

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

**Exigences posées aux destinataires finaux**

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 .....</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: vérification du client / de l'entreprise .....	12
2.4.2	UC002: examen de la demande du client .....	12
2.4.3	UC003: obtention du résultat de la vérification .....	12
2.4.4	UC004: marquage de données-test .....	12
2.4.5	UC005: application des règles de sécurité .....	12
2.4.6	UC006: vérification de l'accessibilité .....	12
2.4.7	UC007: fixation d'une fenêtre de maintenance .....	12
2.4.8	UC008: support; réalisation de clarifications manuelles .....	13
2.4.9	UC009: gestion des doublons .....	13
2.5	Use cases et opérations correspondantes .....	13
<b>3.</b>	<b>Use cases .....</b>	<b>14</b>
3.1	Use case 001: vérification du client / de l'entreprise .....	14
3.2	Use case 002: examen de la demande du client .....	15
3.2.1	Cas particulier des fiduciaires .....	15
3.2.2	Cas particulier de l'absence de relation contractuelle .....	15
3.3	Use case 003: obtention du résultat de la vérification .....	16
3.4	Use case 004: marquage de données-test .....	16
3.5	Use case 005: application des règles de sécurité .....	16
3.6	Use case 006: vérification de l'accessibilité .....	17
3.7	Use case 007: fixation d'une fenêtre de maintenance .....	17
3.8	Use case 008: support; réalisation de clarifications manuelles .....	18
3.9	Use case 009: gestion des doublons .....	18
<b>4.</b>	<b>Exigences complémentaires .....</b>	<b>19</b>
4.1	Création de fichiers d'archives .....	19
4.2	Version de la SUA .....	19
4.3	Normes de communication .....	19
4.4	Compression facultative .....	19
4.5	Disponibilité .....	19
4.6	Périodes définies .....	20
4.7	Plages de valeurs définies .....	20
4.8	Évolutivité .....	20
4.9	Modifications de l'interface .....	20
4.10	Support et temps de réaction .....	20
4.11	Performance / débit .....	21
<b>5.</b>	<b>Annexe .....</b>	<b>22</b>
5.1	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

## Liste des tableaux

Tableau 1: Caractère contraignant des exigences .....	5
Tableau 2: Use cases et opérations .....	13
Tableau 3: Use case 001: transmission de la déclaration des salaires .....	14
Tableau 4: Use case 004: vérification de l'accessibilité.....	17
Tableau 5: Use case 007: fixation d'une fenêtre de maintenance .....	17

## Vue d'ensemble des modifications – Version 20190301

Directives relatives à la norme suisse en matière d'authentification d'entreprises Swissdec (SUA) – Exigences posées aux destinataires finaux, version 20190301, édition 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> [www.swissdec.ch/fr](http://www.swissdec.ch/fr)

## 1. Introduction

Le présent document rassemble les exigences fonctionnelles et complémentaires posées aux destinataires finaux utilisés dans le cadre de la norme suisse en matière d'authentification d'entreprises Swissdec (SUA). Il a pour objet les exigences en matière de commande de certificats. Les mesures de garantie de la sécurité (authentification et caractère contraignant) des processus Swissdec utilisant l'authentification d'entreprises Swissdec sont décrites dans les spécifications des processus concernés. Le présent document traite des aspects techniques de cette norme, et non de sa logique sous-jacente. Dans le cadre de la commande de certificats, un destinataire final sert à identifier une entreprise et à vérifier son IDE-OFS.

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.).

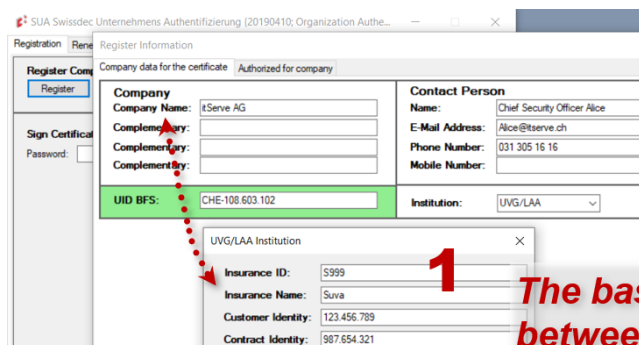
La répartition / l'obtention d'un certificat SUA s'articule généralement autour de deux étapes essentielles:

- 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.



