Authentification d’entreprises

Spécifications détaillées

Version

Version actuelle	Édition 10.05.2019, Version 1.5
Date actuelle:	12.05.2021
Date d’enregistrement:	01.04.2020
Date d’impression:	12.05.2021
Modèle:	Richtlinien.docx
Commentaire:	reproduction autorisée avec indication de la source

Les spécifications détaillées pour l'authentification d'entreprises ont été elaborées en collaboration avec les entitées suivantes:

- Association Swissdec
- Haute école spécialisée bernoise (Technique et informatique)
  - Stefan Agosti, Annett Laube, Gerhard Hassenstein, Pascal Mainini, Anton Böhm

Éditeur

Swissdec
Fluhmattstrasse 1
6004 Lucerne
www.swissdec.ch

Table des matières

1 Introduction

1.1 Contexte

La plateforme d'information centralisée exploitée par l'Association Swissdec en vue d'établir une norme pour l'échange de données électroniques permet dès aujourd'hui de transmettre des données salariales par voie entièrement électronique dans le cadre de la «norme suisse en matière de salaire (ELM)». La «norme suisse en matière de prestations (KLE)» est actuellement mise au point sur cette base en complément du processus, de la demande de prestations à leur fourniture. Les comptabilités salariales et systèmes ERP certifiés Swissdec simplifient ainsi les procédures au sein des entreprises, permettent d'établir des déclarations correctes et réduisent les charges administratives.
Le traitement électronique des processus d'affaires, de la déclaration de l'événement (p. ex. déclaration d'accident à l'assureur) au décompte des indemnités journalières, implique de satisfaire à de nouvelles exigences en matière d'identification et d'authentification des entreprises participantes.
Lors de la première phase de l'élaboration de l'authentification d'entreprises Swissdec, les objectifs et exigences relatifs à un tel système ont été définis et rassemblés au sein d'un concept de solution qui constitue le cadre de la mise en œuvre technique d'une authentification des entreprises participantes sur la base de l'IDE-OFS. Ce concept de solution sert de base aux présentes spécifications détaillées qui énumèrent les règles nécessaires à une mise en œuvre pilote du système.

1.2 Finalité du document

Les spécifications détaillées décrivent point par point la mise en œuvre et l'organisation des processus d'authentification d'entreprises SUA déjà définis dans le concept de solution en matière d'enregistrement, de configuration initiale, de validité, de renouvellement et de blocage. Les exigences des processus Swissdec en matière de sécurité sont approfondies à la lumière des exigences posées à la SUA en vertu du concept de solution et la mise en œuvre via des certificats IDE Swissdec décrite. Le présent document définit également la structure des données d'identification (mots de passe, certificats IDE) utilisés dans le cadre des processus.
Il sert ainsi de base à la mise en œuvre du système dans le cadre d'un projet pilote durant lequel il conviendra de veiller à respecter les règles et les concepts définis dans les spécifications et de vérifier la compatibilité de ces dernières avec une utilisation pratique. Les expériences issues de cette première mise en œuvre pratique seront ensuite intégrées dans une version remaniée des spécifications détaillées.

1.3 Délimitation

Le contenu des présentes spécifications détaillées se concentre sur une première mise en œuvre de l'authentification d'entreprises Swissdec dans le cadre d'un projet pilote. Les variantes prévues dans le concept de solution ont ainsi été réduites au strict minimum. Qui plus est, les différents composants des spécifications sont décrits sous l'angle de leur applicabilité technique. Les règles présentées ici ont été identifiées à la lumière d'enseignements tirés dans des contextes similaires et s'inspirent largement de bonnes pratiques établies. Cela étant, seule la mise en œuvre pratique de la norme permettra de déceler dans les spécifications d'éventuelles lacunes ou problématiques qu'il s'agira alors d'éliminer dans une version ultérieure.
À l'instar du concept de solution, les spécifications détaillées de l'authentification d'entreprises Swissdec se limitent explicitement à l'authentification univoque et sécurisée d'entreprises dans le cadre de la communication avec le répartiteur Swissdec ou l'A&A en tant que destinataire final. Les présentes spécifications traitent des authentifications dans le cadre de la communication automatisée de machine à machine (M2M) entre un système ERP (transmetteur) et le répartiteur, ainsi que, au niveau du back-end, entre le répartiteur et les systèmes des destinataires finaux. Les autres cas d'application pouvant nécessiter une authentification (p. ex. accès d'un utilisateur au portail d'un assureur ou à un portail de Swissdec) sont traités dans un document distinct.
Les processus d'affaires spécialisés, par exemple dans le cadre de la norme suisse en matière de salaire (ELM) ou de la norme suisse en matière de prestations (KLE), ne sont abordés ici que de façon marginale. Le cas échéant, toute adaptation nécessaire de directives existantes ou à rédiger concernant la compatibilité avec la SUA incombe aux groupes de travail compétents de Swissdec.

1.4 Objectifs et exigences

Le document «Authentification d'entreprises Swissdec – Concept de solution et de recensement des exigences» (version 1.1) rassemble les objectifs et exigences identifiés dans le cadre de la première phase du projet. Ces objectifs

et exigences servent de base aux spécifications détaillées et sont présentés dans le détail au chapitre 2. Le chapitre 8 indique dans quelle mesure les différentes exigences ont pu être prises en compte dans les spécifications.

1.5 Vue d'ensemble de l'architecture Swissdec

L'architecture Swissdec est brièvement présentée ici afin de dépeindre plus précisément le contexte de la SUA. La plateforme centralisée d'échange des données, à savoir le répartiteur Swissdec, contribue à optimiser et à automatiser les processus entre pas moins de 200 000 entreprises et leurs assureurs ainsi que les autorités en Suisse. Actuellement (état: 2018), plus de 12 millions de données personnelles, dont des informations relatives aux salaires, sont distribuées chaque année entre les participants.

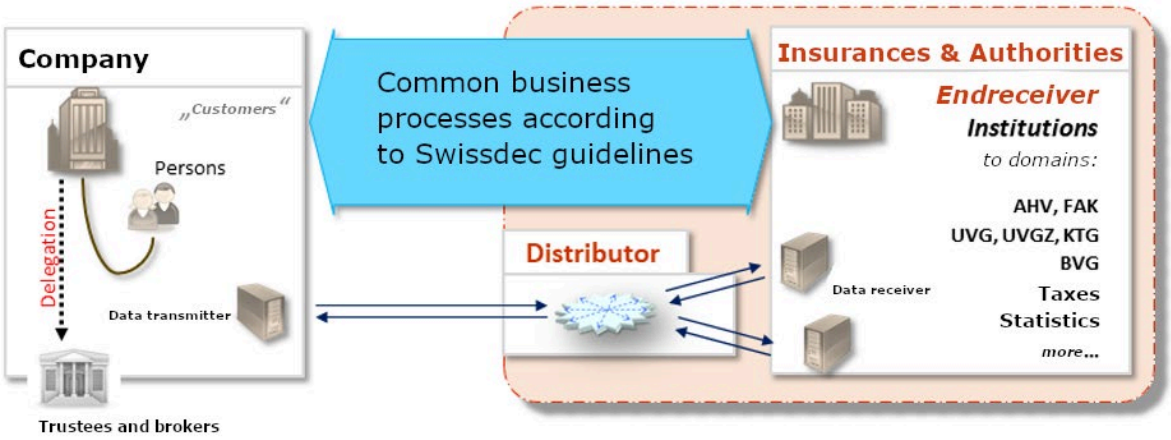

Illustration 1: Vue d'ensemble des processus Swissdec

Les participants aux processus sont:

- les entreprises, avec leurs systèmes ERP et les concepteurs de ces derniers, qui utilisent un «transmetteur»,
- et les assureurs et autorités (A&A), avec leurs systèmes back-end spécialisés, appelés «destinataires finaux».

Les systèmes connectés par le biais du processus communiquent via des interfaces M2M au moyen de protocoles standardisés.

La relation problématique n:m entre les entreprises et les A&A est convertie via un répartiteur centralisé en une relation simple «n:répartiteur:m» (cf. illustration 2). Le répartiteur communique avec les entreprises à la place des A&A et transfère les données aux destinataires finaux après les avoir vérifiées et filtrées.
Le répartiteur Swissdec intervient ainsi vis-à-vis des entreprises en tant que représentant des destinataires finaux (A&A).[1] Il bénéficie donc de la confiance totale des destinataires finaux et assure la gestion et le bon déroulement des processus de communication en leur nom vis-à-vis des systèmes ERP des entreprises. Pour ce qui est du contenu, le répartiteur se contente de transférer les messages. Les systèmes des destinataires finaux et des entreprises sont seuls responsables de l'exactitude spécifique des messages et processus d'affaires.
Le recours au répartiteur Swissdec présente les avantages suivants:

- simplification des phases de développement, de test et de production pour les entreprises, car les systèmes ERP ne communiquent qu'avec le répartiteur;
- limitation des doublons dans les données et les processus;
- pare-feu personnalisé: des versions différentes peuvent être bypassées au niveau du répartiteur par le biais de la transformation. Le cycle de vie des versions est fluidifié et optimisé;
- assurance qualité dynamique (plausibilisation) et filtrage des données par le répartiteur;
- pas de stockage de données au niveau du répartiteur: la communication entre entreprises et A&A intervient «en temps réel» (7 jours sur 7, 24 heures sur 24);

[1] Le rôle de représentant du répartiteur Swissdec ainsi que les rôles et obligations des participants au processus sont définis dans les CG du répartiteur, cf. https://www.swissdec.ch/fr/conditions-generales/.

- Swissdec contrôle et certifie les concepteurs de logiciels pour les transmetteurs et destinataires finaux afin de garantir une qualité élevée en termes d'interopérabilité et de données ainsi qu'une configuration «Plug and Play» pour les participants au processus.

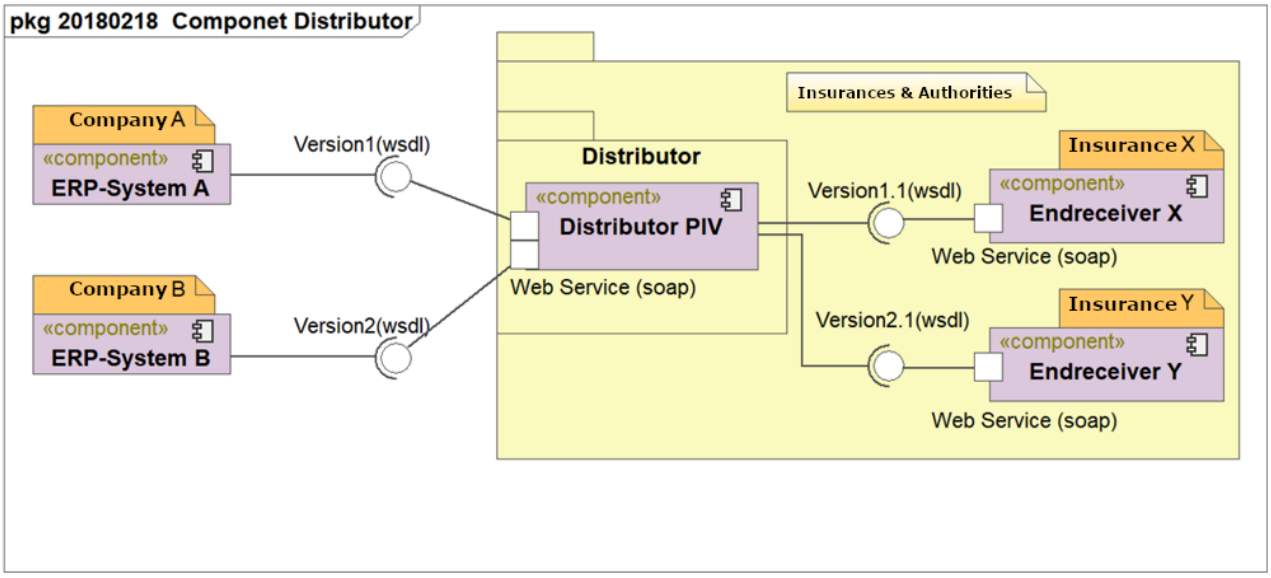

Illustration 2: Relations de communication Swissdec

L'architecture technique est celle de services Web en cascade basés sur un appel synchrone du transmetteur (système ERP) au destinataire final (assureurs & autorités) via le répartiteur. Une relation «en temps réel» est ainsi établie via le répartiteur et permet l'interaction rapide entre les systèmes dans le cadre du processus M2M. En plus du canal sécurisé au niveau du transport (SSL/TLS), les services Web sont protégés par les concepts de sécurité standardisés de WSS (Web Services Security; SOAP Message Security: signature + cryptage).

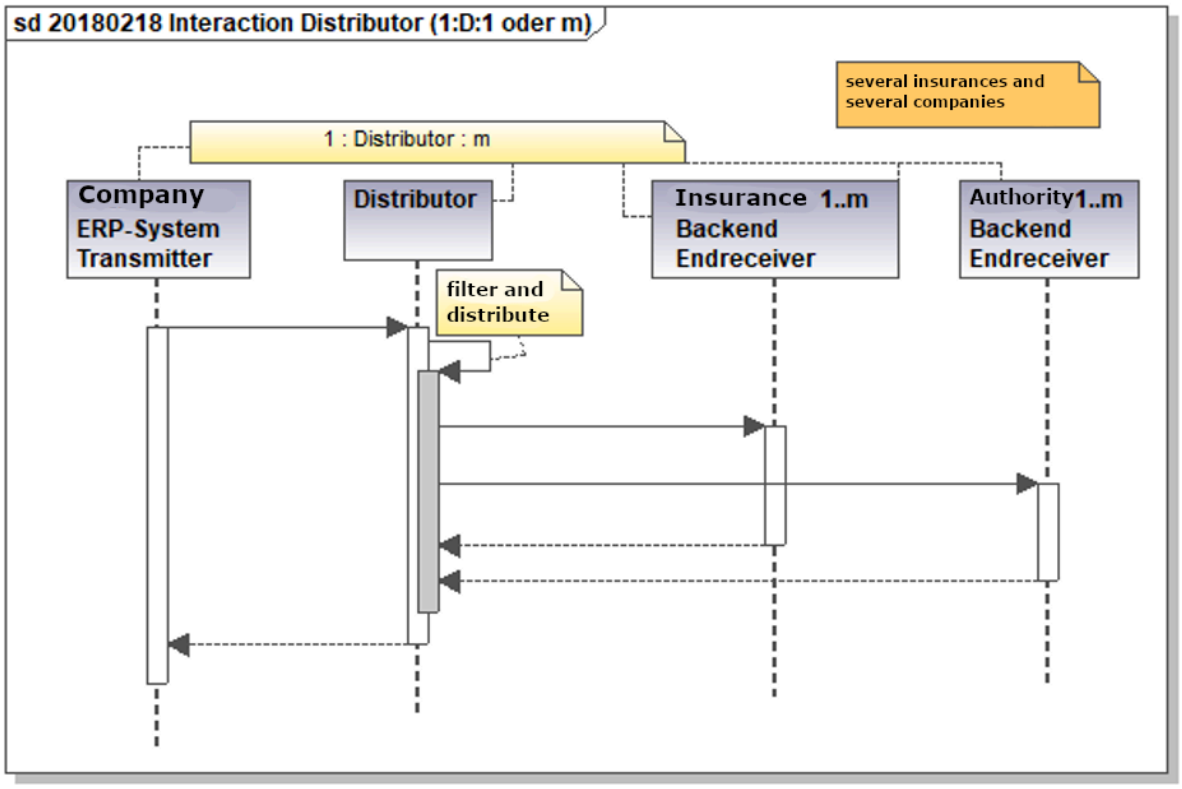

Illustration 3: Communication 1:répartiteur:m

Les processus urgents sont traités de façon asynchrone: après l'appel, le transmetteur reprend immédiatement le contrôle, puis essaie de récupérer plus tard sa réponse par scrutation.

2 Exigences des processus Swissdec en matière de sécurité

Ce chapitre détaille les exigences posées à la communication Swissdec en matière de sécurité. Les exigences (cf. également le tableau 14 chapitre 8) formulées dans le concept de solution sont précisées et complétées par de nouvelles exigences découlant notamment de la norme suisse en matière de prestations (KLE), développée en parallèle.

2.1 Canal sécurisé

L'architecture Swissdec prévoit que toutes les relations de communication entre le système ERP d'une entreprise, le répartiteur Swissdec et les systèmes des destinataires finaux (A&A) soient protégées via un canal sécurisé au niveau du transport (SSL/TLS). Du point de vue technique, il est tout à fait pertinent, pour la sécurité, que la relation au niveau du transport exige une authentification mutuelle par certificat (cryptage SSL bidirectionnel).

- Élargit l'exigence A-16 (autorisation du système ERP).

2.2 Authentification au niveau des messages

Swissdec nécessite aussi, pour l'extension de ses services, une authentification univoque de tous les participants au niveau des messages (par la signature des données transmises).

- Élargit les exigences A-17 (authentification de l'entreprise) et A-19 (authentification de l'entreprise)

2.3 Confidentialité au niveau des messages

Pour pouvoir, parallèlement au canal sécurisé, protéger aussi les informations transmises contre d'autres vecteurs d'attaques, il faut crypter le contenu des données pour leur destinataire.

- Nouvelle exigence A-27 (confidentialité au niveau des messages)

2.4 Environnement d'exploitation

Selon le processus, les données qui doivent être signées peuvent être très volumineuses ou devoir être signées peu de temps après leur transmission. Le processus de signature doit donc être extrêmement performant, pour le système ERP comme pour le répartiteur Swissdec. Par le passé, des certificats logiciels ont permis de répondre à cette exigence, car les applications bénéficiaient à tout instant d'un accès simple et rapide à la clé de signature.

- Élargit l'exigence A-17 (authentification de l'entreprise)

2.5 Non-répudiation

Tout au long du processus de communication, les entités participantes ne doivent pouvoir nier ni l'envoi, ni la réception de données. Cette non-répudiation est indispensable au caractère contraignant.
Le but est de faire en sorte qu'il soit impossible de réfuter l'envoi ou la réception de données et d'informations. Il convient à ce titre d'établir une distinction entre:

- *la non-répudiation de l'origine*: l'expéditeur d'un message ne doit pas pouvoir contester ultérieurement l'envoi d'un message donné;
- *la non-répudiation de la réception*: le destinataire d'un message ne doit pas pouvoir contester ultérieurement la réception d'un message envoyé;
- *la preuve d'une liaison de communication:* dans le cas de processus urgents, un émetteur doit pouvoir apporter ultérieurement la preuve qu'il a envoyé un message donné.

Ainsi, il doit être possible, même a posteriori, de rétablir un processus de communication et de le retracer intégralement. Aucun émetteur participant à un échange de données ne doit pouvoir nier avoir envoyé un message donné. De même, un destinataire ne doit pas pouvoir nier avoir reçu un message.

- Élargit l'exigence A-20 (traçabilité)

2.6 Caractère contraignant

Les prestations d'assurance sont fournies en fonction des données transmises. Il est donc crucial que les processus de communication soient sécurisés en termes de non-répudiation. Ce niveau de sécurité est garanti par le fait que toutes les données et informations pertinentes pour un processus de communication (y compris la signature et le timbre horodateur) doivent être consignées et archivées.

- Élargit l'exigence A-20 (traçabilité)

2.7 Enregistrement

Les entreprises doivent être identifiées et enregistrées par l'intermédiaire de Swissdec en vue de l'émission de certificats IDE. Le contrôle de l'identité d'une entreprise nécessaire à cet effet peut être réalisé sur la base de relations existantes avec les entreprises à l'origine des demandes. Sans cela, les processus d'enregistrement ne pourraient pas être à la fois simplifiés, sécurisés et en partie automatisés.

- Élargit les exigences A-09 (organisme d'enregistrement), A-10 (identification univoque de l'entreprise) et A-11 (identification par une instance autorisée)

3 Certificats Swissdec

Pour pouvoir satisfaire à ces exigences, Swissdec doit, dans le cadre de l'authentification d'entreprises, recourir à des certificats à différents niveaux et/ou dans différents champs d'application.
L'illustration 4 indique les systèmes nécessitant et ayant installé les différents types de certificats. Le but dans lequel ces certificats sont utilisés est précisé aux chapitres suivants.

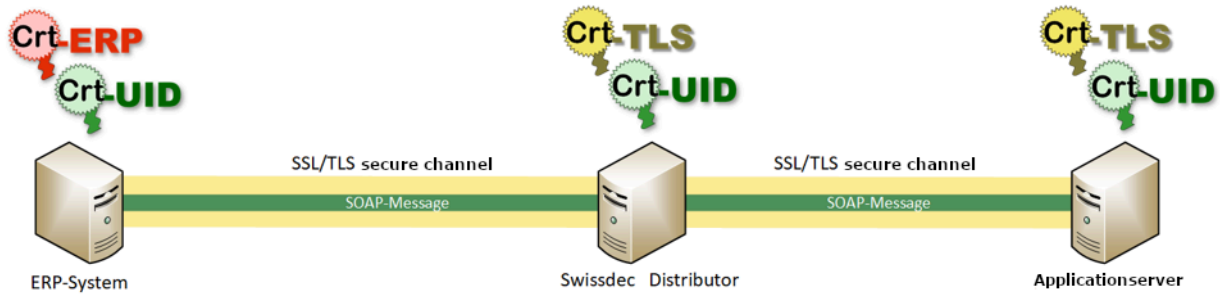

Illustration 4: Vue d'ensemble des certificats Swissdec

3.1 Certificats IDE Swissdec

Les données au niveau SOAP sont signées et cryptées. Pour ce faire, le transmetteur, le répartiteur et les systèmes des destinataires finaux utilisent des certificats IDE Swissdec. Ces certificats sont soumis à des règles précises en matière de contenu, décrites au chapitre 5.1.5.
Les certificats IDE étant utilisés à la fois pour signer et pour crypter des messages SOAP, il serait logique de recommander le recours à deux certificats différents par application.
Toutefois, comme ces données ne doivent être cryptées que très brièvement (pour leur transport) et non archivées sous forme cryptées pour être ensuite décryptées, il n'y a pas lieu d'archiver de clés privées. Par conséquent, et dans un souci de simplification de la gestion des certificats, mieux vaut renoncer à une limitation de l'application des certificats IDE au profit de l'utilisation d'un même certificat pour l'authentification, la signature et le cryptage.
Le destinataire doit chaque fois confirmer l'échange de données entre les différentes sections de communication. Cette confirmation de transaction est également signée avec le certificat IDE.

