swissdec

Autentificazione delle aziende

Specifica dettagliata

Versione

Versione aggiornata	Edizione 10.05.2019, versione 1.5

Data attuale:	12.05.2021
Data di registrazione:	01.04.2020
Data di stampa:	12.05.2021
Progetto:	Richtlinien.docx
Commento:	Riproduzione autorizzata con citazione della fonte

La specifica dettagliata per l'autentificazione delle aziende è stata elaborata in collaborazione con:

- Associazione Swissdec
- Scuola universitaria professionale Berna (Tecnologia e informatica)
  - Stefan Agosti, Annett Laube, Gerhard Hassenstein, Pascal Mainini, Anton Böhm

Editore

Swissdec
Fluhmattstrasse 1
6004 Lucerna
www.swissdec.ch

Indice

1 Introduzione

1.1 Contesto

La piattaforma centrale d'informazione per la standardizzazione dello scambio elettronico di dati gestita dall'Associazione Swissdec consente già oggi di trasmettere i dati salariali in modo completamente elettronico grazie allo «Standard salari CH (ELM)». Attualmente è in fase di sviluppo lo «Standard prestazioni CH (KLE)», basato su questo stesso sistema e concepito come sua estensione, che consentirà di gestire l'intero processo dalla notifica di una richiesta fino all'erogazione della prestazione. I programmi di contabilità salariale certificati Swissdec e i sistemi ERP permettono quindi di semplificare le procedure delle aziende, stilare dichiarazioni corrette e ridurre l'onere amministrativo.
La gestione elettronica dei processi di business, dalla notifica dei casi (ad es. notifica di infortunio all'assicuratore) fino al conteggio dell'indennità giornaliera, comporta ulteriori requisiti in termini di identificazione e autentificazione delle imprese coinvolte nel processo.
Nella prima fase di elaborazione dell'autentificazione delle aziende Swissdec sono stati definiti gli obiettivi e i requisiti relativi al sistema auspicato. Su tali basi è stato elaborato un progetto di soluzione che funge da quadro di riferimento per implementare, a livello tecnico, l'autentificazione delle imprese coinvolte utilizzando l'IDI dell'UST. La presente specifica dettagliata si basa sulla soluzione così definita e contiene le indicazioni per l'implementazione del sistema nella fase pilota.

1.2 Obiettivo del documento

La specifica dettagliata descrive in modo approfondito l'implementazione e le caratteristiche dei processi SUA già integrati nella soluzione che riguardano la registrazione, la configurazione iniziale, l'esercizio (durata), il rinnovo e il blocco dell'identità aziendale. I requisiti di sicurezza dei processi Swissdec sono illustrati in modo ancora più dettagliato in base ai requisiti definiti per la SUA nella soluzione; sono inoltre descritte le modalità di implementazione dei processi mediante i certificati IDI Swissdec. La specifica stabilisce con precisione anche i requisiti per le credenziali (password, certificati IDI) da utilizzare nei vari processi.
La specifica dettagliata rappresenta quindi il punto di partenza per la realizzazione del sistema nella fase pilota. Servirà a implementare gli standard e i modelli della specifica e a verificarne la praticabilità. L'esperienza acquisita con questa prima applicazione pratica dovrà essere tenuta in considerazione durante l'elaborazione di nuove versioni della specifica dettagliata.

1.3 Inquadramento

I contenuti della specifica dettagliata si concentrano su una prima realizzazione del sistema di autentificazione delle aziende Swissdec nella fase pilota. Le varianti previste nella soluzione sono state limitate il più possibile. Inoltre, per i singoli componenti della specifica viene indicata la possibilità di attuazione dal punto di vista tecnico. Le indicazioni qui contenute prendono come riferimento le conoscenze disponibili in contesti analoghi e si basano rigorosamente su approcci consolidati fondati sulle prassi migliori (best practice). Tuttavia, una prima applicazione pratica potrebbe portare alla luce eventuali lacune o problemi che dovranno poi essere risolti in una versione successiva della specifica.
Proprio come il progetto di soluzione, anche la specifica dettagliata del sistema di autentificazione delle aziende Swissdec si limita a illustrare l'autentificazione univoca e sicura delle imprese nell'ambito della comunicazione con il distributore Swissdec e le A&A come destinatari finali. La presente specifica comprende i processi di autentificazione nel quadro della comunicazione automatizzata da macchina a macchina (m2m), tra il sistema ERP (trasmettitore) e il distributore, nonché a livello di back-end, tra il distributore e i sistemi dei destinatari finali. Sono invece illustrati in un documento separato altri casi d'uso che pure richiedono un'autentificazione (come l'accesso di un utente a un portale di assicurazioni o a un portale Swissdec).
La presente specifica affronta solo in via marginale i processi di business specialistici, ad esempio nel quadro dello Standard salari CH (ELM) o dello Standard prestazioni CH (KLE). Ove necessario, eventuali adeguamenti di direttive preesistenti o future per quanto riguarda la compatibilità con la SUA sono di competenza dei rispettivi gruppi di lavoro Swissdec.

