

Richtlinien Swissdec Unternehmens-Authentifizierungsstandard-CH (SUA)

Anforderungen Endreceiver

Die Richtlinien für den Swissdec Unternehmens-Authentifizierungsstandard-CH (SUA) wurden in Zusammenarbeit mit folgenden Beteiligten erarbeitet:

- Suva
- Schweizerischer Versicherungsverband

Herausgeber

Swissdec
Fluhmattstrasse 1
6004 Luzern
www.swissdec.ch

Inhaltsverzeichnis

1.	Einleitung	6
1.1	Vereinfachter Ablauf einer Zertifikatsbeschaffung	7
1.2	Institution und Domäne	9
2.	Übersicht Use Cases	10
2.1	Übersichtsdiagramme zu den Use Cases	11
2.2	Erläuterungen zu den Use Cases	12
2.3	Tests	12
2.4	Summary Use Cases	13
2.4.1	UC001 Kunden / Unternehmen verifizieren	13
2.4.2	UC002 Kundenanfrage prüfen	13
2.4.3	UC003 Prüfungsergebnis erstellen	13
2.4.4	UC004 Testdaten kennzeichnen	13
2.4.5	UC005 Security anwenden	13
2.4.6	UC006 Erreichbarkeit prüfen	13
2.4.7	UC007 Wartungsfenster setzen	13
2.4.8	UC008 Support; manuelle Klärung durchführen	13
2.4.9	UC009 Duplikat behandeln	13
2.5	Use Cases und zugehörige Operationen	14
3.	Use Cases	15
3.1	Use Case 001: Kunden / Unternehmen verifizieren	15
3.2	Use Case 002: Kundenanfrage prüfen	17
3.2.1	Sonderfall Treuhänder	17
3.2.2	Sonderfall keine bestehende Vertragsbeziehung	17
3.3	Use Case 003: Prüfungsergebnis erstellen	18
3.4	Use Case 004: Testdaten kennzeichnen	19
3.5	Use Case 005: Security anwenden	20
3.6	Use Case 006 Erreichbarkeit prüfen	21
3.7	UC007 Wartungsfenster setzen	22
3.8	UC008 Support, manuelle Klärung durchführen	23
3.9	UC009 Duplikat behandeln	24
4.	Zusätzliche Anforderungen	25
4.1	Archiv-Files erstellen	25
4.2	SUA Version	25
4.3	Kommunikationsstandards	25
4.4	Optionale Komprimierung	25
4.5	Verfügbarkeit	25
4.6	Definierte Zeitbereiche	26
4.7	Definierte Wertebereiche	26
4.8	Skalierbarkeit	26
4.9	Änderungen an der Schnittstelle	26
4.10	Support und Reaktionszeit	26
4.11	Performance / Durchsatz	28
5.	Anhang	29
5.1	Referenzen	29

Abbildungsverzeichnis

Abbildung 1: Skizze SUA Registration Configuration Schritt 1	7
Abbildung 2: Skizze SUA Registration Configuration Schritte 2, 3, 4 und 5	8
Abbildung 3: Prozess Skizze SUA Registration und Configuration.....	10
Abbildung 4: Use Cases	11
Abbildung 5: Sequenzdiagramm zur Beschaffung eines SUA-Zertifikats	16

Tabellenverzeichnis

Tabelle 1: Verbindlichkeit von Anforderungen	5
Tabelle 2: Use Cases und Operationen.....	14
Tabelle 3: Use Case 001 LM übermitteln	15
Tabelle 4: Use Case 004 Erreichbarkeit prüfen	21
Tabelle 5: Use Case 007 Wartungsfenster setzen	22

Übersicht der Änderungen Version 20190301

Richtlinien für den Swissdec Unternehmens-Authentifizierungsstandard-CH (SUA) - Anforderungen für Endreceiver, Version 20190301 Ausgabe vom 10.05.2021.

Kapitel	Änderung
Initial Version	

Konventionen in diesem Dokument

Folgende Schriftarten werden in diesem Dokument verwendet:

Text	Dokumentation
Text	Code
<Text>	XML-Element
[TEXT]	Referenz auf ein anderes Dokument

Die Verbindlichkeit von Anforderungen ist wie folgt definiert:

Verbindlichkeit	Wort
Pflicht	<i>Muss</i>
Wunsch	<i>soll (sollte)</i>
Absicht	<i>Wird</i>
Vorschlag	<i>Kann</i>

Tabelle 1: Verbindlichkeit von Anforderungen

Achtung:

Für das konzeptionelle Verständnis genügen oft ältere Schemabilder, d. h. **verbindlich sind immer nur die offiziellen¹ XML-Files** (z.B. Web Services Description Language (WSDL), XML Schema Definition (XSD), Extensible Stylesheet Language (XSL) Transformation und XML Instance Documents).

¹ www.swissdec.ch

1. Einleitung

Dieses Dokument enthält funktionale und zusätzliche Anforderungen an Endreceiver, die im Rahmen des Swissdec Unternehmens-Authentifizierungsstandards-CH (SUA) eingesetzt werden. Inhalt dieses Dokuments sind die Anforderungen an die Zertifikatsbestellung. Die Prozesssicherung (Authentifizierung und Verbindlichkeit) innerhalb der Swissdec-Prozesse, bei welchen die Swissdec Unternehmens-Authentifizierung verwendet wird, ist in den Spezifikationen der entsprechenden Prozesse beschrieben. In diesem Dokument werden die technischen Aspekte des Standards adressiert, nicht die fachliche Logik. Ein Endreceiver wird bei der Zertifikatsbestellung dazu verwendet, ein Unternehmen zu identifizieren und die UID-BFS zu verifizieren.

Eine Gesamtübersicht des standardisierten Verfahrens ist zum Verständnis der nachfolgenden Spezifikation hilfreich. Diese wird durch das Übersichtsdokument «OverviewUnternehmensAuthentifizierung.pdf» (OVOA, 2019) vermittelt, auf welches an dieser Stelle verwiesen wird.

1.1 Vereinfachter Ablauf einer Zertifikatsbeschaffung

Grundlage einer Registrierung ist eine bestehende Vertragsbeziehung mit einer Versicherung. Im weiteren Text werden „Endreceiver“ mit dem „Endempfänger bei Versicherer und Behörden (V&B)“ gleichgesetzt.

Es wird davon ausgegangen, dass die Versicherung bei Vertragsabschluss das Unternehmen überprüft und jederzeit aktuelle UID-Daten (UID-BFS, Name des Unternehmens laut Handelsregister, ...) in ihren Stammdaten-Systemen führt.

In der Verteilung bzw. Beschaffung eines SUA-Zertifikats wird oft von zwei wesentlichen Schritten gesprochen

- die «Bestellung» mittels *Registrierung* (RLOA, 2019)
- die «Aktivierung» mittels *Konfiguration* (RLOA, 2019)

Skizze SUA Registration Configuration Schritt 1:

Möchte sich ein Unternehmen für SUA registrieren, so wählt ein zuständiger Mitarbeiter des Unternehmens im ERP-System eine Versicherung (V&B Endempfänger) aus, der für die Identifikation des Unternehmens genutzt werden soll. Die zur Registrierung notwendigen Informationen (Vertragsinformationen, UID-BFS, 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 für eine UID-BFS möglich sind. Dem ERP-System wird das Ergebnis der Verifikation durch das Senden einer generierten CertificateRequest-ID (CRID), die das ERP-System und den Request eindeutig identifiziert, mitgeteilt.