3.2 Certificats de serveur SSL/TLS

Au niveau du transport, des certificats de serveur SSL/TLS sont utilisés pour le répartiteur et les destinataires finaux. Selon la section / direction de la communication, il peut s'agir d'une instance de serveur ou de client. Il convient de laisser à l'exploitant la possibilité d'utiliser pour cela soit deux certificats différents, soit un seul certificat. Pour ces systèmes, les certificats IDE Swissdec doivent toutefois être utilisés pour l'authentification au niveau du transport en tant que certificats de clients Web TLS.
Le transmetteur du système ERP d'une entreprise, en revanche, peut jouer uniquement le rôle de client. Seuls les certificats IDE Swissdec peuvent dans ce cadre servir de clients Web TLS.
Les certificats de serveur Web TLS peuvent être émis par des CA (de l'anglais «Certificate Authorities», autorités de certification) publiques ou internes à l'entreprise. Dans le cas de certificats émis par une CA publique, mieux vaut opter pour un fournisseur membre du CAB-Forum[2] et certifié par WebTrust[3].
Si, en vertu des directives d'un destinataire final, un partenaire de communication ne doit posséder que des certificats d'une PKI interne en vue de l'authentification, il est possible d'émettre un certificat de client Web TLS d'une CA interne pour le répartiteur.

3.3 Certificats ERP Swissdec

La capabilité processus d'une version donnée d'un système ERP est démontrée via un autre type de certificat qui est aussi utilisé au niveau SOAP pour signer des messages. Ces certificats devraient être émis également à l'avenir par une CA interne à Swissdec. Swissdec établit à ce sujet une distinction entre deux CA internes:

- CA1, qui émet des certificats destinés à un usage productif, et

[2] https://cabforum.org
[3] https://webtrust.org

- CA2, qui émet des certificats pour l'environnement de développement.

3.4 Autres certificats

3.4.1 Enregistrement avec des certificats tiers

Les entreprises peuvent s'enregistrer au moyen de certificats réglementés ayant été émis par une CA accréditée pour des personnes morales au sens de l'art. 7 SCSE (voir processus «Enregistrement au moyen d'un certificat réglementé selon la SCSE», chap. 6.1.2).)

3.4.2 Certificats utilisateur

Dans une phase ultérieure, Swissdec aura aussi besoin de certificats pour authentifier les utilisateurs et pourra utiliser à cet effet des certificats simples avancés ou des certificats réglementés pour des personnes physiques. Le type de certificats qui sera utilisé n'est pas encore connu. Ce point est abordé dans un document distinct.

4 Sécurité et confiance

La sécurité de la communication et la confiance dans les processus électroniques entre l'entreprise (transmetteur), le répartiteur et le système du destinataire final reposent sur trois piliers:

1. un canal de transport authentifié et sécurisé,
2. la sécurité et la confiance au niveau des messages (message SOAP), et
3. le caractère contraignant de la transmission des messages via la confirmation de la transaction.

4.1 Canal de transport authentifié et sécurisé

Le certificat IDE est appliqué à deux niveaux. Comme le montre l'illustration 5, le système ERP utilise ce certificat pour s'authentifier vis-à-vis du proxy inverse situé en amont dans une relation bidirectionnelle SSL/TLS.

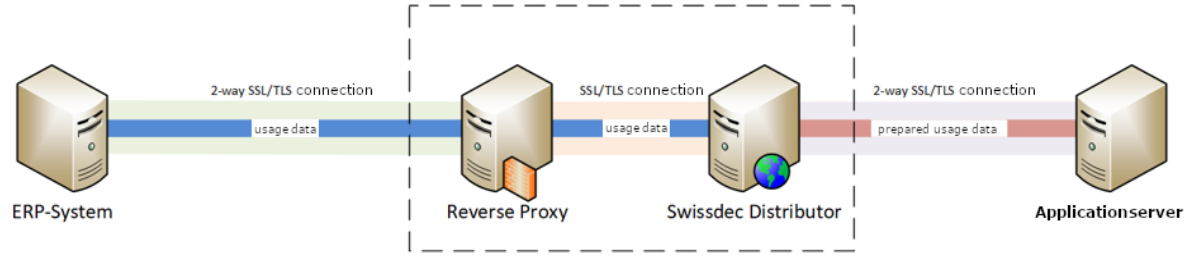

Illustration 5: Sections de communication SUA

Le système de proxy inverse en amont du répartiteur Swissdec, constitué d'une cascade de composants (notamment d'un proxy inverse SSL/TLS et d'un pare-feu applicatif Web), est ainsi en mesure de vérifier l'authenticité de paquets entrants dès le niveau du transport.
Le transmetteur signe avec son certificat IDE l'en-tête SOAP des données utiles et les crypte à l'aide du certificat IDE du répartiteur. Le proxy inverse retransmet les données utiles telles quelles au répartiteur Swissdec via une seconde liaison SSL/TLS.

Il est indispensable de disposer d'un certificat IDE valable pour pouvoir envoyer des paquets de données au répartiteur Swissdec. L'existence d'un tel certificat est vérifiée en amont par le point d'extrémité TLS,
ce qui décharge le répartiteur.

Le proxy inverse peut examiner l'authenticité d'un message, mais n'est pas capable d'en lire le contenu, qui a été crypté pour le répartiteur.

Le répartiteur examine la signature SUA des données utiles, ce qui lui permet de vérifier l'origine et l'intégrité des données. Dans le sens inverse, le répartiteur envoie au système ERP les données utiles également signées et cryptées via le certificat IDE.
Les étapes suivantes de l'échange de messages entre le répartiteur et les systèmes des destinataires finaux sont également sécurisées via le protocole SSL/TLS au niveau du transport. Comme dans la première section de la communication, les données utiles préparées par le répartiteur sont signées par ce dernier et transmises cryptées.

4.2 Sécurité et confiance au niveau des messages (message SOAP)

Comme indiqué au chapitre précédent, l'en-tête SOAP est signé à l'aide du certificat IDE en tant que composant des données utiles. Lors de cette étape, les demandes adressées par le système ERP au répartiteur («Request») et les réponses du répartiteur au système ERP («Response») sont signées. La forme de ces messages, en termes de signature et de cryptage, est décrite de manière plus détaillée ci-après et représentée sur l'illustration 6.
Si l'on observe de plus près un message adressé par le système ERP au répartiteur, un timbre horodateur (<wsu:Timestamp>) est inséré en en-tête de chaque message. Cet en-tête est signé à l'aide du certificat ERP et du certificat IDE. La signature réalisée au moyen du certificat ERP permet de vérifier la capabilité processus du système ERP émetteur. Cette signature doit être conservée, car les analyses statistiques établies par le répartiteur s'appuient sur les informations provenant du certificat ERP.

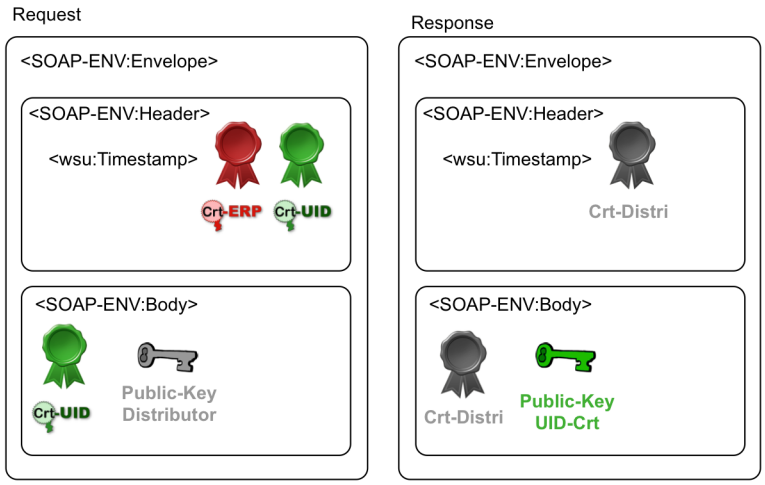

Illustration 6: Authentification à l'aide de certificats IDE

La signature du timbre horodateur effectuée avec le certificat IDE permet de vérifier l'origine d'un message dès la lecture de son en-tête. Le répartiteur est ainsi en mesure de déterminer s'il s'agit d'un expéditeur légitime. Cette information est importante, notamment car contrairement au corps (c'est-à-dire au contenu) du message, les informations figurant en en-tête ne sont pas cryptées. Le répartiteur peut ainsi vérifier les signatures du timbre horodateur sans devoir préalablement décrypter le message.
Le corps du message est également signé par l'expéditeur au moyen d'un certificat IDE afin de garantir l'intégrité et l'authenticité de son contenu. Ensuite, la totalité du corps du message est décryptée à l'aide de la clé publique du répartiteur, ce qui permet de garantir la confidentialité.
La réponse du répartiteur au système ERP contient également un timbre horodateur en en-tête, qui est signé à l'aide du certificat IDE du répartiteur. Le corps du message est signé au moyen du certificat IDE du répartiteur pour garantir là encore l'intégrité et l'authenticité. Le corps du message est ensuite crypté à l'aide de la clé publique du certificat IDE du système ERP qui reçoit le message.
Pour chaque message échangé, les certificats utilisés sont envoyés en en-tête sans la chaîne de certification. Ainsi, les participants à la communication n'ont pas besoin d'enregistrer les certificats. Pour des raisons de sécurité, la chaîne de certification doit toutefois être préalablement échangée et enregistrée en vue de la vérification du certificat.
Un examen préalable efficace du message à l'aide des informations contenues est possible et permet d'identifier et de bloquer d'éventuelles attaques contre le répartiteur à un stade très précoce. Par rapport à l'état actuel (certificat ERP uniquement), des informations supplémentaires sur l'expéditeur (contenu du certificat IDE, cf. chapitre 5.1) sont ainsi incluses dans le message. Ces informations figurent dans la partie non cryptée du message, mais sont suffisamment protégées contre d'éventuelles attaques grâce au canal sécurisé situé en amont. L'ajout des informations sur l'expéditeur dans le certificat ne dégrade donc pas le niveau de sécurité et peut se justifier par les gains apportés par l'examen préalable des messages.

4.3 Non-répudiation

Il y a lieu de garantir le caractère contraignant de l'échange des données (traçabilité) tout au long des processus de transmission des messages Swissdec (cf. exigence 2.6). Le but est de pouvoir, a posteriori, vérifier à tout instant qu'un message a bien été transmis. Comme décrit au chapitre 4.1, la communication entre l'entreprise et le destinataire final passe par le répartiteur, qui agit donc comme un intermédiaire dans la communication de machine à machine. Tous les paquets de communication passent par le répartiteur.
Les mécanismes rassemblés au présent chapitre décrivent le comportement général des entités participantes (transmetteur, répartiteur et destinataire final) afin de pouvoir pleinement garantir le caractère contraignant des données et informations transmises sur un évènement Swissdec.

4.3.1 Conditions requises

Les hypothèses de base / conditions requises sont les suivantes.

- En cas de défaillance dans la communication de la part du répartiteur (p. ex. de problème technique), une tentative d'envoi est, après un certain délai, interrompue, consignée et répétée ultérieurement par les partenaires de communication. L'exploitant du répartiteur informe les partenaires de communication des dysfonctionnements et/ou défaillances éventuels.

- Un événement est toujours initié par le système ERP d'une entreprise (transmetteur).
- Après le déclenchement d'un nouvel événement par l'entreprise, le répartiteur crée un ID interne (identifiant) permettant d'identifier clairement l'événement et l'échange de messages qu'il provoque entre l'entreprise et les destinataires finaux concernés. Le répartiteur transfère cet ID à tous les systèmes participants et/ou le renvoie via une confirmation. Cet ID peut servir de numéro de cas pour une éventuelle demande d'assistance ou pour garantir la traçabilité d'une transaction, voire d'un évènement complet.
- Tous les systèmes impliqués dans une procédure de communication disposent d'un certificat d'entreprise Swissdec (certificat IDE) et font confiance à l'émetteur du certificat (ancre de confiance).
- Un cas peut être traité via plusieurs messages, lesquels peuvent s'étendre sur une durée indéterminée.
- Le système ERP d'une entreprise doit consulter régulièrement la progression d'un cas pour comparer le statut avec l'assureur.
- Les messages de confirmation du système d'un destinataire doivent parvenir à l'expéditeur au terme d'une période maximale autorisée.

4.3.2 Schémas de messages Swissdec

Avant de pouvoir mettre au point un système de conservation fiable des messages pour garantir la traçabilité d'un cas, il faut définir un schéma de communication homogène indépendamment des processus à représenter. Le schéma de communication envisagé, voire déjà utilisé, dans le cadre de la norme suisse en matière de salaire (ELM) et de la norme suisse en matière de prestations (KLE) comprend deux phases.

1. Initialisation d'un événement
2. Échange spécialisé

Ces deux phases suivent des modèles de communication classiques qui peuvent être résumés et désignés de la manière suivante.

Phase 1 – 1:D:n: il s'agit du modèle typique d'initialisation d'un événement. L'entreprise déclare un nouvel événement pour un ou plusieurs systèmes de destinataires finaux (1). Le répartiteur reçoit la déclaration et confirme sa réception directement à l'entreprise. Le répartiteur prépare les données relatives à l'événement (2) et les répartit en fonction du nombre de systèmes destinataires (3). Chaque système destinataire confirme également la réception directement au répartiteur. Entre-temps, le système ERP peut consulter le statut de la répartition aux destinataires finaux auprès du répartiteur (4). Cette consultation peut se répéter [loop 1,n] jusqu'à ce que toutes les confirmations aient été reçues et que le répartiteur puisse annoncer à l'entreprise la réussite de la répartition via son statut.

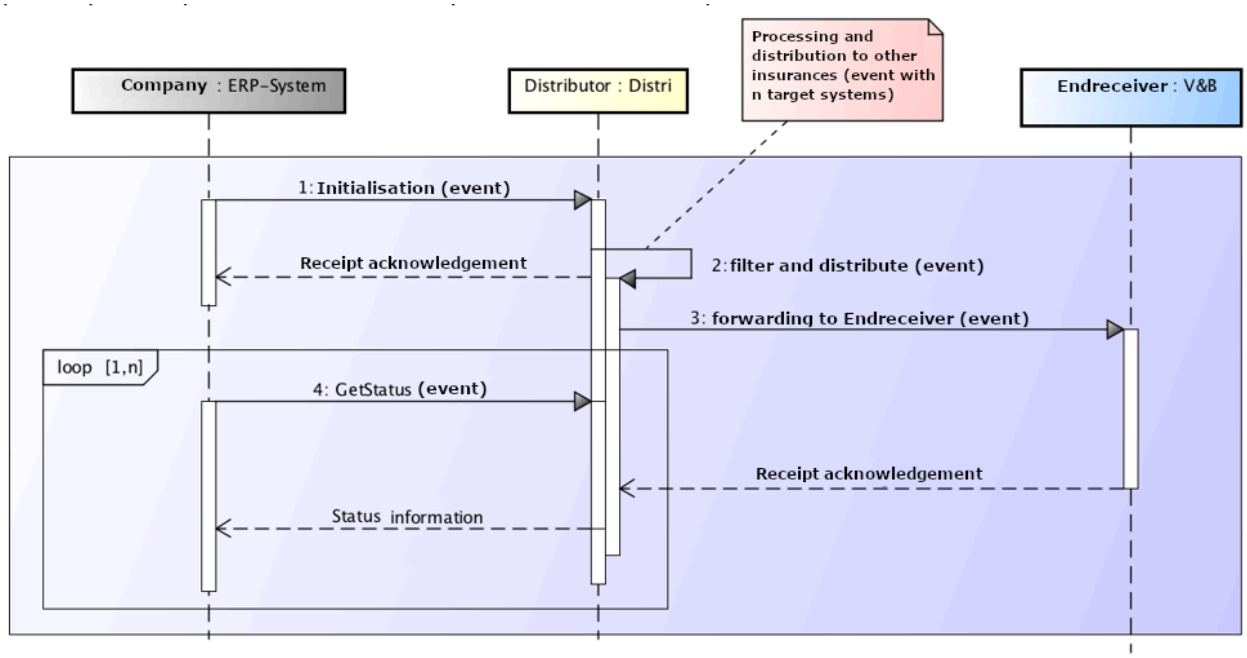

Illustration 7: Déroulement de la communication lors de l'initialisation (1:D:n)

Phase 2 – 1:D:1: selon la norme (en matière de salaire ou de prestations) et le cas, le système ERP de l'entreprise peut demander indirectement, via le répartiteur, le statut ou le résultat d'un message spécifique aux différents destinataires finaux (5). Le répartiteur transmet la demande au système du destinataire final concerné (6), lequel renvoie sa réponse en fonction de la progression du processus. Ce message peut éventuellement inclure une

demande de confirmation au système ERP de l'entreprise pour cette réponse. Quand une confirmation est exigée du système du destinataire, le système ERP répond en donnant la confirmation demandée (7), qui est également transférée au répartiteur (8). Pour finir, le système du destinataire final confirme la réception de cette confirmation. Selon la réponse et le déroulement du processus, cet échange de messages peut se répéter [loop 0,n].

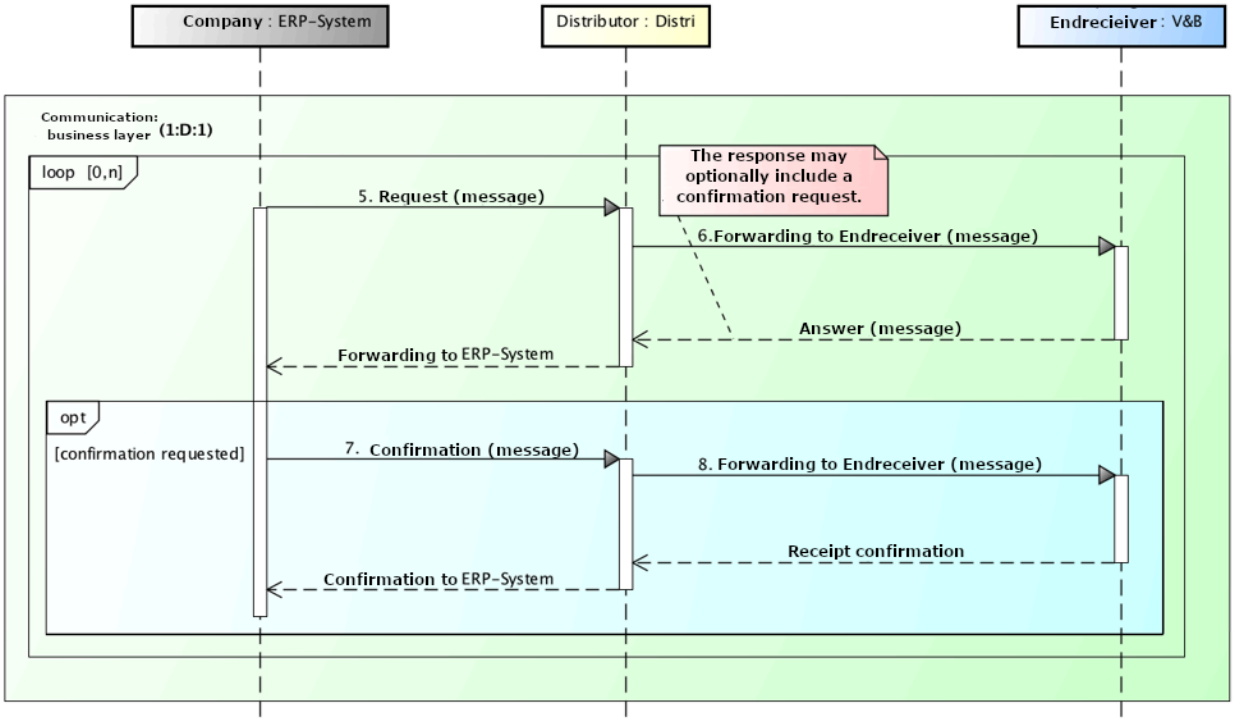

Illustration 8: Déroulement de la communication en cas d'échange de messages spécialisés (1:D:1)

Les exigences en matière de non-répudiation sur le plan spécialisé dans un processus de communication Swissdec peuvent être résumées via le tableau suivant. Il y a lieu de noter qu'un échange de messages ne peut être initié que par l'entreprise.

	Entreprise ***(client)***	**Assureurs et autorités** ***(serveur)***
Non-répudiation de l'origine des données (envoi)	*Message signé*	*Message signé*
Non-répudiation de la réception	*Confirmation spécialisée*	*Confirmation signée*

4.3.3 Non-répudiation de l'origine des données

Il y a lieu d'observer les règles suivantes pour garantir la non-répudiation de l'origine des données.

