

**Directives Swissdec relatives à la norme suisse en matière d'authentification d'entreprises Swissdec (SUA)**

**Exigences posées aux transmetteurs**

Les directives relatives à la norme suisse en matière d'authentification d'entreprises Swissdec (SUA) ont été rédigées en collaboration avec les entités suivantes:

- la Suva,
- l'Association Suisse d'Assurances (ASA).

**Éditeur**

Swissdec  
Fluhmattstrasse 1  
6004 Lucerne  
[www.swissdec.ch/fr](http://www.swissdec.ch/fr)

## Table des matières

<b>1.</b>	<b>Introduction.....</b>	<b>6</b>
1.1	Procédure simplifiée d'obtention d'un certificat .....	6
1.2	Institutions et domaines .....	8
<b>2.</b>	<b>Vue d'ensemble des use cases de transmetteur .....</b>	<b>10</b>
2.1	Vue d'ensemble des use cases .....	11
2.2	Explications concernant les use cases .....	12
2.3	Tests .....	12
2.4	Récapitulatif des use cases .....	12
2.4.1	UC001: obtention d'un certificat SUA.....	12
2.4.2	UC002: commande / enregistrement .....	12
2.4.3	UC003: activation.....	12
2.4.4	UC004: vérification de l'accessibilité.....	12
2.4.5	UC005: Vérification de l'interopérabilité (signature simple).....	12
2.4.6	UC006: renouvellement d'un certificat .....	12
2.4.7	UC007: vérification de l'interopérabilité avec CRT-IDE (double signature).....	13
2.4.8	UC008: marquage de données-test .....	13
2.4.9	UC009: application des règles de sécurité.....	13
2.4.10	UC010: support; réalisation de clarifications manuelles.....	13
2.5	Use cases et opérations correspondantes .....	13
<b>3.</b>	<b>Use cases .....</b>	<b>14</b>
3.1	Use case 001: obtention d'un certificat SUA.....	14
3.2	Use case 002: commande / enregistrement.....	15
3.2.1	Obtention d'un certificat pour les fiduciaires.....	15
3.2.2	Obtention d'un certificat en l'absence de relation contractuelle .....	16
3.3	Use case 003: activation .....	16
3.4	Use case 004: vérification de l'accessibilité .....	17
3.5	Use case 005: vérification de l'interopérabilité .....	18
3.5.1	Exigences spéciales.....	18
3.5.2	Conditions préalables.....	19
3.5.3	Conditions ultérieures .....	19
3.6	Use case 006: renouvellement d'un certificat.....	20
3.7	Use case 007: double vérification de l'interopérabilité .....	20
3.8	Use case 008: marquage de données-test .....	20
3.9	Use case 009: application des règles de sécurité .....	20
3.10	Use case 010: informations de support; réalisation de clarifications manuelles.....	21
3.11	Exigences spéciales.....	21
3.11.1	Création de fichiers d'archives .....	21
<b>4.</b>	<b>Annexe .....</b>	<b>22</b>
4.1	Références.....	22

## Liste des illustrations

Illustration 1: Croquis de l'étape 1 de la configuration de l'enregistrement SUA .....	7
Illustration 2: Croquis des étapes 2, 3, 4 et 5 de la configuration de l'enregistrement SUA.....	8
Illustration 3: Croquis du processus d'enregistrement et de configuration SUA .....	10
Illustration 4: Use cases .....	11
Illustration 5: Diagramme de séquence de l'obtention d'un certificat SUA.....	15
Illustration 7: Use case 010: vérification de l'accessibilité .....	17
Illustration 8: Use case 011: vérification de l'interopérabilité .....	18

## Liste des tableaux

Tableau 1: Caractère contraignant des exigences .....	5
Tableau 2: Use cases et opérations .....	13
Tableau 3: Use case 001: transmission d'une déclaration des salaires .....	14
Tableau 4: Use case 010: vérification de l'accessibilité .....	17
Tableau 5: Description du use case de vérification de l'interopérabilité .....	18
Tableau 6: Conditions préalables (transmetteur).....	19
Tableau 7: Analyse et réponse du répartiteur .....	19
Tableau 8: Analyse du transmetteur .....	19

## Vue d'ensemble des modifications – Version 20190301

Directives relatives à la norme suisse en matière d'authentification d'entreprises Swissdec (SUA) - Exigences posées aux transmetteurs, version 1.0, édition 20190301 du 10.05.2021.

Chapitre	Modification
Création du document	

## Conventions au sein du présent document

Les polices suivantes sont utilisées dans le présent document:

Texte	Documentation
Texte	Code
<Texte>	Élément XML
[TEXTE]	Référence à un autre document

Le caractère contraignant des exigences est défini comme suit:

Caractère contraignant	Expressions / Formules
Obligation	<i>doit / il faut / est obligatoire</i>
Souhait	<i>devrait</i>
Intention	<i>sera</i>
Proposition	<i>peut</i>

Tableau 1: Caractère contraignant des exigences

### Attention:

Nous recourons à d'anciens schémas pour présenter le concept proposé. En d'autres termes, seuls les **fichiers XML officiels<sup>1</sup> sont contraignants**, (par exemple Web Services Description Language (WSDL), XML Schema Definition (XSD), Extensible Stylesheet Language (XSL) Transformation et XML Instance Documents).

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

## 1. Introduction

Le présent document rassemble les exigences fonctionnelles, techniques et complémentaires posées aux transmetteurs utilisés dans le cadre de la norme suisse en matière d'authentification d'entreprises Swissdec (SUA). Les transmetteurs servent à gérer (obtenir, activer, vérifier et renouveler) les certificats SUA.

Une vue d'ensemble complète de la procédure standardisée, qui permet de bien comprendre les spécifications suivantes, est disponible dans le document récapitulatif «OverviewUnternehmensAuthentifizierung.pdf» (OVOA, 2019). Il convient de s'y référer.

### 1.1 Procédure simplifiée d'obtention d'un certificat

L'enregistrement présuppose l'existence d'un contrat conclu avec un assureur. Le terme de «destinataires finaux» désigne ici les «destinataires finaux auprès d'assureurs et d'autorités (A&A)».

On considère qu'au moment de la conclusion du contrat, l'assureur examine l'entreprise et tient constamment à jour dans ses systèmes de données de base les données IDE de celle-ci (IDE-OFS, raison sociale d'après le registre du commerce, etc.).

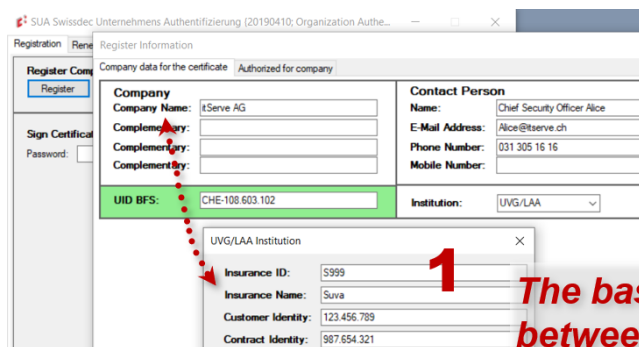
La répartition / l'obtention d'un certificat SUA s'articule généralement autour de deux étapes essentielles:

- la «commande», qui passe par un *enregistrement* (RLOA, 2019), et
- l'«activation», via une *configuration* (RLOA, 2019).

#### *Croquis de l'étape 1 de la configuration de l'enregistrement SUA:*

Lorsqu'une entreprise souhaite s'enregistrer à la SUA, l'un de ses collaborateurs compétents sélectionne dans le système ERP une assurance (destinataire final A&A) à utiliser pour identifier l'entreprise. Les informations nécessaires à l'enregistrement (informations relatives au contrat, IDE-OFS, nom de l'entreprise) sont pour la plupart préremplies dans le système ERP et envoyées au répartiteur. Il faut aussi choisir ou indiquer un interlocuteur responsable en fournissant des données qui permettent de l'identifier (nom, adresse e-mail, numéro de téléphone / téléphone portable, fonction / service).