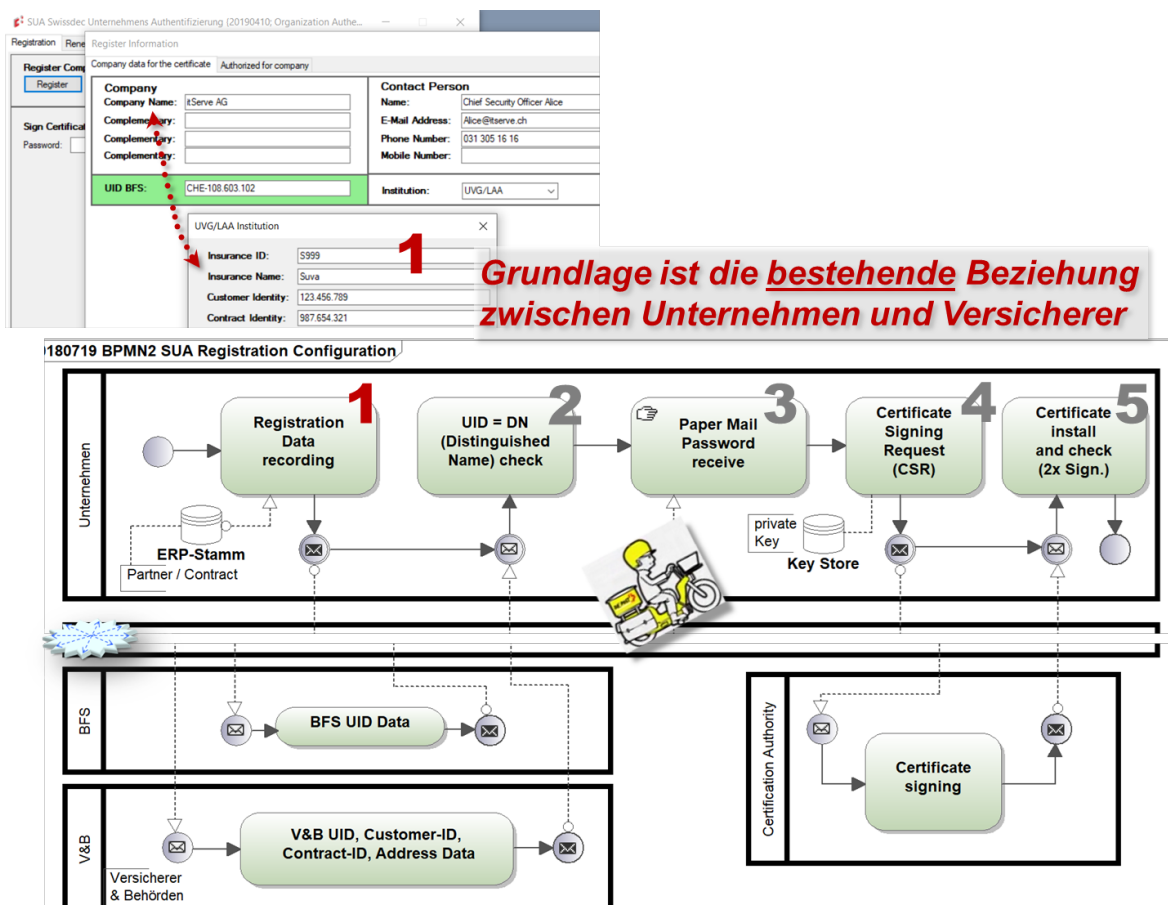


Abbildung 1: Skizze SUA Registration Configuration Schritt 1

Skizze SUA Registration Configuration Schritt 2:

Wurde die Nachricht erfolgreich vom Distributor verifiziert, werden die Informationen zum Unternehmen aus dem UID-Register des BFS angefragt. Mit Hilfe der UID-BFS 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 Institution weitergeleitet. Die V&B Institution prüft mit Hilfe ihrer Stammdaten die vom Unternehmen gesendeten Daten 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 zurückgeschickt.

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).

Skizze SUA Registration Configuration Schritt 3:

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 SUA-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 bereitgestellte Adresse (Geschäftsleitung), der 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.

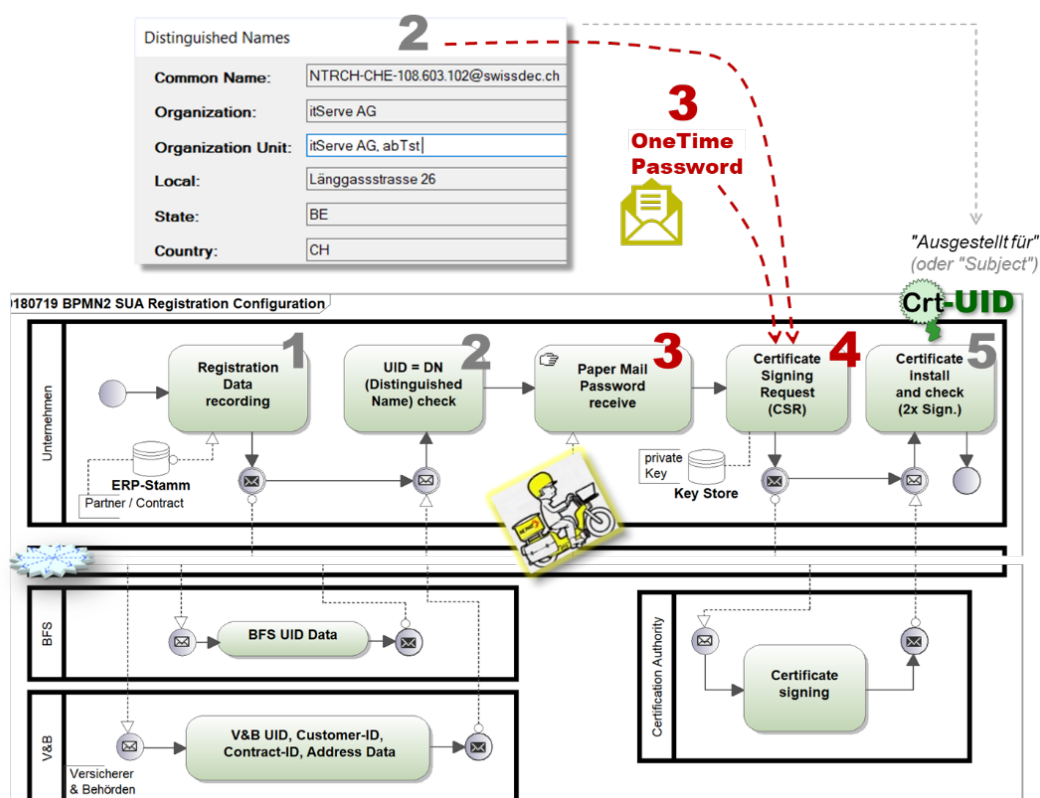


Abbildung 2: Skizze SUA Registration Configuration Schritte 2, 3, 4 und 5

Skizze SUA Registration Configuration Schritte 4 und 5:

Der Mitarbeiter kann nun das bestellte Zertifikat mittels CSR und dem Passwort, das die Unternehmung im Brief (Schritt 3) erhalten hat, abholen und bei sich automatisch im ERP-System installieren. Als Abschluss wird die korrekte Funktion des neuen SUA-Zertifikats mindestens mittels einer entsprechend 2x signierten `Operation OrganizationAuthenticationRenewPort.CheckInteroperability()` geprüft.