- Chaque message est signé par un système émetteur (transmetteur, répartiteur, destinataire final) au niveau SOAP avec le certificat IDE, ce qui permet d'attribuer clairement l'origine et l'intégrité d'un message à un émetteur.
- Chaque système destinataire vérifie la signature IDE contenue dans l'en-tête SOAP et l'examine au vu de la chaîne de certification jusqu'au certificat racine.
- Si la vérification de la signature IDE aboutit à un résultat non concluant, le message reçu doit être rejeté, et un message d'erreur émis et communiqué à l'émetteur.

4.3.4 Non-répudiation de la réception

Il y a lieu d'observer les règles suivantes pour garantir la non-répudiation de la réception de données.

- Pour les *systèmes serveurs*: lorsqu'un message a été vérifié avec succès, le destinataire (répartiteur, destinataire final) envoie une confirmation via un message qu'il signe («Response»). Ce message doit contenir la signature du message initialement reçu de l'émetteur. On peut utiliser à cet effet une Web Service Security *Signature Confirmation* à des fins de consignation.
- Pour les *systèmes clients*: quand le système ERP de l'entreprise confirme la réception d'un message, certains composants pertinents du message reçu par le système ERP doivent être renvoyés signés à l'émetteur. Cette confirmation doit intervenir au niveau spécialisé en raison de l'absence de possibilité technique de consignation.
- L'émetteur du message initial doit vérifier la signature IDE contenue dans la «Response» et l'examiner au vu de la chaîne de certification jusqu'au certificat racine.
- Si la vérification de la signature IDE aboutit à un résultat non concluant, la «Response» reçue doit être rejetée et un message d'erreur émis.

4.3.5 *Preuve d'une liaison de communication:* dans le cas de processus urgents, pour qu'un système ERP puisse prouver ultérieurement l'envoi d'un message donné, tous les paquets de demandes envoyés par le système ERP au répartiteur doivent être renvoyés signés à des fins de confirmation.

4.3.6 Garantie de la traçabilité

Pour garantir la traçabilité de l'intégralité d'un processus de communication Swissdec (toutes les transactions relatives à un cas donné), le répartiteur doit enregistrer toutes les informations sur la connexion (relations) en tant qu'intermédiaire. Comme, en règle générale, le répartiteur prépare aussi les données et en transforme ainsi le contenu entre les partenaires de communication (mappage), il casse la signature de l'émetteur initial. Il doit donc, lui aussi, signer les paquets sortants.

La signature d'un message Swissdec contient notamment:

- une empreinte du contenu signé;
- une référence au contenu signé dans le corps du message;
- un timbre horodateur correspondant à l'heure du système;[4],
- des informations clés.

Le répartiteur doit enregistrer les informations suivantes sur un processus de communication:

- le numéro de cas;
- la signature de chaque message reçu;
- la signature de chaque message transformé et envoyé;
- la version du logiciel du répartiteur;
- le modèle de communication (1:D:n, 1:D:1).

Le répartiteur **n'enregistre pas** le contenu des messages, mais les conserve seulement brièvement dans sa «mémoire de travail». Les partenaires de communication doivent archiver eux-mêmes le contenu des messages. Ils sont soumis dans ce cadre aux règles suivantes.

- Chaque émetteur (entreprise ou assureur) d'un message enregistre le message qu'il a signé sous forme de texte non formaté avant de l'envoyer afin de pouvoir le consulter ultérieurement.
- Le destinataire (entreprise ou assureur) vérifie la signature du message qu'il reçoit et l'archive sous forme non cryptée selon sa propre procédure.

Pour qu'un cas puisse être entièrement reconstitué, il faut compiler les données et informations de tous les partenaires de communication impliqués concernant un processus de communication ainsi que les données relatives à la connexion du répartiteur. Cela permet, en cas de litige, de déceler une erreur involontaire ou un comportement fautif.

[4] Il est recommandé que les participants à Swissdec disposent d'une base temporelle commune (serveur NTP).

5 Données d'identification SUA

Il convient d'utiliser, pour l'authentification d'entreprises Swissdec, des certificats avancés répondant à des spécifications propres. Ce choix exclut certes le support juridique prévu par la SCSE tel que décrit au chapitre 5.1.6, mais le recours à ces certificats «sur mesure» offre en contrepartie plus de flexibilité et de marge de manœuvre.

5.1 Certificats IDE

5.1.1 But de l'utilisation de certificats IDE

Comme les certificats IDE sont utilisés à la fois pour signer et pour crypter des messages SOAP, il pourrait être recommandé d'utiliser deux certificats différents (l'un pour le cryptage et l'autre pour l'authentification / la signature). Toutefois, étant donné que ces données ne doivent être cryptées que très brièvement (pour leur transport) et non archivées sous forme cryptée pour être ensuite décryptées, il n'y a pas lieu d'archiver de clés privées.
Par conséquent, et dans un souci de simplification de la gestion des certificats (notamment pour les systèmes ERP), mieux vaut renoncer à une limitation de l'application des certificats IDE au profit de l'utilisation d'*un* même certificat pour l'authentification, la signature et le cryptage.

5.1.2 Formes d'émission

Des certificats IDE sont en principe émis en tant que certificats logiciels X.509[5] par une CA mandatée. Ils sont ensuite transférés de manière sécurisée aux systèmes destinataires, où ils sont automatiquement installés. Si les exigences de sécurité d'une entreprise le requièrent, il est tout à fait possible d'organiser la création des clés du certificat IDE sur du matériel certifié de l'entreprise. Dans ce cas, le processus d'enregistrement / l'émission du certificat ne change pas.

5.1.3 Gestion des clés privées

La paire de clés d'un certificat IDE étant créée dans l'environnement sécurisé de l'entreprise (système ERP ou matériel spécial), il est impossible d'effectuer une sauvegarde de la clé privée, car ni Swissdec, ni la CA émettrice ne possède la clé privée d'un certificat IDE dans le cadre de ce processus. L'infrastructure de l'entreprise doit permettre de veiller à ce que la clé privée soit conservée en lieu sûr et garantir la possibilité, pour les applications autorisées, d'y accéder à tout moment. Avec un jeton logiciel, la clé privée doit être enregistrée par un système ERP sous une forme lisible. Si, en vertu des exigences de sécurité d'une entreprise, les clés privées ne doivent être émises et enregistrées que sur du matériel certifié (jeton matériel, boîte noire transactionnelle), il est nécessaire de veiller à ce que le système ERP puisse accéder à tout instant à ces clés enregistrées sur le matériel certifié.

5.1.4 CP/CSP

Pour les certificats IDE Swissdec, la CA émettrice doit établir une «Certificate Policy» (CP) et une «Certificate Practice Statement» (CPS) conformément aux règles visées à la RFC 7382[6].

5.1.5 Contenu d'un certificat IDE

Quel que soit leur support, les certificats IDE doivent contenir les informations suivantes:

Désignation	Description
Version	Version du certificat (selon RFC 5280: version 3)
Serial Number	Identification univoque du certificat, selon les règles de la CA émettrice
Certificate Signature Algorithm	Spécifications de l'algorithme de signature du certificat, dans le respect des normes usuelles et en concertation avec la CA émettrice. Exigence minimale: SHA256 avec cryptage RSA (taille de la clé: 2048 bits)
Issuer	Informations sur l'émetteur du certificat (CA): commonName, organizationName, organizationalUnitName, countryName[7]

[5] Network Working Group, 2008. RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, en ligne: https://www.ietf.org/rfc/rfc5280.txt (3.11.2015).

[6] https://tools.ietf.org/html/rfc7382

[7] Il est aussi possible d'indiquer ici le numéro IDE de l'émetteur du certificat, p. ex. l'IDE de Swissdec: Object Identifier (2 5 4 97) = NTRCH-CHE-113.865.903

Validity		Durée de validité du certificat: 1 an
Subject		Informations sur le détenteur du certificat (cf. tableau 2)
Subject Public Key Info		Informations sur la clé du détenteur du certificat
	Public Key Algorithm	Algorithme de la clé publique
	Subject's Public Key	Clé publique du détenteur du certificat
Extensions:		
	Authority Key Identifier	Identification de la clé publique utilisée par l'émetteur du certificat
	Authority Information Access	URI concernant d'autres informations de l'émetteur du certificat: OCSP, CA Issuers
	Certificate Policies	Renvoi (URI) à d'autres règles (techniques, juridiques et de processus) à observer pour utiliser le certificat émis. Il convient de contacter le préposé à la protection des données de Swissdec pour déterminer si de telles règles sont nécessaires et, le cas échéant, s'il convient d'en rédiger.
	CRL Distribution Points	URI d'une «Certificate Revocation List» (CRL) de la CA émettrice
	Key Usage	But de l'utilisation de la clé contenue dans le certificat: *keyEncipherment* *digitalSignature*
	Extended Key Usage	*TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)* *Document Signing (1.3.6.1.4.1.311.10.3.12)*
	Subject Key ID	Identification d'un certificat au moyen d'une clé publique spécifique
Signature Algorithm		Spécifications de l'algorithme de signature du certificat
Signature Value		Signature du certificat

Tableau 1: Éléments d'un certificat IDE

Les informations sur le détenteur du certificat sont récupérées dans le registre IDE de l'OFS, de façon partiellement automatisée. L'entreprise peut déterminer librement l'OrganizationalUnit (OU). Le tableau suivant décrit les attributs contenus dans le certificat au sujet du détenteur ainsi que leur origine.

Abréviation	Désignation	Contenu	Source	Priorité
CN	commonName	NTRCH-{UID-BFS}@swissdec.ch[8]	Registre IDE de l'OFS	OBLIGATOIRE
O	organizationName	<Name> d'après le registre IDE de l'OFS	Registre IDE de l'OFS	OBLIGATOIRE
OU	organizationalUnitName	Sous-unité de l'organisation; peut être choisie librement et configurée en cascade	Saisie de l'utilisateur	FACULTATIF
L	localityName	Siège de l'entreprise d'après le registre IDE, <town> selon le registre IDE	Registre IDE de l'OFS	OBLIGATOIRE
ST	stateOrProvinceName	Canton du siège de l'entreprise <locality> selon le registre IDE	Registre IDE de l'OFS	OBLIGATOIRE
C	countryName	<country> selon le registre IDE	Registre IDE de l'OFS	OBLIGATOIRE
IDE	OID 2.5.4.97	OrganizationIdentifier: n° IDE d'après le registre IDE de l'OFS, NTRCH-{UID-OFS}	Registre IDE de l'OFS	OBLIGATOIRE
BC	OID 2.5.4.15	Business Category («Private Organization» ou «Government Entity»)[9]	Registre IDE de l'OFS	FACULTATIF[10]

Tableau 2: Attributs du détenteur du certificat («Subject»)

Il est aussi possible d'enregistrer l'adresse de l'entreprise concernée dans le «Subject» du certificat IDE. Cette adresse ne peut être vérifiée qu'au moment de l'émission du certificat. Comme elle est susceptible de changer au cours de la durée de validité du certificat, il n'est pas impératif de la renseigner.

Informations facultatives dans «Subject»:

- OID 2.5.4.9: (streetAdress)
- OID 2.5.4.17: (postalCode)
- OID 1.3.6.1.4.1.311.60.2.1.2: (State) → correspond à ST
- OID 1.3.6.1.4.1.311.60.2.1.3: (Country) → correspond à C
- OID 2.5.4.15 (BusinessCategory): désigne le type d'organisation. Une distinction peut être effectuée entre *PrivateOrganization*, *Business Entity*, *Non-Commercial Entity* et *Government Entity*.

Il est aussi possible d'enregistrer les informations relatives à la RA (de l'anglais «Registration Authority», autorité d'enregistrement) à la partie «Extensions». Cette solution n'est judicieuse que s'il faut aussi utiliser les certificats IDE dans un contexte autre que celui de Swissdec.

Informations facultatives pour *Certificate Subject Alt Name*:

- Object Identifier (2 5 4 97) = {UID-OFS}
- Object Identifier (2 5 4 13) = IDE-OFS de l'entreprise

Informations facultatives pour *Certificate Issuer Alt Name*:

- Object Identifier (2 5 4 97) = {UID-OFS}
- Object Identifier (2 5 4 13) = entité chargée de valider l'IDE-OFS de l'entreprise

➔ Un exemple de certificat IDE est joint à l'annexe A.

[8] Correspond au *legalperson semantics identifier* selon la norme ETSI EN 319412-1, chap. 5.1.
(http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.00_30/en_31941201v010100v.pdf)

[9] Les données <legal Form> figurant dans le registre IDE de l'OFS peuvent aussi être reprises ici.

[10] Après consultation de QuoVadis, il a été décidé de renoncer à indiquer la «Business Category» dans le certificat SUA.

5.1.6 Utilisation de certificats réglementés pour l'authentification d'entreprises Swissdec

Les clarifications auprès de l'OFCOM ont permis d'établir que la révision totale (SCSE)[11], l'ordonnance sur la révision totale de la loi sur la signature électronique (OSCSE)[12] et les adaptations de l'ordonnance concernant les données et les informations électroniques (OeIDI)[13] ne simplifient pas l'authentification d'entreprises pour Swissdec. La révision totale de la SCSE inclut notamment la définition des formats de certificats réglementés pour les applications suivantes:

1. signature électronique d'une personne physique ou cachet électronique d'une entité IDE;
2. identification électronique d'une personne physique ou d'une entité IDE;
3. cryptage de données électroniques.

Les documents susmentionnés n'apportent pas plus de précisions sur l'utilisation des certificats indiqués aux points 2 et 3. Les PTA relatives à la SCSE[14] renvoient à ce sujet à la norme européenne (EN) ETSI 319 411, selon laquelle l'émission d'un certificat avancé utilisé à des fins d'identification électronique serait aussi possible sous forme de jeton logiciel. Comme indiqué dans la prise de position de Swissdec du 28 juillet 2016 sur les projets de SCSE, d'OSCSE et de PTA, les conditions-cadres concernant l'utilisation de certificats réglementés en vue de l'identification électronique pour la communication de machine à machine manquent de précision. En particulier, le lien éventuel entre l'émission de tels certificats et un jeton matériel, les modalités du processus d'enregistrement et le coût engendré par ce type de certificats ne sont pas clairs.
Swissdec adopte donc dans un premier temps (indépendamment du développement de certificats réglementés sur le marché suisse) l'approche initialement envisagée qui consiste à utiliser pour *l'authentification d'entreprises Swissdec* des certificats avancés selon des spécifications propres.

5.2 Certificate Signing Request (CSR)

Une CSP fournit une interface standardisée (CSR ou CMP[15]) permettant à Swissdec de traiter de manière automatisée une requête («Request») contenant les données sur le «Subject» indiquées dans le tableau 3 ci-après. La structure de la demande de certificat électronique utilisée est standardisée en tant que PKCS#10[16]. Une CSR doit contenir les informations suivantes sur le titulaire («Subject») et sur la clé:

Désignation	Description
Subject	Informations sur le détenteur du certificat, notamment commonName (CN), organizationName (O), organizationalUnitName (OU), localityName (L), stateOrProvinceName (ST), countryName (C) et l'IDE de l'entreprise (OID 2.5.4.97) → Pour de plus amples informations, se reporter au tableau 2
PublicKey	Clé publique du détenteur du certificat (clé RSA 2048 bits)

Tableau 3: Attributs d'une «Certificate Signing Request» (CSR)

5.3 Normes cryptographiques

On considère que tous les systèmes impliqués utilisent les algorithmes cryptographiques et longueurs de clé actuellement recommandés. Un autre système est chargé de sélectionner les algorithmes cryptographiques utilisés selon la section de communication (cf. à ce sujet l'illustration 5). Il faut par conséquent respecter le principe suivant:

> Tous les composants de communication participants (y compris le transmetteur) doivent prendre en charge les algorithmes prescrits pour la SUA.

Les algorithmes et longueurs de clé minimaux autorisés doivent satisfaire aux recommandations et/ou directives suivantes:

[11] Révision totale (SCSE)

[12] Révision totale de l'ordonnance (OSCSE)

[13] Modification de l'ordonnance concernant les données et informations électroniques (OeIDI)

[14] PTA: prescriptions techniques et administratives de l'OFCOM

[15] CMP (Certificate Management Protocol), IETF RFC 4210

[16] Network Working Group, 2000. RFC2986: PKCS #10: Certification Request Syntax Specification - Version 1.7, en ligne: https://tools.ietf.org/html/rfc2986 (3.11.2015).

- European Telecommunications Standards Institute (ETSI): http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf
- Office fédéral allemand pour la sécurité informatique (*Bundesamt für Sicherheit in der Informatik*, BSI): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile

En outre, les exploitants des services de serveurs Web devraient veiller à ce que la configuration des serveurs Web soit conforme aux recommandations de l'Internet Engineering Task Force (IETF) formulées dans la RFC 7525:

- Recommendations for Secure Use of Transport Layer Security (IETF): https://tools.ietf.org/html/rfc7525 .

5.4 Mots de passe SUA

Deux mots de passe différents sont utilisés dans le cadre des processus SUA décrits ci-après: le mot de passe d'enregistrement et le mot de passe de verrouillage. Tous deux sont envoyés par courrier – c'est-à-dire via un second canal, non électronique – par le répartiteur ou par une A&A à l'entreprise souhaitant s'enregistrer.

5.4.1 Mot de passe d'enregistrement

Le but principal du mot de passe d'enregistrement est de s'assurer qu'un certificat signé est attribué au bon destinataire (système ERP) et à lui seul. Il sert donc à authentifier l'entreprise. Les scénarios suivants sont envisagés.

- Scénario 1: génération d'une paire de clés par le système ERP (cf. point 6.2.1)
  La paire de clés privée/publique est générée par le système ERP et une CSR est transmise au répartiteur selon PKCS#10.
  Dans ce cas, le mot de passe sert uniquement à authentifier le système ERP vis-à-vis du répartiteur. Comme l'authentification est effectuée en ligne au moment de l'envoi de la CSR, il est possible de mettre en place, côté répartiteur, un dispositif de protection efficace contre les attaques par force brute (par exemple en limitant le nombre de tentatives ou en paramétrant des délais entre deux tentatives).
- Scénario 2: jeton matériel (cf. point 6.2.4)
  La paire de clés et le certificat correspondant sont transmis à l'entreprise sur un «jeton matériel» avec le NIP nécessaire. Les détails sont alors laissés à la discrétion de la CA concernée. Le répartiteur reste toutefois l'instance d'authentification (RA) dans ce processus.

5.4.2 Mot de passe de verrouillage

Le mot de passe de verrouillage sert à authentifier l'entreprise lorsque cette dernière demande le verrouillage d'un certificat émis (cf. point 6.6). Une fois ce mot de passe transmis à Swissdec, le certificat est bloqué et révoqué auprès de la CA. Après avoir fait usage de son mot de passe de verrouillage, l'entreprise doit procéder à un nouvel enregistrement.

5.4.3 Exigences relatives aux mots de passe

Les exigences suivantes doivent être prises en compte concernant la forme des mots de passe:

ID	Désignation	Description	Priorité
AP-01	Longueur du mot de passe	Aussi long que nécessaire et aussi court que possible.	OBLIGATOIRE
AP-02	Convivialité	Comme les mots de passe sont transmis sous forme écrite par courrier, il faut veiller à ce qu'ils soient bien lisibles et faciles à saisir.	OBLIGATOIRE
AP-03	Somme de contrôle	Une somme de contrôle permet de vérifier que les informations sont correctes dès leur saisie.	OBLIGATOIRE
AP-04	Unicité	Une entropie suffisante doit garantir l'unicité même avec un grand nombre de mots de passe émis.	OBLIGATOIRE
AP-05	Émission	Pour chaque entreprise (IDE-OFS), il ne doit exister à un instant T qu'un seul mot de passe d'enregistrement valable.	OBLIGATOIRE
AP-06	Marque d'identification	Le mot de passe doit contenir un élément à définir librement et qui identifie par exemple son émetteur ou sa version.	OBLIGATOIRE
AP-07	Cryptage	L'aptitude au cryptage des formats de fichiers pour le transport de certificats et des clés nécessaires est garantie.	FACULTATIF

Tableau 4: Exigences concernant les mots de passe SUA

5.4.4 Création des mots de passe

Le processus de génération d'un mot de passe comprend les étapes suivantes.

1. Génération d'une variable aléatoire entrante au moyen d'un générateur cryptographique de nombres aléatoires (CSPRNG[17])
2. Représentation de la variable aléatoire dans un ensemble de caractères réduit et création d'un mot de passe de la longueur prescrite (12 caractères)
3. Ajout de la marque d'identification (2 caractères)
4. Calcul de la somme de contrôle selon ISO/IEC 7064, MOD 1271-36 (cf. exemple de code) et ajout du chiffre de contrôle (2 caractères)
5. Segmentation en blocs de quatre éléments (voir exemple)
6. Enregistrement dans une base de données à l'aide d'une Key Derivation Function[18] (KDF)

Par ailleurs, il y a lieu d'observer les règles structurelles complémentaires suivantes:

Ensemble de caractères réduit	Chiffres: 2345689 Lettres en majuscules: ABCDEFGHJKLMNPQRTUVWXYZ Caractères exclus: 1, 7, 0, O, S
Longueur du mot de passe	12 caractères (hors chiffre de contrôle et marque d'identification)
Marque d'identification	2 caractères
Chiffre de contrôle	Calcul selon ISO/IEC 7064, MOD 1271-36 2 caractères
Segmentation	Quatre blocs de quatre éléments, soit 16 caractères au total, séparés par des traits d'union
Key Derivation Function	Argon2[19] (vainqueur du «Password Hashing Competition»[20])

Tableau 5: Règles relatives à la structure des mots de passe SUA

5.4.5 Exemple de mot de passe

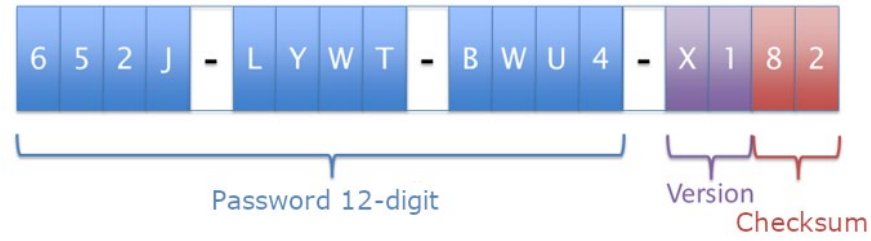

Illustration 9: Exemple de mot de passe SUA

5.4.6 Exemple de code pour la mise en œuvre

Un exemple pour la mise en œuvre des règles ISO/IEC 7064, MOD 1271-36 pour Java est notamment disponible sous:
https://github.com/danieltwagner/iso7064/blob/master/src/main/java/com/github/danieltwagner/iso7064/Mod1271_36.java

En cas de réutilisation d'un code tiers, il convient toutefois de réaliser un contrôle particulièrement approfondi de celui-ci et de tenir compte des éventuels droits d'auteur.

