

# **Anforderungen Endreceiver**

## **Richtlinien Leistungsstandard-CH (KLE)**

Swissdec, 6002 Luzern

[www.swissdec.ch](http://www.swissdec.ch)

Richtlinien für Leistungsstandard (KLE)  
Anforderungen Endreceiver

Die Endreceiver Richtlinien für die Datenübermittlung im Leistungsstandard-CH (KLE) wurden in Zusammenarbeit mit folgenden Beteiligten erarbeitet:

- Suva
- Schweizerischer Versicherungsverband

#### **Herausgeber**

Swissdec  
Fluhmattstrasse 1  
Postfach 4358  
6002 Luzern  
[www.swissdec.ch](http://www.swissdec.ch)

## Inhaltsverzeichnis

<b>1.</b>	<b>Einleitung .....</b>	<b>6</b>
1.1	Tests .....	6
1.2	Abkürzungen .....	6
1.3	Ablauf der Ereignisdatenübermittlung .....	7
<b>2.</b>	<b>Übersicht Use Cases .....</b>	<b>8</b>
2.1	Erläuterungen zu den Use Cases .....	10
2.2	Use Cases und zugehörige Operationen .....	10
2.3	Summary Use Cases .....	10
2.3.1	UC001 Ereignisdeklaration empfangen .....	10
2.3.2	UC002 Ereignissynchronisation empfangen .....	10
2.3.3	UC003 Erreichbarkeit prüfen .....	10
2.3.4	UC004 Security anwenden .....	10
2.3.5	UC005 Wartungsfenster setzen .....	11
2.3.6	UC006 Testdaten erhalten .....	11
2.3.7	UC007 Duplikate behandeln .....	11
2.3.8	UC008 Datenflüsse steuern .....	11
2.3.9	UC009 Supportanfrage bearbeiten .....	11
<b>3.</b>	<b>Use Case Beschreibungen .....</b>	<b>12</b>
3.1	UC001 Ereignisdeklaration empfangen .....	12
3.2	UC002 Ereignissynchronisation empfangen .....	14
3.3	UC003 Erreichbarkeit prüfen .....	16
3.4	UC004 Security anwenden .....	16
3.5	UC005 Wartungsfenster setzen .....	17
3.6	UC006 Testdaten erhalten .....	17
3.7	UC007 Duplikate behandeln .....	18
3.7.1	Declare Duplikate .....	18
3.7.2	Declare Duplikate ohne Distributor Erkennung .....	18
3.7.3	Synchronize Duplikate .....	18
3.7.4	Synchronize identische Story .....	18
3.7.5	Synchronize StoryID nicht unique innerhalb IncidentContext .....	18
3.8	UC008 Datenflüsse steuern .....	19
3.9	UC009 Supportanfrage bearbeiten .....	20
<b>4.</b>	<b>Zusätzliche Anforderungen .....</b>	<b>21</b>
4.1	Leistungsstandard-CH Version .....	21
4.2	Kommunikationsstandards .....	21
4.3	Optionale Komprimierung .....	21
4.4	Todo Verfügbarkeit .....	21
4.4.1	Definierte Zeitbereiche .....	22
4.4.2	Definierte Wertebereiche .....	22
4.5	Todo Skalierbarkeit .....	22
4.6	Änderungen an der Schnittstelle .....	23
4.7	Todo Support und Reaktionszeit .....	23
4.8	Todo Performance / Durchsatz .....	24
4.9	Sicherheit und Datenschutz .....	25
4.10	Adressierung und Filterung .....	25
<b>6.</b>	<b>Anhang .....</b>	<b>26</b>
6.1	Mitgeltende Spezifikationsdokumente .....	26

## Abbildungsverzeichnis

Abbildung 1: Declare und Synchronize im Leistungsstandard, BPMN Diagramm und Schnittstellen.....	7
Abbildung 2: Use Cases - Übersicht Ereignisdeklaration .....	8
Abbildung 3: Use Cases - Übersicht Ereignissynchronisation .....	8
Abbildung 4: Use Cases - Übersicht Konfiguration und Support .....	9
Abbildung 5: Laufzeit .....	<b>Fehler! Textmarke nicht definiert.</b>
Abbildung 6: Instanzdokument für Endreceiver und Zeitangaben .....	24

## Übersicht der Änderungen

Richtlinien zur Ereignisdatenübermittlung - Anforderungen für Endreceiver, Version ID-CH 1.0, Ausgabe **todo**  
2017mmdd vom dd.mm.yyyy.

Kapitel	Änderung
Erste Version des Leistungsstandard Schweiz	

## 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	<b><i>muss</i></b>
Wunsch	<b><i>soll (sollte)</i></b>
Absicht	<b><i>wird</i></b>
Vorschlag	<b><i>kann</i></b>

Tabelle 1: Verbindlichkeit von Anforderungen

### Achtung:

Für das konzeptionelle Verständnis genügen oft ältere Schemabilder, d. h. **verbindlich** sind immer nur die offiziellen<sup>1</sup> **XML-Files**.

Spezielle Ausdrücke sind im Glossar von (RL-IDCH, 2017) erklärt.

---

<sup>1</sup> [www.swissdec.ch](http://www.swissdec.ch)

## 1. Einleitung

Dieses Dokument enthält funktionale und zusätzliche Anforderungen an Endreceiver, die im Rahmen des Leistungsstandard-CH eingesetzt werden. Es adressiert die technischen Aspekte des Leistungsstandards, nicht die fachliche Logik. Ein Endreceiver wird dazu verwendet, Ereignismeldungen, die aus dem ERP eines Unternehmens elektronisch versendet wurden, zu empfangen.

Eine Gesamtübersicht des standardisierten Verfahrens ist zum Verständnis der nachfolgenden Spezifikation hilfreich. Diese wird durch das Übersichtsdokument «IncidentStandardOverview.pdf» (OV-IDCH, 2018) vermittelt, auf welches an dieser Stelle verwiesen wird.

Es sind die mitgeltenden Dokumente im Anhang zu beachten. Besonders in den fachlichen Richtlinien (RL-IDCH, 2017) sind für den Endreceiver wesentliche Aspekte bereits in den Kapiteln «Digitalisierungsbereiche» und «Technische Aspekte des Standards» beschrieben.

### 1.1 Tests

Die Tests der Abnahme beziehen sich auf die Use Cases und zusätzlichen Anforderungen. Sie können bei Swissdec heruntergeladen werden (RCTS-IDCH, 2018). 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.

### 1.2 Abkürzungen

Für die WSDL-Operationen werden folgende Abkürzungen verwendet:

- **Declare:**  
DeclareIncident  
DeclareIncidentConsumer
- **Synchronize:**  
SynchronizelIncident  
SynchronizelIncidentConsumer

### 1.3 Ablauf der Ereignisdatenübermittlung

Die Ereignisdatenübermittlung erfolgt getrennt in Declaration und wiederkehrender Synchronisation.