Der SUA Registrierungsprozess endet, wenn der Transmitter mit dem SUA-Zertifikat eine erfolgreiche Übermittlung durchführen konnte

Achtung:

Der Endreceiver ist hier nur im Schritt 1 und 2 involviert. Weitere Schritte, wie zum Beispiel die Überprüfung der Zertifikate, finden nur zwischen Transmitter und Distributor statt.

Für eine detaillierte Beschreibung des Ablaufs wird auf die Richtlinien bzw. das Detailkonzept (RLOA, 2019) verwiesen.

1.2 Institution und Domäne

SUA kann und wird in mehreren Swissdec Übermittlungsprozessen verwendet werden. Da die Unternehmensauthentifizierung jedoch im Leistungsstandard-CH (KLE) zwingend ist, während sie im Lohnstandard aktuell nur optional verwendet werden kann, beziehen sich folgende Beispiele vor allem auf den Leistungsstandard-CH (KLE). Trotzdem gelten untenstehende Informationen für alle Swissdec Standards, die die Verwendung von SUA erlauben.

Wir unterscheiden in diesem Dokument zwischen den Begriffen Domäne und Institution.

Domäne: Organisation, der Daten übermittelt werden. Domänen, die der Leistungsstandard-CH (KLE) unterstützt sind UVG, UVGZ, KU und KTG.

Institution: Empfänger, die Daten erhalten. Hier handelt es sich um Versicherungen, die der jeweiligen Domänen angehören.

Eine Firma kann innerhalb einer Domäne mehrere Institutionen kontaktieren. Eine Institution kann mehrere Domänen unterstützen.

2. Übersicht Use Cases

Die folgende Skizze zeigt als erste Übersicht den ganzen Prozess zum Erlangen eines SUA-Zertifikats.

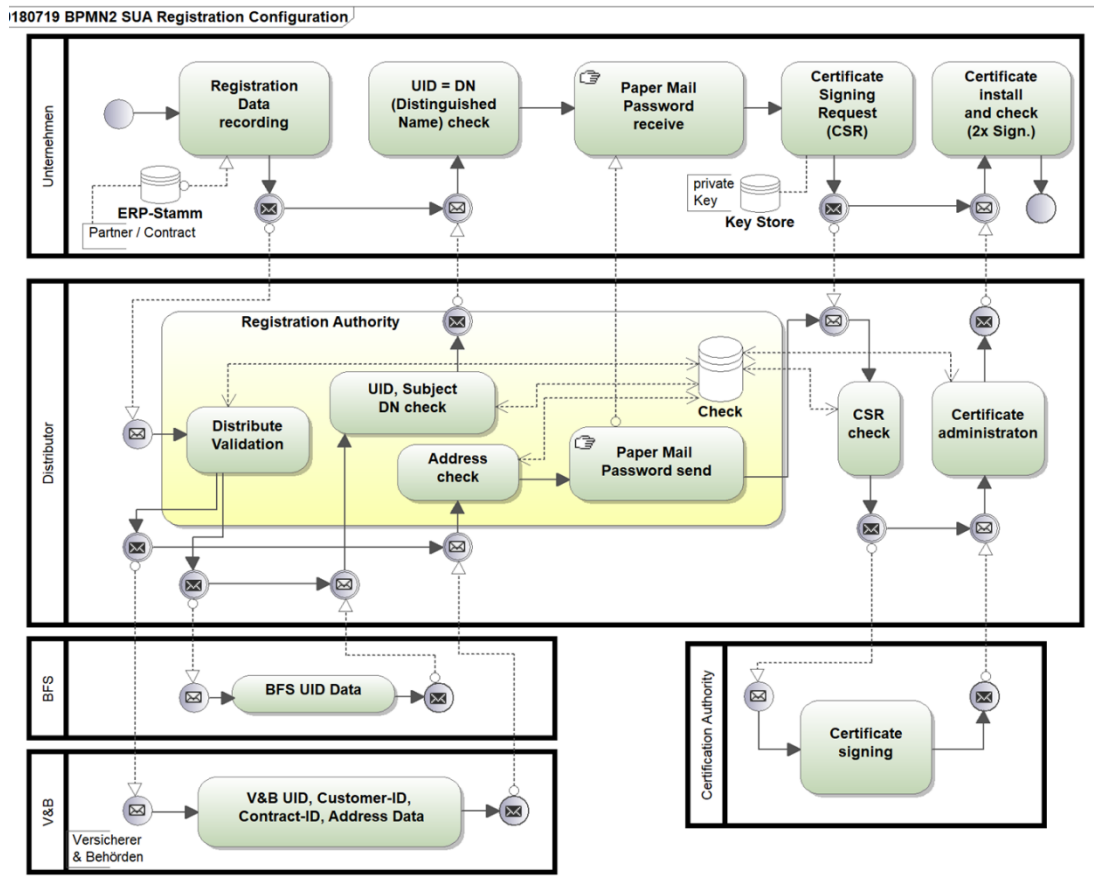


Abbildung 3: Prozess Skizze SUA Registration und Configuration

2.1 Übersichtsdiagramme zu den Use Cases

Ein Teil der Use Cases ist analog zu den anderen Swissdec Standards aufgebaut. In den XML-Schema Elementen kann aus diesem Grund der Begriff UID-BFS vorkommen. Dieser kann analog zum Begriff UID verwendet werden. (historisch und z.B. im DeclareSalary ... CompanyDescription/UID-BFS). Aufgrund der Parallelen zwischen den verschiedenen Standards wurden die veralteten Bezeichnungen teilweise beibehalten, um die Implementierung des Projekts zu vereinfachen.