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

180719 BPMN2 SUA Registration Configuration

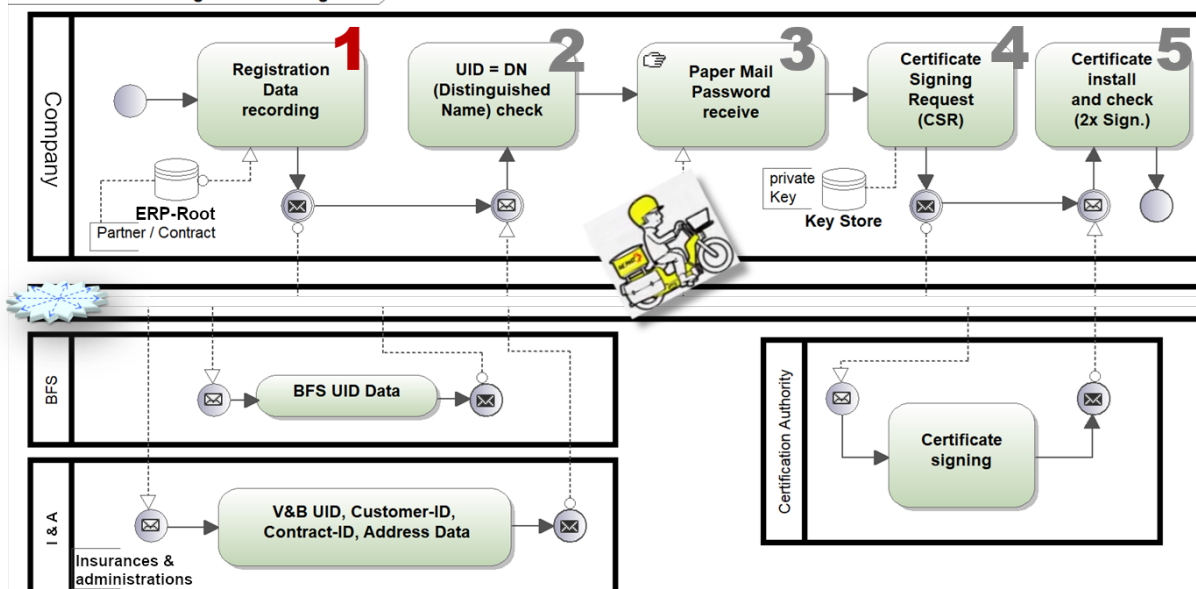


Illustration 1: Croquis de l'étape 1 de la configuration de l'enregistrement SUA

*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.

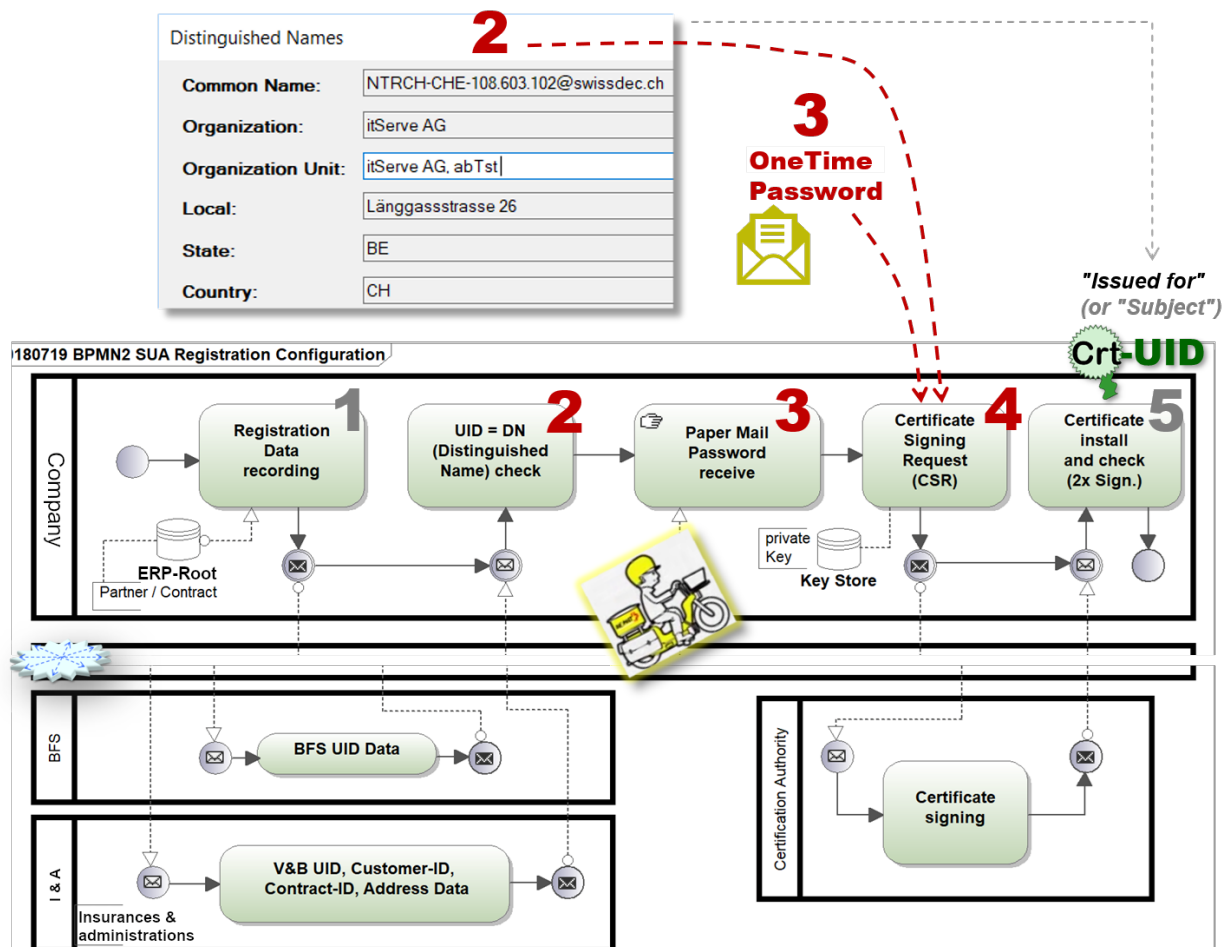


Illustration 2: Croquis des étapes 2, 3, 4 et 5 de la configuration de l'enregistrement SUA

#### 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.

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

#### Attention:

**Le destinataire final n'intervient ici qu'aux étapes 1 et 2. Seuls le transmetteur et le répartiteur participent à la réalisation des autres étapes, notamment la vérification des certificats.**

Il convient de se reporter aux directives /au concept détaillé (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