1.4 Obiettivi e requisiti

Il documento «Autentificazione delle aziende Swissdec – Progetto di rilevamento dei requisiti e di soluzione» (versione 1.1) illustra gli obiettivi e i requisiti elaborati nella prima fase del progetto, utilizzati come base per la specifica

dettagliata e descritti in modo approfondito nel capitolo 2. Il capitolo 8 precisa in che misura i singoli requisiti sono stati effettivamente contemplati nel presente documento.

1.5 Panoramica dell'architettura Swissdec

Per comprendere meglio il contesto in cui si applica la SUA, in questa sezione presentiamo in sintesi l'architettura Swissdec.
La piattaforma centrale per lo scambio di dati, ossia il distributore Swissdec, consente di ottimizzare e automatizzare i processi tra circa 200 000 aziende e i relativi assicuratori e autorità sul territorio svizzero. Allo stato attuale (2018) i soggetti partecipanti scambiano ogni anno più di 12 milioni di dati personali concernenti i salari.

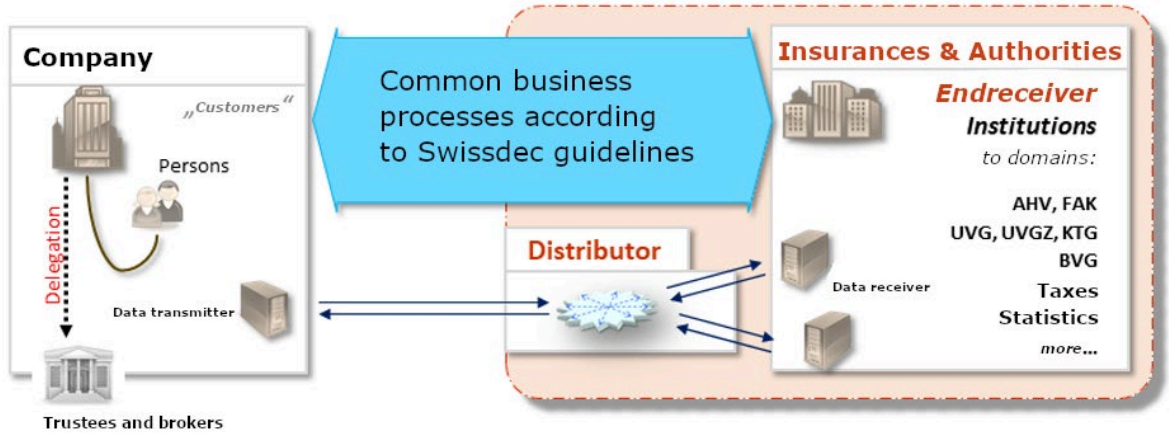

Fig. 1: Panoramica dei processi Swissdec

I partecipanti al processo sono:

- le aziende con i rispettivi sistemi ERP e i relativi produttori ERP, che comunicano mediante un «trasmettitore»;
- gli assicuratori e le autorità con i rispettivi sistemi di back-end specialistici, che comunicano mediante «destinatari finali».

I sistemi collegati in questo processo comunicano tramite interfacce m2m utilizzando protocolli standardizzati.

La problematica relazione n:m tra «aziende» e «assicurazioni e autorità» viene risolta grazie a un distributore centrale, che la trasforma in una semplice relazione «n:distributore:m» (vedi Fig. 2). Il distributore comunica con le aziende per conto di assicurazioni e autorità e trasmette i dati al destinatario finale dopo averli verificati e filtrati.
In questo processo, il distributore Swissdec agisce in veste di rappresentante dei destinatari finali (assicurazioni e autorità) nei confronti delle aziende.[1] In tale ruolo il distributore gode della piena fiducia dei destinatari finali e provvede a gestire e assicurare, a loro nome, i processi di comunicazione nei confronti dei sistemi ERP delle aziende. Quanto ai contenuti, il distributore si limita a trasmettere i messaggi. La responsabilità della correttezza tecnica dei messaggi e dei processi di business compete esclusivamente ai sistemi dei destinatari finali e delle aziende.
L'utilizzo del distributore Swissdec offre i seguenti vantaggi:

- Semplificazione delle attività di sviluppo, test e produzione per le aziende, dato che i sistemi ERP comunicano solo con il distributore.
- Riduzione delle ridondanze di dati e processi.
- Design-firewall, che consente di evitare conflitti tra diverse versioni a livello del distributore grazie a una trasformazione. Il ciclo di vita delle versioni è gestito in modo fluido e intelligente.
- Garanzia di qualità dinamica (GQ, plausibilizzazione) e filtraggio dei dati sul distributore.
- Nessun salvataggio dei dati sul distributore, vale a dire che la comunicazione tra azienda e assicurazioni e autorità avviene «in tempo reale» (7 giorni su 7, 24 ore su 24).

[1] La funzione di «rappresentante» del distributore Swissdec, nonché i ruoli e gli obblighi dei partecipanti al processo sono definiti nelle Condizioni generali per l'uso del distributore, si veda https://www.swissdec.ch/it/condizioni-generali/.

- I produttori SW per trasmettitore e destinatario finale sono controllati e certificati da Swissdec in modo da garantire una qualità elevata a livello di interoperabilità e dati e una funzionalità «plug and play» per i partecipanti ai processi.

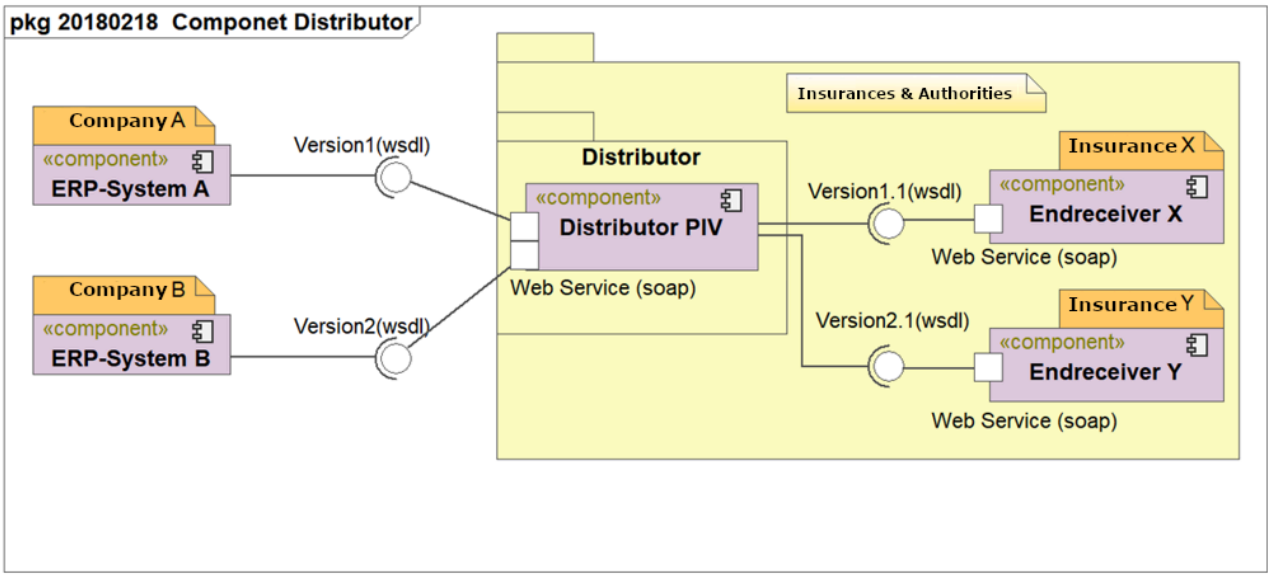

Fig. 2: Relazioni di comunicazione Swissdec

Dal punto di vista tecnico, l'architettura del sistema si basa su servizi web in cascata che generano una chiamata sincrona dal trasmettitore (sistema ERP) al destinatario finale (assicurazioni e autorità) passando per il distributore. In questo modo si stabilisce, attraverso il distributore, una connessione «in tempo reale» che consente ai sistemi di interagire fra loro con determinati vincoli temporali (processi «time-critical») nell'ambito del processo m2m. I servizi web sono protetti mediante il canale sicuro a livello di trasporto (SSL/TLS) e inoltre tramite soluzioni di sicurezza standardizzate di WSS (Web Services Security; SOAP Message Security: signature+encryption).