1. Deklaration des Ereignisses mit Initialdaten (Declare) und Bezug der InsuranceCaseID
2. Ergänzung des deklarierten Ereignisses durch Daten in Form sogenannter Stories und gleichzeitig empfangen von Ergebnissen, geändertem Status etc. (Synchronize)

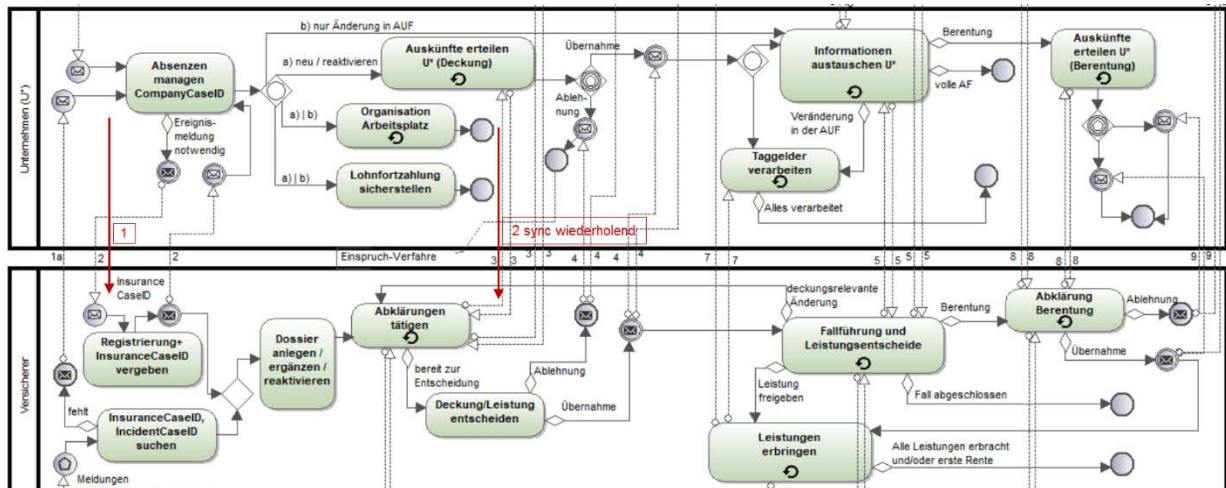


Abbildung 1: Declare und Synchronize im Leistungsstandard, BPMN Diagramm und Schnittstellen

## 2. Übersicht Use Cases

In den folgenden Use Cases werden die essentiellen technischen Anforderungen an den Endreceiver beschrieben. Sie sind zusammen mit den Dokumenten (RL-IDCH, 2017), (ACKNSwissdec, 2018), (DIAL-IDCH, 2018), (WSDL-IDCH, 2018) und (SEC-ERSwissdec, 2018) zu lesen sowie durch die Tests in (RCTS-IDCH, 2018) geprüft.