[17] https://en.wikipedia.org/wiki/Cryptographically_secure_pseudorandom_number_generator

[18] https://fr.wikipedia.org/wiki/Fonction_de_d%C3%A9rivation_de_cl%C3%A9

[19] https://password-hashing.net/argon2-specs.pdf

[20] https://password-hashing.net/

6 Processus SUA

Le processus global d'authentification d'entreprises comprend quatre phases: l'enregistrement, la configuration, l'exploitation ainsi que le renouvellement et le verrouillage (du certificat).
L'illustration 10 ci-après représente les deux principales branches du processus avec leurs éléments les plus importants, répartis dans les quatre phases. Les chapitres suivants décrivent chacune des étapes des processus de manière détaillée.

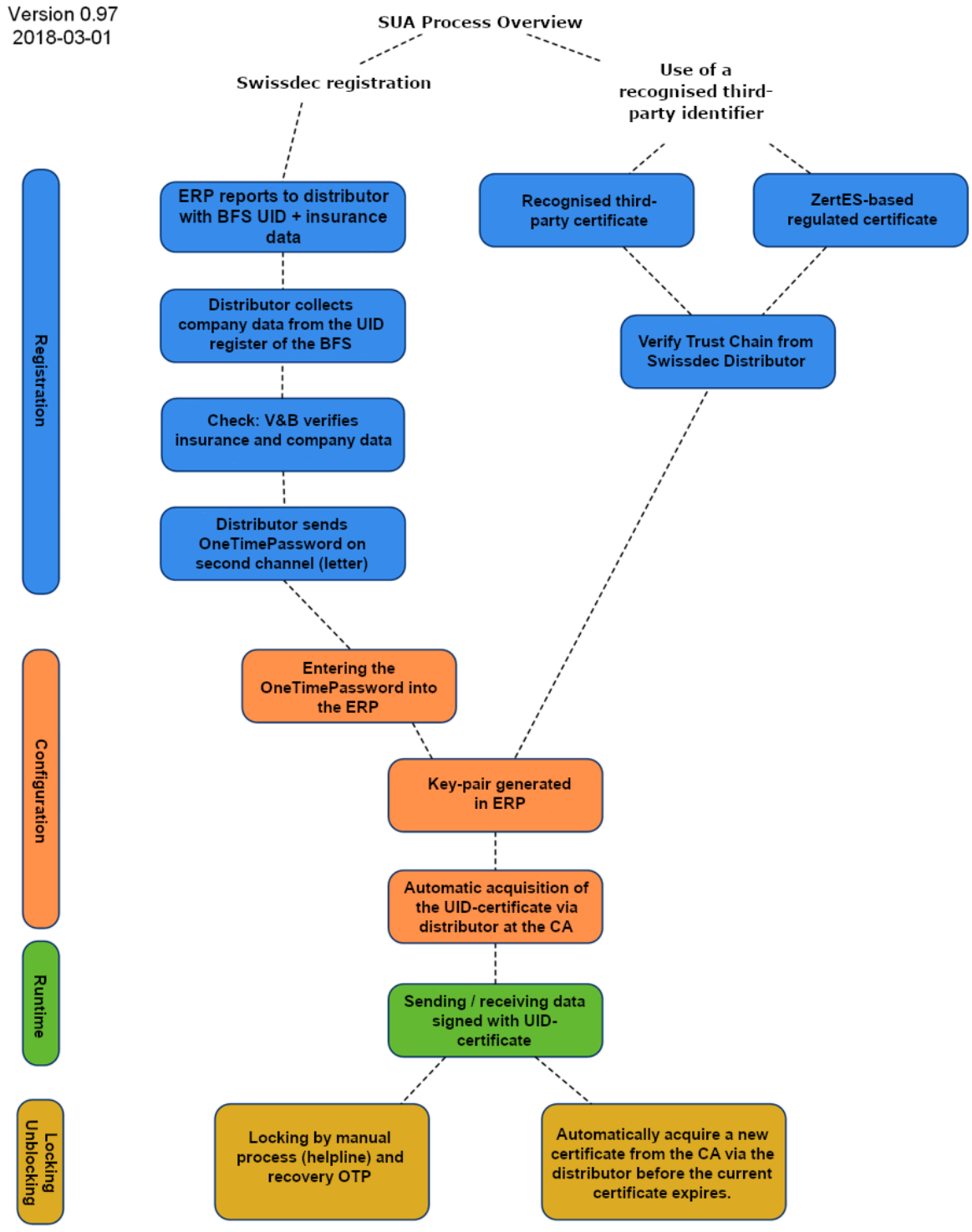

Illustration 10: Processus global d'authentification d'entreprises Swissdec en quatre phases

6.1 Processus d'enregistrement

Deux options sont prévues pour l'enregistrement (cf. illustration): d'une part l'enregistrement auprès de Swissdec, et d'autre part un enregistrement simplifié à l'aide d'un identificateur tiers, par exemple un certificat (réglementé) basé sur la SCSE.
Pour l'heure, il convient de considérer que l'enregistrement direct auprès de Swissdec constituera l'option ordinaire qui permettra aux entreprises d'exécuter des processus d'affaires sur la base de l'authentification d'entreprises Swissdec. À mesure que les certificats d'entreprise émis selon les prescriptions de la SCSE se développeront, le processus d'enregistrement pourra être sensiblement simplifié.

6.1.1 Enregistrement Swissdec

L'enregistrement présuppose l'existence d'un contrat conclu avec un assureur. 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 (numéro IDE, raison sociale d'après le registre du commerce, etc.).
Les entreprises sans relation contractuelle existante doivent appliquer la procédure d'enregistrement direct à l'aide d'un certificat réglementé (cf. chapitre 6.1.2).
Les fiduciaires, qui seront ultérieurement amenées à signer des données des entreprises dont elles assurent la gestion avec leur certificat IDE, devront elles aussi se soumettre au processus normal d'enregistrement et de configuration.
Les fiduciaires sont considérées comme des entreprises ayant des relations contractuelles avec les A&A permettant un enregistrement.
L'enregistrement auprès de Swissdec peut se faire selon deux variantes: dans l'une, les A&A sont en contact avec les entreprises, tandis que dans l'autre, elles délèguent ces contacts à Swissdec. Le point 6.1.1.1 décrit la procédure à privilégier, dans le cadre de laquelle les informations nécessaires à l'enregistrement sont envoyées par le répartiteur de Swissdec aux entreprises. Le point 6.1.1.2 retrace ensuite brièvement le processus d'enregistrement possible via une prise de contact par les A&A.
Dans les deux cas de figure, les informations nécessaires à la configuration initiale, qui proviennent du processus d'enregistrement, sont envoyées aux entreprises via un second canal, non électronique. Ce canal doit satisfaire aux exigences suivantes:

ID	Désignation	Description	Priorité
AB-01	Vérification de l'adresse	L'adresse (adresse e-mail, numéro de téléphone portable, adresse postale) doit être connue de l'assurance auprès de laquelle l'entreprise est enregistrée et vérifiée par cette assurance.	OBLIGATOIRE
AB-02	Sécurité	Il faut veiller à ce que les informations parviennent à leur destinataire et ne puissent pas être reçues par des tiers.	OBLIGATOIRE
AB-03	Aptitude au transfert	Les informations transmises doivent être transférées à la personne compétente (interlocuteur).	OBLIGATOIRE
AB-04	Aptitude à l'archivage	Les informations transmises devraient être faciles à enregistrer et à archiver.	FACULTATIF
AB-05	Durée	Les informations transmises doivent être parvenir à leur destinataire dans un délai raisonnable.	OBLIGATOIRE
AB-06	Contenu	Les informations doivent être simples à comprendre afin de permettre la réalisation des actions consécutives (transfert à l'interlocuteur).	OBLIGATOIRE
AB-07	Traçabilité	Il doit être possible de déterminer le lieu de stockage, le statut d'envoi et l'archivage chez le destinataire des informations envoyées.	OBLIGATOIRE
AB-08	Coûts	Les coûts devraient être raisonnables.	FACULTATIF

Tableau 6: Exigences vis-à-vis du canal non électronique

Le tableau 7 indique dans quelle mesure les différents canaux satisfont à chacune de ces exigences.

ID	Désignation	E-mail	SMS	Courrier
AB-01	Vérification de l'adresse	Si connue	Si connue	L'adresse postale de la direction de l'entreprise est connue (composant de la relation d'affaires)
AB-02	Sécurité	Réception relativement sûre (confirmation de réception éventuellement nécessaire))	Réception non sûre	Garantie par une entreprise postale; dans certains cas, recours au courrier recommandé nécessaire
AB-03	Aptitude au transfert	Informations faciles à transférer (à l'adresse e-mail de l'interlocuteur)	Informations faciles à transférer, à condition toutefois de connaître le numéro de téléphone portable	Remise en mains propres ou via la conciergerie de l'entreprise
AB-04	Aptitude à l'archivage	Archivage/impression d'e-mails	Difficile	Possible immédiatement
AB-05	Durée	Très rapide	Normalement très rapide	Dépend du type d'envoi (entre 1 jour et 1 semaine)

AB-06	Contenu	Satisfaisant	Insuffisant	Satisfaisant
AB-07	Traçabilité	Traçabilité difficile, uniquement confirmation de réception	Impossible	Possible avec courrier A Plus ou lettre recommandée
AB-08	Coûts	Nuls	Faibles	Dépendent du type d'envoi

Tableau 7: Satisfaction des exigences vis-à-vis du canal non électronique par les différents supports

Le tableau 7 montre que l'envoi par courrier est actuellement le plus à même de satisfaire aux exigences définies et garantit le meilleur équilibre entre les critères de sécurité, de coût et de durée. Le second canal, non électronique évoqué ci-après est donc celui d'un envoi par courrier recommandé (ou A Plus).
Le processus d'enregistrement est représenté sous forme de diagramme BPMN ainsi que sous forme de diagramme de séquence. Ces deux représentations sont axées d'une part sur le déroulement concret du processus et, d'autre part sur les relations de communication qui ont lieu au cours de ce processus.

6.1.1.1 Le répartiteur envoie un courrier à l'entreprise.

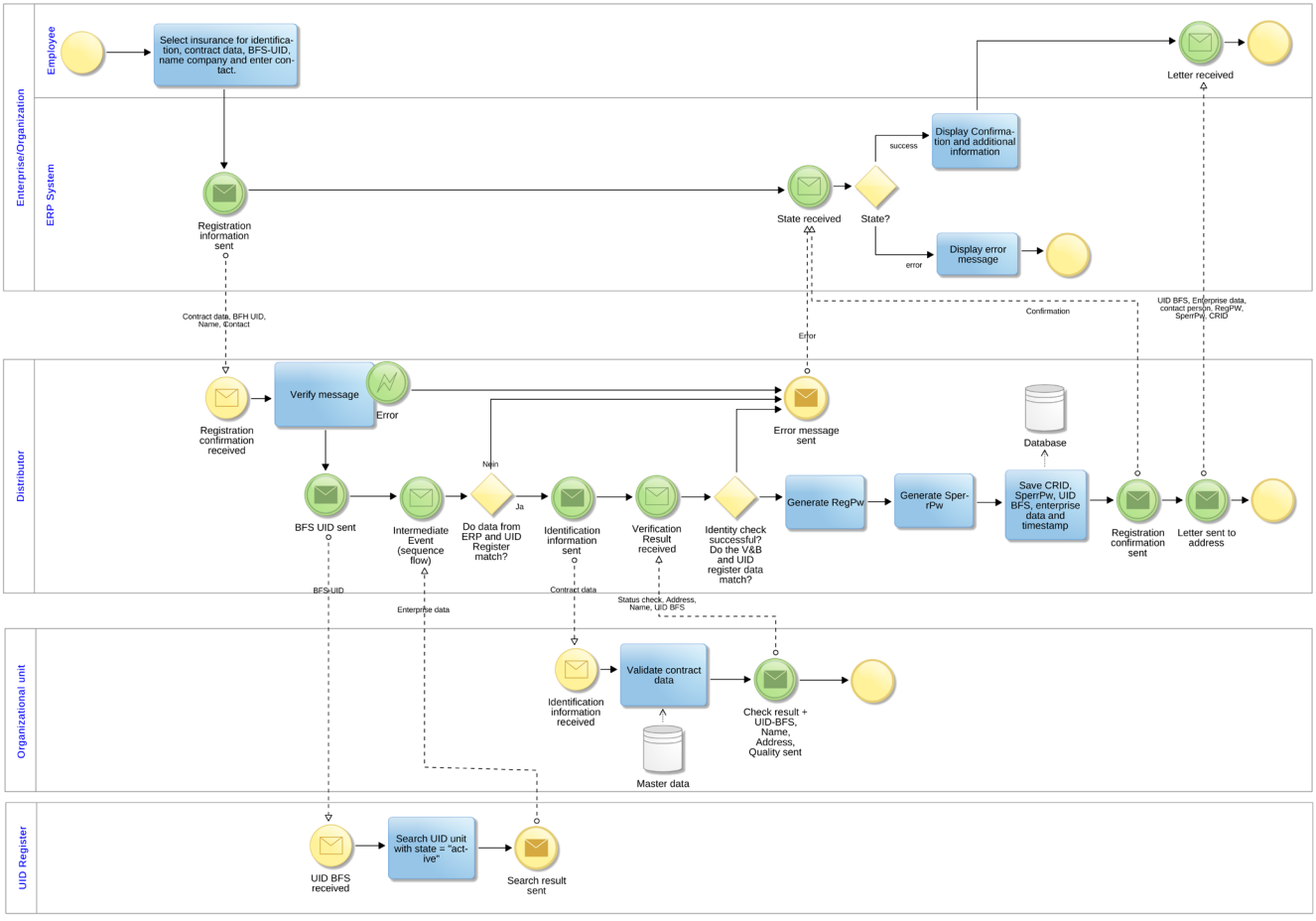

Illustration 11: Processus d'enregistrement

Lorsqu'une entreprise souhaite s'enregistrer à l'authentification d'entreprises Swissdec, 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 IData, IDE-OFS, nom de l'entreprise) sont pour la plupart préremplies par 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/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 (p. ex. 5 maximum)[21]. Le résultat de la vérification est transmis au

[21] Une entreprise peut avoir plusieurs demandes d'enregistrement en cours, par exemple pour plusieurs systèmes ERP. Le fait de limiter le nombre de demandes permettrait d'empêcher que de nouvelles demandes puissent être émises avant que celles en cours ne soient closes (l'envoi du courrier

système ERP via l'envoi d'un identifiant *CertificateRequest* (CRID) généré, qui identifie de façon univoque le système ERP et la requête concernée.
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'A&A précédemment sélectionnée. L'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'&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'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'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).
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 IDE.
Le répartiteur ou un tiers mandaté à cet effet par Swissdec envoie à l'adresse fournie par l'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. D'après les normes d'authentification courantes telles que (le règlement eIDAS de l'UE, la norme eCH-0170v2, la publication NIST SP 800-63 et la norme ISO 29115), cette approche garantit un niveau élevé de vérification d'un destinataire lors de la remise d'un moyen d'authentification.
Si la tierce partie le permet, le statut du courrier envoyé (p. ex. en cours de préparation, envoyé, reçu) peut aussi être transmis par le répartiteur à l'entreprise.
L'intégralité du processus d'enregistrement doit impérativement être exécutée. Les concepts visés au chapitre 2 s'appliquent en sus.
Afin de garantir le bon déroulement de l'enregistrement, puis de la configuration (cf. chap. 6.2), il devrait être possible de réaliser les deux processus en **mode de test**, sans envoyer de courrier ni émettre de certificat. Dans ce cadre, le registre IDE est effectivement consulté et l'A&A procède à une vérification comme s'il s'agissait d'un véritable enregistrement. Cela permettrait de traiter simplement les cas dans lesquels les informations figurant au registre IDE ne seraient pas à jour et devraient tout d'abord être corrigées.

peut en effet prendre un à deux jours). Le but serait d'éviter des demandes superflues au registre IDE de l'OFS et l'envoi inutile de courriers, qui pourrait générer des coûts supplementaires.

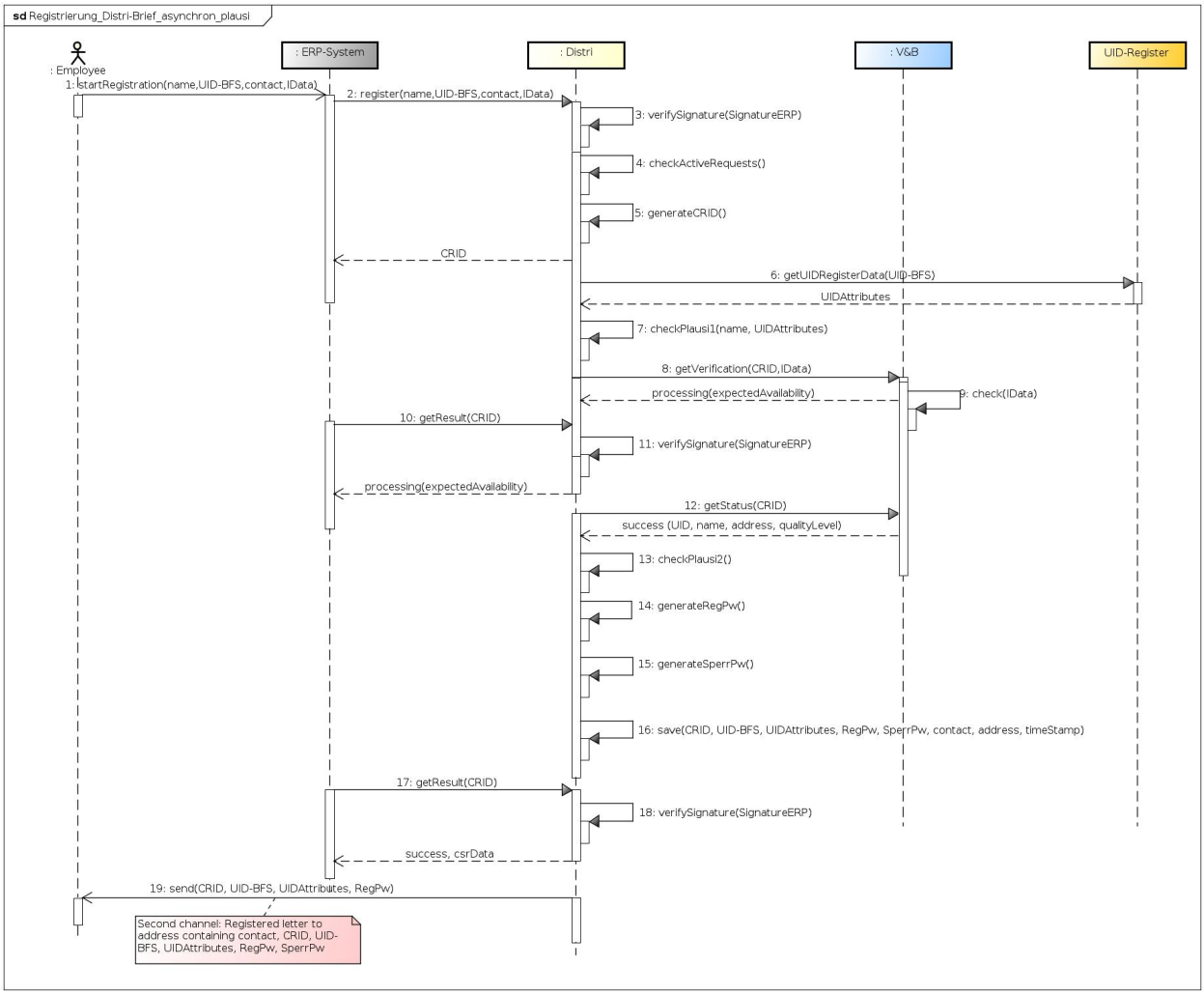

Illustration 12: Diagramme de séquence du processus d'enregistrement

En règle générale, la communication entre l'ERP et le répartiteur est asynchrone, ce qui signifie que le résultat de l'appel (synchrone) register qui renvoie le CRID est récupéré à l'aide de requêtes (synchrones) getResult répétées. La communication entre le registre IDE de l'OFS et les systèmes des A&A se déroule de manière synchrone.

