

Richtlinien Swissdec Unternehmens-Authentifizierungsstandard-CH (SUA)

Anforderungen Transmitter

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 Transmitter	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 SUA-Zertifikat beschaffen	13
2.4.2	UC002 Bestellung / Registrierung	13
2.4.3	UC003 Aktivierung	13
2.4.4	UC004 Erreichbarkeit prüfen	13
2.4.5	Interoperabilität prüfen (1x Signatur)	13
2.4.6	UC006 Zertifikat erneuern	13
2.4.7	UC007 Interoperabilität prüfen mit Crt-UID (2x Signatur)	13
2.4.8	UC008 Testdaten kennzeichnen	13
2.4.9	UC009 Security anwenden	13
2.4.10	UC010 Support; manuelle Klärung durchführen	13
2.5	Use Cases und zugehörige Operationen	14
3.	Use Cases	15
3.1	Use Case 001: SUA-Zertifikat beschaffen	15
3.2	Use Case 002 Bestellung / Registrierung	17
3.2.1	Zertifikatsbeschaffung für Treuhänder	17
3.2.2	Zertifikatsbeschaffung ohne bestehende Vertragsbeziehung	17
3.3	Use Case 003 Aktivierung	18
3.4	Use Case 004 Erreichbarkeit prüfen	19
3.5	Use Case 005: Interoperabilität prüfen	20
3.5.1	Spezielle Anforderungen	20
3.5.2	Vorbedingungen	21
3.5.3	Nachbedingungen	21
3.6	Use Case 006: Zertifikat erneuern	22
3.7	Use Case 007: Interoperabilität prüfen 2x	23
3.8	Use Case 008: Testdaten kennzeichnen	24
3.9	Use Case 009: Security anwenden	25
3.10	UC010 Supportinformationen manuelle Klärung durchführen	26
3.11	Spezielle Anforderungen	27
3.11.1	Archiv-Files erstellen	27
4.	Anhang	28
4.1	Referenzen	28

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 and Configuration.....	10
Abbildung 4: Use Cases	11
Abbildung 5: Sequenzdiagramm zur Beschaffung eines SUA-Zertifikats	16
Abbildung 7: Use Case 010 Erreichbarkeit prüfen.....	19
Abbildung 8: Use Case11: Interoperabilität prüfen	20

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 10 Erreichbarkeit prüfen	19
Tabelle 5: Use Case Beschreibung Interoperabilität prüfen	20
Tabelle 6: Vorbedingungen (Transmitter)	21
Tabelle 7: Auswertung und Antwort Distributor.....	21
Tabelle 8: Auswertung Transmitter	21

Übersicht der Änderungen Version 20190301

Richtlinien für den Swissdec Unternehmens-Authentifizierungsstandard-CH (SUA) - Anforderungen für Transmitter, Version 1.0, Ausgabe 20190301 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 Unter www.swissdec.ch

1. Einleitung

Dieses Dokument enthält funktionale, technische und zusätzliche Anforderungen an Transmitter, die im Rahmen des Swissdec Unternehmens-Authentifizierungsstandards-CH (SUA) eingesetzt werden. Ein Transmitter wird dazu verwendet, das SUA-Zertifikat zu verwalten (beschaffen, aktivieren, prüfen und erneuern).

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.

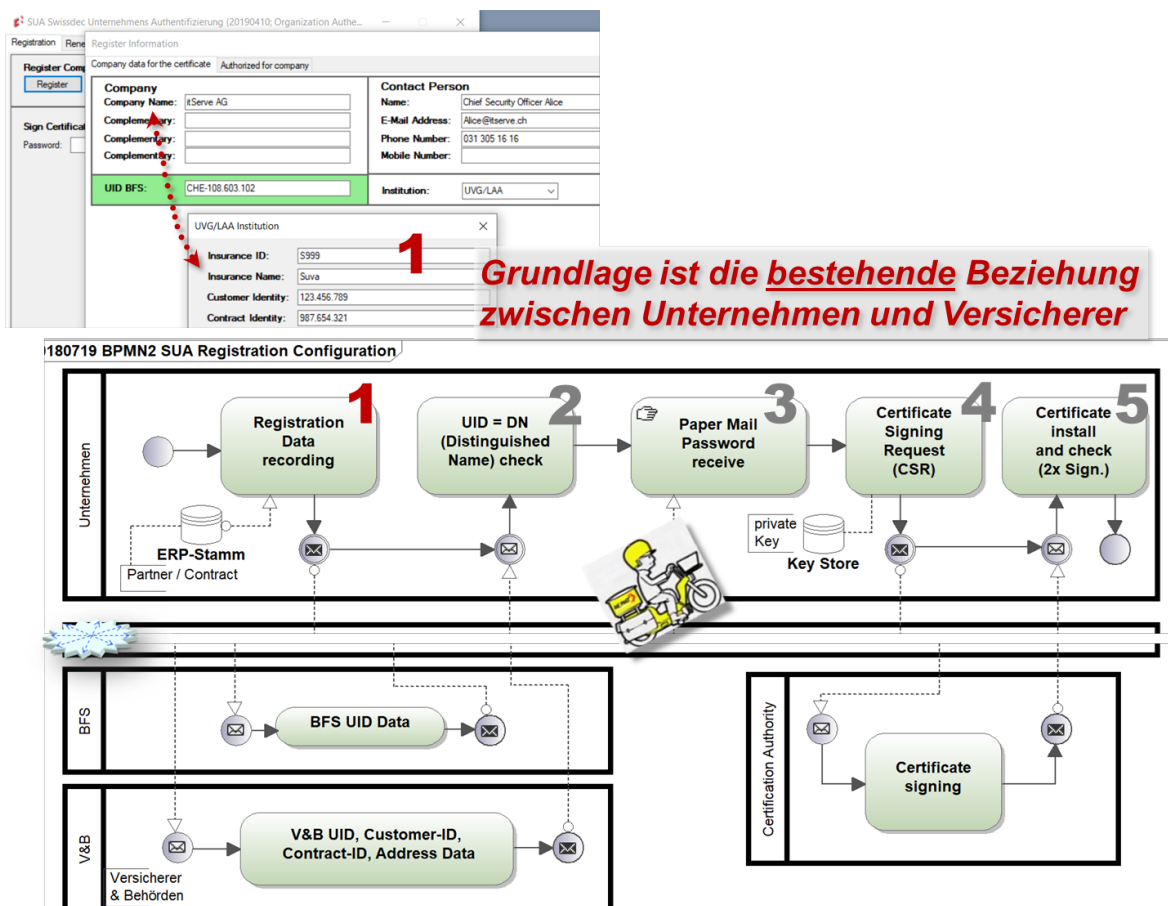


Abbildung 1: Skizze SUA Registration Configuration Schritt 1

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 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).