Le répartiteur vérifie le message reçu. Il s'assure également qu'un nombre limité de demandes d'enregistrement actives est possible pour un même IDE-OFS. Le résultat de la vérification est transmis au système ERP par l'envoi d'un identifiant CertificateRequest (CRID) généré, qui identifie précisément le système ERP et la requête concernée.



Registration Information

Register Company

Authorized for company

Company data for the certificate

Company Name: tServe AG

Company Address:

Complementary:

Complementary:

Contact Person

Name: Chief Security Officer Alice

E-Mail Address: Alice@tsserve.ch

Phone Number: 031 305 16 16

Mobile Number:

UID BFS: CHE-108 603 102

Institution: UVG/LAA

UVG/LAA Institution

Insurance ID: S999

Insurance Name: Suva

Customer Identity: 123 456 789

Contract Identity: 987 654 321

**The base is an existing relationship between the company and the insurance.**

180719 BPMN2 SUA Registration Configuration

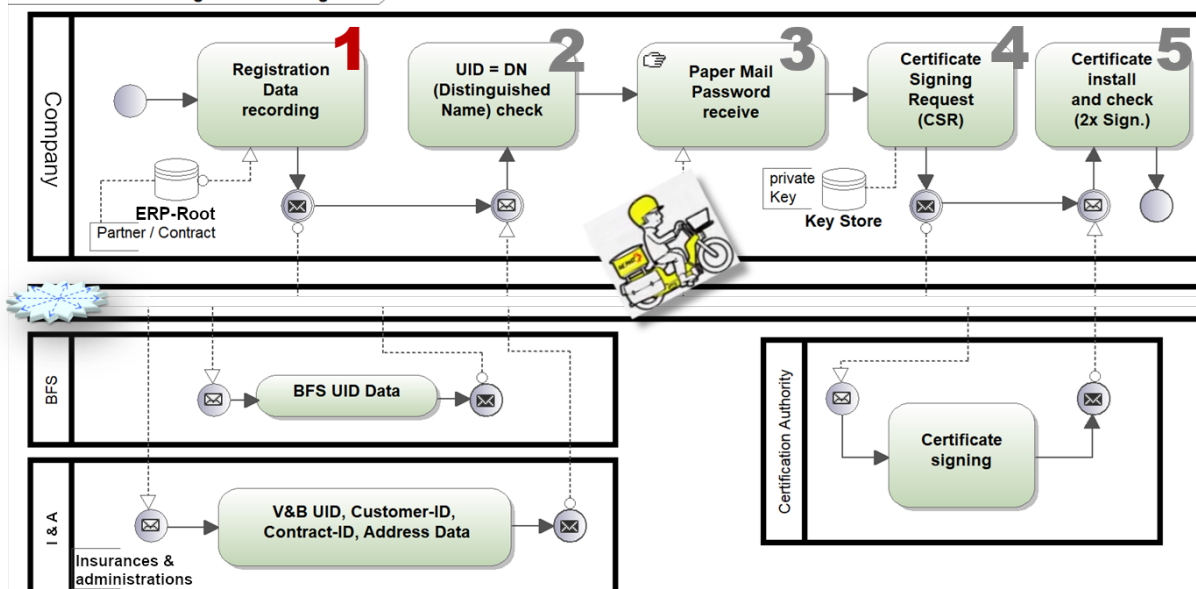


Illustration 1: Croquis de l'étape 1 de la configuration de l'enregistrement SUA

*Croquis de l'étape 2 de la configuration de l'enregistrement SUA:*

Si la vérification du message par le répartiteur est concluante, les informations relatives à l'entreprise sont consultées dans le registre d'identification des entreprises de l'OFS. Un bloc de données «actif» relatif à l'entreprise est recherché à l'aide de l'IDE-OFS, puis comparé aux données transmises par l'entreprise (raison sociale d'après le registre du commerce).

Ensuite, les données relatives au contrat sont transmises par le répartiteur à l'institution A&A précédemment sélectionnée. L'institution A&A vérifie alors la validité des données envoyées par l'entreprise et s'assure qu'elles concordent avec ses données de base. Le résultat de cette vérification est renvoyé au répartiteur avec l'IDE figurant dans les données de base, le nom de l'entreprise et les informations d'adressage (direction).

Si le résultat de la vérification renvoyé par l'institution A&A n'est pas concluant, le répartiteur le signale au système ERP de l'entreprise, lequel émet un message d'erreur à l'intention de l'utilisateur. L'utilisateur doit alors contacter directement l'institution A&A pour comparer les données de l'assureur et de l'entreprise.

Le répartiteur termine la vérification de l'identité par une comparaison entre les données transmises par l'institution A&A et celles provenant du registre d'identification des entreprises. Outre le numéro IDE et le nom de l'entreprise, les données d'adressage peuvent aussi être comparées (automatiquement ou manuellement).

*Croquis de l'étape 3 de la configuration de l'enregistrement SUA:*

Si la vérification de l'identité est concluante, le répartiteur génère un mot de passe d'enregistrement et un mot de passe de verrouillage. Ces deux mots de passe ainsi que l'IDE-OFS, les données provenant du registre IDE de l'OFS, le CRID et un timbre horodateur sont enregistrés. Le mot de passe d'enregistrement est requis pour les étapes ultérieures de la configuration, mais n'est valable que pendant 30 jours. Le répartiteur envoie une confirmation de la réussite de l'identification de l'entreprise au système ERP, lequel en informe l'utilisateur par un message. Cette confirmation contient notamment les données relatives à l'entreprise figurant dans le registre IDE de l'OFS, utilisées pour la création du certificat SUA.

Le répartiteur ou un tiers mandaté à cet effet par Swissdec envoie à l'adresse fournie par l'institution A&A (direction) un courrier (recommandé ou A Plus) comprenant non seulement des informations complémentaires (p. ex. concernant le processus de configuration), mais aussi le mot de passe d'enregistrement, le mot de passe de verrouillage, le CRID,

l'IDE-OFS, les données relatives à l'entreprise provenant du registre IDE de l'OFS et l'identité de l'interlocuteur responsable dans l'entreprise. Les informations sont ainsi délivrées sur un second canal, non électronique de la personne responsable de l'entreprise, ce qui accroît encore la qualité de l'identification.