Tableau 8 : Description des étapes du processus d'enregistrement

Nº	Description
1	**startRegistration(name, UID-OFS, contact, IData)**: L'utilisateur choisit le nom (name) selon les données figurant au registre du commerce, l'IDE-OFS de son entreprise ainsi qu'une relation d'assurance enregistrée dans le système ERP pour identifier l'entreprise. Les informations nécessaires sur l'assurance sont récupérées dans le système ERP. En outre, l'utilisateur indique un interlocuteur et les informations permettant de l'identifier. IData: données d'assurance («insurance data»), informations sur la relation contractuelle. Les attributs suivants doivent être inclus: • le numéro d'assureur / l'identifiant InsuranceID, pour identifier le destinataire final; • le numéro de client / CustomerIdentity; • le numéro de contrat/sous-numéro / ContractIdentity. contact: informations permettant d'identifier la personne responsable. Les attributs suivants devraient être inclus: • le nom complet;

	• l'adresse e-mail; • le numéro de téléphone/portable; • la division/fonction.
2	**register(name, UID-OFS, contact, IData):** Le système ERP envoie les informations sur l'assurance, sur l'entreprise (IDE-OFS) et sur le fiduciaire ainsi que les données de contact au répartiteur.
3	**verifySignature(SignatureERP):** Le répartiteur vérifie la validité de la signature du message ainsi que la compatibilité avec la version de la norme SUA.
4	**checkActiveRequests():** Le répartiteur s'assure que le nombre maximal de demandes d'enregistrement pour un même numéro IDE-OFS n'est pas dépassé. S'il est dépassé, le processus d'enregistrement est interrompu et l'ERP reçoit le statut error à sa prochaine demande getResult().
5	**generateCRID():** Le répartiteur génère pour le cas un identifiant CertificateRequest (CRID) qui identifie de façon univoque le processus d'enregistrement du système ERP.
<--	Le répartiteur envoie au système ERP une confirmation de la réception du message: CRID: identifiant généré pour le cas et permettant de récupérer le résultat de la vérification de l'identité. Identifie le système ERP et la requête correspondante.
6	**getUIDRegisterData(UID-OFS):** Le répartiteur envoie une requête synchrone avec l'IDE-OFS de l'entreprise au registre IDE de l'OFS.
<--	Le répartiteur reçoit en réponse les attributs (UIDAttributes) de l'entreprise nécessaires à la vérification de la CSR. Ces attributs sont les suivants:[22] [23]: • Nom: <root>/eCH-0108:organisation/eCH-0098:organisationIdentification/eCH-0097:organisationName • Pays: <root>/eCH-0108:organisation/eCH-0098:contact/eCH-0046:address[eCH-0046:otherAddressCategory/text()='main']/eCH-0046:postalAddress/eCH-0010:addressInformation/eCH-0010:country • Ville: <root>/eCH-0108:organisation/eCH-0098:contact/eCH-0046:address[eCH-0046:otherAddressCategory/text()='main']/eCH-0046:postalAddress/eCH-0010:addressInformation/eCH-0010:town • Localité (canton)[24]: <root>/eCH-0108:organisation/eCH-0098:contact/eCH-0046:address[eCH-0046:otherAddressCategory/text()='main']/eCH-0046:postalAddress/eCH-0010:addressInformation/eCH-0010:locality • BusinessCategory (forme juridique)[25]: <root>/eCH-0108:organisation/eCH-0098:organisationIdentification/eCH-097:legalForm • PublicStatus[26]: <root>/eCH-0108:uidregInformation/eCH-0108:uidregPublicStatus Dans ce cas, l'IDE-OFS consulté doit être indiqué comme «actif» pour que le système considère bien que les attributs sont à jour / corrects.

[22] Source: Office fédéral de la statistique OFS, 2015. Registre IDE – Interface webservice 3.0. En ligne: https://www.bfs.admin.ch/bfs/fr/home/registres/registre-entreprises/numero-identification-entreprises/registre-ide/interfaces-ide.assetdetail.11007266.html (22.11.2019).

[23] Les normes eCH sur lesquelles repose l'interface du registre IDE de l'OFS ont été mises à jour au 1er trimestre 2018. Par conséquent, il n'est pas possible d'exclure une modification de l'interface.

[24] La localité est une information facultative dans le registre IDE de l'OFS.

[25] La forme juridique est une information facultative dans le registre IDE de l'OFS. Une nomenclature à deux (01, 02, 03) ou quatre caractères est utilisée conformément à la norme eCH-0097 (https://www.ech.ch/fr/standards/54046) et doit ensuite être convertie lors du transfert vers le certificat.

[26] **PublicStatus** indique s'il est autorisé de rendre librement accessibles sur Internet les données d'une entreprise contenues dans le registre IDE de l'OFS. Voir également le chapitre 9.6.

	Statut IDE: <root>/eCH-0108:uidregInformation/eCH-0108:uidregStatusEnterpriseDetail
7	**checkPlausi1(name,UIDAttributes):** Le répartiteur vérifie les données provenant du registre IDE de l'OFS et les compare aux informations de l'entreprise obtenues à l'étape 2. Si les deux jeux de données ne coïncident pas, l'enregistrement est interrompu et un message d'erreur s'affiche.
8	**getVerification(CRID, IData):** Le répartiteur envoie le CRID et les informations sur la relation contractuelle à l'A&A précédemment sélectionnée.
9	**check(IData):** L'A&A vérifie la relation contractuelle avec l'entreprise en comparant les informations à ses données de base. Cette comparaison peut être automatisée ou réalisée manuellement par un collaborateur. Si les deux jeux de données coïncident en tous points, le résultat du contrôle d'identité est concluant. Si les données envoyées ne concordent pas avec les données de base de l'A&A, il est impossible de confirmer l'identité de l'entreprise.
<--	**processing(expectedAvailability):** L'A&A confirme que le traitement a débuté et indique au répartiteur une estimation de la durée restant nécessaire.
10	**getResult(CRID):** Une fois la confirmation (CRID) reçue par le répartiteur, le système ERP demande le statut du traitement en cours. Pour ce faire, il envoie au répartiteur le CRID correspondant dans le cadre d'une requête signée à l'aide du certificat ERP.
11	**verifySignature(SignatureERP):** cf. 3
<--	**processing(expectedAvailability):** Le répartiteur répond au système ERP que le traitement est toujours en cours et indique une estimation de la durée restant nécessaire.
12	**getStatus(DID):** Au terme du délai fixé par l'A&A, le répartiteur se renseigne sur le statut du traitement en émettant une requête ad hoc.
<--	**success(BFS_UID, name, address, qualityLevel, contact):** Le résultat de la vérification est renvoyé par l'assureur au répartiteur. S'il est concluant, la réponse contient les éléments suivants: • success: confirmation du résultat concluant du contrôle d'identité; • BFS-UID: numéro IDE de l'entreprise figurant dans les données de base de l'&A; • name: nom de l'entreprise; • address: coordonnées de l'entreprise, c'est-à-dire nom de l'entreprise (direction), case postale, rue, numéro, numéro postal d'acheminement et localité; • qualityLevel: qualité de la vérification des données (p. ex. 0 – automatique, 10 – manuel, 100 – conforme à la SCSE); • contact: collaborateur de l'A&A ayant réalisé la vérification et à contacter au besoin. Si le résultat n'est pas concluant, un message d'erreur est émis: • error: erreur survenue lors de la vérification de l'identité Dans ce cas, les étapes suivantes ne sont pas réalisées au niveau du répartiteur.
13	**checkPlausi2():** Le répartiteur compare les informations fournies par l'A&A avec les données préalablement obtenues dans le registre IDE. Cette comparaison, qui peut être automatique (par exemple à l'aide de méthodes imprécises basées sur l'intelligence artificielle) ou manuelle, porte sur le numéro IDE, le nom de l'entreprise et l'adresse. Si les données provenant des deux sources coïncident, l'enregistrement réussit et peut se poursuivre via les étapes suivantes.
14	**generateRegPw():** Si le résultat de la vérification de l'identité est concluant (success), le répartiteur génère un mot de passe d'enregistrement (RegPw) conformément aux règles correspondantes (cf. point 5.4).

15	**generateSperrPw():** Le répartiteur génère aussi un mot de passe de verrouillage (SperrPw) dans le respect des règles indiquées au point 5.4. Ce second mot de passe est utilisé lors du processus de verrouillage (voir point 6.6)
16	**save(CRID, UID-BFS, UIDAttributes, RegPw, SperrPw, contact, address, timeStamp):** Le répartiteur enregistre le RegPw, le SperrPw ainsi que l'UID-BFS, les informations sur l'entreprise provenant du registre IDE (UIDAttributes), le CRID, les coordonnées (contact), l'adresse (address) et un timbre horodateur (timeStamp). La validité des RegPw est limitée à 30 jours maximum.
17	**getResult(CRID):** Au terme du délai prescrit (expectedAvailability), le système ERP interroge le répartiteur pour connaître le statut du traitement en cours. Pour ce faire, il envoie le CRID correspondant dans une requête signée à l'aide du certificat ERP.
18	**verifySignature(SignatureERP):** Cf. 3
<--	Si le répartiteur a connaissance du résultat de la vérification de l'identité, il l'envoie en réponse (success | error) au système ERP. Le résultat success est envoyé avec l' UID-BFS confirmé et les informations nécessaires à la création d'une CSR (SubjektInformation)..
19	**send(CRID, UID-BFS, UIDAttributes, RegPw, SperrPw):** Si le résultat de la vérification de l'identité de l'entreprise est concluant (success), le répartiteur ou un tiers mandaté à cet effet par Swissdec envoie à la direction de l'entreprise (address) un courrier (second canal, non électronique) comprenant les données de l'interlocuteur (contact), en utilisant les coordonnées transmises par l'ERP et celles provenant des données de base de l'A&A. Ce courrier contient au minimum les informations suivantes, requises pour la configuration: • le CRID, pour identifier le processus d'enregistrement spécifique; • l'«UID-BFS» et les «UIDAttributes» de l'entreprise concernée; • le RegPw pour la configuration; • le SperrRW pour verrouiller le certificat IDE; • la durée de validité du RegPw..

Si le résultat de la vérification de l'identité par l'A&A est concluant, le collaborateur compétent reçoit, une fois l'enregistrement réalisé avec succès, les informations relatives à l'entreprise obtenues dans le registre IDE de l'OFS (par voie électronique sous forme de réponse à une requête getResult() ou par courrier).

6.1.1.2 L'A&A envoie un courrier à l'entreprise.
Le processus est schématiquement identique à celui dans lequel le répartiteur envoie le courrier à l'entreprise.
Si la vérification par le répartiteur des informations d'enregistrement reçues du système ERP aboutit à un résultat concluant, le répartiteur génère les mots de passe d'enregistrement et de verrouillage. Contrairement à ce que prévoit le premier processus décrit, l'A&A reçoit non seulement les informations nécessaires à l'identification de l'entreprise (profil d'assurance, IDE-OFS), mais aussi les mots de passe.
Elle vérifie alors la validité des informations d'enregistrement envoyées par l'entreprise et s'assure que ces dernières concordent avec ses données de base. Le résultat de la vérification de l'identité est renvoyé.
Si la vérification de l'identité est concluante, l'A&A envoie à la direction de l'entreprise, à l'intention de l'interlocuteur désigné (contact), 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, sa validité, le mot de passe de verrouillage, le CRID et l'IDE-OFS.
S'il est possible, ce processus d'enregistrement est pour l'instant exclu. On pourrait aussi envisager que l'A&A initialise l'enregistrement de l'entreprise, à condition toutefois qu'elle utilise une circulaire (envoi en masse) qui ne contienne que les instructions relatives à l'enregistrement figurant au chapitre 6.1.1.1.

6.1.2 Enregistrement au moyen d'un certificat réglementé selon la SCSE

Le processus d'enregistrement au moyen de certificats réglementés SCSE est décrit de façon détaillée dans un document distinct intitulé «Authentification d'entreprises Swissdec - Spécifications détaillées - Complément sur l'enregistrement avec SCSE» [1].

6.1.3 Avantages et inconvénients des différents processus d'enregistrement

Tableau 9: Avantages et inconvénients des différentes variantes du processus d'enregistrement

Processus	Avantages	Inconvénients
Le répartiteur envoie le courrier.	• Envoi centralisé et standardisé des courriers par Swissdec • Il n'est pas nécessaire de transmettre les informations à l'A&A. • Facultatif: transmission des coordonnées du client superflue[27]	• Les coordonnées du client sont transmises au répartiteur et, le cas échéant, à un tiers. • Pas de contact direct entre l'A&A et le client
L'A&A envoie le courrier.	• Contact direct entre l'A&A et le client • Relation de confiance entre le client et le fournisseur	• L'A&A doit définir un processus d'envoi des courriers. • De nombreuses entités différentes participent directement au processus d'enregistrement. • Le courrier contenant le RegPw peut se perdre dans le flot des courriers d'assurance.
Enregistrement avec certificat SCSE	• Enregistrement et configuration possibles en une seule et même étape (plus besoin d'envoyer de courriers) • Enregistrement pour des entreprises sans relation contractuelle avec une A&A • Identification des entreprises conforme aux prescriptions SCSE • Autorité d'enregistrement accréditée selon la SCSE • Utilisation de l'infrastructure de certification déjà présente • Participation de l'A&A inutile	• Le processus de réception d'un certificat basé sur la SCSE est fastidieux pour les entreprises. • Certificats basés sur la SCSE assez peu répandus, uniquement dans les grandes entreprises

6.2 Enregistrement de fiduciaires

Une fiduciaire ne doit s'enregistrer pour obtenir un certificat SUA que si elle souhaite envoyer des données pour le compte d'une entreprise à des A&A sans passer directement par le système ERP de cette entreprise (dans ce cas, tous les messages sont signés à l'aide du certificat SUA de l'entreprise). L'entreprise se charge alors d'organiser la représentation, et l'assurance n'a pas besoin d'enregistrer de procuration écrite.

Si la fiduciaire utilise un système ERP qui lui est propre pour conserver les données relatives aux entreprises dont elle assure la gestion (différents mandants), il lui faut un certificat SUA.

Il convient de distinguer deux cas de figure dans l'enregistrement de fiduciaires.

a) Comme d'autres entreprises, la fiduciaire entretient déjà une relation contractuelle avec une assurance ou autorité (A&A) enregistrée sur la base de laquelle un enregistrement SUA pourrait être réalisé. On applique alors le processus d'enregistrement classique (cf. chapitre 6.1.1).
b) La fiduciaire n'a pas de relation directe avec une A&A 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 dans ce cadre, en plus des données relatives au contrat

[27] L'adresse n'est pas fournie par l'A&A, mais obtenue directement dans le registre IDE de l'OFS en vue de l'envoi du courrier, conformément à l'étape alternative n° 9 indiquée au tableau 8.

de l'entreprise, ses propres données (nom de la fiduciaire, IDE, données de contact, etc.) à la rubrique «Délégué». L'A&A 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 IDE 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 il assure la gestion.

6.3 Processus de configuration initiale

6.3.1 Configuration initiale avec enregistrement préalable

Le processus de configuration initiale commence dans le système ERP par le choix d'une procédure d'enregistrement (saisie du CRID et de l'IDE-OFS) pour un enregistrement préalablement effectué (en cours ou réalisé avec succès). Le système ERP propose au collaborateur compétent les informations sur le «Subject» pour le certificat IDE qui était contenu dans la confirmation d'enregistrement.

Le collaborateur concerné vérifie alors ces informations. Si la procédure d'enregistrement choisie a déjà été achevée et que le collaborateur a déjà reçu le courrier contenant le mot de passe d'enregistrement, la configuration peut se poursuivre.

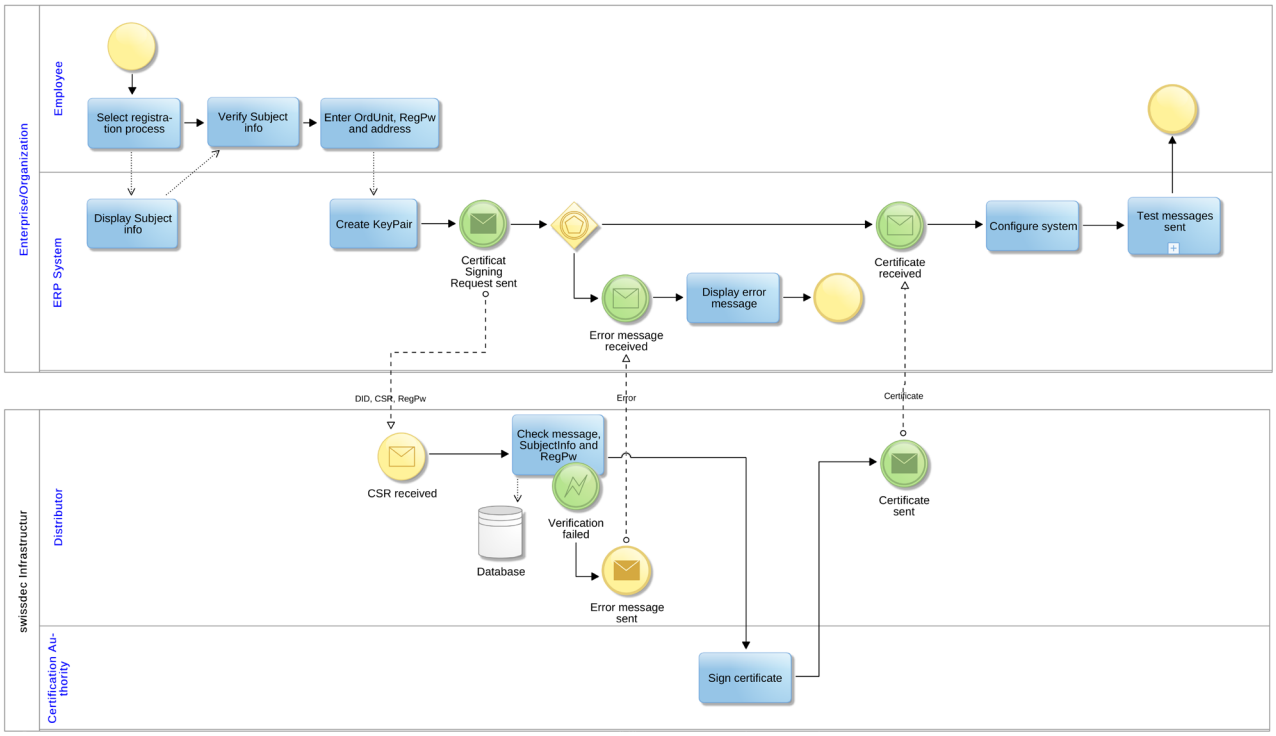

Illustration 13: Processus de configuration initiale

Le collaborateur compétent doit ensuite saisir le mot de passe d'enregistrement reçu. Il peut aussi compléter les données relatives à l'entreprise pour le certificat IDE en indiquant une sous-unité (cf. également le tableau 2).

Le système ERP génère alors la paire de clés, puis envoie au répartiteur une CSR accompagnée du mot de passe d'enregistrement, du CRID et de l'IDE-OFS.

Le répartiteur vérifie que le message reçu est valide (signature du certificat ERP) et complet (informations requises pour la création du certificat) ou conforme (structure de la CSR), puis s'assure que le mot de passe d'enregistrement envoyé correspond bien au numéro d'enregistrement. Les informations sur le «Subject» contenues dans la CSR sont comparées avec les données sur l'entreprise sauvegardées lors de l'enregistrement. Si ces vérifications n'aboutissent pas à un résultat concluant, le système ERP en est immédiatement informé par un message d'erreur et le processus est interrompu.

Si le répartiteur a reçu une CSR valide, cette dernière est envoyée directement à la CA, qui signe automatiquement le certificat avant de le renvoyer au répartiteur.

Le répartiteur envoie à son tour le certificat signé au système ERP, lequel l'intègre.

Une fois le certificat IDE reçu et intégré au système ERP, son bon fonctionnement peut être vérifié à l'aide de messages CheckInteroperability. Si le test est concluant, le mot de passe d'enregistrement utilisé est dès lors invalide.