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 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.

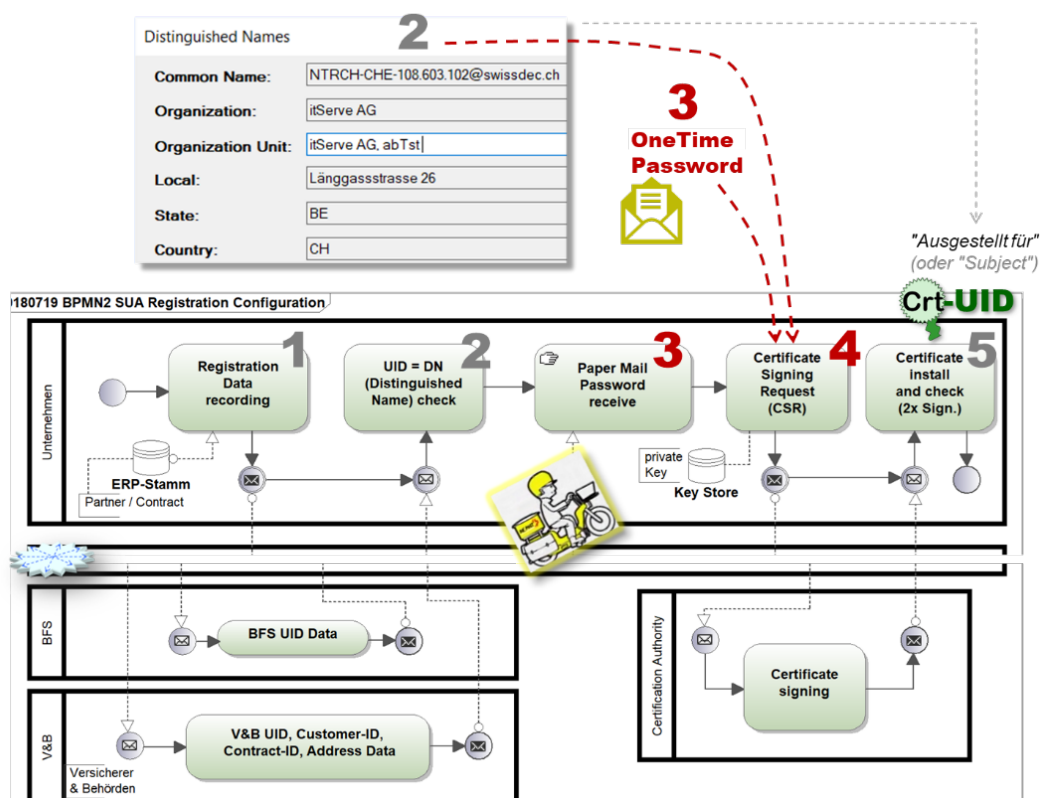


Abbildung 2: Skizze SUA Registration Configuration Schritte 2, 3, 4 und 5

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. Weitere Test-Übermittlungen sind möglich.

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

Für eine detaillierte Beschreibung des Ablaufs wird auf die Richtlinien bzw. Detailspezifikation (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 Transmitter