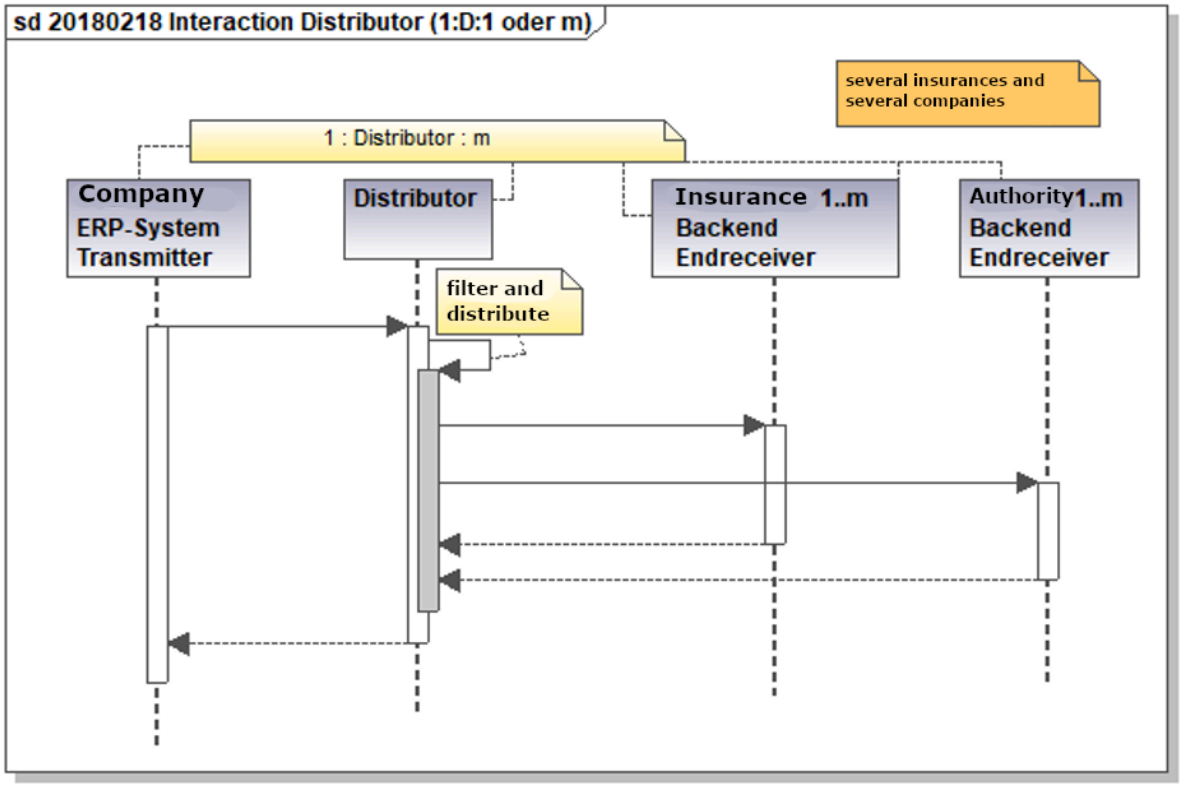

Fig. 3: Comunicazione 1:distributore:m

I processi «time-critical» sono eseguiti in modo asincrono: in altre parole, il trasmettitore riacquista il controllo subito dopo la chiamata e cerca di ottenere la risposta in un secondo momento mediante polling.

2 Requisiti di sicurezza dei processi Swissdec

In questa sezione presentiamo i requisiti di sicurezza previsti per la comunicazione nei processi Swissdec. I requisiti contenuti nel progetto di soluzione (vedi anche Tabella 14 capitolo 8) sono descritti in modo più preciso e ne vengono illustrati di nuovi, previsti fra l'altro dallo «Standard prestazioni CH (KLE)» sviluppato in parallelo.

2.1 Canale sicuro

L'architettura Swissdec prevede che tutte le comunicazioni tra il sistema ERP di un'azienda, il distributore Swissdec e i sistemi dei destinatari finali (assicurazioni e autorità) siano protette a livello di trasporto (SSL/TLS) mediante un canale sicuro. Dal punto di vista tecnico, per garantire la sicurezza è senz'altro opportuno prevedere un obbligo di autentificazione reciproca basata su certificato (cifratura SSL a 2 vie) per il collegamento a livello di trasporto.

- Estensione del requisito A-16 (Autorizzazione del sistema ERP).

2.2 Autentificazione a livello di messaggi

Per l'estensione dei suoi servizi, Swissdec richiede inoltre un'autentificazione univoca di tutte le parti interessate a livello di messaggi (mediante la firma dei dati trasmessi).