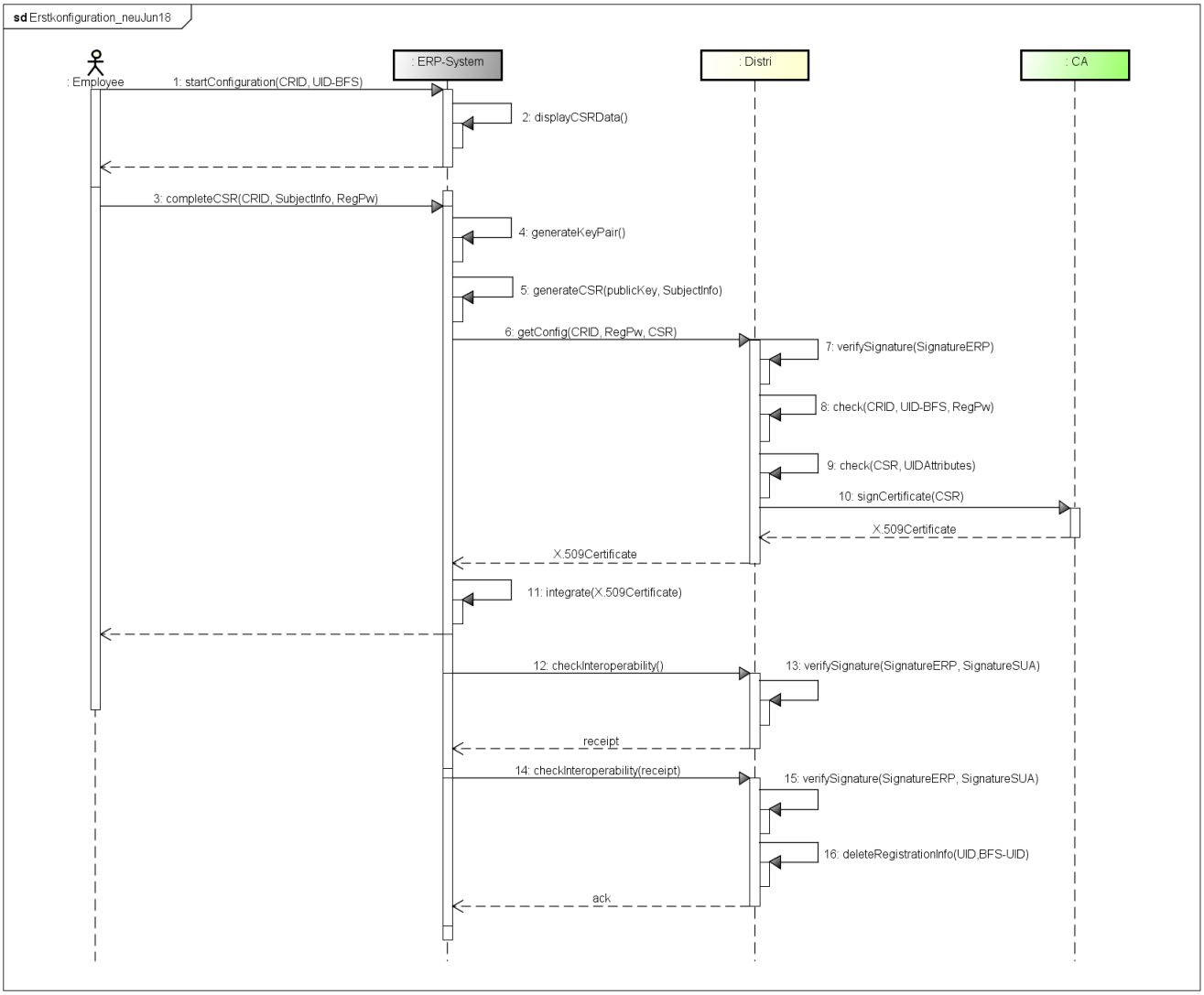

Illustration 14: Diagramme de séquence du processus de configuration initiale

Tableau 10: Description des étapes du processus de configuration initiale

Nº	Description
1	**startConfiguration(CRID, UID-BFS):** Le processus de configuration est directement enclenché dans le système ERP. Un collaborateur responsable choisit dans le système ERP le CRID et l'IDE-OFS pour lesquels un enregistrement a déjà été effectué.
2	**displayCSRData():** Le système ERP montre à l'utilisateur les informations reçues concernant la CSR.
<--	Le système ERP montre à l'utilisateur le statut reçu.
3	**completeCSR(CRID, SubjectInfo, RegPw):** L'utilisateur transmet les informations complétées sur le «Subject» (les données proviennent du registre IDE de l'OFS, seule la sous-unité de l'organisation peut être ajoutée; voir également le tableau 2) ainsi que le RegPw.
4	**generateKeyPair():** Le système ERP génère la paire de clés (clé privée et clé publique) selon les règles indiquées au point 5.3.
5	**generateCSR(publicKey, SubjectInfo):** Le système ERP établit une CSR conformément aux règles indiquées au tableau 3.

6	**getConfig(CRID, RegPw, CSR):** Le système ERP envoie au répartiteur une requête contenant le CRID, la CSR et le RegPw.
7	**verifySignature(SignatureERP):** Le répartiteur s'assure que la signature du message est valide et compatible avec la version de la norme SUA.
8	**check(CRID, UID-BFS, RegPw):** Le répartiteur vérifie que le RegPw correspond bien à l'IDE-OFS et au CRID concernés à l'aide des informations figurant dans la base de données.
9	**check(CSR, UIDAttribute):** La satisfaction des règles structurelles de la norme SUA (point 5.1.6) par la CSR établie par le système ERP est vérifiée. En outre, les informations qu'elle contient sur le «Subject» sont comparées avec celles figurant dans la base de données du répartiteur. En cas de non-respect des règles ou de divergence avec les informations archivées au niveau du répartiteur, le système ERP reçoit un message d'erreur.
10	**signCertificate(CSR):** Le répartiteur envoie la CSR à la CA. La forme précise de cette interface et des données transmises doit être définie de concert avec la CA choisie.
<--	La CA répond avec le certificat X.509 signé.
<--	Le répartiteur répond au système ERP en lui envoyant le certificat signé (X.509Certificate) en tant que certificat codé en base64 (PEM).
11	**integrate(X.509Certificate):** Le système ERP intègre le certificat X.509.
12	**checkInteroperability():** Une fois le certificat intégré par le système ERP, ce dernier envoie au répartiteur un message checkInteroperability.
13	**verifySignature(SignatureERP, SignatureSUA):** Le répartiteur vérifie les signatures du message, qui doivent être conformes aux spécifications relatives à la signature et au cryptage à l'aide de certificats ERP et de certificats IDE.
<--	Si le test est concluant, le répartiteur envoie au système ERP une confirmation ad hoc (receipt).
14	**checkInteroperability(receipt):** Pour que le répartiteur puisse s'assurer que le système ERP est capable non seulement d'envoyer des messages, mais aussi d'en recevoir, le système ERP renvoie au répartiteur la confirmation reçue (receipt) dans un second message.
15	**verifySignature(SignatureERP, SignatureSUA):** voir l'étape 13.
16	**deleteRegistrationInfo(CRID, UID-BFS, RegPw):** Si le second message-test a été vérifié avec succès, le répartiteur supprime toutes les informations relatives à la procédure d'enregistrement (notamment le RegPw) de sa base de données.
<--	**ack:** Le répartiteur confirme au système ERP la réception du second message-test.

6.3.2 Variante dans laquelle le répartiteur génère la paire de clés et le certificat

Au cours de l'élaboration des présentes spécifications détaillées, nous avons mis au point une variante qui permettrait au répartiteur de générer les clés et d'établir le certificat IDE de manière centralisée quand le système ERP n'en est pas capable pour des raisons techniques. Dans un tel cas, le certificat IDE serait envoyé par voie électronique au système ERP, qui se contenterait de l'intégrer. De plus amples informations à ce sujet sont disponibles dans le document complémentaire «Authentification d'entreprises Swissdec - Spécifications détaillées - Génération de la paire de clés et du certificat par le répartiteur».

Les clés, en particulier la clé privée, sont générées hors du système destiné à les utiliser, ce qui présente les inconvénients majeurs suivants en termes de sécurité:

- Les clés doivent être transmises par voie électronique.

- Les clés et le certificat doivent être enregistrés dans un format conteneur adapté et protégées contre tout accès non autorisé.
- Le mot de passe d'enregistrement est utilisé non seulement lors de l'authentification, dans le cadre du mot de passe de configuration, mais aussi pour crypter le fichier conteneur, ce qui implique une exigence supplémentaire en matière de forme.
- La gestion et l'enregistrement temporaire du fichier conteneur accroissent les risques pour la sécurité; ces derniers doivent donc être limités par des règles techniques, mais aussi organisationnelles.

En outre, les cadres normatifs utilisés par la grande majorité des systèmes ERP proposent la génération d'une paire de clés et l'établissement d'une CSR correspondante, ce qui facilite l'implémentation du côté des systèmes ERP. La fourniture d'échantillons de codes peut aussi être utile à cet effet.

6.3.3 Variante de configuration avec enregistrement automatique (envoi en masse)

Une variante d'enregistrement automatique à l'aide d'un envoi en masse de courriers d'enregistrement par les A&A a également été élaborée et examinée. Les résultats correspondants sont disponibles dans le document distinct intitulé «Authentification d'entreprises Swissdec - Spécifications détaillées de l'envoi en masse».
Cette variante a été jugée inadaptée et n'est donc pas envisagée pour les motifs suivants:

- Pour des raisons de sécurité, l'initiative de participation à l'authentification d'entreprises Swissdec et de fourniture d'un mot de passe d'enregistrement doit toujours venir d'une entreprise et donc d'un système ERP. On peut ainsi partir de l'hypothèse que les personnes responsables dans l'entreprise possèdent les informations et instructions nécessaires à l'exécution du processus d'enregistrement et de configuration.
- Si une entreprise ne s'enregistre pas à la SUA de son propre chef, il est impossible d'évaluer quand un mot de passe d'enregistrement envoyé sera effectivement utilisé. Il faudrait donc assortir les RegPw envoyés d'une durée de validité plus longue, ce qui augmenterait le risque d'abus.
- Si les A&A envoyaient des mots de passe d'enregistrement en masse, on ne pourrait exclure la possibilité qu'une même entreprise reçoive plusieurs courriers valables contenant différents mots de passe d'enregistrement. Or, conformément au point 5.4, il ne doit exister à un instant T qu'un seul mot de passe d'enregistrement valable par entreprise / IDE-OFS.

6.3.4 Variante de configuration avec jeton matériel

La paire de clés d'un certificat IDE étant toujours créée du côté de l'entreprise, le certificat Swissdec est établi et archivé en tant que jeton logiciel dans l'environnement sécurisé du système ERP ou sur un composant matériel certifié (boîte noire transactionnelle ou jeton cryptographique). Dans un cas comme dans l'autre, le processus d'enregistrement est à peu près le même pour Swissdec et pour la CA émettrice.
La CA est responsable de l'émission, de la révocation et du renouvellement d'un certificat IDE Swissdec. Avec un jeton matériel, la forme concrète et la mise en œuvre technique doivent être définies avec la CA responsable. Quelle que soit la forme du jeton, Swissdec joue le rôle de RA et les différentes variantes du processus d'enregistrement doivent être préalablement exécutées conformément au point 6.1.
Vu le niveau de sécurité élevé garanti par l'utilisation d'un jeton matériel, il est possible de prolonger la validité du certificat concerné. Si un renouvellement automatique d'un an à trois reprises est prévu avec un certificat logiciel, la durée d'utilisation devrait être limitée à trois ans pour un jeton matériel. Au terme de ces trois ans, une nouvelle vérification de l'identité de l'entreprise doit toutefois être effectuée par le biais d'un nouvel enregistrement, même avec un jeton matériel.
Le processus de configuration est donc semblable à celui décrit au point 6.2.1, si ce n'est que la CA envoie à l'entreprise le jeton matériel que cette dernière doit ensuite mettre à la disposition d'un système ERP. Les messages checkInteroperability décrits aux étapes 12 à 16 (chapitre 6.2.1 tableau 10) peuvent servir à vérifier que le système ERP est configuré correctement. L'échange de ces données permet de mettre un terme au processus et, ainsi, de s'assurer que le jeton matériel a bien été installé.
Ce processus fonctionne aussi pour les jetons de boîtes noires transactionnelles: dans ce cas, il incombe à l'entreprise de veiller à ce que le système ERP ait accès aux clés.
Les avantages et inconvénients de cette variante sont rassemblés au tableau 11.

Tableau 11: Avantages et inconvénients des jetons matériels

Avantages	Inconvénients
• Le certificat et les clés sont stockés sur un dispositif matériel sécurisé. • Authentification à deux facteurs (jeton + NIP)	• Les systèmes ERP doivent prendre en charge le jeton matériel (interface physique, ERP dans le cloud).

• La CA est seule responsable de l'émission et de la gestion du jeton matériel.	• Gestion du NIP: saisie ou stockage temporaire (mise en cache) à chaque utilisation du certificat

6.4 Processus d'exécution: exemple de la norme suisse en matière de prestations (KLE)

Voici un exemple d'utilisation du certificat IDE dans le cadre de processus d'exécution de la norme suisse en matière de prestations (KLE).

6.4.1 Déclaration d'un événement

L'entreprise signale la survenue d'un événement («Incident») à une A&A compétente. Elle utilise à cet effet la déclaration d'événement directement depuis son système ERP. Il est possible d'envoyer une déclaration d'événement simultanément à plusieurs assurances et autorités et de transmettre à ces dernières les informations requises.
Le diagramme de séquence suivant montre le déroulement d'une déclaration d'événement selon la norme suisse en matière de prestations. Dans l'illustration comme dans la description, l'accent est explicitement mis sur les points pertinents pour l'authentification d'entreprises Swissdec. Les informations spécifiques relatives au processus figurent dans le document correspondant consacré à la norme suisse en matière de prestations.

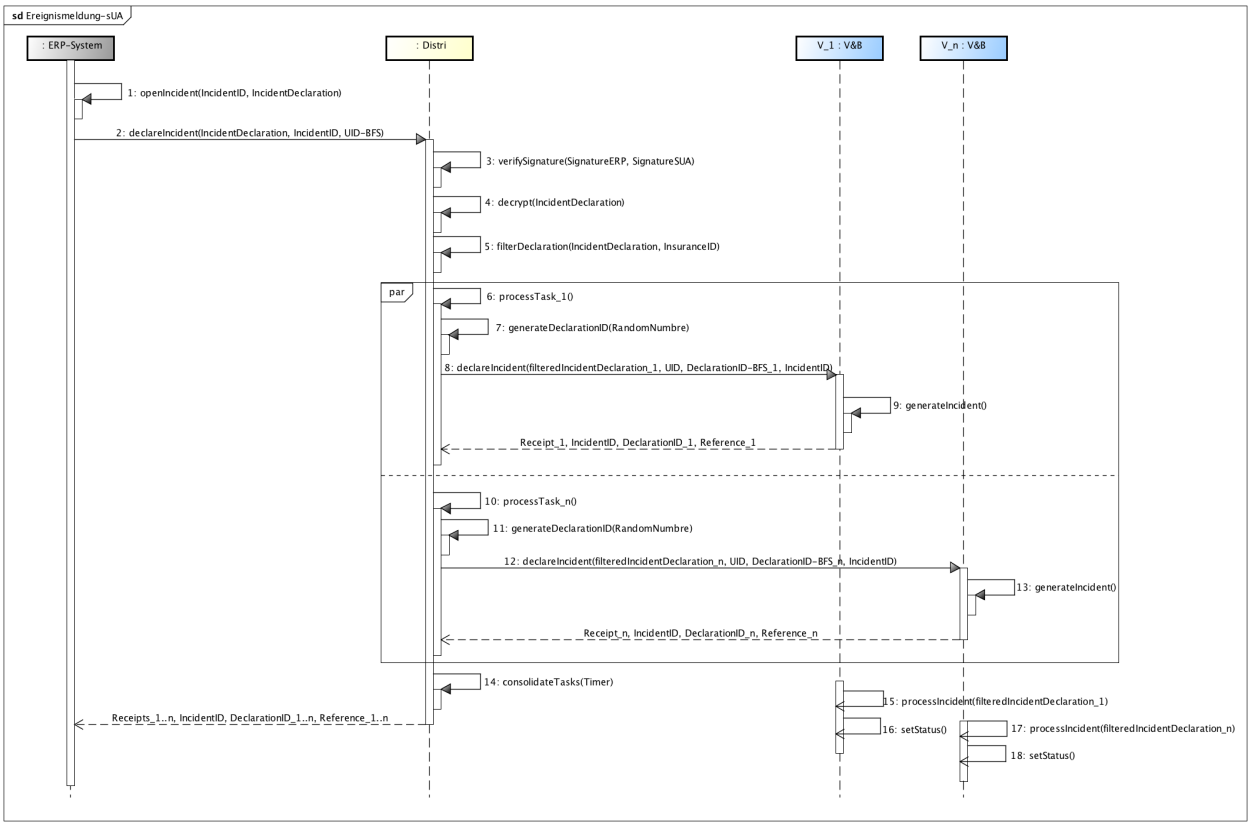

Illustration 15: Déclaration d'événement selon la norme suisse en matière de prestations (KLE) avec SUA

Tableau 12 : Description des étapes de déclaration d'un événement selon la norme suisse en matière de prestations avec SUA

N°	Description
1	**openIncident(IncidentID, IncidentDeclaration):** Un nouvel événement est créé et un numéro d'identification ad hoc (IncidentID) attribué dans le système ERP. Les informations pertinentes pour l'A&A sont saisies dans une IncidentDeclaration.

N°	Description
2	**declareIncident(IncidentDeclaration, IncidentID, UID-BFS):** Une fois l'IncidentDeclaration intégralement remplie, elle peut être envoyée aux A&A concernées via le répartiteur. L'IncidentID et l'UID-BFS sont également communiqués.
3	**verifySignature(SignatureERP, SignatureSUA):** Le répartiteur vérifie les signatures du message qui doivent être conformes aux spécifications relatives à la signature et au cryptage à l'aide de certificats ERP et de certificats IDE.
4	**decrypt(IncidentDeclaration):** Le répartiteur décrypte le contenu du message envoyé.
5	**filterDeclaration(IncidentDeclaration, InsuranceID):** Les données concernées ne sont envoyées qu'une seule fois via l'IncidentDeclaration afin d'éviter les doublons. Le répartiteur prépare les données à envoyer à chaque destinataire, de sorte à ne transmettre aux différents destinataires que les parties du message qui les concernent. L'InsuranceID identifie les différents destinataires finaux de l'IncidentDeclaration envoyée..
6 / 10	**processTask():** Le répartiteur lance une tâche distincte pour chaque message à retransmettre. Le nombre de tâches dépond du nombre de destinataires finaux indiqués dans l'IncidentDeclaration.
7 / 11	**generateDeclarationID(RandomNumber):** Pour chaque message à envoyer, le répartiteur génère un numéro d'identification unique et univoque dans le contexte des processus d'affaires Swissdec, un DeclarationID.
8 / 12	**declareIncident(filteredIncidentDeclaration_1..n, UID-BFS, DeclarationID_1..n, IncidentID):** Les informations compilées pour chacun des destinataires finaux (filteredIncidentDeclaration) sont envoyées à ces derniers avec l'IDE-OFS des entreprises du DeclarationID correspondant ainsi que de l'IncidentID. Le message est signé par le répartiteur et crypté à l'aide de la clé publique du destinataire final.
10 / 13	**generateIncident():** L'assureur ou l'autorité traite le message reçu.
<--	Un Receipt contenant l'IncidentID, le DeclarationID ainsi qu'une «Reference» est renvoyé en réponse. • Reference: numéro de cas de l'assurance ou de l'autorité.
14	**consolidateTasks(Timer):** Si le répartiteur a créé plusieurs tâches avec une IncidentDeclaration, il rassemble toutes les réponses reçues des destinataires finaux concernés. Ces réponses doivent parvenir au répartiteur dans un délai prescrit («Timer»). Si ce n'est pas le cas, le processus est interrompu et un message d'erreur envoyé au système ERP. Il faut alors renvoyer la déclaration d'événement.
<--	Le répartiteur renvoie au système ERP tous les «Receipts», «IncidentID», «DeclarationIDs» et «References» reçus, ce qui confirme la bonne exécution de la déclaration d'événement. La déclaration est alors signée par le répartiteur et cryptée à l'aide de la clé publique du système ERP (certificat IDE).
15 / 17	**processIncident(filteredIncidentDeclaration):** Indépendamment de la déclaration d'événement, le traitement de l'incident ouvert auprès du destinataire final se poursuit.

N°	Description
16 / 18	**setStatus():** Lors d'étapes ultérieures du traitement de l'incident, l'assurance / autorité peut choisir l'un des statuts prédéfinis, qui est alors transmis au système ERP de l'entreprise si ce dernier émet un appel de communication.

6.4.2 Scrutation

Une fois la déclaration d'événement réalisée, une communication spécifique est établie entre le système ERP de l'entreprise et chaque destinataire final (A&A) pour poursuivre le traitement de l'incident. Bien que chaque échange passe toujours par le répartiteur, le système ERP ne s'adresse qu'à un destinataire final donné. Comme précisé dans la norme suisse en matière de prestations (KLE), on utilise à cet effet une procédure de scrutation[28]. Le répartiteur joue ici le rôle de point d'extrémité sécurisé vis-à-vis des différentes A&A. Il authentifie chaque message envoyé par une entreprise à l'aide de la signature du certificat IDE et est responsable, vis-à-vis des entreprises, du cryptage des messages envoyés en réponse par les A&A.

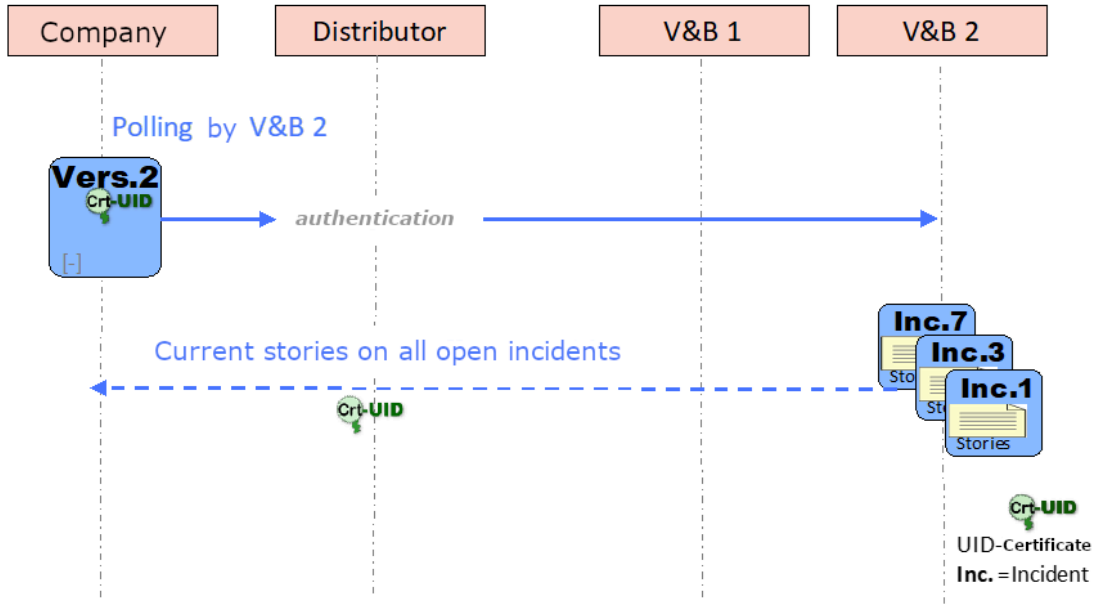

Illustration 16: Procédure de scrutation (schématisée)

L'utilisation de l'authentification d'entreprises Swissdec est l'assurance que les entreprises sont toujours clairement identifiables en tant qu'expéditeurs dans la communication entre système ERP et A&A, ce qui garantit une communication aussi efficace que possible. Par conséquent, en réponse à un appel du système ERP («Request»), des données relatives à différents incidents en cours auprès d'un destinataire final peuvent être envoyées au système ERP. Les informations ou exigences liées à l'incident concerné peuvent ainsi être traitées directement dans le système ERP.