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

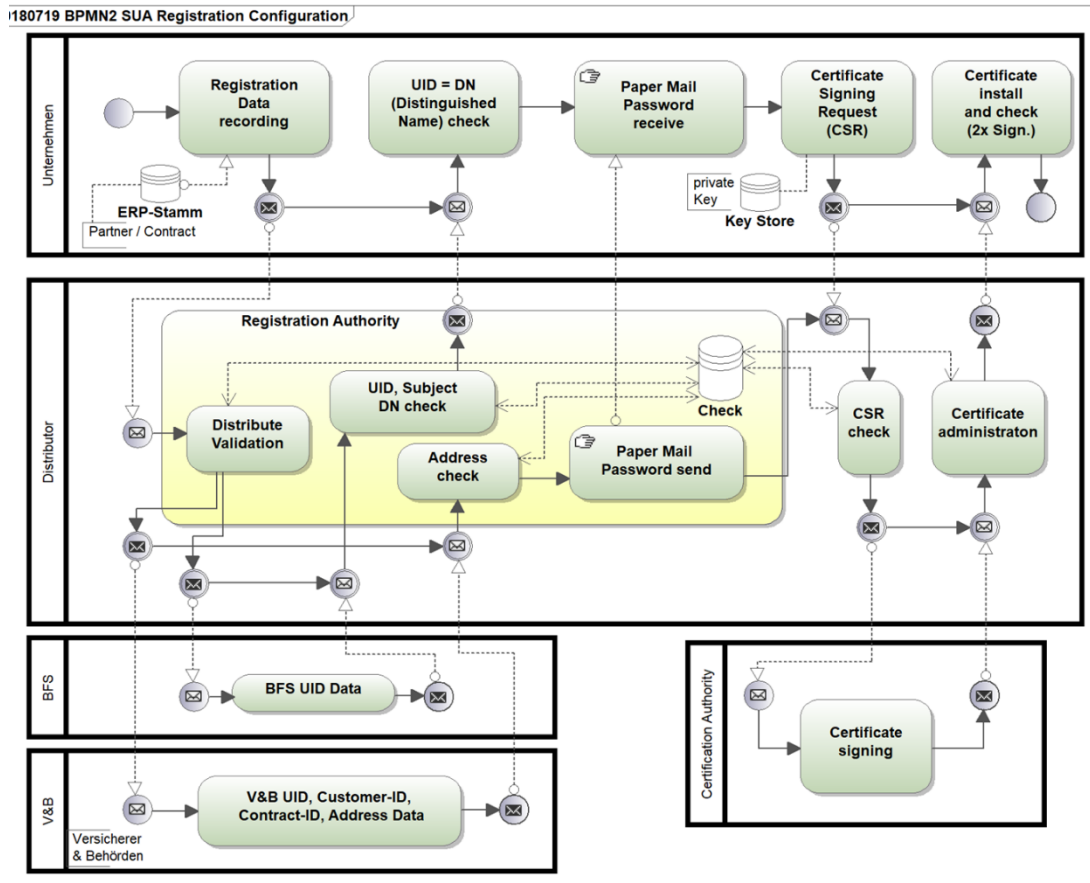


Abbildung 3: Prozess Skizze SUA Registration and Configuration

2.1 Übersichtsdiagramme zu den Use Cases

Ein Teil der Use Cases ist analog zu den anderen Swissdec Standards aufgebaut. Wurde ein solcher bereits umgesetzt, können dieselben Funktionalitäten auch für SUA verwendet werden (z.B. Erreichbarkeit, Interoperabilität).

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.

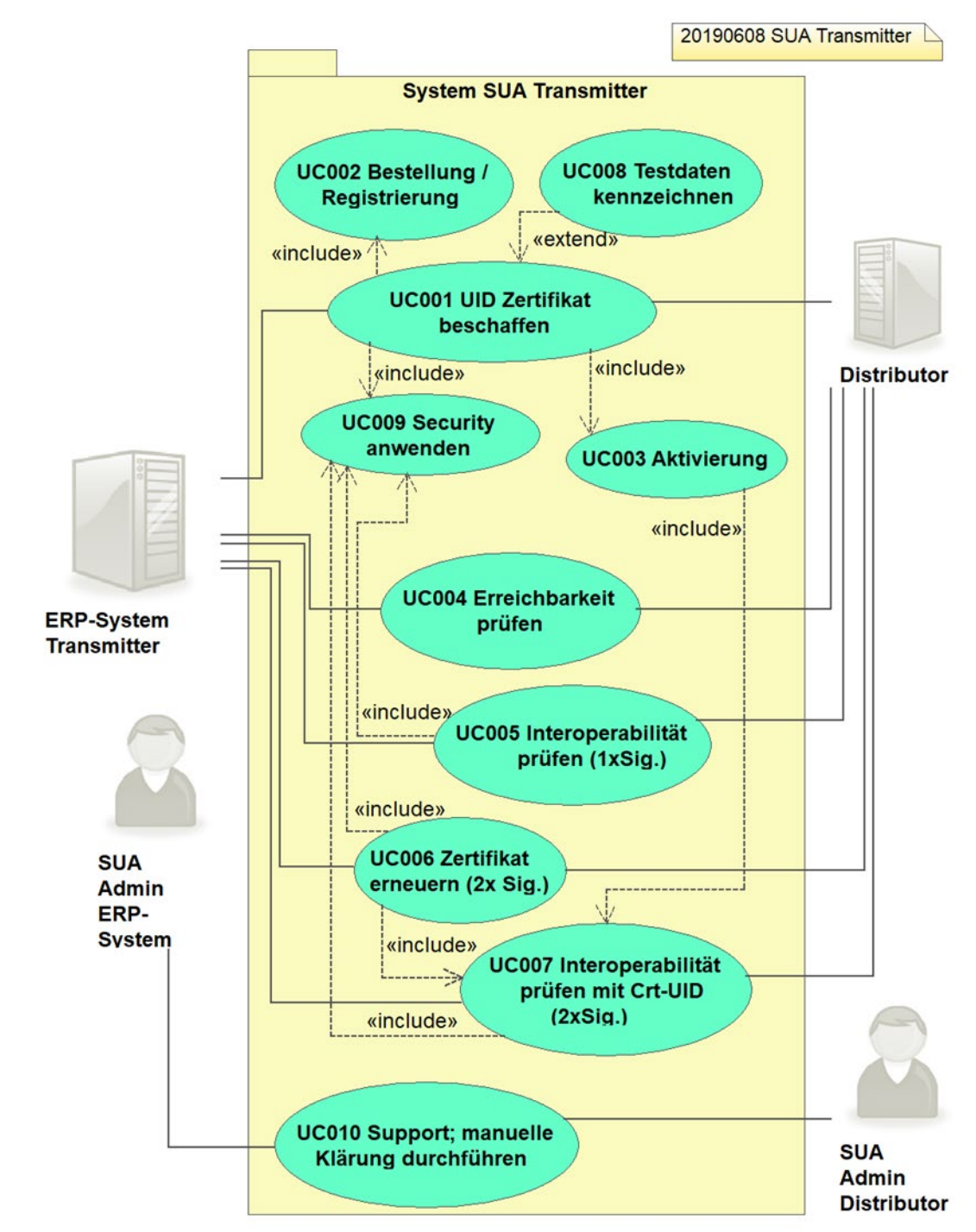


Abbildung 4: Use Cases

2.2 Erläuterungen zu den Use Cases

Die als Use Cases abgebildeten Anforderungen beziehen sich auf den technischen Teil eines Systems aus ERP-System und Transmitter, welcher die elektronische Aufbereitung und Übermittlung von Daten zur Beschaffung eines SUA-Zertifikats übernimmt.

Ein ERP-System mit Transmitter *muss* für die Zertifizierung immer die folgenden Systemanforderungen erfüllen:

- UC001 Zertifikat beschaffen
- UC002 Bestellung / Registrierung
- UC003 Aktivierung
- UC004 Erreichbarkeit prüfen
- UC005 Interoperabilität prüfen (1x Signatur)
- UC006 Zertifikat erneuern
- UC007 Interoperabilität prüfen mit Crt-UID (2x Signatur)
- UC008 Testdaten kennzeichnen
- UC009 Security anwenden
- UC010 Support; manuelle Klärung durchführen

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

Im Rahmen der Zertifizierung werden Tests durchgeführt, die auf den Use Cases basieren und so gut wie möglich auch in der Reihenfolge der Use Cases aufgebaut sind. 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 SUA-Zertifikat beschaffen

Ein neues Zertifikat wird via Distributor beschafft. Die Antwort vom Distributor wird gesichert, vgl. Kap. 3 "Use Case". Dazu werden weitere Use Cases verwendet: UC002, UC003, UC009 und UC008.