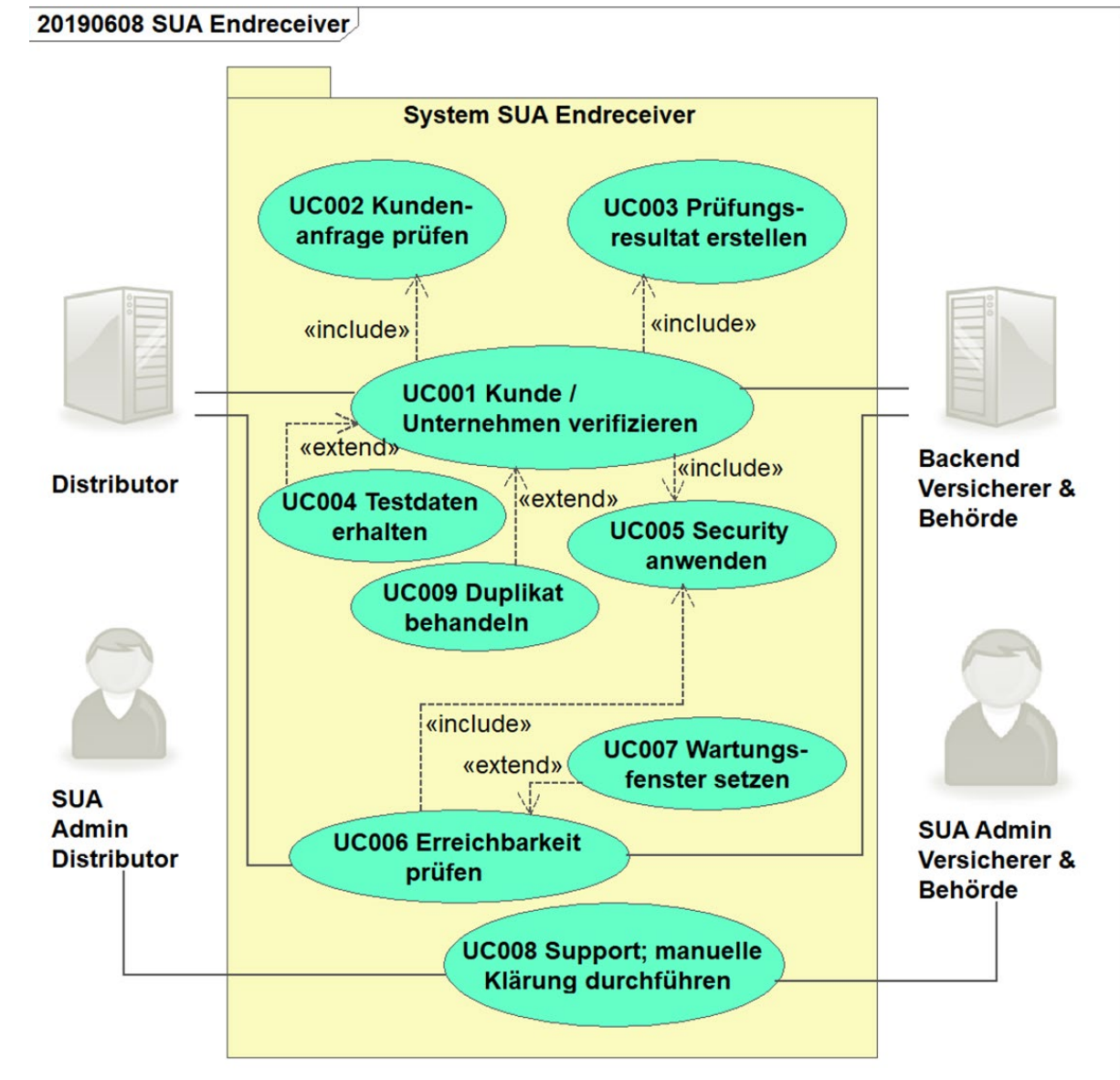


Abbildung 4: Use Cases

2.2 Erläuterungen zu den Use Cases

Die als Use Cases abgebildeten Anforderungen beziehen sich auf den technischen Teil eines Systems des Endreceivers, welcher die Bestellung eines SUA-Zertifikats entgegennimmt und beantwortet.

Ein Endreceiver *muss* für die Abnahme immer die folgenden Systemanforderungen erfüllen:

- UC001 Kunden / Unternehmen verifizieren
- UC002 Kundenanfrage prüfen
- UC003 Prüfungsergebnis erstellen
- UC004 Testdaten kennzeichnen
- UC005 Security anwenden
- UC006 Erreichbarkeit prüfen
- UC007 Wartungsfenster setzen
- UC008 Support; manuelle Klärung durchführen
- UC009 Duplikat behandeln

Wie die Interaktion zwischen Benutzer und System gestaltet wird, liegt in der Entscheidung der Systemhersteller und wird in dieser Spezifikation nicht beschrieben.

2.3 Tests

Die Tests der Abnahme beziehen sich auf die Use Cases. Zusammen mit den Anforderungen tragen sie zum Gesamtverständnis des zu bauenden Systems bei. Die Tests werden mit Vorteil bereits während der Entwicklung vom Hersteller mit einbezogen (Test Driven Development).

2.4 Summary Use Cases

2.4.1 UC001 Kunden / Unternehmen verifizieren

Ein neues Zertifikat wird via Distributor bestellt. Dazu müssen die Vertragsangaben des Kunden / Unternehmens vom Versicherer (V&B) geprüft werden. Dabei werden weitere Use Cases verwendet: UC002, UC003, UC004 und UC005.

2.4.2 UC002 Kundenanfrage prüfen

Mit der eigentlichen Bestellung / Registrierung wird die Identität des Antragstellers vom Endempfänger (V&B) überprüft. Hierzu werden die gemeldeten Daten mit den Vertrags- bzw. Stammdaten beim V&B verglichen.
Bemerkung: Aus Sicherheitsgründen wird vom Distributor keine UID-BFS mitgeliefert.

2.4.3 UC003 Prüfungsergebnis erstellen

Nach der erfolgreichen Prüfung (UC002) werden alle Angaben gemäss dem Element `<Success>` bereitgestellt (inkl. UID-BFS).

2.4.4 UC004 Testdaten kennzeichnen

Eine beliebige Meldung kann als Testfall gekennzeichnet werden. Sie wird somit über das produktive System versendet, vom Endreceiver jedoch nicht produktiv verarbeitet. Im Falle von SUA reagiert der Endreceiver immer gleich, unabhängig davon, ob es sich um einen Testfall oder eine produktive Meldung handelt.

2.4.5 UC005 Security anwenden

Jede übermittelte Meldung muss signiert und verschlüsselt sein.

2.4.6 UC006 Erreichbarkeit prüfen

Zyklisch aufgerufene Meldung, die die Verfügbarkeit des Endreceivers und allenfalls gesetzte Wartungsfenster in regelmässigen Abständen prüft.

2.4.7 UC007 Wartungsfenster setzen

Ein Zeitfenster und eine Meldung für Wartungsarbeiten müssen konfiguriert und dem Request des Distributors als Response mitgegeben werden können.

2.4.8 UC008 Support; manuelle Klärung durchführen

Sämtliche Supportinformationen (Notifications, Faults) müssen dem Endbenutzer klar verständlich dargestellt werden. Der Benutzer muss wissen, woher die Meldung kommt, und wie er darauf zu reagieren hat. Auf Supportanfragen muss dem Unternehmen Auskunft gegeben werden können.