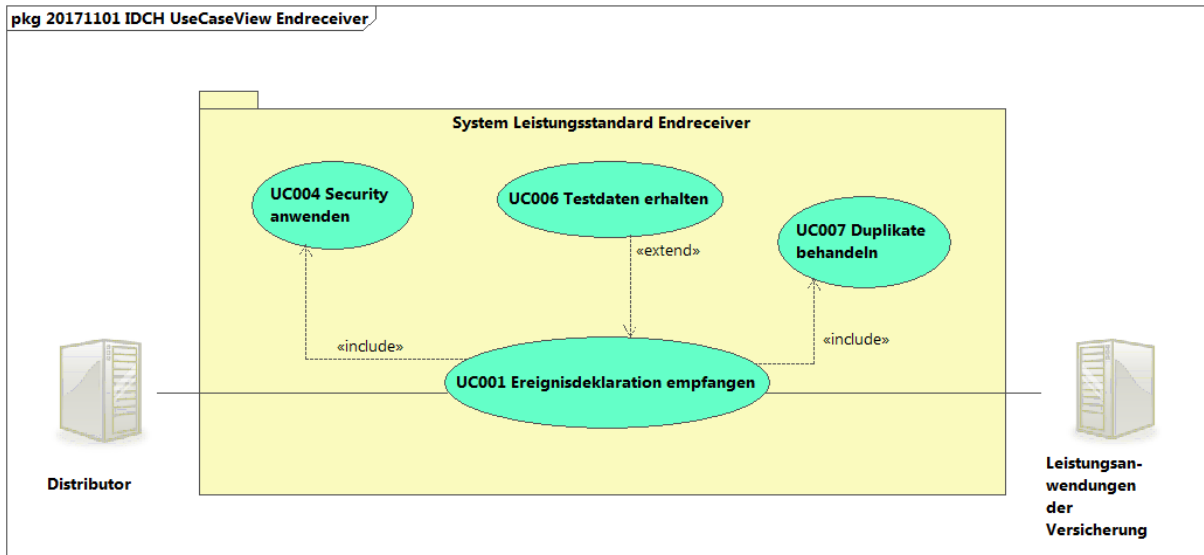


Abbildung 2: Use Cases - Übersicht Ereignisdeklaration

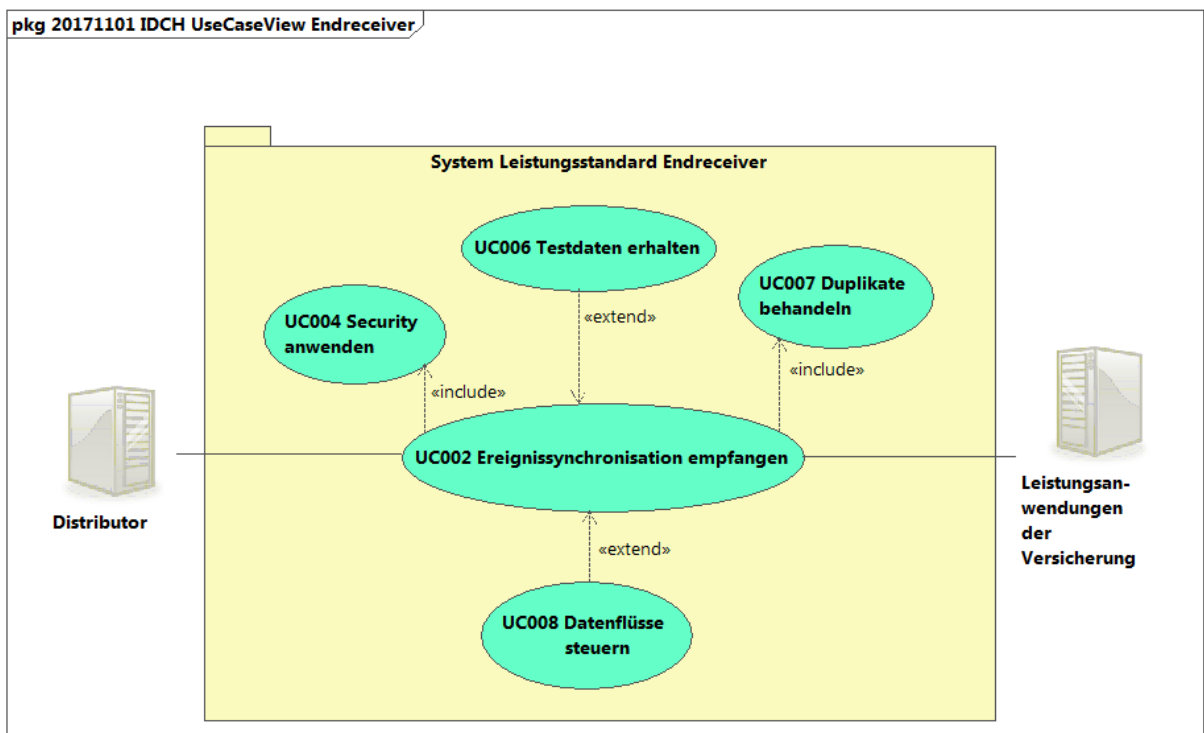


Abbildung 3: Use Cases - Übersicht Ereignissynchronisation



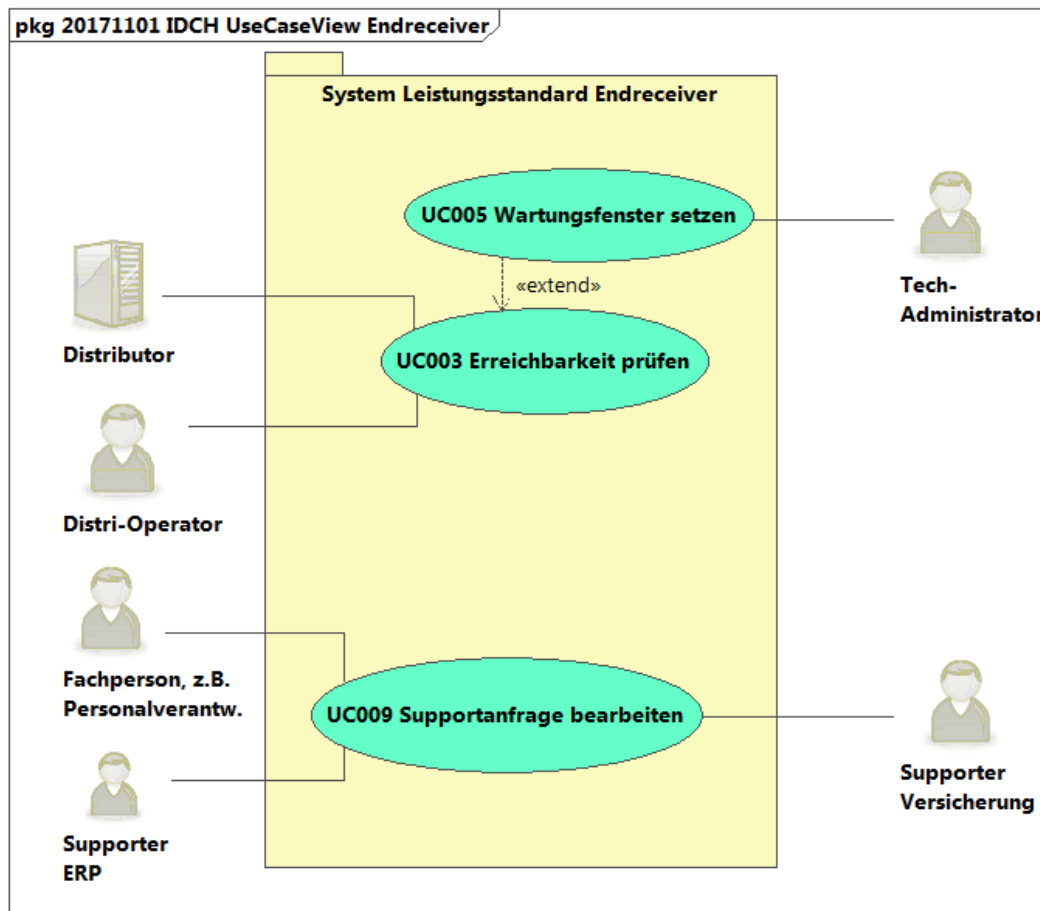


Abbildung 4: Use Cases - Übersicht Konfiguration und Support

Die Akteure lassen sich in drei Gruppen ordnen:

- Operator, Administrator [Tech-Gruppe]
- Fachpersonen, Personalverantwortliche inkl. Treuhänder [Fach-Gruppe]
- Supporter [Mix aus Tech- und Fach-Gruppe]

Die Herkunft der Akteure lässt sich wie folgt beschreiben:

- Distri-Operator: Techniker auf Distributor-Ebene
- Fachperson: Endbenutzer beim Unternehmen
- Supporter: Wahlweise Supporter des Unternehmens oder des ERP-Herstellers, Supporter beim Endempfänger
- Tech-Administrator: Techniker auf Endreceiver-Ebene

## 2.1 Erläuterungen zu den Use Cases

Die als Use Cases abgebildeten Anforderungen beziehen sich auf den technischen Teil eines Leistungsverarbeitungssystems, das Ereignisdatendaten empfängt, die Meldungen quittiert, mit dem System eines Unternehmens kommuniziert und die Ereignisbearbeitung steuert.

Fachliche Anforderungen, die sich auf die Datenverarbeitung nach deren Übermittlung etc. beziehen, sind nicht Teil dieser Spezifikation.

Ein Leistungsverarbeitungssystem mit Receiver **muss** für die Abnahme innerhalb eines Digitalisierungsbereichs (RL-IDCH, 2017) immer alle Systemanforderungen an diesen Digitalisierungsbereich erfüllen. Bei nicht unterstützten Use Cases für weitere Digitalisierungsbereiche wird eine in (ACKNSwissdec, 2018) spezifizierte Fehlermeldung zurückgemeldet.

## 2.2 Use Cases und zugehörige Operationen

Das zugrundeliegende Modell ist ein Client – Server System mit dem Endreceiver als Server und dem Distributor als Client. Verwendet werden die XML-Standards WSDL und XML-Schema. Die nachfolgenden Operationen und Elemente befinden sich im zugehörigen WSDL-File (WSDL-IDCH, 2018) und in den dazugehörigen Schemas. Verfahren und Protokoll sind in (OV-IDCH, 2018) erläutert.

Alle Aufrufe des Transmitters Richtung Distributor und anschliessend an den Endreceiver sind synchron. Um grosse Datenmengen zu verarbeiten, kann die Anzahl der zu übermittelnden Stories (RL-IDCH, 2017) innerhalb eines Requests gesteuert werden (UC008 «Datenflüsse steuern»).