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

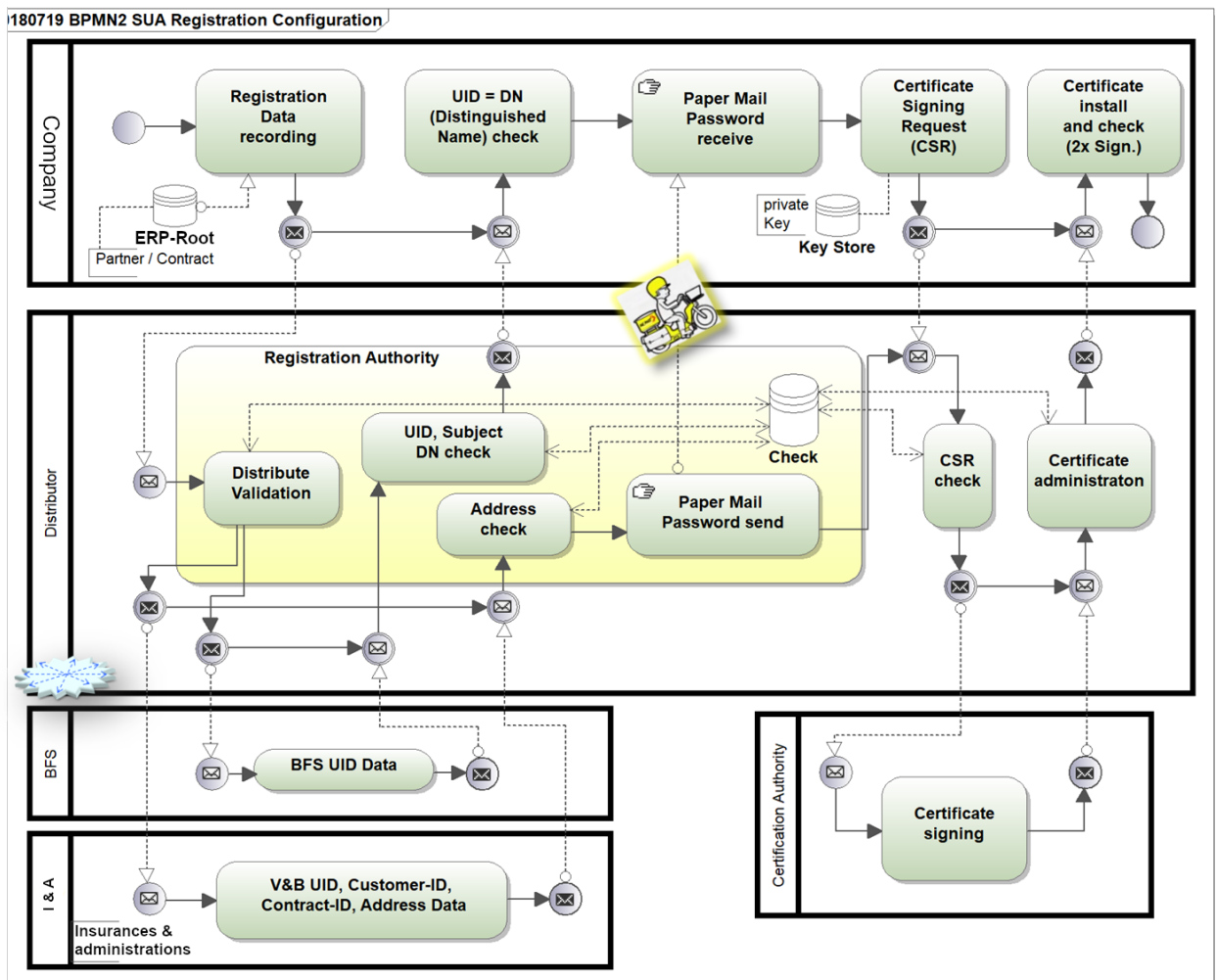


Illustration 3: Croquis du processus d'enregistrement et de configuration SUA

## 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. 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.

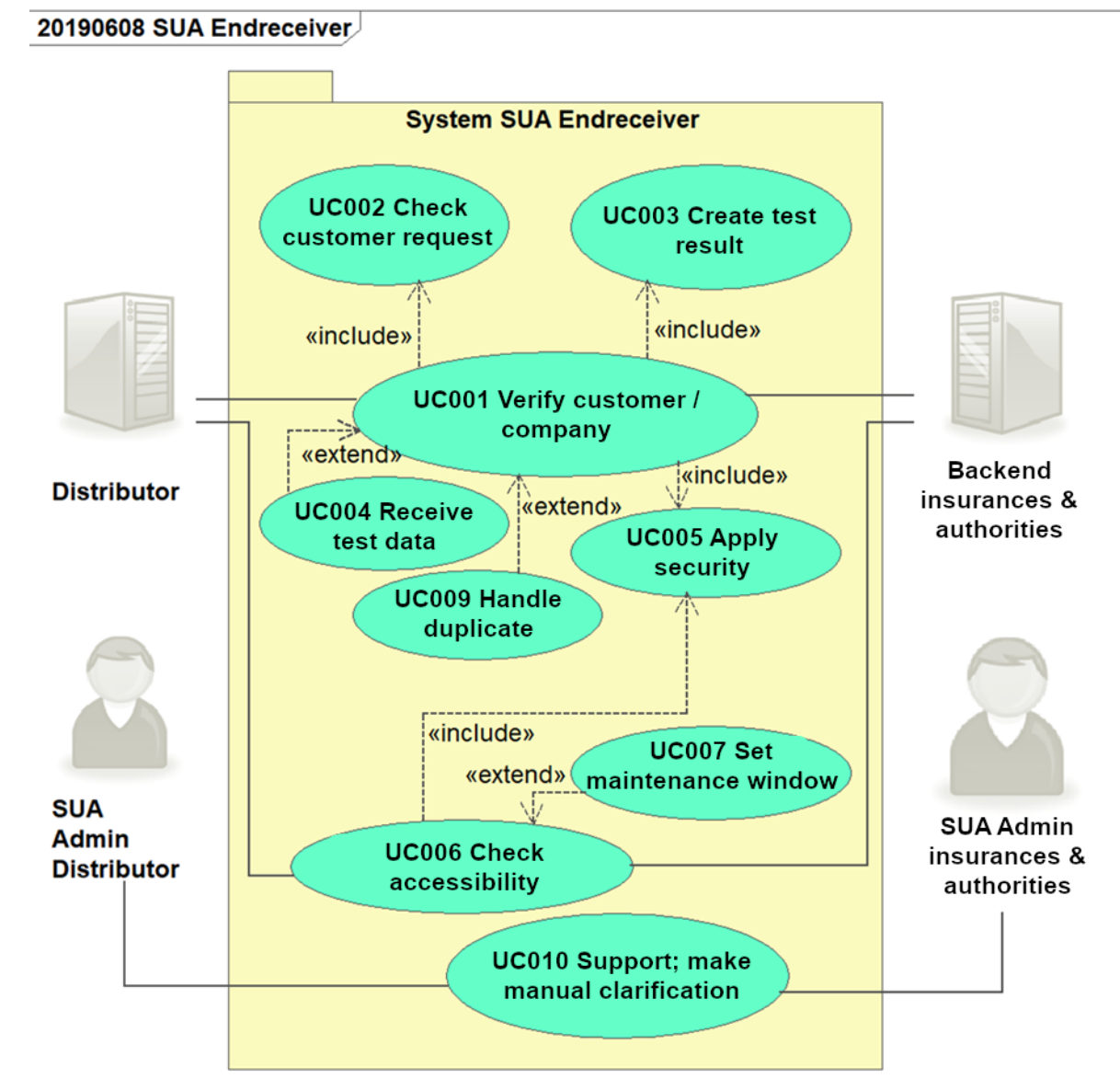


Illustration 4: Use cases

## 2.2 Explications concernant les use cases

Les exigences représentées comme des use cases portent sur la partie technique d'un dispositif du destinataire final qui reçoit la commande d'un certificat SUA et y répond.

Un destinataire final *doit* toujours remplir les exigences système suivantes:

- UC001: vérification du client / de l'entreprise
- UC002: examen de la demande du client
- UC003: obtention du résultat de la vérification
- UC004: marquage de données-test
- UC005: application des règles de sécurité
- UC006: vérification de l'accessibilité
- UC007: fixation d'une fenêtre de maintenance
- UC008: support; réalisation de clarifications manuelles
- UC009: gestion des doublons

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

Les tests de réception se rapportent aux use cases. Conjointement avec les exigences, ces derniers 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: vérification du client / de l'entreprise

Un nouveau certificat est commandé via le répartiteur, ce qui nécessite la vérification par l'assureur (A&A) des données relatives au contrat conclu par le client / l'entreprise. On utilise pour cela d'autres use cases: UC002, UC003, UC004 et UC005.

### 2.4.2 UC002: examen de la demande du client

Le destinataire final (A&A) vérifie l'identité de la personne à l'origine de la demande au moment de la commande / de l'enregistrement. Il compare pour cela les informations transmises avec les données de base / du contrat dont il dispose.

Remarque: pour des raisons de sécurité, le répartiteur ne fournit pas l'IDE-OFS.

### 2.4.3 UC003: obtention du résultat de la vérification

Si le résultat de la vérification (UC002) est concluant, toutes les informations sont fournies selon l'élément <Success> (y compris l'IDE-OFS).

### 2.4.4 UC004: 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. Avec la SUA, le destinataire final réagit toujours de la même manière, qu'il s'agisse d'un cas-test ou d'un message productif.

### 2.4.5 UC005: application des règles de sécurité

Chaque message transmis doit être signé et crypté.