- Estensione del requisito A-17 (Autenticazione dell'azienda) e A-19 (Autentificazione dell'azienda)

2.3 Riservatezza a livello di messaggi

Per poter proteggere in modo ancor più efficace le informazioni trasmesse contro vettori di attacchi nonostante l'uso di un canale sicuro, i contenuti inviati devono essere criptati per il rispettivo destinatario.

- Nuovo requisito A-27 (Riservatezza a livello di messaggi)

2.4 Ambiente operativo

A seconda del processo, i dati da firmare possono essere molto cospicui e talvolta è necessario firmarli nel giro di poco tempo. Il processo di firma richiede pertanto prestazioni elevate sia a livello del sistema ERP che del distributore Swissdec. In passato i certificati software hanno permesso di rispondere a questa esigenza, poiché le applicazioni potevano accedere in modo semplice e rapido alla chiave di firma in qualsiasi momento.

- Estensione del requisito A-17 (Autenticazione dell'azienda)

2.5 Non disconoscibilità

Lungo l'intero processo di comunicazione, nessuna delle entità coinvolte deve poter negare di avere inviato o ricevuto dati. La non disconoscibilità è un requisito imprescindibile affinché un'azione risulti vincolante.
L'obiettivo è garantire che l'invio e la ricezione di dati e informazioni non possano essere contestati. A tal proposito si distinguono due casistiche:

- *Non disconoscibilità dell'origine*: un mittente che invia uno specifico messaggio non deve poter negare a posteriori di averlo inviato.
- *Non disconoscibilità della ricezione*: un destinatario che riceve un messaggio inviato non deve poter negare a posteriori di averlo ricevuto.
- *Prova di connessione:* nei processi soggetti a vincoli temporali («time-critical»), un mittente che invia uno specifico messaggio deve poter dimostrare a posteriori di averlo inviato.

Di conseguenza deve essere possibile ricostruire e tracciare integralmente qualsiasi processo di comunicazione anche in un momento successivo. Nessuno dei mittenti coinvolti in uno scambio di dati deve poter negare di avere inviato un determinato messaggio dopo la trasmissione, e nessun destinatario deve poter contestare la ricezione di un messaggio dopo averlo ricevuto.

- Estensione del requisito A-20 (trasparenza)

2.6 Carattere vincolante

Sulla base dei dati trasmessi vengono corrisposte prestazioni assicurative. È quindi importante che i processi di comunicazione siano a tutti gli effetti incontestabili mediante il requisito della «non disconoscibilità». Per soddisfare questo requisito, tutti i dati e le informazioni rilevanti concernenti una determinata comunicazione (incl. firma e timestamp) devono essere registrati e archiviati.

- Estensione del requisito A-20 (trasparenza)

2.7 Registrazione

Le procedure di identificazione e registrazione delle aziende per il rilascio di certificati IDI devono essere svolte da Swissdec. A tal fine, la verifica dell'identità di un'impresa può basarsi su relazioni preesistenti con le aziende richiedenti. Solo così è possibile automatizzare in parte il processo di registrazione, riducendo le formalità burocratiche pur garantendo la massima sicurezza.

- Estensione del requisito A-09 (Centro di registrazione), A-10 (Identificazione univoca dell'azienda), A-11 (Identificazione mediante centro autorizzato)

3 Certificati Swissdec

Per soddisfare i suddetti requisiti Swissdec richiede, nell'ambito dell'autentificazione delle aziende, una serie di certificati a diversi livelli e in diversi campi di applicazione.
La Fig. 4 mostra i vari sistemi e i rispettivi tipi di certificati richiesti e installati. I capitoli che seguono illustrano le destinazioni d'uso dei vari certificati.

