature Algorithm:
PKCS #1 SHA-256 With RSA Encryption
Certificate Signature Value:
Size: 256 Bytes / 2048 Bits
43 b9 b6 b6 71 13 62 9c 6c 13 23 ab 53 87 06 a3
58 59 53 b6 18 1a d2 8e 0b 2f 4e 0b 24 77 e3 8a
04 ac 84 c6 5c 13 e8 42 64 47 e4 ee e9 b1 4d 19
df 04 bf 43 20 0c 1f f9 c1 14 a6 81 12 a1 27 57
6e b6 d6 80 46 da 8f fb 50 fa ef 05 a5 f2 d2 29
1d f3 60 97 02 2b c7 e5 5f 82 f7 3f 26 12 57 33
f9 ba ad dc ca e7 4f a5 ff ef 3e 9e 47 e9 af 89
ea a0 55 66 7f 13 e4 e4 3b 72 3f a8 64 a0 d9 e5
1c ca ad de e2 2d 7e d9 2f 7f 36 ac b1 7b 91 97
68 fe 01 65 8b e6 ec 8c 22 a8 9a ba 8a 99 a0 48
8e 50 7b b2 04 7d 95 47 fd 48 69 d1 80 1d 31 1c
53 02 f1 55 b1 58 a6 e2 67 a0 76 83 1d 09 e2 80
d9 0d f8 a2 70 ea 88 b2 42 e3 6e ce 91 5a dd 8d
13 6b 25 e7 17 0c be fb 1e 33 8e 52 2f 07 a5 e6
a7 62 52 2d a0 ff 6d 6d 33 54 01 0b 54 05 5b 39
5d 56 39 b0 67 67 63 68 c9 d1 e1 07 17 ed a5 b0