2.4.2 UC002 Bestellung / Registrierung

Mit der eigentlichen Bestellung / Registrierung wird die Identität des Antragstellers überprüft. Dabei werden vor allem die UID-BFS Daten durch einen Endempfänger (Versicherer & Behörden) und das BFS-Register geprüft. Als Success Resultat erhält der Transmitter/ERP-System eine CertificateRequest-ID und ein X509Subject zur Kontrolle. Zusätzlich wird ein Passwort mittels eines Briefes und dem Postweg an das Unternehmen gesendet.

2.4.3 UC003 Aktivierung

Nach der erfolgreichen Registrierung (UC002) kann nun das SUA-Zertifikat mit dem Passwort aus dem Brief (UC002) abgeholt werden. Danach wird das neue SUA-Zertifikat im ERP-System aktiviert und kann mittels der Interoperabilität (UC007) getestet werden.

2.4.4 UC004 Erreichbarkeit prüfen

Eine spezielle Meldung wird via Internet an den Distributor gesendet, um zu prüfen, ob dieser erreichbar ist.

2.4.5 Interoperabilität prüfen (1x Signatur)

Eine spezielle Meldung wird an den Distributor gesendet, um die Interoperabilität (z.B. Encoding, Marshalling, Zeitangaben etc.) zwischen Transmitter und Distributor zu prüfen. Dabei wird der Request nur mit dem ERP Zertifikat signiert.

2.4.6 UC006 Zertifikat erneuern

Ein SUA-Zertifikat kann jederzeit erneuert werden. Dazu wird ein CSR (Certificate Sign Request) an den Distributor gesendet und in der Response erhält der Transmitter das neue Zertifikat. Aus Sicherheitsgründen können nicht beliebig viele Erneuerungen gemacht werden. (siehe Detailspezifikation (RLOA, 2019))

2.4.7 UC007 Interoperabilität prüfen mit Crt-UID (2x Signatur)

Eine spezielle Meldung wird an den Distributor gesendet, um die Interoperabilität (z.B. Encoding, Marshalling, Zeitangaben etc.) zwischen Transmitter und Distributor zu prüfen. Dabei wird der Request mit den ERP- und SUA-Zertifikaten 2x signiert.

2.4.8 UC008 Testdaten kennzeichnen

Eine beliebige Meldung kann als Testfall gekennzeichnet werden. Sie wird somit über das produktive System versendet, vom Endreceiver jedoch nicht produktiv verarbeitet.

2.4.9 UC009 Security anwenden

Jede übermittelte Meldung muss mindestens einmal signiert (ERP Zertifikat) und verschlüsselt sein.

2.4.10 UC010 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.

2.5 Use Cases und zugehörige Operationen

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

Use Case	Operation / Element
	<i>OrganizationAuthenticationService WSDL / XSD</i>
UC001 SUA-Zertifikat beschaffen UC002 Bestellung / Registrierung	<ul style="list-style-type: none"> RegisterOrganization RegisterOrganizationResponse GetResultFromRegisterOrganization GetResultFromRegisterOrganizationResponse OrganizationAuthenticationFault
UC003 Aktivierung	<ul style="list-style-type: none"> SignCertificate SignCertificateResponse OrganizationAuthenticationFault
UC004 Erreichbarkeit prüfen	<ul style="list-style-type: none"> Ping PingResponse
UC005 Interoperabilität prüfen	<ul style="list-style-type: none"> CheckInteroperability CheckInteroperabilityResponse
	<i>OrganizationAuthenticationRenewService WSDL / XSD</i>
UC006 Zertifikat erneuern	<i>2x signiert (ERP- und SUA-Zertifikat)</i> <ul style="list-style-type: none"> RenewCertificate RenewCertificateResponse OrganizationAuthenticationFault
UC007 Interoperabilität prüfen	<i>2x signiert (ERP- und SUA-Zertifikat)</i> <ul style="list-style-type: none"> CheckInteroperability CheckInteroperabilityResponse

Tabelle 2: Use Cases und Operationen

3. Use Cases

3.1 Use Case 001: SUA-Zertifikat beschaffen

Use Case Diagramm: siehe Abbildung 4: Use Cases auf Seite 11.

Kurzbeschreibung	Ein neues SUA-Zertifikat wird via Distributor beschafft. Die Rückantworten des Distributors werden ausgewertet und abgelegt. Ein Archiv-File der gesendeten Meldung wird ebenfalls gesichert.
Akteure	ERP-System, Distributor, Endreceiver
Auslöser	Ein Angestellter des Unternehmens (Sicherheitsbeauftragte) möchte ein SUA-Zertifikat beschaffen.
Vorbedingungen	Das ERP-System ist in der Lage, elektronische Ereignismeldungen zu versenden und zu empfangen und ist im Besitz eines ERP-Zertifikats.
Nachbedingungen	<ul style="list-style-type: none"> Die SUA-Zertifikatsbeschaffung wurde erfolgreich durchgeführt Das SUA-Zertifikat wurde aktiviert und erfolgreich getestet Bei einem Fehlschlag: <ul style="list-style-type: none"> Fehlermeldung
Included Use Cases	UC002 Bestellung / Registrierung UC003 Aktivierung UC007 Interoperabilität prüfen mit Crt-UID (2x Signatur) UC009 Security anwenden
Standardablauf	<ol style="list-style-type: none"> UC002: Das Zertifikat wird beim Distributor bestellt. Dazu ist eine bestehende Versicherung mit den aktuellen Vertragsbeziehung anzugeben. Die Meldung wird dazu 1x signiert (UC009). Das Resultat dazu wird asynchron abgeholt und geprüft. Die Meldung wird dazu 1x signiert (UC009). Das X509Subject entspricht dann dem Zertifikatsantrag und <i>muss</i> vom Antragsteller geprüft werden. Es wird auf den Brief mit dem OneTimePassword von der Post gewartet. UC003: Es wird ein CSR erstellt und mit dem OneTimePassword an den Distributor gemeldet. Die Meldung wird dazu 1x signiert (UC009). Dabei <i>müssen</i> alle Angaben gemäss X509Subject vom Schritt 2 identisch sein. Einzig der OU (Organization Unit) im Distinguished Names darf angepasst werden. Der private Key bleibt dabei auf dem Transmitter. Im Response erhält der Transmitter das SUA-Zertifikat. Das SUA-Zertifikat wird installiert und aktiviert. Danach <i>muss</i> alles mit dem UC007 überprüft werden. Weiter Test-Übermittlungen mit bestehenden Swissdec-Standards <i>sollen</i> zusätzlich erfolgen.
Alternative Abläufe	{UC008} Daten als Testdaten versenden Wie Standardablauf Schritte 1 bis 4 siehe Skizze Aber in Schritt: <ol style="list-style-type: none"> Es wird kein Brief versendet. Das OneTimePassword ist im <code>GetResultFromOrganizationRegistrationResponse ... Success/Comment</code> Im Response wird kein SUA-Zertifikat zurückgegeben.
Fehlerliste	Fachliche Fehler: <ul style="list-style-type: none"> die Meldung verstösst gegen die Plausibilisierungsregeln Technische Fehler: <ul style="list-style-type: none"> Fehler beim Signieren oder Verschlüsseln der Endreceiver ist nicht erreichbar die vom ERP-System aufbereitete Meldung entspricht nicht dem Schema (Validität nicht gegeben)