### 2.4.6 UC006: vérification de l'accessibilité

Un message est initié de manière cyclique pour vérifier régulièrement la disponibilité du destinataire final et, le cas échéant, les fenêtres de maintenance définies.

### 2.4.7 UC007: fixation d'une fenêtre de maintenance

Une période et un message doivent être configurés pour les travaux de maintenance et pouvoir être communiqués en réponse à la requête du répartiteur.

#### 2.4.8 UC008: 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. Il doit être possible de renseigner l'entreprise en cas de demande de support.

#### 2.4.9 UC009: gestion des doublons

Le répartiteur marque les doublons de requêtes complètes. Si un doublon contient des informations n'ayant pas encore été traitées, il faut répondre à la requête ad hoc. Les autres types de doublons doivent pouvoir être identifiés et traités via `RegisterOrganizationConsumer` et `GetResultFromOrganizationRegistrationConsumer`.

### 2.5 Use cases et opérations correspondantes

Le modèle de base est un système client-serveur dans lequel le répartiteur est le client. Les normes XLM utilisées sont le WSDL et les schémas XML. Les opérations et éléments suivants se trouvent dans le fichier 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>OrganizationAuthenticationConsumerService WSDL / XSD</i></b>
UC001: vérification du client / de l'entreprise UC002: examen de la demande du client UC003: obtention du résultat de la vérification UC004: marquage de données-test UC005: application des règles de sécurité	<ul style="list-style-type: none"> <li>▪ <code>RegisterOrganizationConsumer</code></li> <li>▪ <code>RegisterOrganizationConsumerResponse</code></li> <li>▪ <code>GetResultFromRegisterOrganizationConsumer</code></li> <li>▪ <code>GetResultFromRegisterOrganizationConsumerResponse</code></li> <li>▪ <code>OrganizationAuthenticationConsumerFault</code></li> </ul>
UC006: vérification de l'accessibilité UC007: fixation d'une fenêtre de maintenance	<ul style="list-style-type: none"> <li>▪ <code>PingConsumer</code></li> <li>▪ <code>PingConsumerResponse</code></li> <li>▪ <code>OrganizationAuthenticationConsumerFault</code></li> </ul>