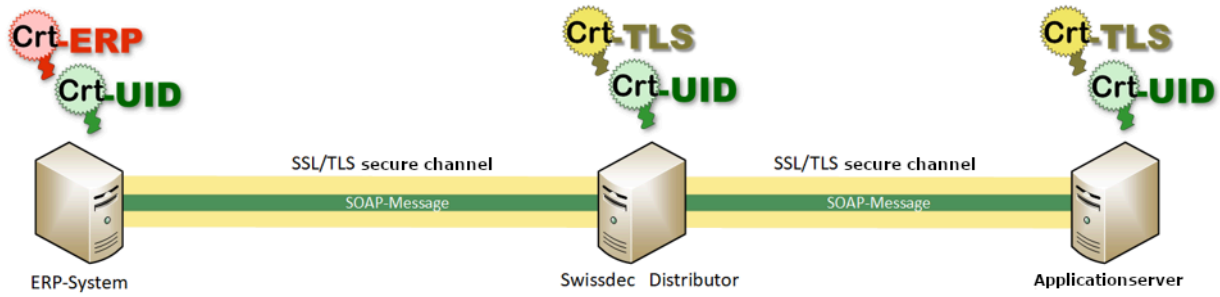

Fig. 4: Panoramica dei certificati Swissdec

3.1 Certificati IDI Swissdec

I dati a livello SOAP vengono firmati e criptati. A tal fine il trasmettitore, il distributore e i sistemi dei destinatari finali utilizzano i certificati IDI Swissdec, che presentano specifici requisiti a livello di contenuti, come descritto al paragrafo 5.1.5.
Dato che i certificati IDI si utilizzano sia per firmare che per cifrare i messaggi SOAP, in linea di principio sarebbe opportuno utilizzare due diversi certificati per ogni applicazione.
Ma poiché questi dati vengono criptati solo per un breve periodo di tempo necessario al trasporto e non devono essere salvati in forma criptata per poi essere decifrati in un secondo momento, non è necessario archiviare chiavi private. Di conseguenza, onde evitare inutili complicazioni nella gestione dei certificati IDI, non bisogna prevedere restrizioni d'uso e conviene permettere di utilizzare un solo certificato per le operazioni di autenticazione, firma e cifratura.
Il destinatario deve sempre confermare lo scambio dei dati in ogni singola fase di comunicazione. Anche questa conferma di transazione viene firmata con il certificato IDI.

3.2 Certificati server SSL/TLS

A livello di trasporto vengono utilizzati certificati server SSL/TLS sia presso il distributore che presso i destinatari finali. In base alla sezione e alla direzione della comunicazione, un'istanza può fungere da server o da client. A tale riguardo è bene lasciare all'operatore la possibilità di utilizzare due diversi certificati o uno soltanto. Per questi sistemi, tuttavia, bisogna utilizzare i certificati IDI Swissdec, in qualità di certificati client Web TLS, per l'autenticazione a livello di trasporto.
Il trasmettitore del sistema ERP di un'azienda può invece rivestire soltanto il ruolo di client. A tale scopo bisogna impiegare esclusivamente i certificati IDI Swissdec come client Web TLS.
I certificati server Web TLS possono essere emessi da Certification Authority (CA) pubbliche o da una CA interna all'azienda. Se si utilizzano certificati di una CA pubblica, il relativo fornitore dovrebbe essere membro del CAB Forum[2] e munito di certificazione Webtrust[3].
Se le direttive di un destinatario finale ammettono l'autentificazione di un interlocutore solo con certificati di un'infrastruttura PKI interna, in tal caso può essere emesso, per il distributore, un certificato client Web TLS di una CA interna all'azienda.

3.3 Certificati ERP Swissdec

In un sistema ERP, la capacità di processo in funzione della versione è attestata in un altro certificato. Questi certificati, utilizzati anche a livello SOAP per firmare i messaggi, dovrebbero essere emessi anche in futuro da una Certification Authority interna di Swissdec. Swissdec distingue a tal proposito due categorie di CA interne:

- CA1, che emette certificati per uso operativo;

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

- CA2, che emette certificati per ambienti di sviluppo.

3.4 Altri certificati

3.4.1 Registrazione con certificati di terzi

Per la registrazione, le aziende possono utilizzare certificati regolamentati rilasciati a persone giuridiche ai sensi dell'art.7 FiEle da una CA accreditata (vedi processo «Registrazione con certificato regolamentato secondo FiEle» al par. 6.1.2)

3.4.2 Certificati per utenti

In una fase successiva, Swissdec richiederà anche certificati per l'autentificazione degli utenti. Su questo fronte sono disponibili certificati semplici, avanzati o regolamentati per persone fisiche. Al momento non è ancora stato definito quale tipo di certificato verrà utilizzato: la questione sarà trattata in un documento separato.

4 Sicurezza e fiducia

La sicurezza della comunicazione e la fiducia nelle procedure elettroniche tra l'azienda (trasmettitore), il distributore e il sistema del destinatario finale si fondano su tre pilastri:

1. canale di trasporto autenticato e sicuro
2. sicurezza e fiducia a livello di messaggi (messaggio SOAP)
3. carattere vincolante della trasmissione di messaggi mediante conferma di transazione

4.1 Canale di trasporto autenticato e sicuro

Il certificato IDI si applica a due livelli. Come si vede nella Fig. 5, in una connessione SSL/TLS a 2 vie il sistema ERP lo utilizza per autenticarsi con il reverse proxy a monte.