2.4.9 UC009 Duplikat behandeln

Duplikate eines kompletten Requests werden vom Distributor gekennzeichnet. Falls die im Duplikat enthaltenen Informationen noch nicht verarbeitet und beantwortet wurden, muss dies nachgeholt werden. Weitere Duplikate müssen sowohl bei `RegisterOrganizationConsumer` wie auch bei `GetResultFromOrganizationRegistrationConsumer` erkannt und behandelt werden können.

2.5 Use Cases und zugehörige Operationen

Das zugrundeliegende Modell ist ein Client – Server System mit dem Distributor als Client. Verwendet werden die XML-Standards WSDL und XML-Schema. Die nachfolgenden Operationen und Elemente befinden sich im zugehörigen WSDL-File (WSDLOA, 2019) und im beschreibenden Schema (XSDOA, 2019). Verfahren und Protokoll sind in (RLOA, 2019) erläutert.

Use Case	Operation / Element
	<i>OrganizationAuthenticationConsumerService WSDL / XSD</i>
UC001 Kunden / Unternehmen verifizieren	<ul style="list-style-type: none"> ▪ RegisterOrganizationConsumer ▪ RegisterOrganizationConsumerResponse ▪ GetResultFromRegisterOrganizationConsumer ▪ GetResultFromRegisterOrganizationConsumerResponse ▪ OrganizationAuthenticationConsumerFault
UC002 Kundenanfrage prüfen	
UC003 Prüfungsergebnis erstellen	
UC004 Testdaten kennzeichnen	
UC005 Security anwenden	
UC006 Erreichbarkeit prüfen	<ul style="list-style-type: none"> ▪ PingConsumer ▪ PingConsumerResponse ▪ OrganizationAuthenticationConsumerFault
UC007 Wartungsfenster setzen	

Tabelle 2: Use Cases und Operationen

3. Use Cases

3.1 Use Case 001: Kunden / Unternehmen verifizieren

Kurzbeschreibung	Ein neues SUA-Zertifikat wird via Distributor bestellt. Dazu müssen die Vertragsangaben des Kunden / Unternehmen vom Versicherer (V&B) geprüft werden.
Akteure	Distributor, Endreceiver
Auslöser	Ein Angestellter des Unternehmens (Sicherheitsbeauftragter) möchte ein SUA-Zertifikat beschaffen und der Distributor erhält eine entsprechende Anfrage.
Vorbedingungen	Das ERP-System ist in der Lage, elektronische SUA-Meldungen zu versenden und zu empfangen und ist im Besitz eines ERP-Zertifikats.
Nachbedingungen	<ul style="list-style-type: none"> Die Unternehmensangaben wurden erfolgreich geprüft Die entsprechenden Daten (inkl. UID-BFS) wurden abgeholt. Bei einem Fehlschlag: <ul style="list-style-type: none"> Fehlermeldung
Included Use Cases	UC002 Kundenanfrage prüfen UC003 Prüfungsergebnis erstellen UC004 Testdaten erkennen UC005 Security anwenden
Standardablauf	1. UC002: Mit der eigentlichen Bestellung / Registrierung, Operation <code>RegisterOrganizationConsumer</code> , wird die Identität des Antragstellers vom Endempfänger (V&B) überprüft. Hierzu werden die gemeldeten Daten mit den Vertrags- bzw. Stammdaten beim V&B verglichen. Bemerkung: Aus Sicherheitsgründen wird <i>keine</i> UID-BFS mitgeliefert. 2. Nach der erfolgreichen Prüfung (UC002) <i>müssen</i> alle Angaben gemäss dem Element <code><Success></code> bereitgestellt werden (inkl. UID-BFS). Das Resultat wird dann asynchron mit der Operation <code>GetResultFromOrganizationRegistrationConsumer</code> abgeholt. Sofern im Ursprünglichen <code>RegisterOrganizationConsumer</code> ein <code>WithDelegate</code> stehen, handelt es sich um eine „Treuhänder“ () Anfrage. Dann <i>müssen</i> alle <code>Delegate</code> im <code>GetResultFromOrganizationRegistrationConsumer</code> geliefert werden.
Alternative Abläufe	{UC008} Daten werden als Testdaten erkannt Wie Standardablauf Schritte 1 bis 2 {Schritt 1: Wartungsfenster / Dienst ist nicht verfügbar} Die Information zum Wartungsfenster (von-bis) wurde bereits mittels UC006 «Erreichbarkeit prüfen» an den Distributor übermittelt. In dieser Zeit werden Response-Meldungen mit dieser Unterbruch-Information vom Distributor direkt an das anfragende ERP-System zurückgegeben. {Schritt 1: ungeplanter Unterbruch / Dienst ist nicht verfügbar} In dieser Zeit werden Fehlermeldungen vom Distributor direkt an das anfragende ERP-System zurückgegeben, s. (ACKNSwissdec, 2020). An den Distributor wird eine Fehlermeldung zurückgegeben. {Schritt 1: Dublette wurde erkannt, Vorgehen UC009 «Duplikate behandeln»} {Schritt 1: Security nicht gültig, Rückweisung der Meldung}
Fehlerliste	Fachliche Fehler: <ul style="list-style-type: none"> die Meldung verstösst gegen die Plausibilisierungsregeln Technische Fehler: <ul style="list-style-type: none"> Fehler bei Signatur/Verschlüsselung/Entschlüsselung die vom Distributor aufbereitete Meldung entspricht nicht dem Schema (Validität nicht gegeben)

Tabelle 3: Use Case 001 LM übermitteln

I 20190531 SUA Certificate distribution (1:D:1)