Tableau 2: Use cases et opérations

### 3. Use cases

#### 3.1 Use case 001: vérification du client / de l'entreprise

Brève description	Un nouveau certificat SUA est commandé via le répartiteur, ce qui nécessite la vérification par l'assureur (A&A) des données relatives au contrat conclu par le client / l'entreprise.
Acteurs	Répartiteur, destinataire final
Élément déclencheur	Un employé de l'entreprise (préposé à la sécurité) souhaite obtenir un certificat SUA. Le répartiteur reçoit sa demande.
Conditions préalables	Le système ERP doit être en mesure d'envoyer et de recevoir des messages électroniques SUA et doit posséder un certificat ERP.
Conditions ultérieures	<ul style="list-style-type: none"> <li>Les informations relatives à l'entreprise ont été vérifiées et sont correctes.</li> <li>Les données correspondantes (y compris l'IDE-OFS) ont été importées.</li> </ul> En cas d'erreur: <ul style="list-style-type: none"> <li>Message d'erreur</li> </ul>
Use cases inclus	UC002: examen de la demande du client UC003: obtention du résultat de la vérification UC004: marquage de données-test UC005: application des règles de sécurité
Procédure standard	<ol style="list-style-type: none"> <li>UC002: l'identité de la personne à l'origine de la demande est vérifiée au moment de la commande / de l'enregistrement (via l'opération <code>RegisterOrganizationConsumer</code>) par le destinataire final (A&amp;A). Ce dernier compare pour cela les informations transmises avec les données de base / du contrat dont il dispose. Remarque: pour des raisons de sécurité, l'IDE-OFS n'est pas transmis.</li> <li>Si le résultat de la vérification (UC002) est concluant, toutes les informations <i>doivent</i> être fournies selon l'élément <code>&lt;Success&gt;</code> (y compris l'IDE-OFS). Le résultat est importé via l'opération <code>GetResultFromOrganizationRegistrationConsumer</code> de manière asynchrone. Si l'attribut <code>WithDelegate</code> apparaît dans l'opération initiale <code>RegisterOrganizationConsumer</code>, cela signifie qu'il s'agit de la demande d'un «fiduciaire». Dans ce cas, <i>il faut</i> fournir toutes les entrées <code>Delegate</code> dans l'opération <code>GetResultFromOrganizationRegistrationConsumer</code>.</li> </ol>
Processus alternatifs	<p>{UC008} Les données sont identifiées en tant que données-test. Appliquer les étapes 1 et 2 de la procédure standard.</p> <p>{Étape 1: fenêtre de maintenance / service indisponible} Les informations relatives à la fenêtre de maintenance (heures de début et de fin) ont déjà été transmises au répartiteur via l'UC006 «Vérification de l'accessibilité». Au cours de cette période, le répartiteur transmet directement au système ERP à l'origine de la demande les messages de réponse ainsi que l'information relative à cette interruption.</p> <p>{Étape 1: interruption imprévue / service indisponible} Pendant cette période, le répartiteur renvoie directement les messages d'erreur au système ERP à l'origine de la demande, voir (ACKNSwissdec, 2020). Le répartiteur reçoit un message d'erreur.</p> <p>{Étape 1: doublon identifié, procéder selon l'UC009 «Gestion des doublons»}</p> <p>{Étape 1: sécurité insuffisante, renvoi du message}</p>
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/cryptage/décryptage</li> <li>Le message mis au point par le répartiteur ne correspond pas au schéma (non valide).</li> </ul>