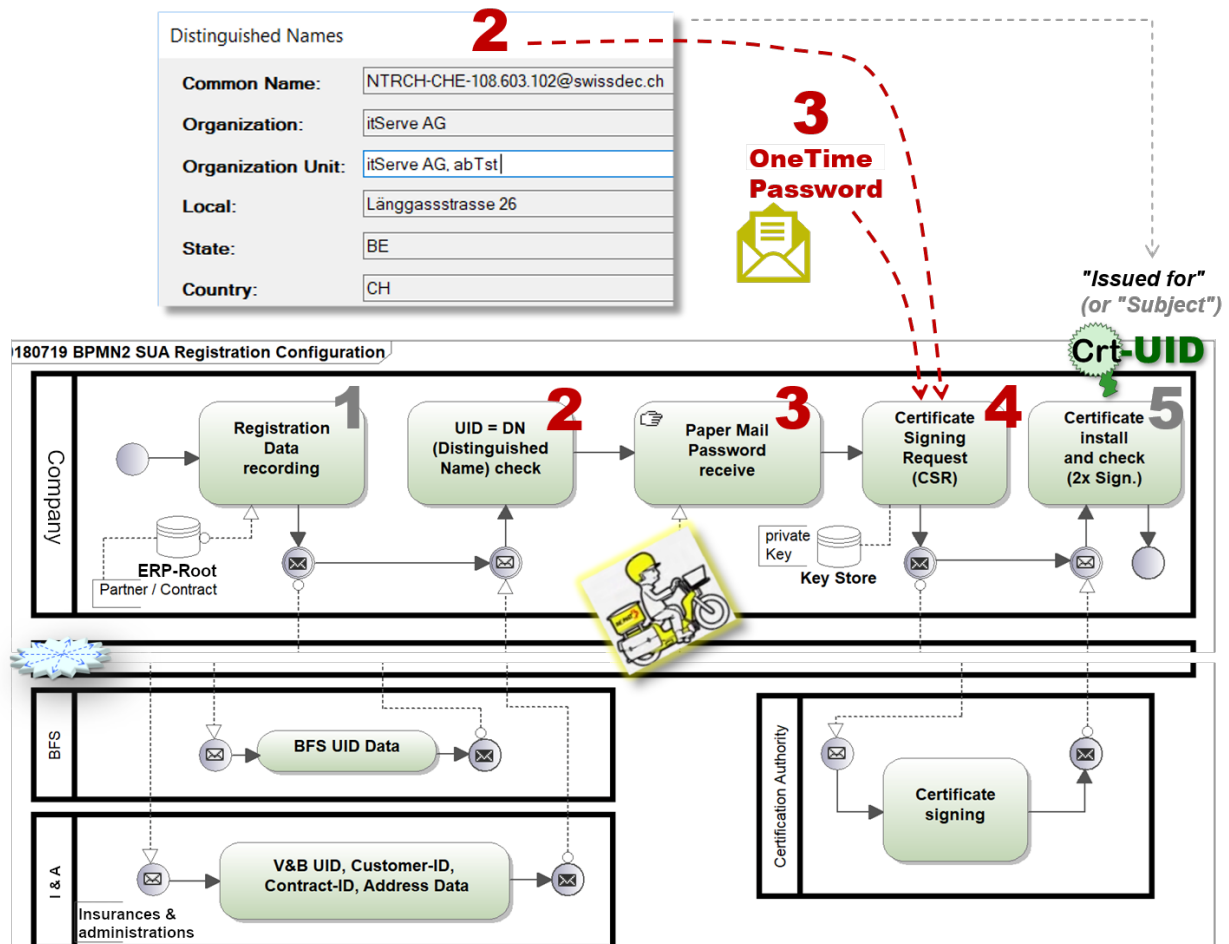


Illustration 2: Croquis des étapes 2, 3, 4 et 5 de la configuration de l'enregistrement SUA

#### Croquis des étapes 4 et 5 de la configuration de l'enregistrement SUA:

Le collaborateur peut à présent obtenir le certificat commandé au moyen d'une CSR et du mot de passe envoyé par courrier (étape 3) et l'installer automatiquement dans le système ERP de son entreprise. Enfin, le bon fonctionnement du nouveau certificat SUA est vérifié au minimum à l'aide d'une opération `OrganizationAuthentication-RenewPort.CheckInteroperability()` signée à deux reprises. D'autres transferts-test sont possibles.

Le processus d'enregistrement SUA est terminé dès lors que le transmetteur parvient à réaliser un transfert au moyen du certificat SUA.

Il convient de se reporter aux directives / spécifications détaillées (RLOA, 2019) pour une description plus précise de la procédure.

## 1.2 Institutions et domaines

La SUA peut être et sera utilisée dans le cadre de plusieurs processus de transmission Swissdec. Néanmoins, comme l'authentification d'entreprises est obligatoire dans la norme suisse en matière de prestations (KLE) alors qu'elle n'est pour le moment que facultative avec la norme suisse en matière de salaire, les exemples suivants se rapportent avant tout à la norme suisse en matière de prestations (KLE). Les informations suivantes sont toutefois valables pour toutes les normes Swissdec permettant l'utilisation de la SUA.

Une distinction est réalisée dans le présent document entre domaines et institutions.



**Domaines:** organisations au sujet desquelles des données sont transmises. Les domaines pris en charge par la norme suisse en matière de prestations (KLE) sont la LAA, la LAAC, l'assurance-accidents collective et les IJM.

**Institutions:** destinataires recevant les données. Il s'agit d'assurances rattachées aux domaines concernés.

Une entreprise peut contacter plusieurs institutions d'un domaine. Une institution peut prendre en charge plusieurs domaines.

## 2. Vue d'ensemble des use cases de transmetteur

Le croquis suivant donne un premier aperçu du processus global d'obtention d'un certificat SUA.

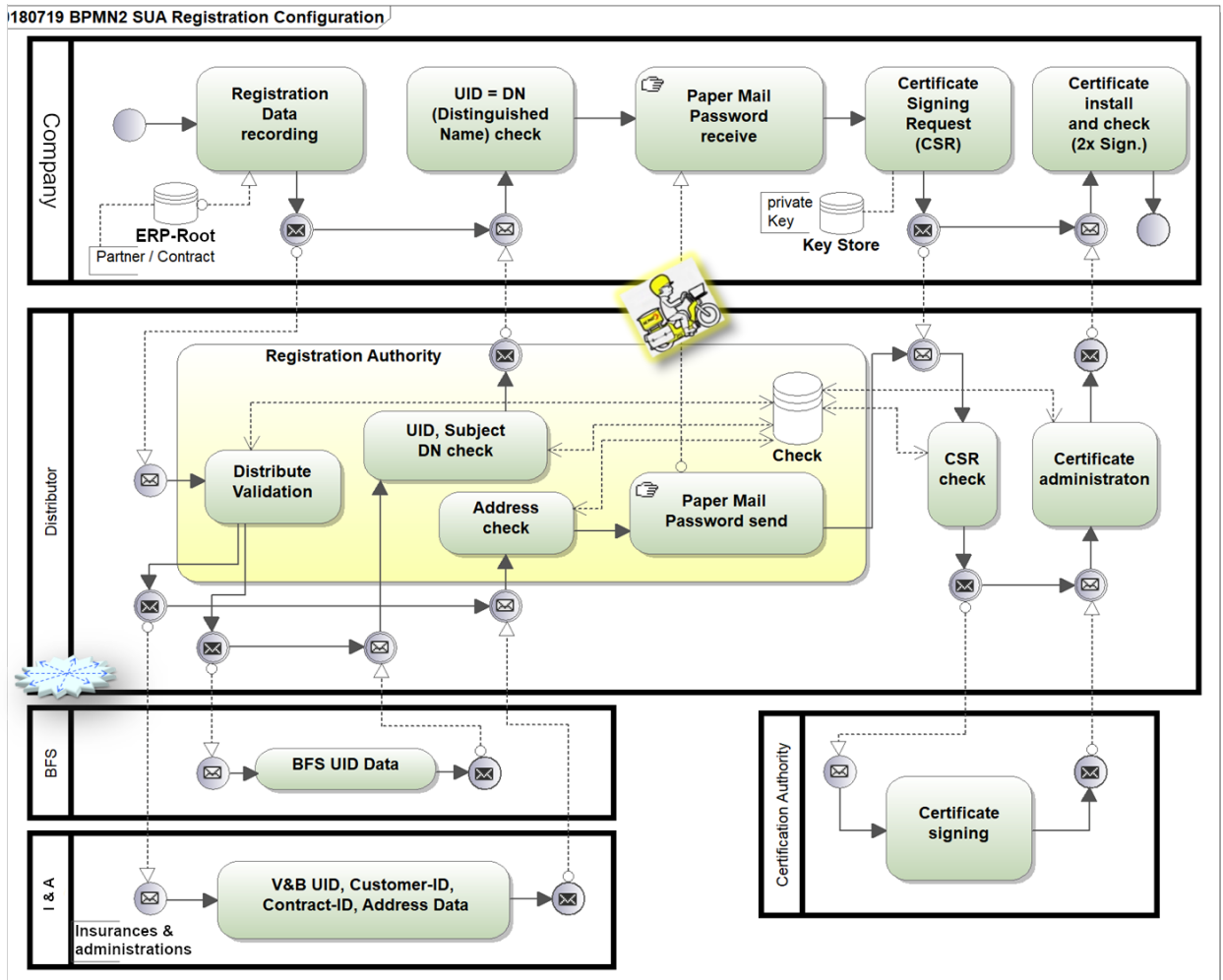


Illustration 3: Croquis du processus d'enregistrement et de configuration SUA

## 2.1 Vue d'ensemble des use cases

Une partie des use cases est présentée sur le même modèle que pour les autres normes Swissdec. Si une autre norme Swissdec a déjà été mise en œuvre, les mêmes fonctionnalités peuvent aussi être utilisées pour la SUA (p. ex. l'accessibilité et l'interopérabilité).