Use Case	Operation / Element
UC001 Ereignisdeklaration empfangen	<ul style="list-style-type: none"><li>▪ DeclareIncidentConsumer</li><li>▪ DeclareIncidentConsumerResponse</li><li>▪ IncidentDeclarationConsumerFault</li></ul>
UC002 Resultat Ereignissynchronisation empfangen	<ul style="list-style-type: none"><li>▪ SynchronizeIncidentConsumer</li><li>▪ SynchronizeIncidentConsumerResponse</li><li>▪ IncidentDeclarationConsumerFault</li></ul>
UC003 Erreichbarkeit prüfen	<ul style="list-style-type: none"><li>▪ PingConsumer</li><li>▪ PingConsumerResponse</li></ul>

Tabelle 2 UseCases und Operationen

## 2.3 Summary Use Cases

### 2.3.1 UC001 Ereignisdeklaration empfangen

Eine Ereignisdeklaration wird vom Distributor an einen Endreceiver gesendet, von diesem geprüft und verarbeitet. Die Antwort des Endreceivers enthält die notwendigen Daten zur Weiterbearbeitung des Ereignisses im Leistungsprozess.

### 2.3.2 UC002 Ereignissynchronisation empfangen

Eine Ereignissynchronisation wird vom Distributor an einen Endreceiver gesendet. Der Endreceiver verarbeitet die empfangenen Transmitter-Stories und Transmitter-Quittungen. Dabei führt der Endreceiver eine Transaktionskontrolle durch. Gegebenenfalls wird der Datenfluss aktiv gesteuert.

### 2.3.3 UC003 Erreichbarkeit prüfen

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

### 2.3.4 UC004 Security anwenden

Der Endreceiver prüft die empfangenen Zertifikate und entschlüsselt die Meldung. Richtung Distributor signiert und verschlüsselt er die Response. Die Security ist in (SEC-ERSwissdec, 2018) beschrieben.

### **2.3.5 UC005 Wartungsfenster setzen**

Ergänzend zu UC003 «Erreichbarkeit prüfen», muss ein Wartungsfenster in der Response an den Distributor eingetragen werden können.

### **2.3.6 UC006 Testdaten erhalten**

Eine Testmeldung entspricht einer Meldung wie bei UC001 oder UC002, einzelne Ereignisse sind aber als Testereignisse gekennzeichnet. Die Testereignisse dürfen nicht produktiv verarbeitet werden. In der Response müssen die Testereignisse ebenfalls als TestCases gekennzeichnet werden.

### **2.3.7 UC007 Duplikate 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 Declare wie auch bei Synchronize erkannt und behandelt werden können.

### **2.3.8 UC008 Datenflüsse steuern**

Die Datenmenge der Responses an den Distributor wird durch die Aufteilung der Daten in mehrere Request-Response Zyklen reduziert. Die Maximalgrösse von Requests wird sich nach «Today Best Practices» richten. (RL-IDCH, 2017) 11.2.

### **2.3.9 UC009 Supportanfrage bearbeiten**

Um eine Supportanfrage bearbeiten zu können, muss die dafür zuständige Person beim Versicherer die Möglichkeit haben, auf die betroffene Ereignismeldung, sowie damit verbundene Logdateien, zuzugreifen.

### 3. Use Case Beschreibungen

#### 3.1 UC001 Ereignisdeklaration empfangen

Kurzbeschreibung	Der Distributor schickt die Ereignisdeklaration des Unternehmens an den Endreceiver. Die Ereignisdeklaration enthält nur wenig Details zum Ereignis selbst (WSDL-IDCH, 2018). Sie wird vom Endreceiver geprüft und verarbeitet. Die Antwort des Endreceivers enthält unter anderem die von der Versicherung für dieses Ereignis vergebene InsuranceCaseID, die vom Distributor vergebene IncidentCaseID und die vom Unternehmen vergebene CompanyCaseID, vgl. (RL-IDCH, 2017) «Identifikationssystem».
Akteure	Distributor
Auslöser	Der Distributor hat eine Ereignisdeklaration eines Transmitters erhalten.
Vorbedingungen	Der Distributor hat die Ereignisdeklaration validiert und plausibilisiert gem. (ACKNSwissdec, 2018).
Nachbedingungen	Der Endreceiver hat die Deklarationsdaten gesichert und inklusive InsuranceCaseID an den Distributor zurückgeliefert.
Included Use Cases	UC004 Security anwenden, UC007 Duplikate behandeln
Standardablauf	<ol style="list-style-type: none"> <li>1. Die Daten der Ereignisdeklaration werden empfangen.</li> <li>2. Die Distributor-Transport-Daten müssen gemäss Distributor Kopplung geprüft werden. Die Security wird geprüft UC004. Dubletten<sup>2</sup> werden detektiert UC007. Anomalien in der Ereignisdeklaration können geprüft werden.</li> <li>3. Die Ereignisdeklaration wird gemäss Leistungsstandard-CH geprüft (Akzeptanz).</li> <li>4. Alle notwendigen Daten der Ereignisdeklaration werden gemäss Datenschutz gesichert.</li> <li>5. Es wird eine InsuranceCaseID für das Ereignis vergeben.</li> <li>6. Die Rückantwort zum Distributor bzw. Unternehmen wird gemäss Leistungsstandard-CH / (ACKNSwissdec, 2018) inklusive der vom Distributor bereits erstellten Nachrichten &lt;ProducerResponseNotifications&gt; (ACKNSwissdec, 2018) aufgebaut. Ab Vorliegen mindestens einer Warnung <i>muss</i> ein acceptedWithWarning-Code zurückgegeben werden (. / ResponseState/Code). Die Antwort <i>muss</i> die Angabe des Digitalisierungsbereichs des Empfängers, siehe (RL-IDCH, 2017) Kapitel «Digitalisierungsbereiche», enthalten.</li> </ol>
Alternative Abläufe	<p>{ Schritt 4: bei Testdaten werden diese nach UC006 als Testdaten gekennzeichnet und nicht produktiv verarbeitet}</p> <p>{ Schritt 1: Wartungsfenster / Dienst ist nicht verfügbar}</p> <p>Die Information zum Wartungsfenster (von-bis) wurde bereits mittels UC003 «Erreichbarkeit prüfen» an den Distributor übermittelt. In dieser Zeit werden Response-Meldungen mit dieser Unterbruch-Information vom Distributor direkt an das anfragende ERP zurückgegeben.</p> <p>{ Schritt 1: ungeplanter Unterbruch / Dienst ist nicht verfügbar}</p> <p>In dieser Zeit werden Fehlermeldungen vom Distributor direkt an das anfragende ERP zurückgegeben, s. (ACKNSwissdec, 2018).</p> <p>{ Schritt 2: Dublette wurde erkannt, Vorgehen nach UC007 «Duplikate behandeln»}</p> <p>{ Schritt 2: Security nicht gültig, Rückweisung der Meldung}</p> <p>{ Schritt 3: Es wird ein Ereignis deklariert und es wurde bereits eine InsuranceCaseID mitgegeben}</p>