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

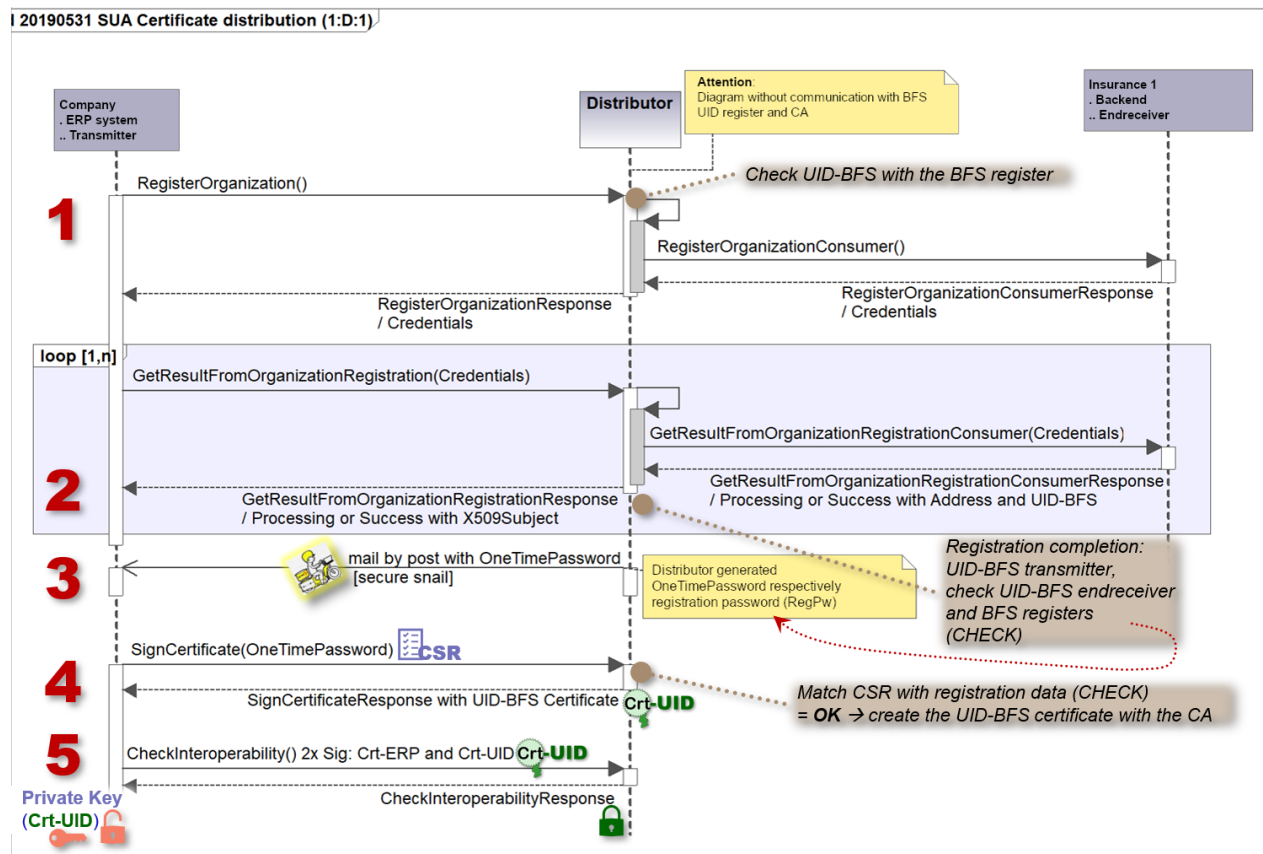


Illustration 5: Diagramme de séquence de l'obtention d'un certificat SUA

### 3.2 Use case 002: examen de la demande du client

Le destinataire final compare les données qu'il a reçues du répartiteur à ses propres données de base / relatives au contrat et renvoie ces dernières au répartiteur. Pour des raisons de sécurité, il est toutefois interdit de transmettre l'IDE-OFS.

Le destinataire final peut ainsi soit permettre la poursuite du processus SUA, soit l'interrompre. Il veille à ce que des certificats SUA ne soient émis que pour les cas de relations contractuelles valables.

#### 3.2.1 Cas particulier des fiduciaires

Quand une entreprise est gérée par une fiduciaire, cette dernière peut demander un certificat SUA pour elle à condition d'être connue du destinataire final.

Dans ce cas, la fiduciaire communique au répartiteur les informations requises concernant l'entreprise pour demander un certificat SUA. Elle fournit également au répartiteur des informations à son sujet.

Le répartiteur ne transmet pas aux A&A de données détaillées sur la fiduciaire, mais uniquement l'attribut `WithDelegate`.

Le destinataire final détermine alors si une ou plusieurs fiduciaires sont connues pour l'entreprise en question. Si oui, il renvoie au répartiteur les informations connues au sujet de la fiduciaire de cette entreprise. Le répartiteur compare à son tour ces informations à celles du transmetteur et, si elles coïncident, décide de la possibilité d'émettre un certificat SUA pour l'une des fiduciaires. Si des irrégularités sont relevées dans les informations relatives à la fiduciaire, le processus est annulé et devra être réenclenché au terme de clarifications menées entre l'entreprise et l'A&A en vue de mettre à jour les informations concernant la fiduciaire.

#### 3.2.2 Cas particulier de l'absence de relation contractuelle

Il peut arriver, dans de rares cas, qu'une entreprise et une A&A doivent échanger des informations alors que les deux parties n'ont conclu aucun contrat. Cela se produit notamment en cas de rechute, dans le cadre de la norme suisse en matière de prestations (KLE), si le patient concerné a entre-temps changé d'emploi et d'assurance.

Pour l'heure, la norme SUA n'offre pas de solution dans ce genre de situations. Néanmoins, il est prévu d'intégrer à une version ultérieure de la norme une identification IDE via la consultation des autorités fiscales afin de pouvoir réaliser le processus d'enregistrement SUA.

### 3.3 Use case 003: obtention du résultat de la vérification

Si les données concordent, le destinataire final fournit ses informations, que le répartiteur importe au moyen de l'opération `GetResultFromRegisterOrganizationConsumer`.

Le destinataire final renvoie alors sa réponse au répartiteur via `GetResultFromRegisterOrganizationConsumerResponse` si l'examen aboutit à un résultat concluant.

En cas d'erreur (technique ou spécialisée), le destinataire final peut interrompre le processus via une «Fault» (`OrganizationAuthenticationConsumerFault`).

### 3.4 Use case 004: marquage de données-test

Lors de la commande d'un certificat SUA, il est possible de marquer ce dernier 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.

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.

### 3.5 Use case 005: application des règles de sécurité

À l'exception du test d'accessibilité, chaque transmission *doit* être envoyée et traitée sous forme signée et cryptée. De plus amples informations à ce sujet sont disponibles dans les documents relatifs à la sécurité des destinataires (cf. (SECER, 2020))



### 3.6 Use case 006: vérification de l'accessibilité

Le use case «Vérification de l'accessibilité» requiert un cryptage SSL bidirectionnel. La requête et la réponse sont signées, et les données XML cryptées selon (SECER, 2020).

Brève description	Il faut vérifier l'accessibilité du destinataire final depuis le répartiteur. Pour ce faire, une demande PingConsumerRequest simple est envoyée selon (WSDLOA, 2019) au destinataire final, qui confirme alors son accessibilité via la réponse PingConsumerResponse.
Acteurs	Répartiteur, opérateur du répartiteur
Élément déclencheur	Vérification cyclique du répartiteur, opérateur en cas d'incident
Conditions préalables	Aucune
Conditions ultérieures	Aucune
Use cases inclus	UC005: application des règles de sécurité
Procédure standard	<ol style="list-style-type: none"> <li>1. La demande est envoyée par le répartiteur au destinataire final. L'intervalle de scrutation est également communiqué. Cet intervalle est actuellement de 30 minutes (y compris pendant une fenêtre de maintenance; il est donc dynamique).</li> <li>2. La sécurité est contrôlée via l'UC005.</li> <li>3. Le destinataire répond avec son timbre horodateur actuel, cf. &lt;PingConsumerResponse&gt;.</li> </ol>
Processus alternatif	{Étape 3: il est aussi possible d'annoncer au répartiteur une fenêtre de maintenance prévue (indisponibilité de x à y) via l'UC007 «Fixation d'une fenêtre de maintenance». Cette fonction <i>doit</i> être mise en œuvre.}
Liste des erreurs	Erreurs techniques: <ul style="list-style-type: none"> <li>▪ Message non valide</li> <li>▪ Décryptage du message impossible</li> </ul>