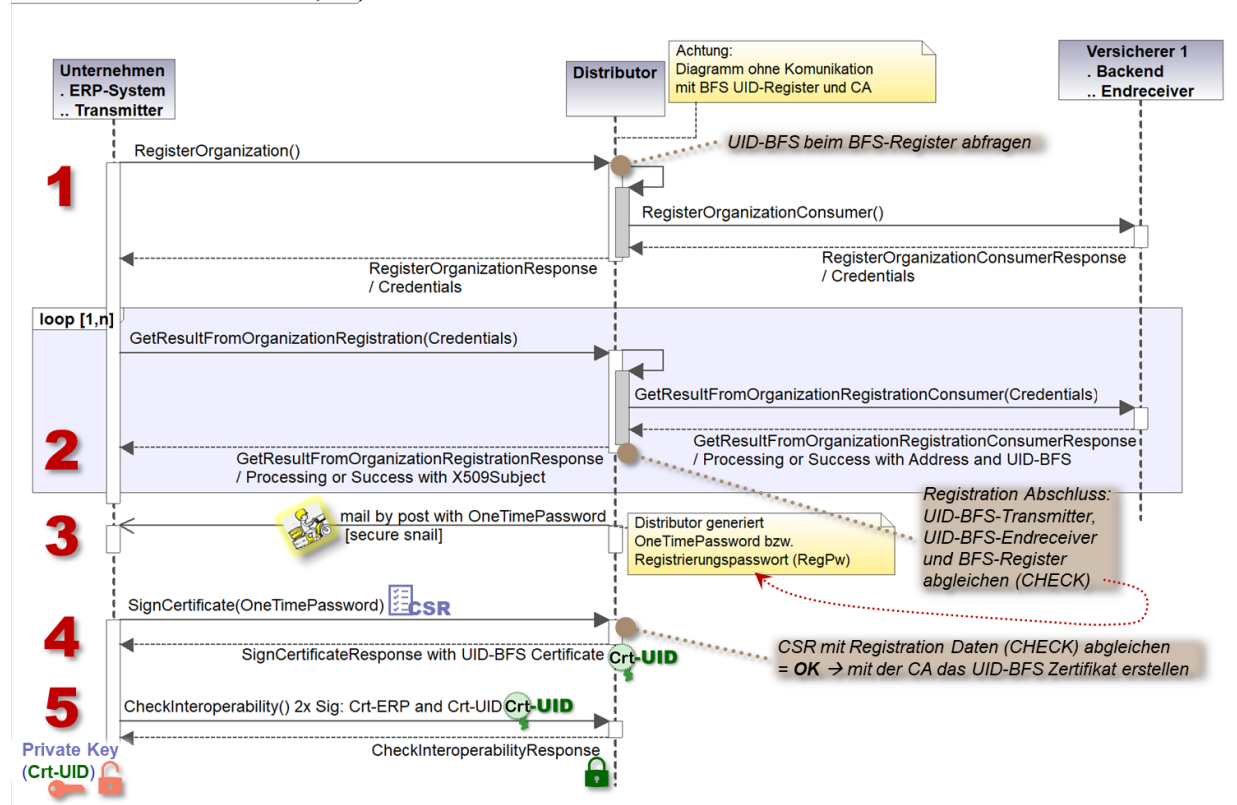


Abbildung 5: Sequenzdiagramm zur Beschaffung eines SUA-Zertifikats

3.2 Use Case 002: Kundenanfrage prüfen

Der Endempfänger vergleicht die vom Distributor erhaltenen Daten mit den eigenen Vertrags- respektive Stammdaten und meldet sie dem Distributor zurück. Aus Sicherheitsgründen darf jedoch keine UID-BFS mitgeliefert werden. Der Endempfänger kann hiermit eine Fortsetzung des SUA-Prozesses ermöglichen oder abbrechen und gewährleistet, dass nur SUA-Zertifikate für gültige Vertragsbeziehungen ausgestellt werden.

3.2.1 Sonderfall Treuhänder

Wird ein Unternehmen von einem Treuhänder betreut, kann dieser ein SUA-Zertifikat für das Unternehmen anfordern. Bedingung dafür ist, dass der Treuhänder dem Endempfänger bekannt ist.

In diesem Fall meldet der Treuhänder dem Distributor die benötigten Unternehmensinformationen, um ein SUA-Zertifikat zu beantragen. Ausserdem liefert er dem Distributor Informationen zu sich selber.

V&B erhalten vom Distributor keine detaillierten Angaben zum Treuhänder, sondern nur das Flag `WithDelegate`. Der Endempfänger überprüft nun, ob bei dem Unternehmen einer oder mehrere Treuhänder bekannt sind. Falls ja, liefert er dem Distributor die bekannten Angaben der Treuhänder für dieses Unternehmen zurück. Der Distributor gleicht diese erhaltenen Informationen mit jenen vom Transmitter ab und entscheidet, ob die Informationen für einen der Treuhänder deckungsgleich sind, dass ein SUA-Zertifikat ausgestellt werden kann. Sollte es zu Widersprüchen in Bezug auf die Treuhänderinformationen kommen, wird der Prozess abgebrochen und muss nach Abklärungen zwischen Unternehmen und V&B zum Aktualisieren der Treuhänder-Informationen neu ausgelöst werden.

3.2.2 Sonderfall keine bestehende Vertragsbeziehung

In seltenen Ausnahmefällen kann es dazu kommen, dass zwischen einem Unternehmen und V&B Informationen ausgetauscht werden müssen, obschon es keine aktuelle Vertragsbeziehung zwischen den beiden Parteien gibt. Dies ist zum Beispiel dann der Fall, wenn im Leistungsstandard-CH (KLE) ein Rückfall auftritt, der betroffene Patient in der Zwischenzeit aber Arbeitsstelle und Versicherung gewechselt hat.

Aktuell ist für solche Situationen keine Lösung innerhalb des Standards möglich. Es ist aber geplant, in einer späteren Version per Abgleich mit Steuerbehörden eine UID-Identifikation durchzuführen, um den SUA-Registrierungsprozess durchführen zu können.

3.3 Use Case 003: Prüfungsergebnis erstellen

Nach erfolgreichem Abgleich der Informationen stellt der Endempfänger seine Informationen bereit. Diese werden dann vom Distributor mittels der Operation `GetResultFromRegisterOrganizationConsumer` abgeholt.

Der Endempfänger liefert seine Antwort daraufhin per `GetResultFromRegisterOrganizationConsumer-Response` an den Distributor zurück, sofern die Prüfung erfolgreich war.

Im Fehlerfall (technisch oder fachlich) kann der Endempfänger den Prozess mit einem Fault (`OrganizationAuthenticationConsumerFault`) abbrechen.

3.4 Use Case 004: Testdaten kennzeichnen

Bei der Bestellung eines SUAZertifikates ist es möglich, dieses als Testfall zu kennzeichnen. Dies geschieht, indem das Element `<TestCase>` an entsprechender Stelle (gemäss Schema) in die XML-Instanz eingefügt wird. Das Ereignis wird vom Distributor normal verarbeitet, vom Endempfänger aber als Testfall behandelt.

Der Use Case dient zur Lokalisierung von Problemen in der produktiven Übermittlungskette. Dabei sollen Meldungen vom Unternehmen durch die gesamte Automatisierungskette der beteiligten Systeme (ERP, Transmitter, Distributor, Endreceiver) und ihrer Komponenten geschleust werden, ohne einen echten Geschäftsvorfall anzustossen. Es werden **keine Zertifikate** erzeugt.

Jegliche weiteren Aufrufe in Bezug auf dieser Verarbeitung *müssen* ebenfalls als Testfall markiert sein.

Es darf keine Mischformen in der Übermittlung geben: Was als Testfall beginnt, *muss* als Testfall beendet werden.

Dieser Use Case soll nur in Ausnahmefällen eine Verwendung finden. Als Demo- oder Entwicklungssystem darf er *nicht* genutzt werden. Für diese Zwecke stehen eine Referenzapplikation oder Show Case zur Verfügung.

3.5 Use Case 005: Security anwenden

Ausser dem Erreichbarkeitstest *muss* jede Übermittlung signiert und verschlüsselt gesendet und beantwortet werden. Einzelheiten dazu finden sich in den Dokumenten zur Sicherheit auf Empfängerseite (siehe (SECER, 2020))

3.6 Use Case 006 Erreichbarkeit prüfen

Der UseCase Erreichbarkeit prüfen setzt die 2-Way SSL Verschlüsselung voraus. Request und Response sind signiert und die XML-Daten sind verschlüsselt gemäss (SECER, 2020).