<sup>2</sup> Auch bei Dubletten werden die gesamten Daten übermittelt

	Hier liegt ein Sonderfall (UVG, UVGZ, KU) vor. Implementierung nach (RL-IDCH, 2017) Kapitel 3 «Erläuterungen zum Soll-Prozess»
Fehlerliste	<p>Fehler:</p> <ul style="list-style-type: none"><li>▪ Meldung ist nicht valid nach (WSDL-IDCH, 2018)</li><li>▪ Meldung kann nicht entschlüsselt werden</li><li>▪ usw.</li></ul> <p>siehe (ACKNSwissdec, 2018)</p>

### 3.2 UC002 Ereignissynchronisation empfangen

Kurzbeschreibung	<p>Stories (RL-IDCH, 2017) und Quittungen vom Distributor werden empfangen, in der Antwort werden Stories, Quittungen und Zustände an den Distributor zurückgeschickt.</p> <p>Es wird eine Transaktionskontrolle durchgeführt.</p> <p>Gegebenenfalls wird der Datenfluss aktiv gesteuert.</p>
Akteure	Distributor
Auslöser	Der Transmitter hat eine Ereignissynchronisierung an den Distributor geschickt. Dies kann unterschiedliche fachliche Gründe haben, wie z.B. die Lieferung von fehlenden Stories im Leistungsprozess oder eine Anfrage, ob neue Daten vorliegen.
Vorbedingungen	<p>Der Distributor hat die Ereignissynchronisation validiert und plausibilisiert gem. (ACKNSwissdec, 2018).</p> <p>Standardablauf: Eine Ereignisdeklaration wurde vorgängig übermittelt und quittiert.</p>
Nachbedingungen	<p>Die empfangenen Transmitter-Stories sind gemäss Datenschutz gesichert.</p> <p>Bei einem Synchronize ohne IncidentStories ist der Synchronize, z.B. in einem Access Log, mit CustomerIdentity registriert.</p> <p>Die bereits ausgelieferten Endreceiver-Stories, zu welchen die empfangenen Quittungen gehören, sind als quittiert gekennzeichnet.</p> <p>Der aktuelle Prozess-Status und der aktuelle Übernahme-Status des Ereignisses wurden in der Response zurückgegeben, s. (RL-IDCH, 2017) Kapitel 7.</p> <p>Gegebenenfalls wurden Quittungen für die übermittelten Transmitter-Stories in der Response an das Unternehmen geliefert.</p> <p>Gegebenenfalls wurden noch fehlende Transmitter-Stories in der Response angefordert.</p> <p>Gegebenenfalls wurden zur Abholung bereitgestellte Endreceiver-Stories in der Response an das Unternehmen geliefert (RL-IDCH, 2017) «SynchronizeIncident Request und Response -Verhalten».</p> <p>Gegebenenfalls wurden weitere abholbereite Endreceiver-Stories in der Response an das Unternehmen aufgelistet.</p> <p>Gegebenenfalls wurden in einzelnen empfangenen Stories enthaltene &lt;Error&gt;, &lt;Warning&gt; oder &lt;Info&gt; - Elemente gesichert.</p>
Included Use Cases	UC004 Security anwenden, UC007 Duplikate behandeln.
Standardablauf	<ol style="list-style-type: none"> <li>1. Die Daten der Ereignissynchronisation werden empfangen.</li> <li>2. Die zusätzlichen Distributor-Transport-Daten müssen gemäss Distributor Kopplung geprüft werden (SEC-ERSwissdec, 2018). Die Security wird geprüft UC004. Dubletten<sup>3</sup> werden detektiert UC007.</li> <li>3. Die Ereignissynchronisation wird gemäss Leistungsstandard-CH geprüft (Akzeptanz).</li> <li>4. Alle notwendigen Daten der Ereignissynchronisation, insbesondere neue Stories, werden gemäss Datenschutz gesichert.</li> <li>5. Die Transaktionskontrolle wird durchgeführt (RL-IDCH, 2017) Kapitel 11. Empfangene Transmitter-Stories werden in der Antwort quittiert. Zu den empfangenen Quittungen werden die zugehörigen Endreceiver-Stories gesucht und als quittiert gekennzeichnet. Fehlende Transmitter-Stories werden ange-</li> </ol>

<sup>3</sup> Auch bei Dubletten werden die gesamten Daten übermittelt

	<p>fordert. Noch nicht gesendete Endreceiver-Stories, Quittungen und Statusmeldungen werden in die Response aufgenommen (RL-IDCH, 2017) «SynchronizeIncident Request und Response -Verhalten».</p> <p>6. Allenfalls wird der Datenfluss aktiv gesteuert - UC008 «Datenflüsse steuern»</p> <p>7. (Die Rückantwort zum Distributor bzw. Unternehmen wird gemäss Leistungsstandard-CH / (ACKNSwissdec, 2018) inklusive der vom Distributor bereits erstellten Nachrichten &lt;ProducerResponseNotifications&gt; (ACKNSwissdec, 2018) aufgebaut. Ab Vorliegen mindestens einer Warnung <i>muss</i> ein acceptedWithWarning-Code zurückgegeben werden (.. /ResponseState/Code). Die Antwort <i>muss</i> die Angabe des Digitalisierungsbereichs des Empfängers, siehe (RL-IDCH, 2017) Kapitel «Digitalisierungsbereiche», enthalten.)</p>
Alternative Abläufe	<p>{ Schritt 4: bei Testdaten werden diese nach UC006 als Testdaten behandelt und nicht produktiv verarbeitet}</p> <p>{ Schritt 3: Das Ereignis kann mit den empfangenen Daten nicht identifiziert werden, da keine InsuranceCaseID mitgeschickt wurde. Gleichzeitig existiert ein Element «StoriesWithoutDeclaration» im Request}</p> <p>Dies ist der Sonderfall «Ereignismeldung fehlt» (RL-IDCH, 2017) Kapitel Sonderfälle. Der Endreceiver muss nach dem dort beschriebenen Vorgehen reagieren können.</p> <p>{Schritt 6: Die Story zu einer empfangenen Quittung ist nicht vorhanden} Wird eine Story zu einer empfangenen Quittung nicht gefunden, kann die Quittung ignoriert werden.</p>
Fehlerliste	<p>Fehler:</p> <ul style="list-style-type: none"> <li>▪ Meldung ist nicht valid nach (WSDL-IDCH, 2018)</li> <li>▪ Meldung kann nicht entschlüsselt werden</li> <li>▪ Meldung beinhaltet Stories, die mit dem implementierten Digitalisierungsbereich des Endreceivers nicht verarbeitet werden können.</li> <li>▪ Keine InsuranceCaseID und kein Element StoriesWithoutDeclaration: Der Request wird zurückgewiesen (ACKNSwissdec, 2018)</li> <li>▪ usw.</li> <li>▪ siehe (ACKNSwissdec, 2018)</li> </ul>

Die meisten der Sonderfälle in (RL-IDCH, 2017) Kapitel «Sonderfälle» sind fachlicher Natur und werden, um Redundanzen zu vermeiden, in dieser Spezifikation des Endreceivers nicht nochmal beschrieben.