Tabelle 3: Use Case 001 LM übermitteln

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

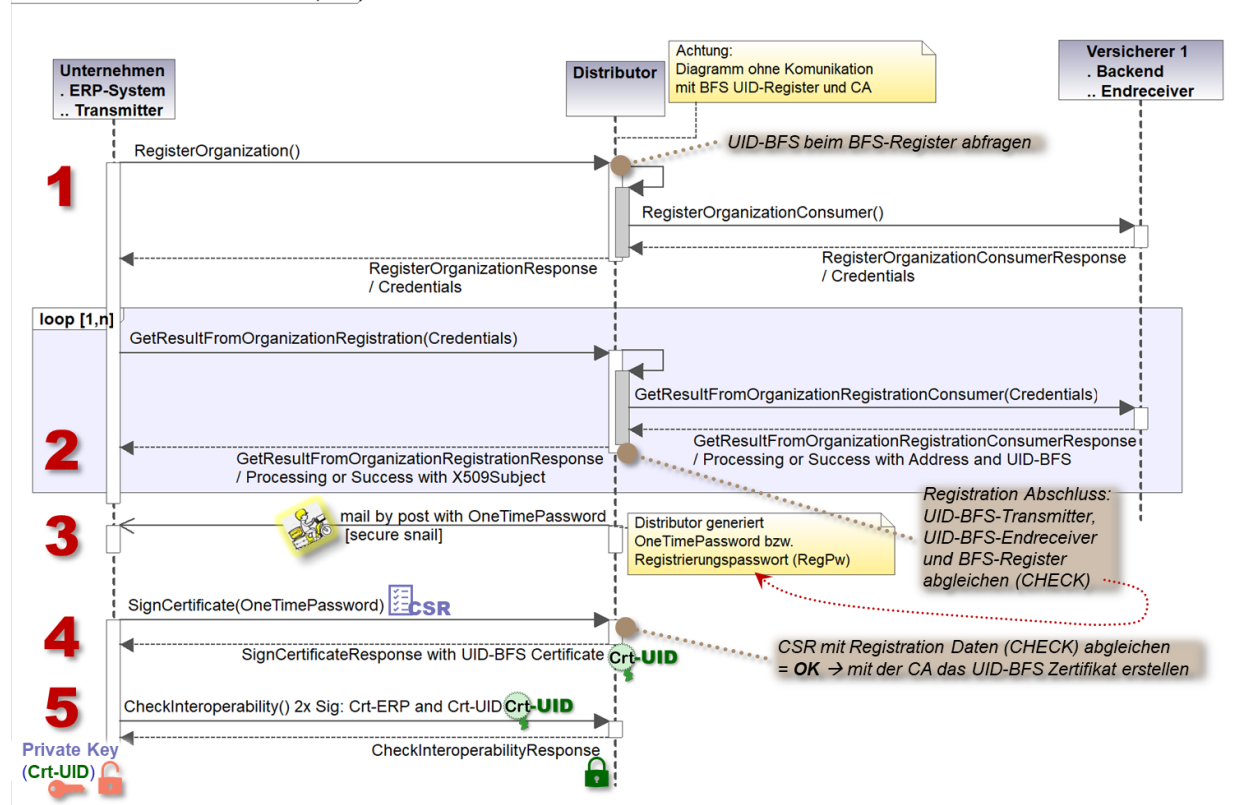


Abbildung 5: Sequenzdiagramm zur Beschaffung eines SUA-Zertifikats

3.2 Use Case 002 Bestellung / Registrierung

In einem ersten Schritt muss das Zertifikat vom Unternehmen angefordert werden (siehe UC001). Dies geschieht in zwei Schritten:

Mit dem Aufruf `RegisterOrganization` wird die Beschaffung des Zertifikates eingeleitet. Das Unternehmen liefert die benötigten Informationen für eine Zertifikatserstellung an den Distributor, welcher den Endempfänger über den Antrag informiert.

Der Endempfänger prüft die Gültigkeit der Anfrage und liefert dem Distributor seine Antwort zurück.

Mit dem Aufruf `GetResultFromRegisterOrganization` kann das Unternehmen nun die Informationen vom Endempfänger auf dem Distributor abholen.

Grundlage für eine Zertifikatsbestellung ist eine bestehende Vertragsbeziehung zwischen Unternehmen und Endempfänger. Ausnahme hierzu bilden Treuhänder (siehe Abschnitt 3.2.1).

Ein Unternehmen kann parallel mehrere aktive Registrierungs-Anfragen haben, z.B. dann, wenn es über mehrere, unterschiedliche ERP-Systeme verfügt. Die Anzahl dieser Anfragen ist aktuell auf fünf beschränkt, um überflüssige Anfragen ans UID-Register des BFS und den unnötigen Versand von Briefen zu vermeiden. Das Versenden von Informationen per Briefpost kann 1-2 Tage dauern. Mit der Limitierung soll verhindert werden, dass der Benutzer in dieser Zeit weitere Anfragen zur selben UID mit demselben ERP-System stellt.