L'IDE-OFS peut donc apparaître dans les éléments de schéma XML et être utilisé au même titre que l'IDE (dans l'historique et p. ex. sous DeclareSalary ... CompanyDescription/IDE-OFS). Au vu des parallèles entre les différentes normes, les désignations obsolètes ont été en partie conservées afin de simplifier l'implémentation du projet.

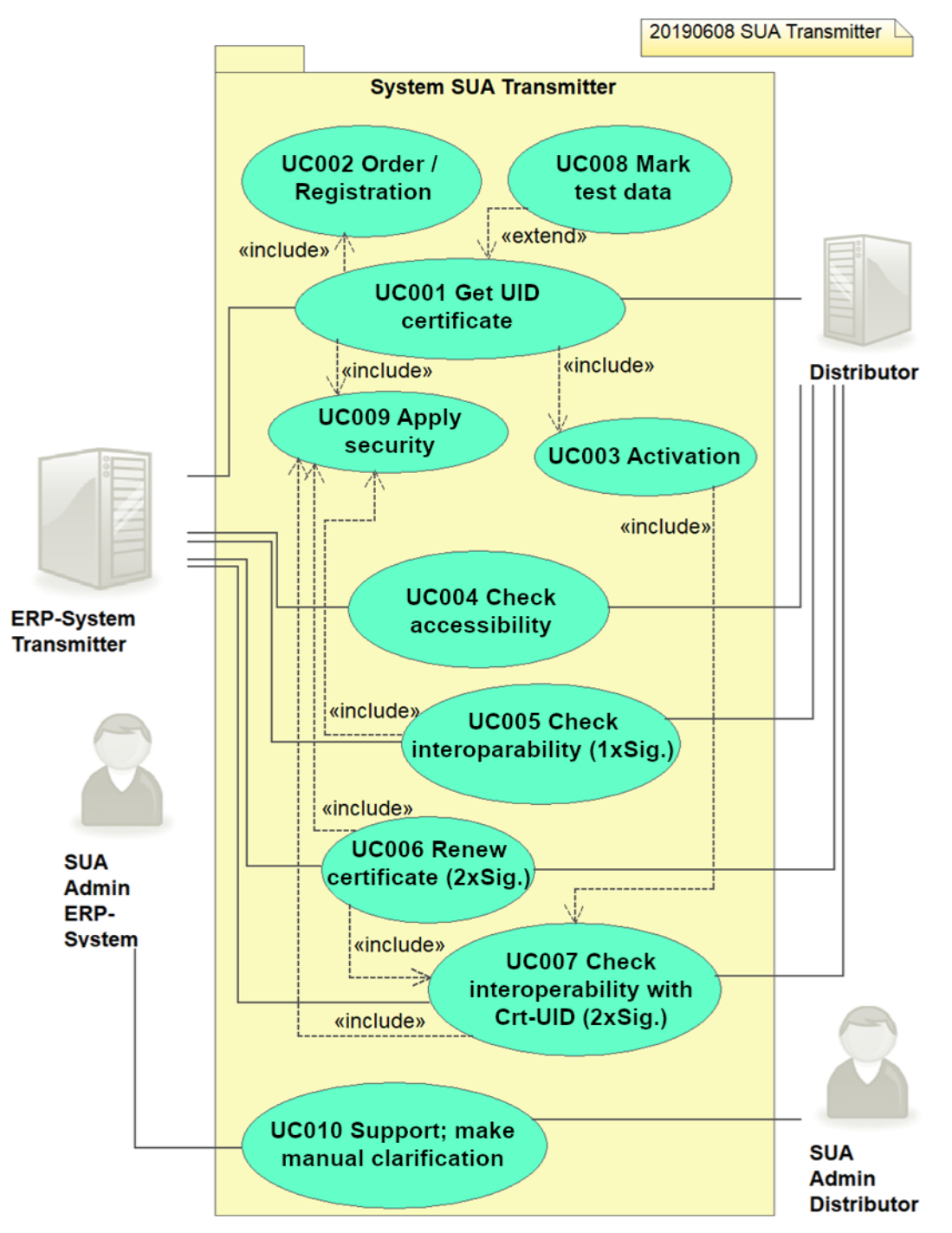


Illustration 4: Use cases

## 2.2 Explications concernant les use cases

Les exigences représentées comme des use cases portent sur la partie technique d'un dispositif constitué d'un système ERP et d'un transmetteur se chargeant du traitement électronique et de la transmission de données en vue de l'obtention d'un certificat SUA.

Un système ERP avec transmetteur *doit* toujours remplir les exigences système suivantes pour la certification:

- UC001: obtention d'un certificat SUA
- UC002: commande / enregistrement
- UC003: activation
- UC004: vérification de l'accessibilité
- UC005: vérification de l'interopérabilité (signature simple)
- UC006: renouvellement d'un certificat
- UC007: vérification de l'interopérabilité avec CRT-IDE (double signature)
- UC008: marquage de données-test
- UC009: application des règles de sécurité
- UC010: support; réalisation de clarifications manuelles

Les modalités de l'interaction entre les utilisateurs et le système, déterminées par le concepteur du système, ne sont pas décrites dans les présentes spécifications.

## 2.3 Tests

Dans le cadre de la certification, des tests basés sur les use cases sont réalisés, si possible dans le même ordre que les use cases. Conjointement avec les exigences, ils contribuent à la compréhension globale du système à élaborer. Le concepteur a tout intérêt à intégrer les tests dès la phase de développement (Test Driven Development).

## 2.4 Récapitulatif des use cases

### 2.4.1 UC001: obtention d'un certificat SUA

Un nouveau certificat est obtenu via le répartiteur. La réponse de ce dernier est enregistrée, cf. chapitre 3 "Use cases. On utilise pour cela d'autres use cases: UC002, UC003, UC009 et UC008.

### 2.4.2 UC002: commande / enregistrement

La commande / l'enregistrement à proprement parler permet de vérifier l'identité de la personne à l'origine de la demande. Il s'agit avant tout de vérifier les données IDE-OFS via un destinataire final (assureurs et autorités) et le registre IDE.

Si le résultat est concluant, le transmetteur / système ERP reçoit un identifiant CertificateRequest et un X509Subject à des fins de contrôle. Un mot de passe est aussi envoyé par courrier à l'entreprise.

### 2.4.3 UC003: activation

Une fois l'enregistrement réalisé (UC002), le certificat SUA peut être obtenu à l'aide du mot de passe fourni par courrier (UC002). Le nouveau certificat SUA est ensuite activé dans le système ERP et peut être testé au moyen de l'interopérabilité (UC007).