Tableau 4: Use case 004: vérification de l'accessibilité

### 3.7 Use case 007: fixation d'une fenêtre de maintenance

Brève description	Variante étendue de l'UC006 «Vérification de l'accessibilité». Le destinataire final <i>doit</i> implémenter une fonctionnalité permettant la saisie des données relatives à une fenêtre de maintenance et leur annonce au répartiteur dans la réponse à l'UC006 «Vérification de l'accessibilité».
Acteurs	Administrateur technique du destinataire final
Élément déclencheur	Vérification cyclique du répartiteur, opérateur en cas d'incident
Conditions préalables	Aucune
Conditions ultérieures	Aucune
Use cases inclus	Aucune
Procédure standard	<ol style="list-style-type: none"> <li>1. L'administrateur technique du destinataire final saisit les données relatives à la fenêtre de maintenance.</li> <li>2. La réponse du destinataire final (PingConsumerResponse) au répartiteur contient les données relatives à la fenêtre de maintenance saisies.</li> </ol>
Processus alternatifs	Aucun
Liste des erreurs	Erreur technique: <ul style="list-style-type: none"> <li>▪ Message non valide</li> </ul>

Tableau 5: Use case 007: fixation d'une fenêtre de maintenance

### 3.8 Use case 008: support; réalisation de clarifications manuelles

Il doit être possible, en cas de demande de support, de renseigner l'entreprise sur une commande de certificat donnée. Le gestionnaire travaillant pour le destinataire doit par conséquent pouvoir localiser les problèmes d'après les fichiers-journaux et les messages d'erreur. Les requêtes erronées doivent donc elles aussi être enregistrées dans les fichiers-journaux, et leur traçabilité garantie à l'aide des identifiants utilisés.

### 3.9 Use case 009: gestion des doublons

Les doublons strictement identiques de demandes `RegisterOrganization` complètes pourraient être techniquement identifiés par le répartiteur et marqués sous `DistributorRequestContext` via un attribut `<Duplicate>`. Cela exigerait toutefois que le répartiteur puisse identifier un doublon sans le moindre doute, c'est pourquoi l'attribut `<Duplicate>` n'est pas utilisé dans la pratique.

Il n'y aura donc pas de doublon, car le répartiteur octroiera un nouvel identifiant `CertificateRequest` à chaque nouvelle requête. Par conséquent, il faut répondre normalement aux requêtes `RegisterOrganization` réitérées pour une entreprise.

## 4. Exigences complémentaires

### 4.1 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 ne doivent pas être cryptés.

### 4.2 Version de la SUA

Le schéma contient l'élément `<RequestContext/UserAgent/StandardVersion>`, qui renseigne sur la version utilisée de la norme suisse en matière d'authentification d'entreprises Swissdec (SUA). Cette mention est nécessaire du fait des modifications apportées d'une version à l'autre et qui ne concernent pas le schéma, mais uniquement le contenu des éléments: selon la version de la norme suisse en matière d'authentification d'entreprises Swissdec (SUA), le contenu des éléments peut donc être défini différemment.

### 4.3 Normes de communication

Le raccordement standard *doit* être basé sur la technologie de services Web (SOAP<sup>2</sup> version 1.1, WSDL<sup>3</sup> version 1.1 et WSS<sup>4</sup> version 1.0). Les données *doivent* être cryptées non seulement au niveau de la couche HTTPS<sup>5</sup> (cryptage SSL/TLS bidirectionnel), mais aussi au niveau SOAP selon le protocole WSS (SECER, 2020).

### 4.4 Compression facultative

La compression des requêtes et des réponses est facultative. Vu le grand nombre d'informations redondantes, les données XLM cryptées peuvent toutefois être compressées d'environ 50 % (d'après des données empiriques). Afin de pouvoir distribuer de gros rapports d'événements via le répartiteur tout en ménageant la bande passante, dont l'importance est cruciale pour tous les acteurs, il est possible de compresser les requêtes provenant du répartiteur à l'aide de gzip. La décision de recourir ou non à la compression est prise lors du raccordement.

En cas de compression gzip, les requêtes provenant du répartiteur possèdent au minimum les champs suivants dans l'en-tête http:

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

Le cas échéant, les réponses compressées de destinataires finaux *doivent* contenir le champ suivant:

- Content-Encoding: gzip

Plus d'informations sur <http://www.ietf.org/rfc/rfc1952.txt>.

### 4.5 Disponibilité

L'unité d'observation englobe le répartiteur et tous les destinataires finaux raccordés. Autrement dit, tout le système constitue une entité pour l'entreprise (source des données d'événement). Si l'exploitation d'un destinataire final ne satisfait pas aux exigences de qualité, la fiabilité du système dans son ensemble est compromise. Tous les participants doivent donc se mettre d'accord sur un degré de fiabilité **minimal**.