3.2.1 Zertifikatsbeschaffung für Treuhänder

Wird ein Unternehmen von einem Treuhänder verwaltet, so ist Folgendes zu beachten:

Der Treuhänder hat keine direkte Beziehung zum Endempfänger, auf deren Grundlage eine SUA-Registrierung durchgeführt werden kann. In diesem Fall kann die Vertragsbeziehung eines von ihm verwalteten Unternehmens zur Registrierung verwendet werden. Dazu muss der Treuhänder 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. Der registrierende Endempfänger 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 SUA-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.

Zur Absicherung des Prozesses erhält der Endempfänger nicht die kompletten Treuhänderinformationen, sondern nur die Information `<WithDelegate>`, worauf er auf seine eigenen Informationen zum Unternehmen zurückgreifen und seine damit verknüpften Treuhänderinformationen an den Distributor zurücksenden muss. Nur wenn die Informationen beider Seiten übereinstimmen, kann das Zertifikat ausgestellt werden.

3.2.2 Zertifikatsbeschaffung ohne bestehende Vertragsbeziehung

Im Moment ist eine Zertifikatsbeschaffung ohne bestehende Vertragsbeziehung nicht mit dem regulären SUA-Prozess möglich. In Anbetracht dessen, dass mit der Zeit weitere Swissdec-Prozesse mit SUA abgewickelt werden sollen, wird dies jedoch in absehbarer Zeit notwendig sein. Angedacht sind Varianten mit einer Prüfung über die Steuerbehörde, zu der vom betroffenen Unternehmen aus auf jeden Fall eine Beziehung besteht.

3.3 Use Case 003 Aktivierung

Hat das Unternehmen die nötigen Informationen für die Aktivierung ihres Zertifikates erhalten, kann der nächste Schritt durchgeführt werden. Hierbei erstellt das Unternehmen ein CSR und sendet dieses in Kombination mit dem brieflich erhaltenen OneTimePassword an den Distributor.

Da noch kein gültiges SUA-Zertifikat vorhanden ist, wird diese Meldung einfach signiert (UC009). Dabei müssen alle Angaben gemäss X509Subject von der ursprünglichen Registrierung identisch sein. Einzig der OU (OrganizationUnit) im DistinguishedNames darf angepasst werden.

Der private Key kann auf diese Weise auf dem Transmitter verbleiben, so dass die Sicherheit des Zertifikates gewährleistet ist.

In der Response auf diese Anfrage erhält der Transmitter das gültige SUA-Zertifikat, welches nun für die doppelte Signatur/Verschlüsselung verwendet werden kann. Dieses muss installiert und aktiviert werden, ehe das Ganze mit UC007 überprüft werden kann

3.4 Use Case 004 Erreichbarkeit prüfen

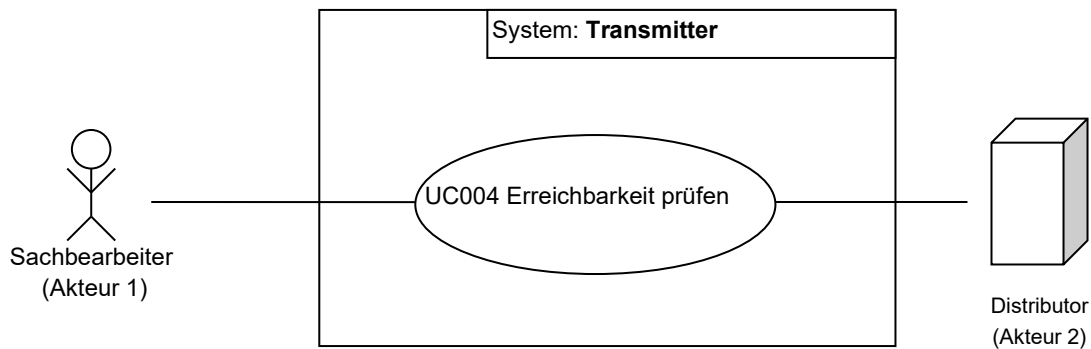


Abbildung 6: Use Case 010 Erreichbarkeit prüfen

Kurzbeschreibung	Die Erreichbarkeit des Distributors <i>muss</i> geprüft werden. Dazu wird eine einfache Anfrage (WSDLOA, 2019) an den Distributor geschickt. Die Rückantwort des Distributors bestätigt die Erreichbarkeit.
Akteure	Akteur 1: Sachbearbeiter, Akteur 2: Distributor
Auslöser	Die Erreichbarkeit des Distributors soll geprüft werden.
Vorbedingungen	Keine
Nachbedingungen	<ul style="list-style-type: none"> Die Rückantwort des Distributors enthält einen Timestamp mit der Systemzeit des Distributors (XSDOA, 2019) <p>Bei einem Fehlschlag:</p> <ul style="list-style-type: none"> Distributor nicht erreichbar: Fehlermeldung Inhalt verschieden (XSDOA, 2019) (ACKNSwissdec, 2018): Fehlermeldung
Included Use Cases	-
Standardablauf	<ol style="list-style-type: none"> Der Akteur löst die Überprüfung aus. Der Transmitter sendet eine einfache Serveranfrage (Ping) an die Zieladresse des Distributors Der Transmitter wertet die Rückantwort des Distributors aus
Alternative Abläufe	<p>Distributor nicht erreichbar</p> <p>{nach Schritt 1}</p> <ol style="list-style-type: none"> Eine Fehlermeldung wird angezeigt. <p>{Ende}</p>
Fehlerliste	<p>technische Fehler:</p> <ul style="list-style-type: none"> der Distributor ist nicht erreichbar der Distributor sendet eine falsche Antwort

Tabelle 4: Use Case 10 Erreichbarkeit prüfen

Mit dem Ping-Aufruf wird die Systemzeit übermittelt, so dass es möglich ist, die Zeiten von Distributor und Absender zu vergleichen. Damit lassen sich Timestamp-Probleme aufdecken.