Kurzbeschreibung	Die Erreichbarkeit des Endreceivers soll vom Distributor aus geprüft werden. Dazu wird eine einfache PingConsumerRequest-Anfrage gemäss (WSDLOA, 2019) an den Endreceiver gesendet, der seinerseits die Erreichbarkeit mit der Antwort PingConsumerResponse bestätigt.
Akteure	Distributor, Operator des Distributors
Auslöser	Zyklische Überprüfung vom Distributor, Operator im Störfall
Vorbedingungen	Keine
Nachbedingungen	Keine
Included Use Cases	UC005 Security anwenden
Standardablauf	<ol style="list-style-type: none"> 1. Die Anfrage wird vom Distributor an den Endreceiver gesendet. Zusätzlich wird das Intervall des Pollings mitgeteilt. Intervall: zurzeit 30 Minuten (auch während eines Wartungsfensters; Intervall ist damit dynamisch) 2. Die Security wird geprüft UC005. 3. Der Endreceiver antwortet mit seinem aktuellen Timestamp, s. <PingConsumerResponse>.
Alternative Abläufe	{Schritt 3: Optional kann dem Distributor ein geplantes Wartungsfenster (Nichtverfügbarkeit von x bis y) mittels UC007 «Wartungsfenster setzen» mitgeteilt werden. Diese Funktion <i>muss</i> umgesetzt werden.}
Fehlerliste	Technische Fehler: <ul style="list-style-type: none"> ▪ Meldung ist nicht valid ▪ Meldung kann nicht entschlüsselt werden

Tabelle 4: Use Case 004 Erreichbarkeit prüfen

3.7 UC007 Wartungsfenster setzen

Kurzbeschreibung	Erweiterung des UC006 «Erreichbarkeit prüfen». Der Endreceiver <i>muss</i> eine Funktionalität implementieren, damit Daten für ein Wartungsfenster eingetragen und diese in der Antwort von UC006 «Erreichbarkeit prüfen» dem Distributor mitgeteilt werden können.
Akteure	Technischer Administrator des Endreceivers
Auslöser	Zyklische Überprüfung vom Distributor, Operator im Störfall
Vorbedingungen	Keine
Nachbedingungen	Keine
Included Use Cases	Keine
Standardablauf	<ol style="list-style-type: none">1. Der technische Administrator des Endreceivers trägt die Daten des Wartungsfensters ein.2. Die Antwort des Endreceivers (PingConsumerResponse) an den Distributor enthält die eingetragenen Daten für das Wartungsfenster.
Alternative Abläufe	keine
Fehlerliste	Technische Fehler: <ul style="list-style-type: none">▪ Meldung ist nicht valid

Tabelle 5: Use Case 007 Wartungsfenster setzen

3.8 UC008 Support, manuelle Klärung durchführen

Auf Supportanfragen muss dem Unternehmen zu einer bestimmten Zertifikatsbestellung Auskunft gegeben werden können. Entsprechend muss es für den Sachbearbeiter auf Empfängerseite möglich sein, aus Logfiles und Fehlermeldungen zu erkennen, wo Probleme aufgetreten sind. So müssen auch fehlerhafte Requests in den Logs verzeichnet werden und anhand der verwendeten IDs nachverfolgbar sein.

3.9 UC009 Duplikat behandeln

Duplikate eines kompletten `RegisterOrganization Requests` könnten vom Distributor technisch (bitgleich) erkannt und mittels eines Elements `<Duplicate>` im `DistributorRequestContext` gekennzeichnet werden. Dies würde aber bedingen, dass der Distributor ein Duplikat eindeutig als solches erkennen kann, weswegen in der Praxis auf die Verwendung des Elements `<Duplicate>` verzichtet wurde.

Es wird also keine Duplikate geben, da vom Distributor bei jedem Request eine neue `CertificateRequest-ID` vergeben wird. Der wiederholte `RegisterOrganization Request` für ein Unternehmen muss normal beantwortet werden.

4. Zusätzliche Anforderungen

4.1 Archiv-Files erstellen

Mit dieser Anforderung wird sichergestellt, dass eine Kopie jeder gesendeten und empfangenen Meldung gesichert wird. Die Daten müssen zu einem SOAP-Request aufbereitet und als XML-Instanzdokument abgelegt werden. Archivdateien müssen signiert sein, dürfen aber nicht verschlüsselt sein.

4.2 SUA Version

Im Schema befindet sich das Element `<RequestContext/UserAgent/StandardVersion>`, welches die verwendete Version des Swissdec-Unternehmens-Authentifizierungsstandard-CH (SUA) bezeichnet. Diese ist aufgrund von Anpassungen zwischen verschiedenen Versionen notwendig, die sich nicht auf das Schema beziehen, sondern ausschliesslich auf den Inhalt der Elemente, d.h. je nach Version des Swissdec-Unternehmens-Authentifizierungsstandard-CH (SUA) kann der Inhalt der Elemente unterschiedlich definiert sein.

4.3 Kommunikationsstandards

Die Standardkopplung *muss* auf der Web Service Technologie (SOAP² Version 1.1, WSDL³ Version 1.1 und WSS⁴ Version 1.0) basieren. Die Daten *müssen* neben dem HTTPS⁵ Layer (two-way SSL/TLS) zusätzlich auf der SOAP-Ebene gemäss WSS verschlüsselt werden (SECER, 2020).

4.4 Optionale Komprimierung

Eine Komprimierung der Requests und Responses ist optional. XML-Daten können auf Grund der vielen redundanten Informationen stark komprimiert werden. Erfahrungsgemäss lassen sich die verschlüsselten Daten um etwa 50% komprimieren. Um grosse Ereignismeldungen durch den Distributor verteilen zu können und um wertvolle Bandbreite aller Beteiligten zu sparen, besteht die Möglichkeit vom Distributor ausgehende Requests auf Basis von GZIP zu komprimieren. Ob Komprimierung eingesetzt wird, wird bei der Kopplung festgelegt.

Ausgehende Requests vom Distributor besitzen bei GZIP-Komprimierung des Bodys mindestens folgende Felder im http-Header:

- Content-Encoding: gzip
- Accept-Encoding: gzip

Komprimierte Antworten von Endreovern *müssen*, sofern Komprimierung eingesetzt wird, folgendes Feld enthalten:

- Content-Encoding: gzip

Weitere Informationen unter <http://www.ietf.org/rfc/rfc1952.txt>.

4.5 Verfügbarkeit

Die Betrachtungseinheit umfasst den Distributor und alle gekoppelten Endreceiver, d. h. das Unternehmen (Ereignisdatenquelle) erlebt das ganze System als Einheit. Sollte ein Endreceiver nicht in geforderter Qualität betrieben werden, vermindert dieser Empfänger die Zuverlässigkeit des ganzen Systems. Alle Teilnehmer müssen sich deshalb auf eine **minimale** Zuverlässigkeit einigen.