6.4.3 Représentation

D'après les exigences définies dans le cadre du concept de solution relatif à l'authentification d'entreprises Swissdec, une entreprise doit pouvoir être représentée, par exemple par une fiduciaire (A-13). De même, l'exigence 14 (A-14) du concept de solution prévoit déjà que la vérification de la validité d'une telle représentation, dans le cadre de la communication entre le système ERP et les destinataires finaux, incombe à l'A&A.
Les processus d'enregistrement et de configuration initiale décrits plus haut restent donc inchangés. Un représentant s'enregistre sous son propre IDE-OFS, conformément au processus prescrit, et peut, au terme de la configuration, envoyer des données à une A&A via le répartiteur au nom d'une autre entreprise. L'A&A concernée doit alors

[28] La structure de communication de Swissdec repose sur une double communication client-serveur (ERP -> répartiteur et répartiteur -> A&A). Les A&A ne peuvent donc pas être à l'initiative d'un échange de messages. Pour que les messages des A&A puissent tout de même parvenir aux systèmes ERP, ces derniers (et le répartiteur) scrutent les systèmes des A&A à intervalles réguliers.

examiner le contenu et l'expéditeur des données pour s'assurer que la représentation est bien légitime et que lesdites données peuvent être traitées.

6.5 Renouvellement

Le processus de renouvellement de certificats IDE (jetons logiciels uniquement) est identique au processus de configuration initiale (point 6.2.1), sauf pour les points suivants:

- Il n'est pas nécessaire de saisir un mot de passe d'enregistrement pour enclencher le processus: ce dernier est initié automatiquement dès lors que la durée de validité du certificat IDE actuellement utilisé est inférieure à 30 jours. Le système ERP peut enclencher le processus autant de fois que nécessaire jusqu'à ce qu'un nouveau certificat valable soit émis et intégré.
- Le mot de passe de verrouillage initialement reçu reste valable même une fois le certificat IDE renouvelé. Le répartiteur n'envoie donc pas d'autre mot de passe de verrouillage par courrier.
- Les clés toujours valables (certificat IDE) sont utilisées pour toute la communication intervenant dans le cadre du processus de renouvellement. Au terme de la configuration réalisée avec le nouveau certificat établi, mais pas avant, un message-test correspondant est envoyé avec ce nouveau certificat, qui est dès lors utilisé.
- Pour s'assurer que les données relatives à l'entreprise (nom, pays, ville) aussi contenues dans le certificat IDE n'ont pas changé, le répartiteur consulte également le registre IDE de l'OFS en saisissant l'IDE-OFS de l'entreprise. Si les informations figurant dans le registre IDE de l'OFS ne concordent pas avec les données contenues dans l'ancien certificat IDE, le renouvellement est interrompu via un message d'erreur et un nouveau processus d'enregistrement (cf. chapitre 6.1) doit être initié.

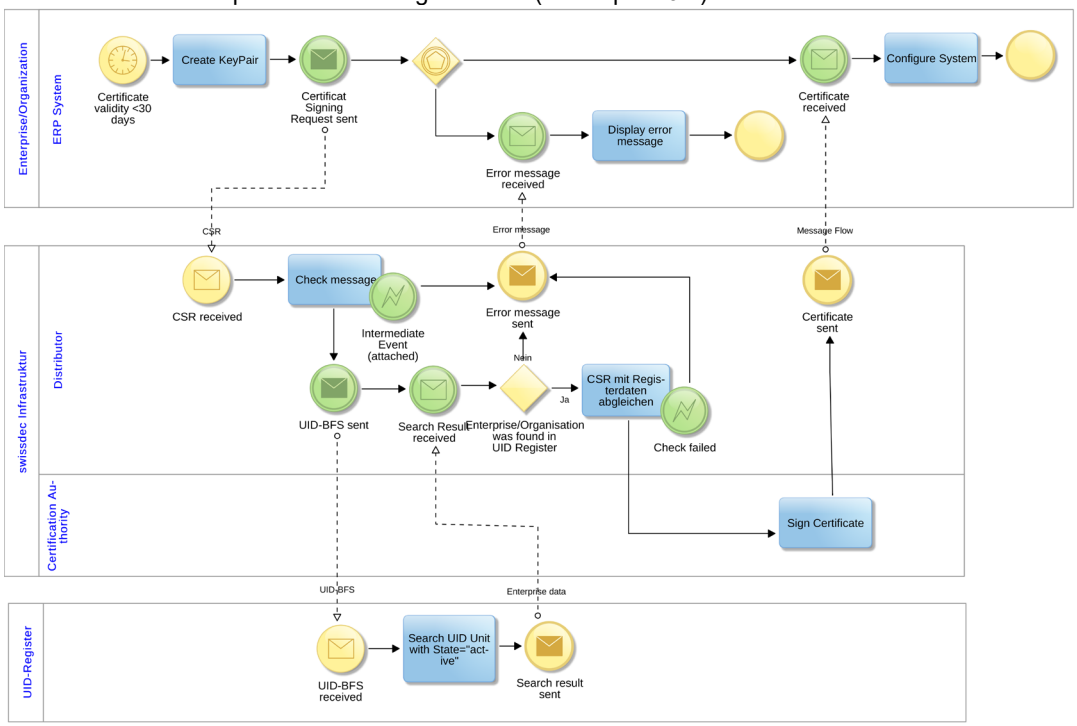

Illustration 17: Processus de renouvellement

Comme il s'agit d'un processus automatisé, une vérification de l'actualité et de l'authenticité de l'entreprise doit être effectuée à intervalles réguliers. Le renouvellement automatique d'un certificat IDE ne peut donc intervenir que trois fois. Dès que le système ERP s'est automatiquement procuré un nouveau certificat à trois reprises, l'entreprise est invitée à recommencer complètement le processus d'enregistrement et à faire confirmer son identité par une A&A via une relation contractuelle en cours.

Un changement de certificat SUA peut engendrer des problèmes en cas de processus de longue durée, par exemple pour la norme suisse en matière de prestations (KLE). Si les certificats sont changés régulièrement, les résultats relatifs à une déclaration d'événement peuvent devoir être cryptés avec des clés plus récentes que celles requises pour le premier message. Le répartiteur doit être capable de gérer ces deux procédures.

6.6 Verrouillage

En cas d'abus (soupçonné ou avéré) en lien avec un certificat IDE, il est possible de procéder à un verrouillage. Il faut utiliser pour cela le mot de passe de verrouillage que l'entreprise a reçu par courrier dans le cadre du processus d'enregistrement.
En règle générale, c'est le détenteur du certificat IDE qui le verrouille. Swissdec peut aussi, à titre exceptionnel, procéder à un verrouillage si une entreprise a perdu le droit d'utiliser les fonctions proposées par Swissdec avant l'expiration de la durée de validité ordinaire du certificat. Le verrouillage est réalisé en deux étapes. Dans un premier temps, un collaborateur d'une entreprise s'authentifie vis-à-vis de Swissdec en vue de déclencher le verrouillage d'un certificat IDE. Une fois la demande examinée, Swissdec verrouille immédiatement le certificat IDE au niveau du répartiteur. Dans un second temps, la demande de verrouillage est transférée à la CA compétente.
Comme le verrouillage au niveau du répartiteur provoque immédiatement la suspension de chaque fonction Swissdec faisant l'objet d'une authentification, les participants n'ont pas besoin de vérifier le statut («Certificate Revocation List» ou «Online Certificate Status Protocol»).

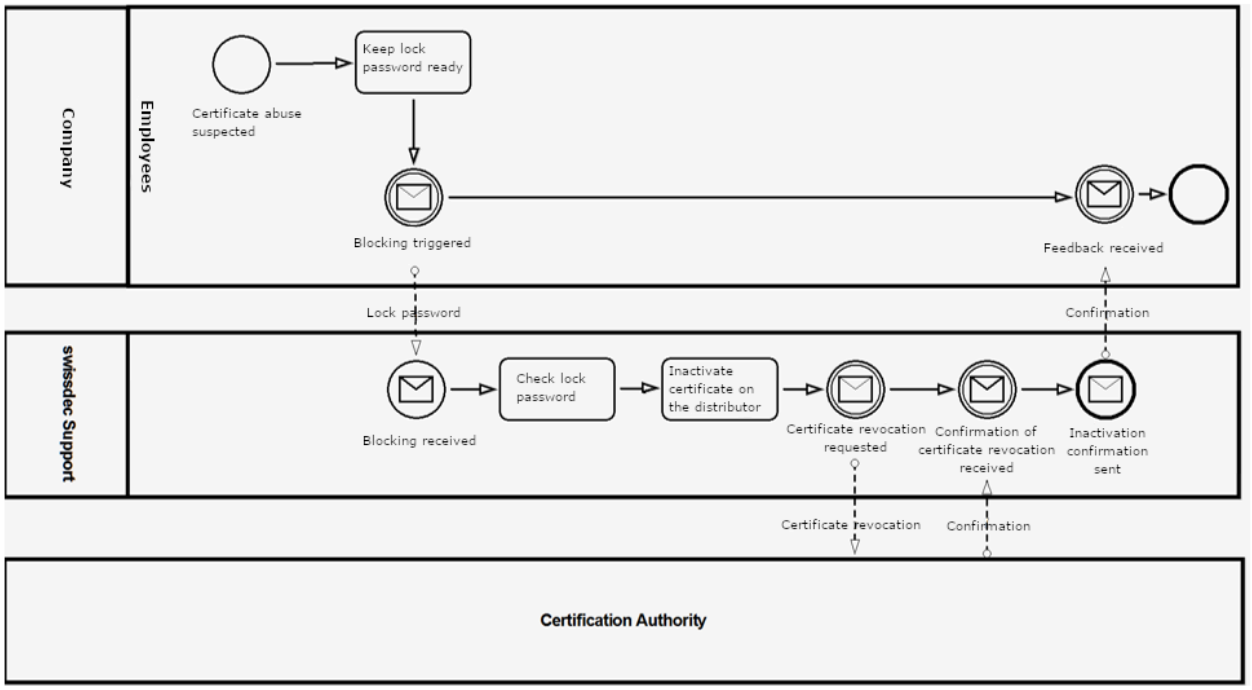

Illustration 18: Processus de verrouillage

Un collaborateur autorisé de l'entreprise déclenche le verrouillage en contactant le support Swissdec et en lui transmettant le mot de passe de verrouillage pour s'identifier. Le support vérifie le mot de passe de verrouillage et apporte son aide à l'entreprise. S'il y a effectivement un abus en lien avec le certificat, le support désactive / verrouille immédiatement le certificat concerné au niveau du répartiteur et ordonne la révocation du certificat à la CA. Une confirmation de la révocation du certificat est envoyée au collaborateur de l'entreprise.
Si l'entreprise concernée ne possède plus le mot de passe de verrouillage ou n'y a pas accès, il faut tout d'abord s'assurer de la légitimité du collaborateur. Pour ce faire, il convient, à l'aide de renseignements spécifiques à la procédure technique et de l'implication d'une A&A, d'examiner si la personne à l'origine de l'appel est autorisée ou non à verrouiller le certificat au nom de l'entreprise concernée.
Attention: le verrouillage d'un certificat est irréversible. Si une entreprise souhaite pouvoir de nouveau communiquer avec le répartiteur alors qu'un verrouillage a été réalisé, il lui faudra suivre une nouvelle fois toute la procédure d'enregistrement (cf. point 6.1).

6.7 Traitement des erreurs et des exceptions

Les diagrammes de séquence relatifs au processus SUA décrit au chapitre 6 traitent principalement du cas positif du déroulement d'un processus donné. Les représentations des processus BPMN correspondantes montrent certains cas d'erreur liés au déroulement du processus, mais ne révèlent pas de problématiques techniques. Il convient ici d'aborder brièvement le principe de traitement des erreurs et des exceptions dans le contexte des processus SUA.

Chaque étape de processus et chaque processus de communication peuvent théoriquement contenir des erreurs ou aboutir à un résultat / état non souhaité. En cas de dysfonctionnement de ce type, toutes les instances de l'authentification d'entreprises Swissdec participant à la communication sont tenues de renvoyer une exception à l'expéditeur d'une requête. Cette exception doit contenir les informations relatives à l'erreur survenue et pouvoir être reçue traitée par l'autre instance de communication.

7 Composants dynamiques des spécifications

Certains éléments des données d'identification SUA (chapitre 5) et des processus SUA (chapitre 6) sont définis dans les présentes spécifications, mais revêtent par nature un caractère dynamique. Le tableau 13 ci-après donne une vue d'ensemble de ces éléments, du contexte dans lequel ils sont utilisés et de leur forme actuellement définie. Comme la forme définie repose sur l'état actuel des connaissances, il conviendra de la réexaminer dans le cadre de l'essai pilote qui interviendra en aval des spécifications ainsi que dans le cadre d'une mise en œuvre ultérieure. La forme de ces composants dynamiques pourra ainsi être régulièrement modifiée à la lumière de nouveaux enseignements tirés lors de la mise en œuvre et de l'utilisation de l'authentification d'entreprises Swissdec.

Tableau 13: Éléments dynamiques des spécifications

Contexte	Élément	Forme
Certificat IDE	Algorithme de cryptage du certificat	SHA256 avec cryptage RSA
	Longueur de la clé («key size»)	2048 bits
	Durée de validité du certificat	1 an Avec jeton matériel: 3 ans
Mot de passe d'enregistrement	Longueur du mot de passe	12 caractères+ 2 caractères pour la marque d'identification + 2 caractères pour le chiffre de contrôle
	Durée de validité du RegPw	30 jours maximum
Mot de passe de verrouillage	Longueur du mot de passe	12 caractères+ 2 caractères pour la marque d'identification + 2 caractères pour le chiffre de contrôle
	Durée de validité du SperrPw	Illimitée
Processus de renouvellement	Moment (situé avant l'expiration du certificat) à partir duquel le système ERP enclenche le renouvellement.	30 jours
	Nombre de renouvellements automatiques possibles	3
Processus d'enregistrement	Nombre de demandes d'enregistrement en cours	5
Processus d'enregistrement	Deuxième canal, non électronique	Courrier recommandé / A Plus

8 Respect des exigences formulées dans le concept de solution

Dans le cadre du concept de solution pour l'authentification d'entreprises Swissdec, des exigences ont été formulées au sujet de la forme de cette norme. Les présentes spécifications détaillées font en sorte de tenir le plus possible compte de ces exigences.
Le tableau 14 ci-après récapitule les exigences formulées dans le concept de solution. La dernière colonne indique dans quelle mesure chaque exigence a été mise en œuvre dans les spécifications détaillées. Le symbole «✓» identifie les exigences intégralement mises en œuvre, «(✓)» les exigences prises en compte de manière partielle ou non explicite, et «x» celles qu'il n'a pas été possible de satisfaire dans le cadre des spécifications détaillées.

Tableau 14: Concept de solution SUA – Exigences

ID	Désignation	Description	Priorité	
A-01	Émission du certificat IDE	Dès lors qu'une entreprise est clairement identifiée, une CA émet des certificats sur la base du numéro d'identification de l'entreprise (IDE).	OBLIGATOIRE	✓
A-02	Émission du certificat du concepteur	Le répartiteur examine la capabilité processus d'un système ERP au moyen d'un certificat spécifique au concepteur ERP.	OBLIGATOIRE	✓
A-03	Certification Authority (CA)	Pour assurer la fiabilité des certificats utilisés, la CA garantit un niveau de qualité de ses certificats et processus en adéquation avec les processus d'affaires.	OBLIGATOIRE	✓
A-04	Attribution de certificats IDE	Un certificat IDE ne contient qu'un IDE.	OBLIGATOIRE	✓
A-05	Certificats par IDE	Plusieurs certificats peuvent être attribués à un même IDE (renouvellement d'un certificat, plusieurs instances ERP).	OBLIGATOIRE	✓
A-06	Durée de validité du certificat IDE	Les certificats IDE émis par une CA sont valables pendant une durée limitée (au moins un an).	OBLIGATOIRE	✓
A-07	Renouvellement d'un certificat IDE	Lorsqu'un certificat atteint le terme de sa durée de validité, le système ERP se procure automatiquement un nouveau certificat auprès de la CA.	OBLIGATOIRE	✓
A-08	Révocation d'un certificat IDE	En cas d'abus, les certificats concernés sont immédiatement révoqués par la CA.	OBLIGATOIRE	✓
A-09	Instance d'enregistrement	Les entreprises s'enregistrent auprès d'une instance autorisée par Swissdec.	OBLIGATOIRE	✓
A-10	Identification univoque de l'entreprise	L'instance autorisée par Swissdec identifie clairement les entreprises souhaitant s'enregistrer, conformément à un processus prescrit.	OBLIGATOIRE	✓
A-11	Identification par une instance autorisée	Une entreprise est identifiée par l'instance autorisée par Swissdec via les renseignements spécifiques à la procédure technique ou un deuxième canal sécurisé.	OBLIGATOIRE	✓
A-12	Identification par un tiers	Un tiers de confiance («Trusted Third Party») identifie l'entreprise.	FACULTATIF	✓
A-13	Représentation (p. ex. fiduciaire)	Le représentant doit s'enregistrer et pouvoir s'authentifier vis-à-vis du répartiteur au moyen de son propre IDE.	OBLIGATOIRE	✓
A-14	Vérification de la représentation	L'assurance / l'autorité vérifie un éventuel représentant en tant que destinataire final d'un message.	OBLIGATOIRE	✓
A-15	Configuration automatique du système ERP	Une fois le processus d'enregistrement réalisé avec succès, le système ERP se procure automatiquement le certificat IDE (éventuellement avec une clé privée) ainsi que d'autres informations de configuration auprès du répartiteur et/ou de la CA. Il est opérationnel en l'espace de quelques minutes.	OBLIGATOIRE	✓
A-16	Autorisation du système ERP	Si le système ERP envoie un message, il doit obtenir du répartiteur l'autorisation relative aux processus d'affaires Swissdec.	OBLIGATOIRE	✓
A-17	Authentification de l'entreprise	Si le système ERP envoie un message, il le signe au moyen du certificat IDE.	OBLIGATOIRE	✓
A-18	Vérification du système ERP	À la réception d'un message, le répartiteur vérifie l'autorisation du système ERP et les processus d'affaires Swissdec.	OBLIGATOIRE	✓
A-19	Authentification de l'entreprise	Quand un message est reçu, le répartiteur vérifie les signatures, traite les données et transfère les informations relatives à l'identité aux destinataires finaux.	OBLIGATOIRE	✓
A-20	Traçabilité	L'échange de messages doit pouvoir être retracé correctement par l'entreprise / le système ERP, le répartiteur ainsi que les assureurs et autorités.	OBLIGATOIRE	✓
A-21	Convivialité	La mise en service et l'utilisation du système doivent être conviviales.	OBLIGATOIRE	(✓)
A-22	Simplicité de la mise en service	La configuration d'un système ERP ne nécessite pas de faire appel à un spécialiste technique.	OBLIGATOIRE	✓
A-23	Rapidité de la mise en service	S'il existe déjà une relation entre l'entreprise et une assurance / autorité, le processus d'enregistrement prend max. 10 minutes, configuration du système ERP comprise.	OBLIGATOIRE	✓

A-24	Accès à un portail depuis un navigateur	L'accès à un portail (A&A) via un navigateur est possible depuis le système ERP.	OBLIGATOIRE	(✓)
A-25	Plausibilisation des messages	Quand le répartiteur reçoit un message, il s'assure que l'IDE qu'il contient coïncide avec celui du certificat.	OBLIGATOIRE	✓
A-26	Infrastructure de certification utilisée	L'infrastructure de clé publique utilisée pour créer les certificats numériques repose sur la norme RFC 5280 X.509 (version 3 actuellement).	OBLIGATOIRE	✓
A-27	Confidentialité au niveau des messages	Pour pouvoir, parallèlement au canal sécurisé, protéger aussi les informations transmises contre d'autres vecteurs d'attaques, il faut crypter le contenu des données pour leur destinataire.	OBLIGATOIRE	✓

Toutes les exigences formulées dans le concept de solution ont donc été prises en compte dans le cadre des spécifications détaillées. Certaines d'entre elles, toutefois, ne sont satisfaites que partiellement ou de manière non explicite.