### 2.4.4 UC004: vérification de l'accessibilité

Un message spécial est envoyé par Internet au répartiteur afin de s'assurer que ce dernier est joignable.

### 2.4.5 UC005: Vérification de l'interopérabilité (signature simple)

Un message spécial est envoyé au répartiteur afin de vérifier l'interopérabilité (p. ex. encodage, marshalling, indications temporelles) entre le transmetteur et le répartiteur. La requête n'est alors signée qu'avec le certificat ERP.

### 2.4.6 UC006: renouvellement d'un certificat

Il est possible de renouveler un certificat SUA à tout moment. Pour ce faire, une CSR (Certificate Sign Request) est envoyée au répartiteur. Le transmetteur reçoit ensuite le nouveau certificat dans le cadre de la réponse. Pour des raisons de sécurité, le nombre de renouvellements possibles est limité (voir spécifications détaillées RLOA, 2019).

#### 2.4.7 UC007: vérification de l'interopérabilité avec CRT-IDE (double signature)

Un message spécial est envoyé au répartiteur afin de vérifier l'interopérabilité (p. ex. encodage, marshalling, indications temporelles) entre le transmetteur et le répartiteur. La requête est alors signée à deux reprises, avec les certificats ERP et SUA.

#### 2.4.8 UC008: marquage de données-test

N'importe quel message peut être marqué comme cas-test. Il est alors envoyé via le système productif, mais n'est pas traité de manière productive par le destinataire final.

#### 2.4.9 UC009: application des règles de sécurité

Chaque message transmis doit être signé au moins une fois (certificat ERP) et crypté.

#### 2.4.10 UC010: support; réalisation de clarifications manuelles

Toutes les informations de support (notifications, erreurs) doivent être indiquées clairement à l'utilisateur final, qui doit pouvoir comprendre d'où vient le message et comment y réagir.

### 2.5 Use cases et opérations correspondantes

Le modèle de base est un système client-serveur dans lequel le transmetteur est le client. Les normes XLM utilisées sont le WSDL et les schémas XML. Les opérations et éléments suivants se trouvent dans le dossier WSDL correspondant (WSDLOA, 2019) et dans le schéma décrit (XSDOA, 2019). La démarche et le protocole sont expliqués dans les spécifications (RLOA, 2019).

Use case	Opération / Élément
	<b><i>OrganizationAuthenticationService WSDL / XSD</i></b>
UC001: obtention d'un certificat SUA UC002: commande / enregistrement	<ul style="list-style-type: none"> <li>RegisterOrganization</li> <li>RegisterOrganizationResponse</li> <li>GetResultFromRegisterOrganization</li> <li>GetResultFromRegisterOrganizationResponse</li> <li>OrganizationAuthenticationFault</li> </ul>
UC003: activation	<ul style="list-style-type: none"> <li>SignCertificate</li> <li>SignCertificateResponse</li> <li>OrganizationAuthenticationFault</li> </ul>
UC004: vérification de l'accessibilité	<ul style="list-style-type: none"> <li>Ping</li> <li>PingResponse</li> </ul>
UC005: vérification de l'interopérabilité	<ul style="list-style-type: none"> <li>CheckInteroperability</li> <li>CheckInteroperabilityResponse</li> </ul>
	<b><i>OrganizationAuthenticationRenewService WSDL / XSD</i></b>
UC006: renouvellement d'un certificat	<i>Double signature (certificats ERP et SUA)</i> <ul style="list-style-type: none"> <li>RenewCertificate</li> <li>RenewCertificateResponse</li> <li>OrganizationAuthenticationFault</li> </ul>
UC007: vérification de l'interopérabilité	<i>Double signature (certificats ERP et SUA)</i> <ul style="list-style-type: none"> <li>CheckInteroperability</li> <li>CheckInteroperabilityResponse</li> </ul>

Tableau 2: Use cases et opérations

### 3. Use cases

#### 3.1 Use case 001: obtention d'un certificat SUA

Diagramme des use cases: cf. illustration 4: Use cases à la page 11.

Brève description	Un nouveau certificat est obtenu via le répartiteur.  Les réponses de ce dernier sont analysées et enregistrées. Un fichier d'archives du message envoyé est aussi enregistré.
Acteurs	Système ERP, répartiteur, destinataire final
Élément déclencheur	Un employé de l'entreprise (préposé à la sécurité) souhaite obtenir un certificat SUA.
Conditions préalables	Le système ERP doit être en mesure d'envoyer et de recevoir des messages électroniques relatifs à des événements et doit posséder un certificat ERP.
Conditions ultérieures	<ul style="list-style-type: none"> <li>▪ L'étape d'obtention d'un certificat SUA doit avoir été réalisée avec succès.</li> <li>▪ Le certificat SUA doit avoir été activé et testé avec succès.</li> </ul> En cas d'erreur: <ul style="list-style-type: none"> <li>▪ Message d'erreur</li> </ul>
Use cases inclus	UC002: commande / enregistrement UC003: activation UC007: vérification de l'interopérabilité avec CRT-IDE (double signature) UC009: application des règles de sécurité
Procédure standard	<ol style="list-style-type: none"> <li>1. UC002: le certificat est commandé auprès du répartiteur. Il faut à cet effet indiquer une relation contractuelle existante avec un assureur. Le message est signé une fois (UC009).</li> <li>2. Le résultat est obtenu et vérifié de manière asynchrone. Le message est signé une fois (UC009). Le X509Subject correspond alors à la demande de certificat et <i>doit</i> être vérifié par la personne à l'origine de la demande.</li> <li>3. L'employé de l'entreprise attend de recevoir le courrier contenant le mot de passe à usage unique.</li> <li>4. UC003: une CSR est établie et transmise au répartiteur avec le mot de passe à usage unique. Le message est signé une fois (UC009). Toutes les données comprises dans le X509Subject <i>doivent</i> être identiques à celles de la deuxième étape. Il n'est permis que de modifier l'OU (Organization Unit) sous DistinguishedNames. Le transmetteur conserve la clé privée. Le transmetteur reçoit le certificat SUA dans le cadre de la réponse.</li> <li>5. Le certificat SUA est installé et activé. Ensuite, tout <i>doit</i> être vérifié via l'UC007. D'autres transmissions-test avec des normes Swissdec existantes <i>devraient</i> être réalisées en sus.</li> </ol>
Processus alternatif	{UC008} Envoyer les données en tant que données-test Cf. étapes 1 à 4 du processus standard, voir croquis Mais à l'étape: 3, aucun courrier n'est envoyé. Le mot de passe à usage unique se trouve sous GetResultFromOrganizationRegistrationResponse ... Success/Comment 4: <b>aucun</b> certificat SUA n'est renvoyé dans le cadre de la réponse.
Liste des erreurs	Erreur spécialisée: <ul style="list-style-type: none"> <li>▪ Le message n'est pas conforme aux règles de plausibilité.</li> </ul> Erreurs techniques: <ul style="list-style-type: none"> <li>▪ Erreur de signature ou de cryptage</li> <li>▪ Destinataire final injoignable</li> <li>▪ Le message mis au point par le système ERP ne correspond pas au schéma (non valide).</li> </ul>