### 3.3 UC003 Erreichbarkeit prüfen

Der UseCase Erreichbarkeit prüfen setzt die 2-Way SSL Verschlüsselung voraus. Der Request und Response sind signiert und die XML-Daten sind verschlüsselt.

Kurzbeschreibung	Die Erreichbarkeit des Endreceivers soll vom Distributor aus geprüft werden. Dazu wird eine einfache PingConsumerRequest-Anfrage gemäss (WSDL-IDCH, 2018) 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	UC004 Security anwenden
Standardablauf	<ol style="list-style-type: none"> <li>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)</li> <li>2. Die Security wird geprüft UC004.</li> <li>3. Der Endreceiver antwortet mit seinem aktuellen Timestamp, s. &lt;PingConsumerResponse&gt; (WSDL-IDCH, 2018).</li> </ol>
Alternative Abläufe	{Schritt 3: Optional kann dem Distributor ein geplantes <b>Wartungsfenster</b> (Nicht-verfügbarkeit von x bis y) mittels UC005 «Wartungsfenster setzen» mitgeteilt werden. Diese Funktion <i>muss</i> umgesetzt werden.}
Fehlerliste	<p>Technische Fehler:</p> <ul style="list-style-type: none"> <li>▪ Meldung ist nicht valid (WSDL-IDCH, 2018)</li> <li>▪ Meldung kann nicht entschlüsselt werden</li> </ul>

### 3.4 UC004 Security anwenden

Der Endreceiver prüft die empfangenen Zertifikate und entschlüsselt die Meldung wie in (SEC-ERSwissdec, 2018) beschrieben. Im Unterschied zum Lohnstandard-CH, erhält der Endreceiver aus der doppelten Signatur zusätzlich das elektronische Zertifikat des sendenden Unternehmens mit enthaltener UID-BfS. Somit ist eine Information über das sendende Unternehmen (Betrieb selbst oder Treuhänder) enthalten, die eine Prüfung ermöglicht, ob das sendende Unternehmen zur Ereignismeldung berechtigt ist.



### 3.5 UC005 Wartungsfenster setzen

Kurzbeschreibung	Erweiterung des UC003 «Erreichbarkeit prüfen». Der Endreceiver <i>muss</i> eine Funktionalität implementieren, damit Daten für ein Wartungsfenster eingetragen und diese in der Antwort von UC003 «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"> <li>1. Der technische Administrator des Endreceivers trägt die Daten des Wartungsfensters ein.</li> <li>2. Die Antwort des Endreceivers (PingConsumerResponse) an den Distributor enthält die eingetragenen Daten für das Wartungsfenster.</li> </ol>
Alternative Abläufe	keine
Fehlerliste	Technische Fehler: <ul style="list-style-type: none"> <li>▪ Meldung ist nicht valid (WSDL-IDCH, 2018)</li> </ul>

### 3.6 UC006 Testdaten erhalten

Der UC006 «Testdaten erhalten» unterscheidet sich nur bezüglich des Ziels zum UC001 «Ereignisdeklaration empfangen» oder UC002 «Ereignissynchronisation empfangen».

Einzelne Ereignisse sind mittels eines <TestCase>-Elements gekennzeichnet. Diese Ereignisse dürfen nicht produktiv verarbeitet werden. In der Response müssen diese Ereignisse ebenfalls als Test Cases mit dem <TestCase>-Element gekennzeichnet sein.

Ziele von UC006:

- Möglichkeit, dem Endbenutzer die elektronische Ereignisdatenübermittlung näher zu bringen.
- Ermöglichung von Tests bei der Installation
- Ermöglichung von Tests bei Problemen in der Produktion

Wird das Ereignis im Declare als TestCase markiert, ist der weitere Ablauf des Leistungsprozesses für dieses Ereignis stets im Testmodus abzuwickeln. Bei der Synchronisation *muss* dieses Ereignis auf Transmitter- wie auf Endreceiverseite daher ebenfalls mit dem <TestCase>-Element markiert werden.

Bei einem versehentlichen «Mix» aus Test-Deklaration und anschliessender produktiver Synchronisation müssen die fälschlich nicht als TestCase gekennzeichnete Stories vom Endreceiver mittels Element «IncidentStories/Error/RequestStoryID» und der aus (ACKNSwissdec, 2018) zugehörigen Notification in Element «IncidentStories/Error/Notification» zurückgewiesen werden.

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

Der Use Case dient zur **Lokalisierung** von Problemen in der **produktiven Übermittlungskette**. Dabei sollen Ereignismeldungen 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 produktiven Ereignisse** und **keine produktiven InsuranceCaseIDs** erzeugt.

Grundsätzlich sollen dabei nur **korrekte** und **vollständige** Test-Ereignisdeklarationen- und Synchronisationen geschickt werden.

### 3.7 UC007 Duplikate behandeln

Hier wird nach den beiden Aufrufen Declare und Synchronize unterschieden.

#### 3.7.1 Declare Duplikate

Duplikate eines kompletten DeclareIncidentConsumerRequests werden vom Distributor technisch (bitgleich) erkannt und mittels eines Elements «Duplicate» im DistributorRequestContext gekennzeichnet.

Falls die im Duplikat enthaltenen Informationen noch nicht verarbeitet und beantwortet wurden, muss dies nachgeholt werden.

Wurde der Originalrequest bereits beantwortet, muss für das Duplikat inhaltlich die gleiche Antwort gesendet werden, welche zuvor als Antwort auf den Originalrequest versandt wurde (idempotentes Verhalten).

#### 3.7.2 Declare Duplikate ohne Distributor Erkennung

Ein veränderter und erneut gesendeter DeclareIncidentConsumerRequest für ein oder mehrere gleiche Ereignisse kann vom Distributor nicht als Duplikat erkannt werden.

Für den Endreceiver bedeutet dies, dass bei einem DeclareIncidentConsumerRequest zusätzliche Prüfungen pro Ereignisdeklaration, z. B. «DeclareIncidentConsumer/IncidentDeclaration/Company/Staff/Person/UVG-LAA-Registration», auf ein vorliegendes Duplikat durchgeführt werden *müssen* (fachliche Prüfung).

Falls innerhalb eines DeclareIncidentConsumerRequests Duplikate von Ereignisdeklarationen enthalten sind und dies vom Distributor nicht erkannt wurde, wurde vom Distributor auch eine neue IncidentCaseID generiert. Trotzdem *muss* ein solches Duplikat einer Ereignisdeklaration vom Endreceiver detektiert werden. Anhand welcher Daten dies geschieht ist Sache des Versicherers. Es *darf kein* neues Ereignis registriert und es *darf keine* neue InsuranceCaseID generiert werden. Die IncidentCaseID und die InsuranceCaseID, mit welcher das Ereignis bereits registriert wurde, *müssen* in der Antwort des Endreceivers an den Distributor verwendet werden. Die Antwort pro Ereignisdeklaration *muss* derjenigen der bereits erfolgten Ereignisdeklaration entsprechen und *muss* zusätzlich eine Duplikatswarnung nach (ACKNSwissdec, 2018) enthalten.