#### Exigence issue de la norme suisse en matière de prestations

- Toutes les transmissions M2M (de machine à machine) sont réalisées en «**temps réel**». (par Internet, **7 jours sur 7 et 24 heures sur 24.**)

D'où les conséquences suivantes pour le destinataire:

- Les institutions / leurs destinataires finaux **doivent** également proposer **un service disponible 7 jours sur 7 et 24 heures sur 24, au moins pour recevoir les données**.
- Les **interruptions prévues**<sup>6</sup> (p. ex. **fenêtres de maintenance**) *doivent* avoir lieu aux heures creuses et *doivent* être préalablement annoncées (cf. use case UC003 «Vérification de l'accessibilité»).
- Après une **interruption imprévue**, les entreprises concernées dont une transmission a échoué *devraient* être informées du fait que le destinataire est de nouveau disponible.

<sup>2</sup> SOAP (initialement pour Simple Object Access Protocol)

<sup>3</sup> Le Web Services Description Language (WSDL) définit une spécification XML indépendante des plateformes, langages de programmation et protocoles servant à décrire des services réseau (services web) d'échange de messages.

<sup>4</sup> Web Services Security (WSS) de l'Organization for the Advancement of Structured Information Standards (OASIS)

<sup>5</sup> http 1.0 ou 1.1; au moins TLS 1.2 avec une longueur de clé de session minimale de 256 bits

<sup>6</sup> Valable pour les travaux de maintenance classiques, hors hotfixes ou patches

- Même si des services internes **ne sont pas disponibles** pour vérifier l'acceptation, il reste *possible* d'envoyer une quittance d'acceptation. L'expéditeur *devrait* en être avisé au moyen d'un avertissement / d'une notification intégrée(e) à la quittance. Si la déclaration est finalement rejetée lors d'une vérification ultérieure des données, le client doit en être informé parallèlement à ces spécifications système.

#### Approche ciblée concernant la disponibilité:

Nous souhaitons adopter **le point de vue du client**. La disponibilité des systèmes est exprimée par des **valeurs cibles** visant à encourager les entreprises à transmettre leurs déclarations sous forme électronique. Aucun contrôle de la disponibilité n'est prévu. Seules les principales valeurs indicatives sont donc définies ci-après. Les bases correspondantes sont jointes en annexe.

#### 4.6 Périodes définies

- Période de fonctionnement du système dans sa globalité (répartiteur, communication et destinataire final; transfert M2M jusqu'à l'envoi de la quittance à l'entreprise)
  - 7 jours sur 7, 24 heures sur 24
  - Heures de pointe: tous les jours entre 6 h et 20 h, hors week-end (toutes les autres plages horaires sont considérées comme des heures creuses)
- Fenêtre de maintenance pour les correctifs et les mises à jour
  - 10 heures par semaine
  - En dehors des heures de pointe, si possible entre 2 h et 5 h du matin
- Période de service et de support pour les participants au système (répartiteur et ses destinataires finaux)
  - Aux heures de bureau habituelles
  - Support pour fenêtres de maintenance sur demande

#### 4.7 Plages de valeurs définies

L'objectif est une solution pragmatique = «lightweight construction» et «Best Effort»

- Aux **heures de pointe**, la disponibilité des destinataires finaux (M2M) **devrait** atteindre au moins 99,52%.
- Aux **heures creuses**, la disponibilité des destinataires finaux (M2M) **devrait** atteindre au moins 93,00%.

#### 4.8 Évolutivité

Les systèmes des destinataires finaux devraient pouvoir évoluer en fonction de la charge. Il serait tout à fait judicieux de commencer par développer une solution minimale, puis d'en accroître la performance au besoin pour garantir la disponibilité et la performance requises.

#### 4.9 Modifications de l'interface

- S'il y a lieu d'activer également des modifications de la norme suisse en matière d'authentification d'entreprises Swissdec (SUA) au niveau du destinataire final, tout le raccordement *doit* être adapté (côté répartiteur et côté destinataire final).
- S'il n'y a pas lieu d'activer de modifications de la norme suisse en matière d'authentification d'entreprises Swissdec (SUA) au niveau du destinataire final, le répartiteur *peut* transformer la structure de données existante (mappage) dans la mesure où le contenu le permet («pare-feu personnalisé»).

Le répartiteur transmettra toujours des données clairement définies. Aucune solution générique n'est prévue pour le moment.

#### 4.10 Support et temps de réaction

Concernant le support, seuls certains aspects techniques, à savoir les structures d'information pour tous les systèmes de la chaîne de processus, sont définis ici.

Les prestations de support *doivent* être fournies en allemand, en français et en italien pour les domaines / acteurs suivants:

- entreprises et leurs concepteurs ERP;
- destinataires finaux d'institutions.

Autrement dit, certains messages d'erreurs doivent également être émis dans la langue choisie. Voir le message:  
.../RequestContext/LanguageCode.

Le temps de réaction est défini selon les **catégories d'erreurs** suivantes:

- Critical = 15 minutes
- Medium = 4 heures
- Uncritical = 1 journée

Ces catégories d'erreurs seront ultérieurement utilisées dans différents systèmes (applications, fichiers-journaux, outil de surveillance, etc.).

En outre, le 2<sup>e</sup> niveau de support *doit* être coordonné avec les développeurs d'applications.

#### 4.11 Performance / débit

- Il convient de déterminer le volume de données maximal pour chaque destinataire final et de dimensionner les systèmes en conséquence.
- Temps de réponse (pour toutes les opérations): tout le processus de transmission doit être exécuté «en temps réel». Le temps nécessaire à la transmission / distribution devrait être **inférieur à une minute**. D'où les conséquences suivantes pour le destinataire final:

- Le temps de traitement dépend du destinataire final, du volume de données et de la capacité de transmission.
- Une réponse *devrait* être donnée en moins de 20 secondes.
  - De plus, le répartiteur définit un temps d'attente maximal pour chaque destinataire final (délai par défaut actuel = 60 secondes).

## 5. Annexe

### 5.1 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. (2020). AcknowledgementNotification. Bern, Schweiz.

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

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

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

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