Tableau 3: Use case 001: transmission d'une déclaration des salaires

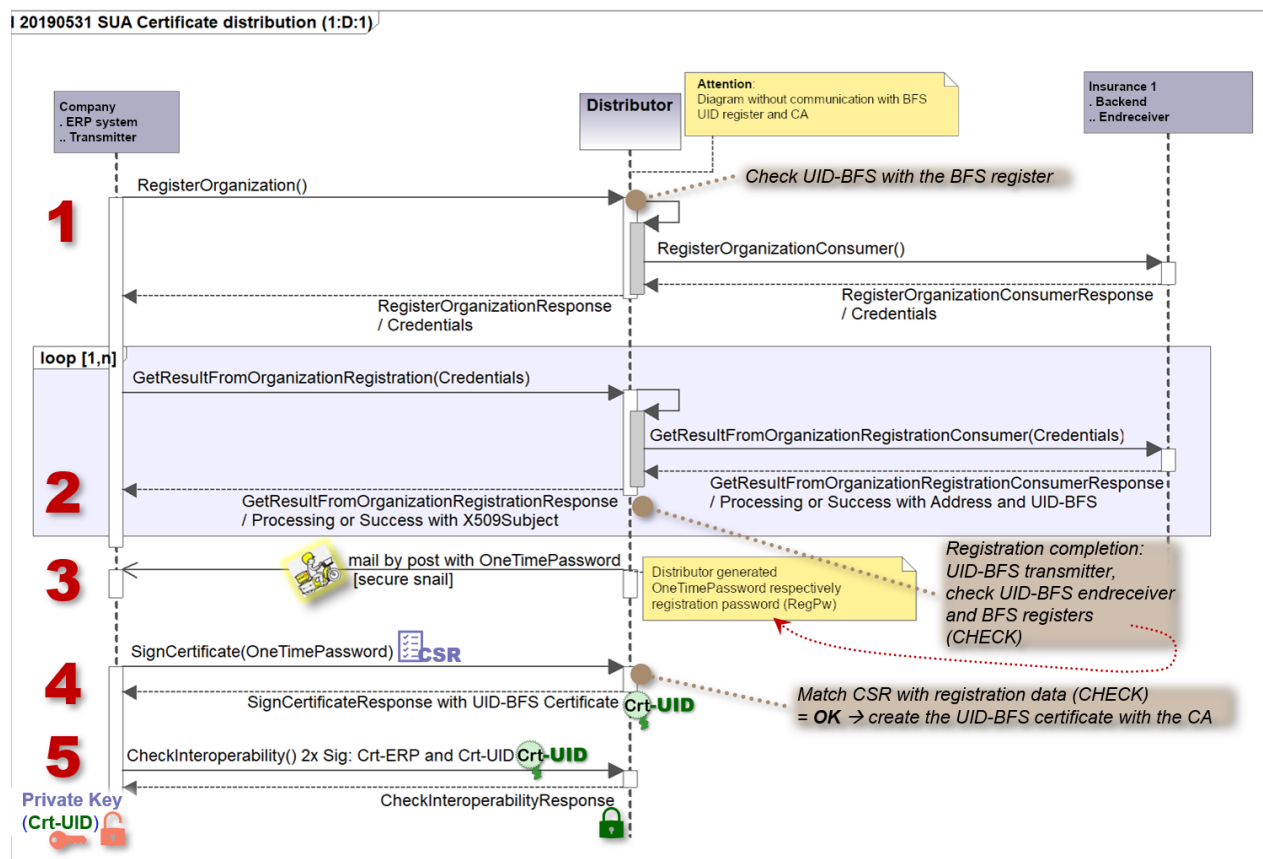


Illustration 5: Diagramme de séquence de l'obtention d'un certificat SUA

### 3.2 Use case 002: commande / enregistrement

Dans un premier temps, l'entreprise doit demander le certificat (cf. UC002). Deux étapes sont nécessaires.

La fonction `RegisterOrganization` permet d'initier l'obtention du certificat. L'entreprise fournit les informations nécessaires à l'établissement d'un certificat au répartiteur, lequel informe le destinataire final de la demande.

Le destinataire final, à son tour, vérifie la validité de la demande et renvoie sa réponse au répartiteur.

La fonction `GetResultFromRegisterOrganization` permet alors à l'entreprise d'obtenir les informations du destinataire final via le répartiteur.

La commande d'un certificat présuppose l'existence d'une relation contractuelle entre l'entreprise et le destinataire final, sauf pour les fiduciaires (cf. chapitre 3.2.1).

Une entreprise peut émettre en parallèle plusieurs demandes d'enregistrement, notamment si elle dispose de plusieurs systèmes ERP différents. Le nombre de demandes de ce type est actuellement limité à cinq afin d'éviter des demandes superflues au registre IDE de l'OFS et l'envoi inutile de courriers. L'envoi d'informations par la poste peut prendre un à deux jours. Si le nombre de demandes est limité, c'est pour que l'utilisateur ne puisse pas, pendant ce laps de temps, envoyer d'autres demandes pour le même IDE avec le même système ERP.

#### 3.2.1 Obtention d'un certificat pour les fiduciaires

Il convient d'observer les points suivants dès lors qu'une entreprise est administrée par une fiduciaire.

La fiduciaire n'a pas de relation directe avec le destinataire final sur la base de laquelle un enregistrement SUA pourrait être réalisé. Dans ce cas, il est possible d'utiliser la relation contractuelle d'une entreprise gérée par la fiduciaire pour procéder à l'enregistrement. Pour ce faire, la fiduciaire doit enclencher un processus d'enregistrement dans son système ERP et indiquer à cette occasion, en plus des données relatives au contrat de l'entreprise, ses propres données (nom de la fiduciaire, IDE, données de contact, etc.) à la rubrique «Délégué». Le destinataire final réalisant l'enregistrement vérifie les données de l'entreprise et de la fiduciaire et s'assure de l'existence d'une procuration. Contrairement à ce que prévoit le processus d'enregistrement classique, le courrier contenant le mot de passe d'enregistrement est

alors envoyé à la fiduciaire, laquelle configure aussi son certificat SUA de fiduciaire, l'enregistre dans son système ERP et signe ainsi avec son certificat SUA tous les messages qu'elle envoie au nom de l'entreprise dont elle assure la gestion.

En vue de sécuriser le processus, le destinataire final ne reçoit pas toutes les informations relatives à la fiduciaire, mais simplement l'information <WithDelegate> qui lui permet d'accéder à ses propres données relatives à l'entreprise et de renvoyer au répartiteur les informations relatives à la fiduciaire y afférentes. Le certificat ne peut être émis que si les informations concordent de part et d'autre.

### 3.2.2 Obtention d'un certificat en l'absence de relation contractuelle

Pour l'heure, il est impossible d'obtenir un certificat sans relation contractuelle existante via le processus SUA ordinaire. Il faudra toutefois offrir prochainement cette possibilité étant donné que d'autres processus Swissdec devraient tôt ou tard être exécutés avec la SUA. Des variantes reposant sur un examen par les autorités fiscales, avec lesquelles les entreprises concernées sont forcément en relation, sont envisagées.

## 3.3 Use case 003: activation

Dès que l'entreprise a reçu les informations nécessaires à l'activation de son certificat, elle peut passer à l'étape suivante. Il lui faut alors établir une CSR et l'envoyer au répartiteur, de même que le mot de passe à usage unique reçu par courrier.

Ce message reçoit une signature simple (UC009) étant donné qu'il n'y a pas encore de certificat SUA valable. Toutes les données doivent être identiques à celles figurant dans le X509Subject de l'enregistrement initial. Il n'est permis que de modifier l'OU (Organization Unit) sous DistinguishedNames.

Le transmetteur peut ainsi conserver la clé privée, de sorte que la sécurité du certificat est garantie.

Dans le cadre de la réponse à cette demande, le transmetteur reçoit le certificat SUA valable, qui peut dès lors être utilisé pour la double signature / le cryptage. Ce certificat doit être installé et activé avant que le tout ne soit vérifié au moyen de l'UC007.