Der Transmitter *muss* die erhaltene Systemzeit des Distributors mit der eigenen abgleichen und den Benutzer im Falle einer grösseren Abweichung darauf hinweisen. Diese Abweichung beträgt höchstens 1 Minute in die Zukunft und 2 Minuten in die Vergangenheit.

Dieser UseCase dient der Qualitätssicherung bei der Installation und der Entwicklung.

3.5 Use Case 005: Interoperabilität prüfen

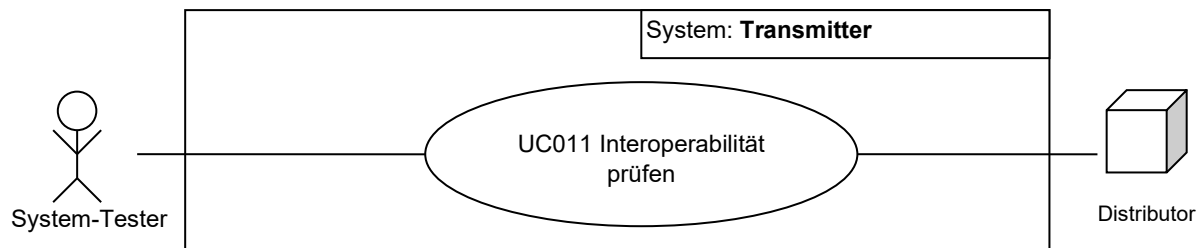


Abbildung 7: Use Case11: Interoperabilität prüfen

Kurzbeschreibung	Damit die Interoperabilität zwischen einem Transmitter und dem Distributor überprüft werden kann, <i>muss</i> der Transmitter einen «CheckInteroperabilityRequest» (WSDLID, 2018) absetzen können.
Akteure	System-Tester, Distributor
Auslöser	Installation soll getestet werden.
Vorbedingungen	Keine
Nachbedingungen	Die Übermittlung war erfolgreich, die Resultate entsprechen den Erwartungen.
Included Use Cases	-
Standardablauf	<ol style="list-style-type: none"> 1. Der Akteur startet die Interoperabilitätsprüfung und gibt Werte für Operand 2 ein. 2. Der Akteur löst das Senden der Daten aus. 3. Der Transmitter bereitet die Serveranfrage auf. 4. Die Meldung wird mit dem privaten Schlüssel/Zertifikat des Herstellers und mit der Unternehmensidentifikation nach Spezifikation (SECTID, 2018) signiert. 5. Der Transmitter sendet die Serveranfrage ssl-verschlüsselt an den Distributor. 6. Der Distributor bearbeitet die gesendeten Daten (Transformation Umlautstring, Berechnung «FirstOperand +- SecondOperand») und schickt die Antwort an den Transmitter. 7. Der Transmitter wertet die Antwort des Distributors aus. 8. Der Transmitter zeigt die Antwort des Distributors an.
Fehlerliste	<p>Fachliche Fehler:</p> <ul style="list-style-type: none"> ▪ Interoperabilität ist nicht gegeben <p>Technische Fehler:</p> <ul style="list-style-type: none"> ▪ Fehler beim Signieren ▪ Fehler beim ver/-entschlüsseln ▪ der Distributor ist nicht erreichbar

Tabelle 5: Use Case Beschreibung Interoperabilität prüfen

3.5.1 Spezielle Anforderungen

Der Interoperabilitätstest wird zu Entwicklungszwecken und bei der Installation verwendet, um die Interoperabilität zwischen einem Transmitter und dem Distributor zu gewährleisten.

Die grössten zu erwartenden Schwierigkeiten liegen dabei in den Bereichen Codierung von Zeichenketten (Encoding) und Interpretation von Fließkommazahlen.

Ausserdem erlaubt der Interoperabilitätstest einen einfachen und schnellen Security-Check.

Beide Systeme (Transmitter und Distributor) müssen dabei bestimmte Auswertungen vornehmen, um bei einem eventuellen Fehler auf den Verursacher schliessen zu können.

Die Parameter in den folgenden Tabellen sind in (WSDLID, 2018) ersichtlich.

3.5.2 Vorbedingungen

Der Transmitter sendet folgende Daten:

Parametername	Wert	Bemerkungen
UmlautString	ÄÖÜÄÉÓÚÄÊÔÛ	fester Wert
FirstOperand	999000000000.00	fester Wert, 999 milliards
SecondOperand	keine Vorgabe	beliebige Fließkommazahl
SystemDateTime	Datum und Zeit des Transmitters	Systemdatum und –zeit

Tabelle 6: Vorbedingungen (Transmitter)

3.5.3 Nachbedingungen

Auswertung und Antwort des Distributors:

Parametername	Auswertung / Berechnung	Bemerkungen
UmlautStringIsCorrect	$UmlautString_{TRANS} = \text{ÄÖÜÄÉÓÚÄÊÔÛ}$	Rückgabe: true / false
FirstOperandIsCorrect	$FirstOperand_{TRANS} = 999000000000.00$	Rückgabe: true / false
UmlautString	äöüäéóúäêôû	Rückgabe: UmlautString _{DISTRI} Gross- zu Kleinbuchstaben.
AdditionResult	$AdditionResult_{DISTRI} = FirstOperand_{TRANS} + SecondOperand_{TRANS}$	Rückgabe: berechneter Wert AdditionResult _{DISTRI}
SubstractionResult	$SubstractionResult_{DISTRI} = FirstOperand_{TRANS} - SecondOperand_{TRANS}$	Rückgabe: berechneter Wert SubstractionResult _{DISTRI}
SystemDateTime	Datum und Zeit des Distributors	Rückgabe: Systemdatum und –zeit

Tabelle 7: Auswertung und Antwort Distributor

Auswertung des Transmitters:

Parametername	Auswertung / Berechnung	Bemerkungen
UmlautStringIsCorrect	$UmlautStringIsCorrect = true$	muss true sein
FirstOperandIsCorrect	$FirstOperandIsCorrect = true$	muss true sein
UmlautString	$UmlautString_{DISTRI} = \text{äöüäéóúäêôû}$	muss äöüäéóúäêôû sein
AdditionResult	$FirstOperand_{TRANS} + SecondOperand_{TRANS} = AdditionResult_{DISTRI}$	Berechnung und Vergleich, Genauigkeitsgrad 2 Nachkommastellen
SubstractionResult	$FirstOperand_{TRANS} - SecondOperand_{TRANS} = AdditionResult_{DISTRI}$	Berechnung und Vergleich, Genauigkeitsgrad 2 Nachkommastellen
SystemDateTime	$ SystemDateTime_{DISTRI} - SystemDateTime_{TRANS} < 1h$	Betrag Zeitdifferenz sollte < 1 Stunde sein

Tabelle 8: Auswertung Transmitter

3.6 Use Case 006: Zertifikat erneuern

Ein SUA-Zertifikat hat normalerweise eine Laufzeit von einem Jahr.