#### 3.7.3 Synchronize Duplikate

Für SynchronizeIncidentConsumer gibt es auf Seiten des Distributors keine Duplikatserkennung. Diese *muss* vom Endreceiver durchgeführt und Duplikate *müssen* vom Endreceiver erkannt werden.

#### 3.7.4 Synchronize identische Story

Bei einem Synchronize könnte es vorkommen, dass eine identische Story empfangen wird. Eine identische Story zeichnet sich durch die gleiche «StoryID», den gleichen «IncidentContext» (CompanyCaseID, IncidentCaseID, InsuranceCaseID), das gleiche «CreationDate» und den gleichen Story Namen aus. Der weitere Inhalt der Story braucht nicht überprüft zu werden.

Wird eine identische Story anhand der beschriebenen Metadaten erkannt, darf die Story nicht nochmals gespeichert werden. Die Antwort an den Distributor muss der bereits vorher auf diese Story gegebenen Antwort entsprechen. Zusätzlich *muss* eine Duplikatswarnung im Element «IncidentStories/Warning» mit der zugehörigen «RequestStoryID» und der «Notification» nach (ACKNSwissdec, 2018) zurückgegeben werden.

#### 3.7.5 Synchronize StoryID nicht unique innerhalb IncidentContext

StoryIDs müssen über den gesamten Prozess für einen Incident unique sein. So muss z.B. das ERP bei der Korrektur einer Story eine neue StoryID vergeben.

Werden bei der Synchronisation eines Incidents einzelne Stories mit gleicher StoryID und gleichem «IncidentContext» (CompanyCaseID, IncidentCaseID, InsuranceCaseID) aber unterschiedlichem Namen des Story-Elements oder unterschiedlichem «CreationDate» empfangen, welche in einem vorherigen oder im gleichen Request enthalten sind, müssen diese als ungültige StoryID-Duplikate zurückgewiesen werden. Dies geschieht mit dem Element «IncidentStories/Error», mit der betroffenen «RequestStoryID» und der entsprechenden «Notification» nach (ACKNSwissdec, 2018) .

### 3.8 UC008 Datenflüsse steuern

UC008 «Datenflüsse steuern» ist Sub-UseCase von UC002 «Ereignissynchronisation empfangen».

Die Datenflüsse *müssen* sowohl vom Endreceiver als auch vom Transmitter kontrolliert und gesteuert werden können. Hintergrund ist, dass die Response-Grösse einzelner Request-Response Zyklen durch Aufteilung in mehrere Request-Response Zyklen reduziert werden kann. (RL-IDCH, 2017) 11.2 «Synchronizer Incident Request und Response -Verhalten»

Der *Endreceiver* kann die Datenmenge reduzieren, indem er nicht alle vorliegenden neuen Daten auf einmal, sondern nur einen Teil davon an den Transmitter ausliefert. Für den Rest der noch bereitliegenden Daten werden die zugehörigen IncidentCaseIDs im Response-Element <Available> aufgelistet.

Der Transmitter führt daraufhin für die in <Available> angegebene IncidentCaseIDs weitere Synchronizer Incidents aus.

Die Maximalgrösse von Requests wird sich nach «Today Best Practices» richten. (RL-IDCH, 2017) 11.2.

Kurzbeschreibung	Die Datenmenge der Responses an den Distributor wird durch die Aufteilung der Daten in mehrere Request-Response Zyklen reduziert.
Akteure	Distributor
Auslöser	Die Datenmenge der auszuliefernden Stories an ein Unternehmen wäre zu gross.
Vorbedingungen	Keine
Nachbedingungen	Für alle IncidentCaseIDs des Unternehmens wurden alle zu übertragenden Stories und Quittungen an den Distributor ausgeliefert.
Included Use Cases	Keine
Standardablauf	<ol style="list-style-type: none"> <li>1. Es wird ein Synchronizer Incident des Distributors für einen oder mehrere Ereignisse empfangen (RL-IDCH, 2017) «Identifikationssystem».</li> <li>2. Das sendende Unternehmen wird anhand der mitgelieferten Daten «CustomerIdentity» und ggf. «ContractIdentity» identifiziert.</li> <li>3. Falls für das Unternehmen und die angefragten Ereignisse eine zu grosse Menge Stories zur Auslieferung bereitsteht, wird nur ein Teil der Stories in der Response mitgegeben. Für die restlichen Stories werden deren IncidentCaseIDs im Element &lt;Available&gt; der Response aufgelistet.</li> <li>4. Schritte 1 bis 3 werden so lange ausgeführt, bis alle Stories der angeforderten Ereignisse für das Unternehmen ausgeliefert wurden.</li> </ol>
Alternative Abläufe	keine
Fehlerliste	<ul style="list-style-type: none"> <li>▪ Das Unternehmen konnte nicht identifiziert werden.</li> </ul>

### 3.9 UC009 Supportanfrage bearbeiten

Kurzbeschreibung	Ausnahmen, Störfall und andere Probleme behandeln
Akteure	Fachperson Unternehmen, Supporter ERP-Hersteller, Supporter Endreceiver
Auslöser	Die Fachperson Unternehmen oder der Supporter ERP-Hersteller stellt per E-Mail oder Telefon eine Supportanfrage.
Vorbedingungen	Keine
Nachbedingungen	Die Supportanfrage konnte erfolgreich bearbeitet werden.
Included Use Cases	Keine
Standardablauf	<ol style="list-style-type: none"> <li>1. Es wird per Mail oder Telefon eine neue Supportanfrage von einer Fachperson Unternehmen oder einem Supporter des ERP-Herstellers gestellt.</li> <li>2. Das Problem wird vom Supporter Endreceivers analysiert und beantwortet.</li> </ol>
Alternative Abläufe	<p>{nach Schritt 1}</p> <ol style="list-style-type: none"> <li>1. Das Problem wird eskaliert und gelangt zum Second oder Third Level Support.</li> </ol> <p>{weiter mit Schritt 2}</p>
Fehlerliste	Keine

Wichtig im Umgang mit Supportfällen ist, dass die Supportinformationen einheitlich kommuniziert werden. Fehler, Warnungen und Informationen müssen gemäss (ACKNSwissdec, 2018) erstellt und in die Response eingefügt werden. Die in (ACKNSwissdec, 2018) beschriebenen Codes sind verbindlich.