### 3.4 Use case 004: vérification de l'accessibilité

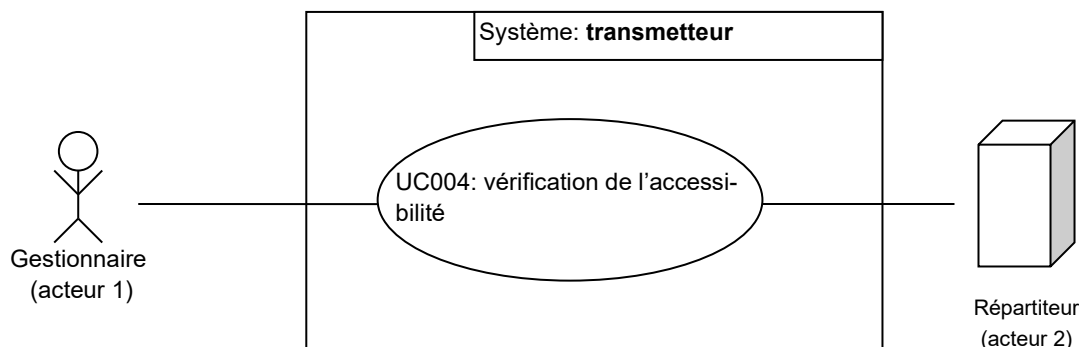


Illustration 6: Use case 010: vérification de l'accessibilité

Brève description	L'accessibilité du répartiteur <i>doit</i> être vérifiée. Pour ce faire, une demande simple (WSDLOA, 2019) est envoyée à ce dernier. La réponse du répartiteur confirme son accessibilité.
Acteurs	Acteur 1: gestionnaire; acteur 2: répartiteur
Élément déclencheur	Il faut vérifier l'accessibilité du répartiteur.
Conditions préalables	Aucune
Conditions ultérieures	<ul style="list-style-type: none"> <li>La réponse du répartiteur doit contenir un timbre horodateur indiquant l'heure du système du répartiteur (XSDOA, 2019).</li> </ul> En cas d'erreur: <ul style="list-style-type: none"> <li>Répartiteur injoignable: message d'erreur</li> <li>Contenu différent (XSDOA, 2019) (ACKNSwissdec, 2018): message d'erreur</li> </ul>
Use cases inclus	-
Procédure standard	<ol style="list-style-type: none"> <li>L'acteur déclenche la vérification.</li> <li>Le transmetteur envoie une demande serveur simple (Ping) à l'adresse de destination du répartiteur.</li> <li>Le transmetteur analyse la réponse du répartiteur.</li> </ol>
Alternative Processus	<b>Répartiteur injoignable</b> {après l'étape 1} <ol style="list-style-type: none"> <li>Un message d'erreur s'affiche.</li> </ol> {Fin}
Liste des erreurs	Erreurs techniques: <ul style="list-style-type: none"> <li>Répartiteur injoignable</li> <li>Le répartiteur envoie une mauvaise réponse.</li> </ul>

Tableau 4: Use case 010: vérification de l'accessibilité

La fonction Ping sert à transmettre l'heure du système afin de permettre la comparaison entre les heures du répartiteur et de l'émetteur. Les problèmes de timbre horodateur peuvent ainsi être identifiés.

Le transmetteur *doit* comparer l'heure du système du répartiteur reçue avec la sienne et informer l'utilisateur en cas d'écart important. L'écart autorisé est compris entre 1 minute d'avance et 2 minutes de retard.

Ce use case sert à l'assurance qualité des phases d'installation et de développement.

### 3.5 Use case 005: vérification de l'interopérabilité

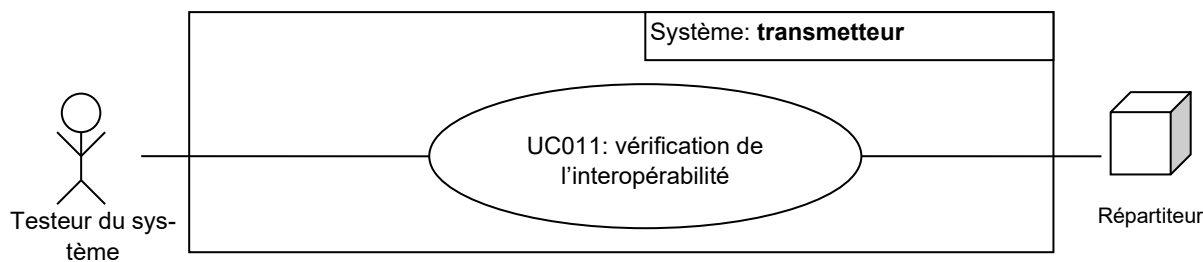


Illustration 7: Use case 011: vérification de l'interopérabilité

Brève description	Le transmetteur <i>doit</i> pouvoir émettre une «CheckInteroperabilityRequest» (WSDLID, 2018) afin de permettre de vérifier l'interopérabilité entre le transmetteur et le répartiteur.
Acteurs	Testeur du système, répartiteur
Élément déclencheur	Il faut tester l'installation.
Conditions préalables	Aucune
Conditions ultérieures	La transmission doit avoir fonctionné et les résultats être conformes aux attentes.
Use cases inclus	-
Procédure standard	<ol style="list-style-type: none"> <li>1. L'acteur débute la vérification de l'interopérabilité et saisit les valeurs pour SecondOperand.</li> <li>2. L'acteur déclenche l'envoi des données.</li> <li>3. Le transmetteur prépare la demande serveur.</li> <li>4. Le message est signé au moyen de la clé privée / du certificat du concepteur et de l'identification d'entreprise selon les spécifications (SECTID, 2018).</li> <li>5. Le transmetteur envoie au répartiteur la demande serveur avec un cryptage SSL.</li> <li>6. Le répartiteur traite les données envoyées (transformation «Umlautstring», calcul «FirstOperand +- SecondOperand») et envoie la réponse au transmetteur.</li> <li>7. Le transmetteur analyse la réponse du répartiteur.</li> <li>8. Le transmetteur affiche la réponse du répartiteur.</li> </ol>
Liste des erreurs	<p>Erreur spécialisée:</p> <ul style="list-style-type: none"> <li>▪ Pas d'interopérabilité</li> </ul> <p>Erreurs techniques:</p> <ul style="list-style-type: none"> <li>▪ Erreur de signature</li> <li>▪ Erreur de cryptage/décryptage</li> <li>▪ Répartiteur injoignable</li> </ul>

Tableau 5: Description du use case de vérification de l'interopérabilité

#### 3.5.1 Exigences spéciales

Le test d'interopérabilité est réalisé à des fins de développement et dans le cadre de l'installation afin de garantir l'interopérabilité entre un transmetteur et le répartiteur.

Les principales difficultés attendues portent sur le codage de chaînes de caractères (encodage) et l'interprétation de nombres à virgule flottante.

Qui plus est, le test d'interopérabilité permet une vérification simple et rapide de la sécurité. Les deux systèmes (transmetteur et répartiteur) doivent dans ce cadre réaliser certaines analyses pour pouvoir identifier la cause d'une éventuelle erreur.

Les paramètres sont visibles dans les tableaux suivants (WSDLID, 2018).