Nach Ablauf dieser Zeit kann das SUA-Zertifikat eine limitierte Anzahl von Malen über den SUA-Prozess erneuert werden². Danach ist die Beschaffung eines neuen SUA-Zertifikates notwendig. Die eingeschränkte Anzahl von Erneuerungen ist notwendig, um sicherzustellen, dass die hinterlegten SUA-Zertifikatsinformationen aktuell gehalten werden (Aktualität und Authentizität).

Sobald die Gültigkeit des hinterlegten SUA-Zertifikates 30 Tage unterschreitet, soll der Erneuerungsprozess automatisch angestossen werden. Für den Erneuerungsprozess wird das bestehende SUA-Zertifikat verwendet, sowie das bei Initial-Registrierung erhaltene Passwort.

Mit der Operation `RenewCertificate` wird die Erneuerung ausgelöst. Der Distributor überprüft die Gültigkeit der Anfrage und führt einen Abgleich mit dem UID-Register des BFS durch, um sicherzustellen, dass die Angaben zum Unternehmen noch aktuell sind. Stimmen die Angaben im UID-Register nicht mit jenen des alten SUA-Zertifikats überein, wird die Anfrage abgebrochen und das Unternehmen muss anstelle einer Erneuerung den kompletten Zertifikatsprozess neu durchlaufen.

Andernfalls kümmert sich der Distributor um die Beschaffung eines neuen SUA-Zertifikates mit erneuter Gültigkeit von einem Jahr und liefert jenes an das Unternehmen aus. Dieses muss nun zur Überprüfung des neuen Zertifikates eine Testmeldung absetzen.

² Wie oft der Erneuerungsprozess möglich ist, wird bestimmt, wenn erste Erfahrungen mit dem produktiven Prozess gesammelt werden konnten.

3.7 Use Case 007: Interoperabilität prüfen 2x

Dieser Use Case ist praktisch identisch mit Use Case 005: Interoperabilität prüfen 1x. Der einzige Unterschied besteht darin, dass nun zusätzlich mit dem ERP-Zertifikat noch mit dem SUA-Zertifikat signiert wird. Dies ermöglicht es dem Benutzer, die Gültigkeit und korrekte Installation des SUA-Zertifikates zu testen.

3.8 Use Case 008: Testdaten kennzeichnen

Bei der Bestellung eines SUA-Zertifikates ist es möglich, diese 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.

Dieser 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 diese Verarbeitung *müssen* ebenfalls als Testfall markiert sein.

Es darf keine Mischformen in der Übermittlung geben: Was als Testfall beginnt, *muss* als Testfall beendet werden. Ebenso kann eine produktiv ausgeführte Registrierung nicht als Testfall weitergeführt 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 ein Showcase zur Verfügung.

3.9 Use Case 009: Security anwenden

Ausser dem Erreichbarkeitstest muss jede Übermittlung signiert und verschlüsselt werden. Einzelheiten dazu finden sich in den Dokumenten zur Sicherheit auf Transmitterseite (siehe (SECTR)).

3.10 UC010 Supportinformationen manuelle Klärung durchführen

Kurzbeschreibung	Fehler, Warnungen und Informationen gemäss (ACKNSwissdec, 2018) <i>müssen</i> ausgewertet und dem Benutzer angezeigt und/oder dem Endempfänger mitgeteilt werden. IDs <i>müssen</i> verwendet werden.
Akteure	Lohnbuchhaltungsapplikation, Transmitter, Distributor
Auslöser	Eine Meldung oder eine Anfrage wurde via Distributor an einen Endempfänger gesendet. Die Antwort wird via Distributor empfangen.
Vorbedingungen	<ul style="list-style-type: none"> Distributor sendet eine Antwort
Nachbedingungen	<ul style="list-style-type: none"> Fehler, Warnungen und Informationen aus der Antwort werden aufbereitet und dem Benutzer vollständig und in verständlicher Form angezeigt. Für den Endbenutzer nicht relevante Informationen müssen dem technischen Support zur Verfügung stehen (StackTrace, Fault-Detail, etc.) Hinweise an den Endreceiver müssen diesem als Notification gesendet werden. Bei einem Fehlschlag: Distributor nicht erreichbar: Fehlermeldung
Included Use Cases	-
Fehlerliste	<p>technische Fehler:</p> <ul style="list-style-type: none"> Fehler beim Signieren der Distributor ist nicht erreichbar die von der Lohnbuchhaltung aufbereitete Meldung entspricht nicht dem Schema (Validität nicht gegeben) Fehler beim ver/ -entschlüsseln <p>Fachliche Fehler:</p> <ul style="list-style-type: none"> Gemäss (RLID, 2018)

3.11 Spezielle Anforderungen

3.11.1 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. Anhang

4.1 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. (2018). AcknowledgementNotification. Bern, Schweiz.

OVID, S. (2018). IncidentOverview. Bern, Schweiz.

OVOA, S. (2019). Overview Unternehmens-Authentifizierung SUA. Bern, Schweiz.

RLID, S. (2018). Richtlinien für den Leistungsstandard-CH. Bern, Schweiz.

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

SECTID, S. (2018). ID_SecurityTransmitter. Bern, Schweiz.

SECTR, S. (kein Datum). SecurityTransmitter. Bern, Schweiz.

WSDLID, S. (2018). IncidentDeclarationService. Bern, Schweiz.

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

XSDID. (2018). IncidentDeclarationServiceTypes.xsd. Bern, Schweiz.

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