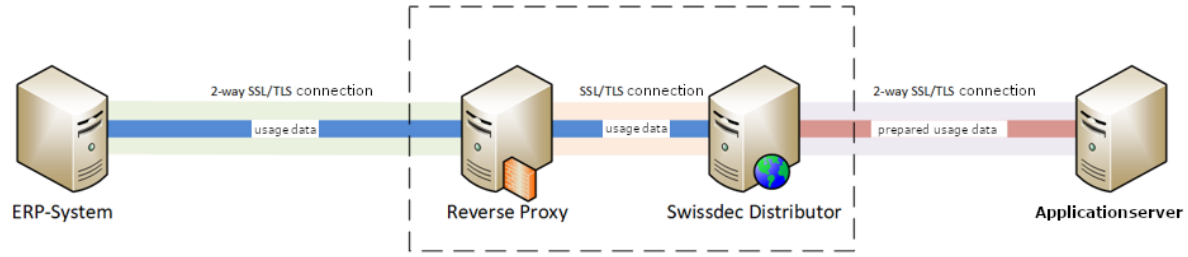

Fig. 5: Fasi di comunicazione SUA

In tal modo il sistema di reverse proxy a monte del distributore Swissdec, costituito da diversi componenti in cascata (tra cui SSL/TLS reverse proxy e web application firewall), è in grado di verificare l'autenticità dei pacchetti in entrata già a livello di trasporto.
Il trasmettitore firma con il proprio certificato IDI l'header SOAP dei dati utente e li cripta con il certificato IDI del distributore. Il reverse proxy inoltra i dati utente invariati al distributore Swissdec mediante una seconda connessione SSL/TLS.

Solo chi dispone di un certificato IDI valido può inviare pacchetti al distributore Swissdec. L'endpoint TLS controlla a monte il certificato,
alleggerendo così il carico di lavoro del distributore.

Il reverse proxy può verificare l'autenticità di un messaggio, ma non può leggerne i contenuti in quanto precedentemente criptati per il distributore.

Il distributore controlla la firma SUA dei dati utente, verificando così l'origine e l'integrità dei dati. Nel percorso inverso il distributore invia i dati utente al sistema ERP, anche in questo caso firmati e criptati con il certificato IDI.
Dopodiché, i messaggi fra il distributore e i sistemi dei destinatari finali continuano a essere protetti a livello di trasporto utilizzando i protocolli SSL/TLS. Come nella prima sezione di comunicazione, il distributore trasmette i dati utente dopo averli firmati e criptati.

4.2 Sicurezza e fiducia a livello di messaggi (messaggio SOAP)

Come illustrato nella sezione precedente, l'header SOAP viene firmato con il certificato IDI in quanto parte dei dati utente. In questa fase vengono firmate sia le richieste inviate dal sistema ERP al distributore (Request), sia le rispettive risposte del distributore al sistema ERP (Response). La struttura dei relativi messaggi per quanto riguarda firma e cifratura è descritta in maggiore dettaglio qui di seguito ed è illustrata nella Fig. 6.
Osservando i messaggi che il sistema ERP invia al distributore, noteremo che ciascuno di essi contiene un timestamp (<wsu:Timestamp>) nell'header. Il timestamp è firmato con certificato ERP e certificato IDI. La firma con certificato ERP consente di verificare la capacità di processo del sistema ERP che invia il messaggio. Tale firma va conservata, in quanto le valutazioni statistiche raccolte dal distributore si basano sulle informazioni contenute nel certificato ERP.