### 3.5.2 Conditions préalables

Le transmetteur envoie les données suivantes:

Nom du paramètre	Valeur	Remarques
UmlautString	ÄËÖÜÄÉÓÚÄÊÔÛÄÊÔÛ	Valeur fixe
FirstOperand	999000000000.00	Valeur fixe, 999 milliards
SecondOperand	Aucune prescription	N'importe quel nombre à virgule flottante
SystemDateTime	Date et heure du transmetteur	Date et heure du système

Tableau 6: Conditions préalables (transmetteur)

### 3.5.3 Conditions ultérieures

Analyse et réponse du répartiteur:

Nom du paramètre	Analyse / Calcul	Remarques
UmlautStringIsCorrect	$UmlautString_{TRANS} = ÄËÖÜÄÉÓÚÄÊÔÛÄÊÔÛ$	Retour: true / false
FirstOperandIsCorrect	$FirstOperand_{TRANS} = 999000000000.00$	Retour: true / false
UmlautString	äëöüäéóúäêôûäêôû	Retour: UmlautString <sub>RÉPAR</sub> majuscules en minuscules
AdditionResult	$AdditionResult_{RÉPAR} = FirstOperand_{TRANS} + SecondOperand_{TRANS}$	Retour: valeur calculée AdditionResult <sub>RÉPAR</sub>
SubstractionResult	$SubstractionResult_{RÉPAR} = FirstOperand_{TRANS} - SecondOperand_{TRANS}$	Retour: valeur calculée SubstractionResult <sub>RÉPAR</sub>
SystemDateTime	Date et heure du répartiteur	Retour: date et heure du système

Tableau 7: Analyse et réponse du répartiteur

Analyse du transmetteur:

Nom du paramètre	Analyse / Calcul	Remarques
UmlautStringIsCorrect	$UmlautStringIsCorrect = true$	Doit être «true»
FirstOperandIsCorrect	$FirstOperandIsCorrect = true$	Doit être «true»
UmlautString	$UmlautString_{RÉPAR} = äëöüäéóúäêôûäêôû$	Doit être «äëöüäéóúäêôûäêôû»
AdditionResult	$FirstOperand_{TRANS} + SecondOperand_{TRANS} = AdditionResult_{RÉPAR}$	Calcul et comparaison, degré de précision de 2 chiffres après la virgule
SubstractionResult	$FirstOperand_{TRANS} - SecondOperand_{TRANS} = AdditionResult_{RÉPAR}$	Calcul et comparaison, degré de précision de 2 chiffres après la virgule
SystemDateTime	$ SystemDateTime_{RÉPAR} - SystemDateTime_{TRANS}  < 1\text{ h}$	L'écart temporel devrait être inférieur à 1 heure.

Tableau 8: Analyse du transmetteur

### 3.6 Use case 006: renouvellement d'un certificat

En principe, les certificats SUA sont valables un an.

Passé ce délai, un certificat SUA peut être renouvelé via le processus SUA à un nombre limité de reprises<sup>2</sup>. Ensuite, il faut obtenir un nouveau certificat SUA. La restriction du nombre de renouvellements possibles est nécessaire pour s'assurer que les informations enregistrées sur les certificats SUA sont à jour (actualité et authenticité).

Dès lors qu'il reste moins de 30 jours de validité pour un certificat SUA enregistré, le processus de renouvellement devrait être automatiquement engagé. Le certificat SUA existant ainsi que le mot de passe reçu lors de l'enregistrement initial sont utilisés dans le cadre du processus de renouvellement.

L'opération `RenewCertificate` déclenche le renouvellement. Le répartiteur vérifie la validité de la demande et procède à une comparaison avec le registre IDE de l'OFS pour s'assurer que les informations relatives à l'entreprise sont à jour. Si les informations figurant au registre IDE de l'OFS ne concordent pas avec celles de l'ancien certificat SUA, la demande est annulée et l'entreprise doit reprendre le processus de certification du début au lieu de réaliser un simple renouvellement.

Dans le cas contraire, le répartiteur se charge d'obtenir un nouveau certificat SUA d'une validité d'un an et le transmet à l'entreprise. Cette dernière doit alors émettre un message-test pour vérifier le nouveau certificat.

### 3.7 Use case 007: double vérification de l'interopérabilité

Ce use case est quasiment identique au use case 005: vérification simple de l'interopérabilité. La seule différence est la suivante: il faut signer non seulement avec le certificat ERP, mais aussi avec le certificat SUA. Cela permet à l'utilisateur de tester la validité et la bonne installation du certificat SUA.

### 3.8 Use case 008: marquage de données-test

Lors de la commande d'un certificat SUA, il est possible de marquer cette dernière comme cas-test. Il convient pour cela d'insérer l'élément `<TestCase>` à l'endroit correspondant (cf. schéma) de l'instance XML. L'événement est traité normalement par le répartiteur, mais en tant que cas-test par le destinataire final.

Ce use case permet de localiser des problèmes dans la chaîne productive de transmission. Dans ce cadre, les messages de l'entreprise passent par toute la chaîne d'automatisation des systèmes concernés (ERP, transmetteur, répartiteur, destinataire final) et de leurs composants, mais sans engager de véritable opération. **Aucun certificat** n'est ici généré.

Toutes les autres consultations liées à ce traitement *doivent* aussi être identifiées comme cas-test.

Les formes hybrides de transmission sont interdites: ce qui débute en tant que cas-test *doit* se terminer en tant que cas-test. Par analogie, un enregistrement exécuté de manière productive ne peut pas être poursuivi en tant que cas-test.

Ce use case devrait être réservé à des cas exceptionnels. Il est *interdit* de s'en servir comme d'un système de démonstration ou de développement: une application de référence et un Showcase sont prévus pour ces usages.

### 3.9 Use case 009: application des règles de sécurité

À l'exception du test d'accessibilité, chaque transmission doit être signée et cryptée. De plus amples informations à ce sujet sont disponibles dans les documents relatifs à la sécurité des transmetteurs (cf. (SECTR)).

---

<sup>2</sup> La fréquence à laquelle le processus de renouvellement pourra être exécuté sera déterminée dès lors que de premières expériences du processus productif auront pu être réalisées.

### 3.10 Use case 010: informations de support; réalisation de clarifications manuelles

Brève description	Les erreurs, avertissements et informations indiqués dans (ACKNSwissdec, 2018) <i>doivent</i> être analysés et portés à la connaissance de l'utilisateur et/ou communiqués au destinataire final. L'utilisation d'identifiants est <i>obligatoire</i> .
Acteurs	Logiciel de comptabilité salariale, transmetteur, répartiteur
Élément déclencheur	Un message ou une demande a été envoyé(e) à un destinataire final via le répartiteur. La réponse est reçue via le répartiteur.
Conditions préalables	<ul style="list-style-type: none"><li>Le répartiteur doit envoyer une demande.</li></ul>
Conditions ultérieures	<ul style="list-style-type: none"><li>Les erreurs, avertissements et informations issus de la réponse doivent être traités et portés à la connaissance de l'utilisateur dans leur intégralité et sous une forme claire.</li><li>Les informations non pertinentes pour l'utilisateur final doivent être mises à la disposition du support technique (StackTrace, Fault-Detail, etc.).</li><li>Les remarques à l'intention du destinataire final doivent être envoyées en tant que notifications.</li><li>En cas d'erreur: Répartiteur injoignable: message d'erreur</li></ul>
Use cases inclus	-
Liste des erreurs	<p>Erreurs techniques:</p> <ul style="list-style-type: none"><li>Erreur de signature</li><li>Répartiteur injoignable</li><li>Le message mis au point par le logiciel de comptabilité salariale ne correspond pas au schéma (non valide).</li><li>Erreur de cryptage/décryptage</li></ul> <p>Erreur spécialisée:</p> <ul style="list-style-type: none"><li>Cf. (RLID, 2018)</li></ul>

### 3.11 Exigences spéciales

#### 3.11.1 Création de fichiers d'archives

Cette exigence permet de veiller à ce qu'une copie de chaque message envoyé et reçu soit sauvegardée. Les données doivent être compilées sous forme de requête SOAP et archivées en tant que document d'instance XML. Les fichiers d'archives *doivent* être signés, mais *peuvent ne pas* être cryptés.

## 4. Annexe

### 4.1 Références

Les références suivantes sont disponibles sur Internet. Certaines sont compressées sous forme de fichiers ZIP. Les fichiers index.html inclus permettent d'accéder à des informations, à la vue d'ensemble et aux différents documents.

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.