Es *muss* eine Möglichkeit bestehen, im Falle einer Supportanfrage auf die nötigen Informationen für die Behandlung des Problems zuzugreifen, wie z. B. mit Hilfe des Zeitpunkts des Requests und der InsuranceCaseID, der IncidentCaseID, der CustomerIdentity und der CompanyCaseID.

## 4. Zusätzliche Anforderungen

### 4.1 Leistungsstandard-CH Version

Im Schema befindet sich das Element `<RequestContext/UserAgent/StandardVersion>`, welches die verwendete Version des Leistungsstandard-CH bezeichnet. Diese ist aufgrund von Anpassungen zwischen verschiedenen Versionen notwendig, die sich nicht auf das Schema beziehen, sondern ausschliesslich auf den Inhalt der Elemente.

### 4.2 Kommunikationsstandards

Die Standardkopplung *muss* auf der Web Service Technologie (SOAP<sup>4</sup> Version 1.1, WSDL<sup>5</sup> Version 1.1 und WSS<sup>6</sup> Version 1.0) basieren. Die Daten *müssen* neben dem HTTPS<sup>7</sup> Layer (two-way SSL/TLS) zusätzlich auf der SOAP-Ebene gemäss WSS verschlüsselt werden (SEC-ERSwissdec, 2018).

### 4.3 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 Endreceivern *müssen*, sofern Komprimierung eingesetzt wird, folgendes Feld enthalten:

- Content-Encoding: gzip

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

### 4.4 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 Unterbrüche<sup>8</sup> (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 werden. Führt eine spätere Datenprüfung zur Ablehnung der Meldung, muss diese dem Kunden ausserhalb dieser Systemspezifikation mitgeteilt werden.

---

<sup>4</sup> SOAP (ursprünglich für Simple Object Access Protocol)

<sup>5</sup> Web Services Description Language (WSDL) definiert eine plattform-, programmiersprachen- und protokollunabhängige XML-Spezifikation zur Beschreibung von Netzwerkdiensten (Web Services) zum Austausch von Nachrichten.

<sup>6</sup> Web Services Security (WSS) von Organization for the Advancement of Structured Information Standards (OASIS)

<sup>7</sup> http 1.0 oder 1.1; mindestens TLS 1.2 mit minimaler Sessionkey-Länge 256Bit

<sup>8</sup> Gilt für normale Wartungsarbeiten; ausgenommen ist ein Hotfix oder Patch

#### 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.

##### 4.4.1 Definierte Zeitbereiche

- Betriebszeit des gesamten Systems (Distributor, Kommunikation und Endreceiver; m2m Strecke bis zur Quitungs-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

##### 4.4.2 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.

##### 4.5 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.

#### 4.6 Änderungen an der Schnittstelle

- Sollen Änderungen des Leistungsstandard-CH auch beim Endreceiver aktiviert werden, *muss* die gesamte Kopplung (Seitens Distributor und Endreceiver) angepasst werden.
- Sollen keine Änderungen des Leistungsstandard-CH 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.

#### 4.7 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.

#### 4.8 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).

- Beim Synchronize kann der Endreceiver mit «UC008 Datenflüsse steuern» gegeben falls die Verarbeitungszeit reduzieren

- Die eigentliche Detailprüfung und Verarbeitung (z. B. Integration von weiteren Diensten) erfolgt nach dem 1. Schritt.

Abbildung 5: Instanzdokument für Endreceiver und Zeitangaben



#### 4.9 Sicherheit und Datenschutz

Sicherheit und Datenschutz sind wichtige konzeptionelle Grundlagen für die Kommunikation im Leistungsstandard-CH, welche für den Bau und Betrieb des Endreceivers zu berücksichtigen sind.

Im Datenschutzbereich liefert der Leistungsstandard-CH bereits Lösungen

- Transparenz mittels Standardisierung (swissdec Leistungsstandard)
- Willenserklärung mittels dem Tag <Job> in der Ereignisdeklaration
- Filter mittels Transformationen auf dem Distributor

Diese Lösungen sind sicher und zuverlässig zu betreiben.

Die Endreceiver Institution *muss* sicherstellen, dass nur «gehärtete» Systeme mit aktuellen Security-Patches, verschlüsselte Kommunikationswege und auf Sicherheit bedachte Konfigurationen verwendet werden. Sie *muss* die Applikation vor DoS und DDoS-Attacken (Denial of Service / Distributed Denial of Service) schützen. Zusätzlich muss sie die Applikation vor Hackern und Viren schützen (IDS (intrusion detection system / prevention); Virenschutz).

- Grundsätzlich gelten die normalen Datenschutzbestimmungen der Institution des Endreceivers.

#### 4.10 Adressierung und Filterung

Ein Request mit falscher Adressierung *muss* abgelehnt werden (Könnte auch die Folge eines Security-Angriffs sein).

Empfehlungen

- Aus Sicht des Datenschutzes sollte beim Endreceiver möglichst rasch eine **Pseudonymisierung**<sup>9</sup> durchgeführt werden.

---

<sup>9</sup> Schwächere Form der Anonymisierung; Verändern personenbezogener Daten durch Zuordnungsvorschrift z.B. zwei separate Tabellen (Person und Ereignis), die mit einem anonymen Schlüssel verknüpft werden.

## 6. Anhang

### 6.1 Mitgeltende Spezifikationsdokumente

Folgende Dokumente sind für Test- und Abnahme mitgeltend.

#### Verweise auf mitgeltende Spezifikationsdokumente

ACKNSwissdec, s. (31. Januar 2018). AcknowledgementNotification. (swissdec, Hrsg.) Bern, Schweiz. Von <https://tst.itserve.ch/swissdec/infopoint/datapool.xhtml> abgerufen

DIAL-IDCH, s. (27. Februar 2018). Anforderungen Darstellung DialogMessage. (swissdec, Hrsg.) Bern, Schweiz. Von <https://www.swissdec.ch/de/releases-und-updates/richtlinien-kle> abgerufen

OV-IDCH, s. (15. Januar 2018). IncidentDeclarationStandardOverview. Bern, Schweiz.

RCTS-IDCH, s. (26. Februar 2018). Receiver Certification Test Suite IncidentDeclaration. (swissdec, Hrsg.) Bern, Schweiz. Von <https://receiver.swissdec.ch> abgerufen

RL-IDCH, s. (09. November 2017). Richtlinien für den Leistungsstandard-CH. (swissdec, Hrsg.) Bern, Schweiz. Von <https://www.swissdec.ch/de/releases-und-updates/richtlinien-kle> abgerufen

SEC-ERSwissdec, s. (15. Februar 2018). SecurityEndreceiver. (swissdec, Hrsg.) Bern, Schweiz. Von <https://tst.itserve.ch/swissdec/infopoint/datapool.xhtml> abgerufen

WSDL-IDCH, s. (15. Januar 2018). IncidentDeclarationConsumerService.wsdl. (swissdec, Hrsg.) Bern, Schweiz. Von <https://www.swissdec.ch/de/releases-und-updates/richtlinien-kle> abgerufen