- A-21 Convivialité
  L'exigence de convivialité a été prise en compte dans le cadre de l'élaboration et des spécifications des processus SUA. S'agissant de la forme des mots de passe, par exemple, la simplicité de leur saisie et la possibilité d'identifier directement une erreur de saisie de l'utilisateur depuis le système ERP (chiffre de contrôle) ont fait l'objet d'une attention particulière. Dans le cadre de l'élaboration des exigences posées à la certification, des spécifications plus poussées, voire une mise en œuvre en collaboration avec les concepteurs de systèmes ERP concernés, seront nécessaires pour certains composants, notamment au niveau des systèmes ERP et de la structure des interfaces utilisateur. La convivialité devra, là encore, occuper une place importante.
- A-24 Accès à un portail depuis un navigateur:
  La possibilité d'accéder aux portails Web d'A&A données via un navigateur directement depuis le système ERP, prévue dans la norme suisse en matière de salaire (ELM)[29], est déjà garantie. Aucune autre règle n'a été fixée à ce sujet dans les spécifications détaillées SUA. Aucune décision n'a été prise, pour l'heure, sur la question de savoir si la norme SUA pourrait ou devrait également servir, à terme, à authentifier des portails Web d'A&A.

[29] Swissdec (2015). Directives, en ligne: https://www.swissdec.ch/fr/versions-et-mises-a-jour/directives-elm/ (2.12.2015).

9 Points en suspens

Certains points n'ont pas pu être définitivement réglés dans les présentes spécifications détaillées. Ils seront toutefois étudiés à nouveau lors d'une révision à venir ou de l'élaboration d'autres documents traitant de la certification et, le cas échéant, réévalués, voire spécifiés de manière plus précise, au vu des informations alors disponibles.

9.1 Processus et règles concernant l'autorité de certification («Certificate Authority», CA)

Il est entendu que l'on aspirera à nouer une collaboration avec une autorité de certification accréditée pour mettre en œuvre l'authentification d'entreprises Swissdec. Il faudrait déterminer, à ce sujet, si des fournisseurs simples tels que Let's Encrypt[30] peuvent proposer des services d'un niveau de qualité équivalent. Les règles indiquées ici au sujet des processus et de la forme de l'infrastructure de certification devraient être prises en compte lors de la procédure de sélection. De même, les détails concernant les procédures concrètes de création de certificats ainsi que la forme du certificat doivent être comparés avec la CA choisie et modifiés au besoin.
L'utilisation de la Business Category (BC), qui correspond à la forme juridique telle qu'indiquée dans le registre IDE de l'OFS, compte notamment parmi les points à clarifier. Ainsi, le registre IDE de l'OFS a recours aux valeurs chiffrées prescrites dans la norme eCH-0097[31] , alors que quatre valeurs seulement sont utilisées dans les principes relatifs à la validation étendue [32] du CAB-Forum.

9.2 Authentification de client TLS

Comme indiqué dans le présent document, l'authentification de l'expéditeur est examinée lors de l'établissement d'un canal sécurisé au moyen d'un certificat client TLS. Cette vérification devrait être réalisée à l'aide d'un certificat IDE. Dans le cadre de l'essai pilote, il faudra examiner à ce titre dans quelle mesure les cadres normatifs existants permettent de procéder de cette manière et si des échantillons de codes simples peuvent être fournis pour les principales plateformes. En outre, il y a lieu d'impliquer le fournisseur d'infrastructures de Swissdec pour pouvoir définir ultérieurement comment passer de l'authentification TLS unilatérale actuellement utilisée à une authentification de client TLS basée sur un certificat.

9.3 Processus SUA et navigation dans les différents systèmes ERP

Une attention particulière a été portée à la convivialité (tant en matière de mise en service que d'exploitation) lors de l'élaboration des processus et des éléments de sécurité. S'agissant de la mise en œuvre concrète des processus SUA dans les systèmes ERP, il convient également d'entretenir le dialogue avec les concepteurs concernés et, le cas échéant, de définir certaines règles pour uniformiser autant que possible la représentation des processus et, par conséquent, la navigation dans les systèmes.

9.4 Remise par voie postale

Dans le cadre du processus d'enregistrement, on considère que la vérification de l'identité de l'entreprise comprend l'envoi d'un courrier (recommandé ou A Plus) à une personne responsable de l'entreprise via un second canal, non électronique. Ce courrier devrait être remis en mains propres. Les conditions cadres, processus et coûts liés à ce mode de remise d'un tel courrier devront être déterminés en concertation avec les services postaux compétents.
Sans doute suffirait-il aussi d'envoyer un courrier recommandé contenant des informations de contact personnelles mais SANS remise en mains propres pour clore l'enregistrement de l'entreprise avec un degré de confiance suffisamment élevé.
Quel type d'accord faudrait-il conclure à cet effet avec la Poste? La Poste offre-t-elle déjà un service qui permettrait au répartiteur de déléguer l'envoi d'un courrier recommandé contenant les données nécessaires?

9.5 Enregistrement d'entreprises sans relation contractuelle avec des A&A

Pour l'heure, l'enregistrement à la SUA nécessite obligatoirement l'existence d'un contrat conclu avec une assurance ou l'utilisation d'un certificat réglementé. Si la norme SUA venait à être adoptée pour d'autres processus (comme le

[30] https://letsencrypt.org/

[31] https://www.ech.ch/fr/standards/54046

[32] https://cabforum.org/wp-content/uploads/CA-Browser-Forum-EV-Guidelines-v1.6.8.pdf chapitre 9.2.4, page 11

prélèvement de l'impôt à la source), il faudrait examiner d'autres possibilités d'enregistrement, par exemple sur la base d'une relation existante avec une autorité fiscale.

9.6 Consultation du registre IDE de l'OFS

L'accès aux informations figurant dans le registre IDE de l'OFS peut être bloqué pour le public, mais pas pour l'administration (cf. eCH-0108 – Norme concernant les données registre d'identification des entreprises, point 3.2.2.2). Il faudrait à ce titre consulter l'OFS pour savoir si Swissdec peut faire office d'administration (p. ex. pour le compte de l'Office fédéral de la statistique) afin de bénéficier d'un accès complet aux données du registre.
Sinon, il est aussi possible, pour comparer les données lors de l'enregistrement (cf. point 6.1.1), de demander à l'entreprise un extrait écrit du registre IDE.

9.7 Renouvellement d'un certificat sans interruption des processus

Les changements de certificats peuvent engendrer des problèmes en cas de processus de longue durée, par exemple pour la norme suisse en matière de prestations (KLE). Ce genre d'erreurs se produirait moins souvent lors de la vérification des signatures si le certificat SUA était fourni à chaque message signé. Le destinataire pourrait ainsi mettre à jour ses clés. Lors du cryptage de messages, le risque est accru si l'expéditeur n'est pas en mesure de mettre à jour les clés à utiliser et crypte sa réponse avec des clés «périmées». Selon les processus concernés, il faudrait définir des mesures permettant de régler ces problèmes, par exemple en faisant en sorte que le certificat soit envoyé à chaque tentative de scrutation.

10 Liste des illustrations

11 Liste des tableaux

12 Glossaire

Office fédéral de la statistique (OFS)
Office statistique de la Suisse, installé à Neuchâtel.

Certification Authority (CA)
Organisation émettant les certificats numériques. Un certificat numérique sert à attribuer une clé publique spécifique à une personne ou à une entité.[33]

Chaîne de certification
Sert à contrôler un certificat numérique en utilisant la CA émettrice comme ancre de confiance pour vérifier la hiérarchie du certificat, ce qui permet de juger de la crédibilité de l'éditeur du certificat.[34]

Certificate Signing Request (CSR)
Format standardisé de demande d'un certificat numérique. La CSR contient la clé publique d'une paire de clés. L'instance d'enregistrement doit s'assurer de son authenticité.[35]

Données d'identification
Les données d'identification permettent de confirmer à un système l'identité d'un autre système ou d'un utilisateur. Leur utilisation présuppose une identité connue dans le système. Généralement, le système / l'utilisateur s'authentifie en indiquant un identifiant et un élément d'authentification.[36]

Declaration-ID
Ce numéro d'identité est déjà utilisé par le système actuel et correspond à un cas d'affaires donné. Le transmetteur n'envoie pas de Declaration-ID dans sa requête initiale. Ce numéro est ajouté par le répartiteur dans ses messages pour simplifier les demandes de renseignements adressées au support.

OeIDI
Ordonnance du DFF concernant les données et informations électroniques

Système ERP
Un système ERP est un logiciel complexe ou un ensemble de logiciels applicatifs / systèmes informatiques communiquant entre eux et dont le but est d'aider à planifier les ressources de l'entreprise dans son ensemble.[37]

OCSP
Le protocole **Online Certificate Status Protocol** (**OCSP**) permet de consulter le statut de certificats X.509 auprès d'un service de validation. Voir également la RFC 6960.

Privacy Enhanced Mail (PEM) – Format de fichier
Format de fichier fréquemment utilisé pour enregistrer des clés et des certificats X.509 au moyen d'un encodage base64.[38]

Confirmation spécialisée
Cette forme de confirmation intervient au niveau spécialisé /du contenu entre l'émetteur et le destinataire. Une confirmation spécialisée est liée à un processus donné et peut s'étendre sur une longue période.

Mot de passe d'enregistrement (RegPw)
Le but principal du mot de passe d'enregistrement est de s'assurer qu'un certificat signé et, le cas échéant, la paire de clés privée / publique sont attribués au bon destinataire (système ERP) et à lui seul. Il permet donc d'authentifier l'entreprise.

Requests for Comments (RFC)
Les «Requests for Comments» (RFC, demandes de commentaires) sont un ensemble de documents techniques et organisationnels rédigés par l'éditeur RFC sur Internet (initialement appelé Arpanet), dont la création remonte au 7 avril 1969.[39]

RSA
RSA (Rivest, Shamir et Adleman) est un algorithme de cryptographie asymétrique pouvant être utilisé à des fins de cryptage et de signature numérique.[40]

[33] https://fr.wikipedia.org/wiki/Autorit%C3%A9_de_certification

[34] http://en.wikipedia.org/wiki/Chain_of_trust

[35] https://fr.wikipedia.org/wiki/Demande_de_signature_de_certificat

[36] https://en.wikipedia.org/wiki/Credential

[37] https://fr.wikipedia.org/wiki/Progiciel_de_gestion_int%C3%A9gr%C3%A9

[38] https://en.wikipedia.org/wiki/Privacy-enhanced_Electronic_Mail

[39] https://fr.wikipedia.org/wiki/Request_for_comments

[40] https://fr.wikipedia.org/wiki/Chiffrement_RSA

SHA256
SHA-2 (de l'anglais secure hash algorithm, algorithme de hachage sécurisé) désigne les quatre fonctions de hachage cryptographique SHA-224, SHA-256, SHA-384 et SHA-512, standardisées en 2001 par l'institut américain NIST pour succéder au SHA-1.[41]

SOAP
SOAP (de l'anglais «Simple Object Access Protocol») est un protocole réseau permettant l'échange de données entre des systèmes et la réalisation d'appels de procédure à distance. SOAP est un standard industriel du World Wide Web Consortium (W3C).[42]

Sécurité au niveau du transport (canal sécurisé)
La sécurité au niveau du transport comprend la transmission des données via un canal TLS (HTTPS) sécurisé. Le système de l'émetteur et celui du destinataire se sont authentifiés et ont convenu d'une clé de session permettant d'authentifier et de crypter les données à transférer.

Sécurité au niveau du message
La sécurité au niveau du message concerne l'authentification supplémentaire et le cryptage des données utiles sur un canal sécurisé. Dans le cas de Swissdec, les messages SOAP sont protégés à l'aide du protocole Web Services Security.

Mot de passe de verrouillage (SperrPw)
Le mot de passe de verrouillage sert à authentifier l'entreprise lorsque cette dernière demande le verrouillage d'un certificat émis.

Subject Information
Il s'agit des informations contenues dans un certificat X.509 concernant l'organisme pour lequel le certificat a été émis.

Authentification d'entreprises Swissdec (SUA)
Processus et conditions techniques requises pour l'identification univoque d'entreprises dans le cadre des processus d'affaires Swissdec.

Confirmation de la transaction
Seule la transmission d'un message est ici confirmée. La forme du message (syntaxe, signature, sémantique, etc.) est vérifiée par le système du destinataire final et intégrée à la confirmation. La vérification du contenu du message fait partie de la confirmation spécialisée. Une confirmation de transaction doit donc être fournie dans un délai défini, faute de quoi l'émetteur peut considérer la fourniture d'un message comme ayant échoué et peut renvoyer le message correspondant.

Transmetteur
Le transmetteur constitue l'interface entre le système ERP et Swissdec. Le système ERP prépare les données à envoyer et les transmet au composant du transmetteur qui envoie au répartiteur les données conformément aux règles Swissdec, via un canal sécurisé. Le transmetteur valide les déclarations XLM du système ERP pour un processus donné selon le schéma de validation XSD Swissdec officiel. Les données sont ensuite transférées par le transmetteur via le canal sécurisé (HTTPS) sous une forme sécurisée (signées et cryptées). Le transmetteur est aussi en charge de l'ensemble du traitement des erreurs, de la réception des réponses du répartiteur et de la vérification de la confirmation de la transaction. Qui plus est, le transmetteur assure l'archivage et la consignation des messages.

Transport Layer Security (TLS) / Secure Sockets Layer (SSL)
«Transport Layer Security» (TLS, littéralement «sécurité de la couche de transport»), plus connu sous son ancien nom «Secure Sockets Layer» (SSL), est un protocole de cryptage hybride permettant de sécuriser la transmission de données via Internet.[43]

Numéro d'identification d'entreprise (IDE-OFS)
Numéro utilisé depuis janvier 2011 par l'Office fédéral de la statistique (OFS) pour toutes les entreprises économiquement actives en Suisse, comme identifiant univoque pour tous les contacts avec des autorités.[44]

Registre IDE de l'OFS
Registre officiel de la Confédération dans lequel sont enregistrées toutes les entreprises économiquement actives sous un identifiant univoque. Le registre IDE de l'OFS est disponible à l'adresse suivante: https://www.uid.admin.ch

Uniform Resource Identifier (URI)

[41] https://fr.wikipedia.org/wiki/SHA-2

[42] https://fr.wikipedia.org/wiki/SOAP

[43] https://fr.wikipedia.org/wiki/Transport_Layer_Security

[44] https://www.bfs.admin.ch/bfs/fr/home/registres/registre-entreprises/numero-identification-entreprises.html

Un «Uniform Resource Identifier» (URI, identifiant uniforme des ressources) est composé d'une suite de caractères permettant d'identifier des ressources abstraites ou concrètes.[45]

A&A
Les assurances et autorités sont les entités qui reçoivent des données et informations de la part des entreprises dans le cadre des processus d'affaires Swissdec.

Profil d'assurance (VProfil)
Informations sur les relations contractuelles entre une entreprise et une assurance.

OSCSE
Ordonnance du 23 novembre 2016 sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques

WS-Security (WSS)
Le protocole «Web Services Security» (WS-Security, WSS) est globalement une extension de SOAP intégrant des aspects relatifs à la sécurité des services Web.

Certificat X.509
Norme d'infrastructure de clé publique visant la création de certificats numériques spécifiés dans la RFC 5280.

SCSE
Loi fédérale du 18 mars 2016 sur la signature électronique (état: 1er janvier 2017)

[45] https://fr.wikipedia.org/wiki/Uniform_Resource_Identifier

13 Bibliographie

[1] A. Laube, G. Hassenstein und A. Böhm, «Swissdec Unternehmens-Authentifizierung - Detailspezifikation - Ergänzung Registrierung mit ZertES,» 2019.

14 Suivi des versions

Version	Date	Description	Auteur
1.0	20.7.18	Rédaction de la première version des spécifications détaillées	Annett Laube
1.1	8.11.18	Mise à jour / modification concernant WSDL	Annett Laube
1.2	31.1.19	Externalisation de l'enregistrement / la configuration selon la SCSE	Annett Laube
1.3	4.4.19	Description de l'enregistrement des fiduciaires	Annett Laube
1.4	26.4.19	Modification du certificat SUA, adaptation de la mise en page	Annett Laube
1.5	10.5.19	Modification du contenu du certificat SUA, des exigences relatives aux CSR et de l'exemple de certificat en annexe	Gerhard Hassenstein

Annexe A

Exemple de certificat IDE:

Certificate:
- Version:
  - Version 3
- Serial Number:
  - 00:01:02:03
- Certificate Signature Algorithm:
  - PKCS #1 SHA-256 With RSA Encryption
- Issuer:
  - CN = Swissdec Root Certificate Authority
  - OU = Digital Certificate Services
  - O = Swissdec
  - C = CH
- Validity:
  - Not Before:
    - 13.10.18, 09:58:30 (13.10.18, 07:58:30 GMT)
  - Not After:
    - 13.10.19, 09:58:30 (13.10.19, 07:58:30 GMT)
- Subject:
  - **CN = NTRCH-CHE-123.456.789@swissdec.ch**
  - **OU = Finanzabteilung**
  - **O = Huggentobler AG**
  - **L = Langnau**
  - **ST = Bern**
  - **C = CH**
  - **Object Identifier (2 5 4 97) = NTRCH-CHE-123.456.789**
- Subject Public Key Info:
  - Subject Public Key Algorithm:
    - PKCS #1 RSA Encryption
  - Subject's Public Key:
    - Modulus (2048 bits):
    - c7 67 67 1f ca e4 10 28 12 e8 64 95 38 4e 74 01
    - 11 f3 96 70 24 1a c8 bd 82 02 6c 7a 4b 10 87 60
    - 4a 18 f8 af ea 46 ea 86 bd 6a 20 b0 da 77 76 e6
    - d2 9d f2 7f bf 2a 15 f3 e4 36 e6 80 38 66 97 b4
    - df 33 f1 56 c0 82 a5 63 d4 22 0f ea 86 36 40 67
    - e6 c9 f3 5b 43 1e 56 cc 94 cd 1d 53 88 5b 9b 5e
    - 2f b0 3f 85 6c cc 16 df 7c fd 59 f7 f2 7a af 36
    - b5 6f 7b 73 b7 22 48 ef 49 45 0f 35 ad 24 f0 c4
    - 93 b9 a7 cf 7b 2d 77 cb b3 29 bf dd 02 53 d0 3a
    - f2 38 d1 2d e1 b5 f2 e5 dd 06 16 e5 49 b3 c0 0d
    - 2e 41 68 b2 f4 f9 01 40 57 79 f7 e7 ea e6 1c 15
    - c7 74 ca 4c 47 87 b1 f8 7e 4c 0b dc 5a ec 5a f1
    - 87 d7 cf 8f cb b4 53 50 a6 4b 9d 3c 3a 5c a1 11
    - cf b1 1e 23 0d 6c 0b 04 d2 d9 d5 83 14 0a 4c d0
    - a6 a4 90 2d 65 36 2e c7 fd 8d 0f 7b d2 3f bf 37
    - 57 d9 9a a2 db 1a 99 2d be a0 e2 27 7e 73 1e 3d
    - Exponent (24 bits):
    - 65537
- Extensions:
  - Certificate Authority Key Identifier:
    - Not Critical
    - Size: 20 Bytes / 160 Bits
    - 37 41 ec 21 1c a9 3e d7 aa 9c 19 96 d0 72 df ed 45 04 d1 15
  - Authority Information Access:

Not Critical
OCSP: URI: https://ocsp.swissdec.ch/sua-issuer
CA Issuers: URI: https://ca.swissdec.ch/sua-issuer.crt
Certificate Policies:
Not Critical
2.16.756.1.83.23.0:
Certification Practice Statement pointer:
https://www.swissdec.ch/cps
CRL Distribution Points:
Not Critical
URI: https://crl.swissdec.ch/sua-issuer.crl
Certificate Key Usage:
Critical
keyEncipherment
digitalSignature
Extended Key Usage:
TLS Web Client Authentication
Document Signing
Certificate Subject Key ID:
Not Critical
Size: 20 Bytes / 160 Bits
64 a8 a2 ab c9 ee 2f 89 47 2c 56 f3 bd 4f c8 26 23 26 23 f7
Certificate Signature Algorithm:
PKCS #1 SHA-256 With RSA Encryption
Certificate Signature Value:
Size: 256 Bytes / 2048 Bits
43 b9 b6 b6 71 13 62 9c 6c 13 23 ab 53 87 06 a3
58 59 53 b6 18 1a d2 8e 0b 2f 4e 0b 24 77 e3 8a
04 ac 84 c6 5c 13 e8 42 64 47 e4 ee e9 b1 4d 19
df 04 bf 43 20 0c 1f f9 c1 14 a6 81 12 a1 27 57
6e b6 d6 80 46 da 8f fb 50 fa ef 05 a5 f2 d2 29
1d f3 60 97 02 2b c7 e5 5f 82 f7 3f 26 12 57 33
f9 ba ad dc ca e7 4f a5 ff ef 3e 9e 47 e9 af 89
ea a0 55 66 7f 13 e4 e4 3b 72 3f a8 64 a0 d9 e5
1c ca ad de e2 2d 7e d9 2f 7f 36 ac b1 7b 91 97
68 fe 01 65 8b e6 ec 8c 22 a8 9a ba 8a 99 a0 48
8e 50 7b b2 04 7d 95 47 fd 48 69 d1 80 1d 31 1c
53 02 f1 55 b1 58 a6 e2 67 a0 76 83 1d 09 e2 80
d9 0d f8 a2 70 ea 88 b2 42 e3 6e ce 91 5a dd 8d
13 6b 25 e7 17 0c be fb 1e 33 8e 52 2f 07 a5 e6
a7 62 52 2d a0 ff 6d 6d 33 54 01 0b 54 05 5b 39
5d 56 39 b0 67 67 63 68 c9 d1 e1 07 17 ed a5 b0