Anforderung aus dem Leistungsstandard-CH

- Alle Übermittlungen m2m (Machine to Machine) erfolgen in **«Echtzeit»**. (**7 x 24h Internet-Verfügbarkeit**)

Diese Anforderung hat für den Empfänger folgende Konsequenzen

- auch die Institutionen bzw. ihre Endreceiver **müssen** mindestens zum **Empfangen der Daten einen 7x24h Dienst anbieten**.
- **Geplante Unterbrüche⁶ (z. B. Wartungsfenster)** *müssen* an Randzeiten durchgeführt und *müssen* vorher angekündigt werden (siehe dazu Use Case UC003: «Erreichbarkeit prüfen»).
- Nach **ungeplantem Unterbruch** *sollten* betroffene Unternehmen, die eine missglückte Übermittlung hatten, über die erneute Verfügbarkeit des Empfängers benachrichtigt werden.
- Sollten interne Dienste zur Überprüfung der Akzeptierung **nicht zur Verfügung** stehen, *kann* trotzdem mit einer Akzeptierung quittiert werden. Dies *sollte* mit einer Warning/Notification in der Quittung dem Absender mitgeteilt

² SOAP (ursprünglich für Simple Object Access Protocol)

³ Web Services Description Language (WSDL) definiert eine plattform-, programmiersprachen- und protokollunabhängige XML-Spezifikation zur Beschreibung von Netzwerkdiensten (Web Services) zum Austausch von Nachrichten.

⁴ Web Services Security (WSS) von Organization for the Advancement of Structured Information Standards (OASIS)

⁵ http 1.0 oder 1.1; mindestens TLS 1.2 mit minimaler Sessionkey-Länge 256Bit

⁶ Gilt für normale Wartungsarbeiten; ausgenommen ist ein Hotfix oder Patch

werden. Führt eine spätere Datenprüfung zur Ablehnung der Meldung, muss diese dem Kunden ausserhalb dieser Systemspezifikation mitgeteilt werden.

Zielorientiertes Vorgehen bezüglich des Themas Verfügbarkeit:

Wir möchten eine **kundenorientierte Sicht** einnehmen. Die Verfügbarkeiten der Systeme sind als **zukünftige Zielwerte** zu verstehen. Damit werden die Unternehmen motiviert, ihre Meldungen elektronisch zu übermitteln. Bezüglich Verfügbarkeit ist keine Kontrolle vorgesehen. Deshalb werden hier nur die wesentlichen Richtwerte definiert und entsprechende Grundlagen in den Anhang verschoben.

4.6 Definierte Zeitbereiche

- Betriebszeit des gesamten Systems (Distributor, Kommunikation und Endreceiver; m2m Strecke bis zur Quittungs-Response an das Unternehmen)
 - 7 Tage pro Woche mal 24 Stunden
 - Spitzenzeiten: Ausser an Wochenenden täglich zwischen 6 Uhr bis 20 Uhr (die restliche Zeit ist Randzeit)
- Wartungsfenster für Korrekturen und Updates
 - 10 Stunden pro Woche
 - Ausserhalb der Spitzenzeiten, wenn möglich zwischen 2 Uhr und 5 Uhr morgens
- Service- und Support-Zeit für die Systemteilnehmer (Distributor und seine Endreceiver)
 - Zu den üblichen Bürozeiten
 - Support für Wartungsfenster auf Anmeldung

4.7 Definierte Wertebereiche

Ziel ist eine Pragmatische Lösung = «lightweight construction» und «Best Effort»

- In den **Spitzenzeiten** soll die Verfügbarkeit der Endreceiver (m2m) mindestens 99.52% sein.
- In den **Randzeiten** soll die Verfügbarkeit der Endreceiver (m2m) mindestens 93.00% sein.

4.8 Skalierbarkeit

Die Endempfängersysteme sollten nach der anstehenden Last skalieren können. Es ist durchaus denkbar mit einer minimalen Lösung zu starten und bei Bedarf die Leistung auszubauen, um die geforderte Verfügbarkeit und Performance zu garantieren.

4.9 Änderungen an der Schnittstelle

- Sollen Änderungen des Swissdec-Unternehmens-Authentifizierungsstandard-CH (SUA) auch beim Endreceiver aktiviert werden, *muss* die gesamte Kopplung (Seitens Distributor und Endreceiver) angepasst werden.
- Sollen keine Änderungen des Swissdec-Unternehmens-Authentifizierungsstandard-CH (SUA) beim Endreceiver aktiviert werden, *kann* der Distributor die bestehende Datenstruktur transformieren (mapping), sofern dies inhaltlich möglich ist («Design-Firewall»).

Der Distributor wird immer fachlich klar definierte Daten weitergeben. Im Moment ist keine generische Lösung geplant.

4.10 Support und Reaktionszeit

Es werden nur technische Aspekte zum Support festgelegt, d. h. hier werden nur Informationsstrukturen für alle Systeme in der Prozesskette definiert.

Der Support *muss* in den Sprachen Deutsch, Französisch und Italienisch für folgende Bereiche bzw. Akteure erbracht werden:

- Unternehmen und ihre ERP-Hersteller
- Endreceiver Institutionen

D.h. auch Fehlermeldungen sind zum Teil in den entsprechenden Sprachen auszugeben. Siehe in der Meldung:

.../RequestContext/LanguageCode

Zur Bestimmung einer Reaktionszeit werden folgende **Fehlerklassen** definiert

- Critical = 15 Min
- Medium = 4 h

- Uncritical = 1 Tag

Diese Fehlerklassen werden in verschiedenen Systemen (Applikationen, Logfiles, Überwachungstool, ...) später entsprechend verwendet.

Zusätzlich *muss* der 2nd Level Support zu den Applikationsentwicklern koordiniert werden.

4.11 Performance / Durchsatz

- Die maximale Datenmenge ist von jedem Endreceiver zu bestimmen und die Systeme entsprechend zu skalieren.
- Response-Time (alle Operationen): Die gesamte Übermittlung soll in «Echtzeit» ablaufen. Die Übermittlungs- bzw. Verteilungszeit soll **unter einer Minute** sein. Für den Endreceiver ergibt das:

- Verarbeitungszeit ist abhängig von Endreceiver, Datenmenge und der Leitungskapazität
 - Eine Antwort *sollte* unter 20 Sekunden vorliegen
 - Zusätzlich wird vom Distributor pro Endreceiver eine maximale Wartezeit definiert (Timeout: aktueller Default = 60 Sekunden).

5. Anhang

5.1 Referenzen

Die folgenden Referenzen können, zum Teil gebündelt als zip-Files, über das Internet bezogen werden. Die darin enthaltenen index.html - Files geben Zugang zu Informationen, der Übersicht und den einzelnen Dokumenten.

ACKNSwissdec, S. (2020). AcknowledgementNotification. Bern, Schweiz.

RLOA, S. (2019). Unternehmens-Authentifizierung Detailspezifikation. Bern, Schweiz.

SECER, S. (2020). Security Endreceiver. Bern, Schweiz. Von <https://tst.itserve.ch/swissdec/infopoint/> abgerufen

WSDLQA, S. (2019). OrganizationAuthenticationService, OrganizationAuthenticationRenewService WSDL. Bern, Schweiz.

XSDQA. (2019). OrganizationAuthenticationServiceTypes XSD. Bern, Schweiz.