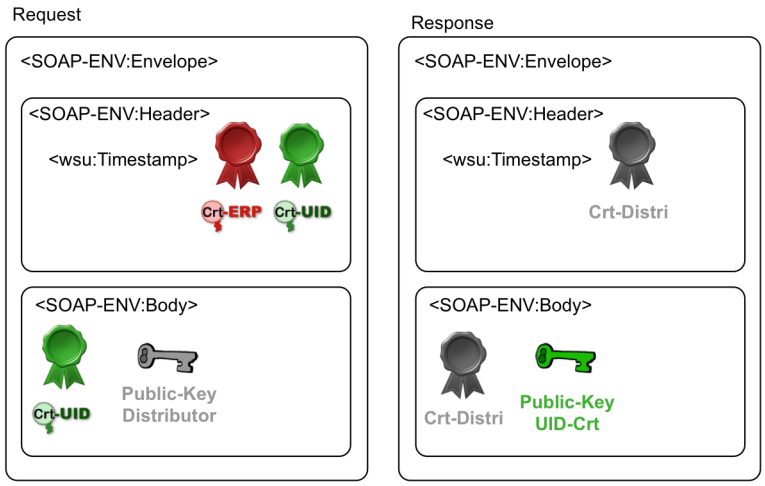

Fig. 6: Autenticazione con certificati IDI

La firma del timestamp con il certificato IDI consente di verificare l'origine di un messaggio già dal suo header, permettendo così al distributore di accertare se il mittente del messaggio sia o meno autorizzato. Questa verifica è importante soprattutto perché, a differenza del «body» del messaggio, ossia il contenuto vero e proprio, le informazioni incluse nell'header non vengono criptate. Il distributore è quindi in grado di verificare le firme del timestamp senza dover prima decifrare il messaggio.
Anche il corpo (body) di un messaggio viene firmato dal mittente con un certificato IDI per assicurare l'integrità e l'autenticità dei relativi contenuti. Dopodiché l'intero body viene cifrato con una chiave pubblica (public key) del distributore per garantirne la riservatezza.
La risposta del distributore al sistema ERP contiene anch'essa un timestamp nell'header, firmato con il certificato IDI del distributore. Il corpo del messaggio viene firmato con il certificato IDI del distributore per assicurarne ancora una volta l'integrità e l'autenticità. A questo punto il body viene criptato con la public key del certificato IDI del sistema ERP che riceve il messaggio.
Ogni volta che viene scambiato un messaggio, i certificati utilizzati vengono inviati nell'header senza la relativa catena. Il vantaggio è che in questo modo i partecipanti alla comunicazione non devono salvare i certificati. Tuttavia, per motivi di sicurezza, la catena del certificato deve essere preventivamente scambiata e archiviata per poter poi verificare il certificato in questione. Le informazioni già presenti permettono di effettuare un efficace controllo preliminare del messaggio, consentendo così di rilevare precocemente e bloccare eventuali attacchi al distributore. Rispetto alla situazione attuale (solo certificato ERP), il messaggio conterrà informazioni aggiuntive sul mittente (contenuto del certificato IDI, vedi sezione 5.1). Queste informazioni saranno contenute nella parte non criptata del messaggio, ma saranno sufficientemente protette dagli attacchi grazie al canale sicuro allestito in precedenza. Il fatto che in futuro le informazioni sul mittente verranno pubblicate nel certificato non andrà quindi a compromettere il livello di sicurezza, ed è giustificato dai vantaggi che si otterranno in termini di verifica preliminare dei messaggi.

4.3 Non disconoscibilità

Occorre garantire il carattere vincolante dello scambio di dati (tracciabilità) lungo l'intero processo di trasporto dei messaggi Swissdec (vedi Requisito 2.6), così da poter verificare la trasmissione a posteriori in qualsiasi momento. Come già illustrato nella sezione 4.1, le aziende e i destinatari finali comunicano passando per il distributore, che funge quindi da intermediario nella comunicazione da macchina a macchina. Tutti i pacchetti di comunicazione inviati passano infatti attraverso il distributore.
I meccanismi riepilogati in questo capitolo illustrano i comportamenti generali che le entità coinvolte (trasmettitore, distributore e destinatario finale) devono seguire per garantire correttamente il carattere vincolante delle informazioni e dei dati trasmessi in relazione a un caso Swissdec.

4.3.1 Requisiti

In linea di massima si devono rispettare i seguenti presupposti e requisiti:

- In caso di errore di comunicazione del distributore (ad es. per un problema tecnico), un tentativo di invio viene interrotto dai partner di comunicazione dopo un certo timeout, quindi viene registrato e ripetuto in un momento successivo. Il gestore del distributore informa i partner di comunicazione in merito a eventuali guasti o anomalie.
- Un evento viene sempre attivato dal sistema ERP di un'azienda (trasmettitore).

- Dopo l'attivazione di un nuovo evento da parte dell'azienda, il distributore genera un ID (identificativo) interno che identifica in modo univoco l'evento e il successivo scambio di messaggi tra l'azienda e i destinatari finali coinvolti. Il distributore inoltra l'ID a tutti i sistemi partecipanti, ovvero lo restituisce in una conferma. L'ID così generato si può utilizzare come numero di caso da indicare in una richiesta di supporto, o per tracciare una transazione o un intero caso (trasparenza).
- Tutti i sistemi coinvolti in un processo di comunicazione devono disporre di un certificato Swissdec per l'azienda (certificato IDI) e fare affidamento, in qualità di «relying party», sull'emittente del certificato (c.d. «àncora di fiducia» o trust anchor).
- Per completare un caso possono essere necessari diversi messaggi, che si possono protrarre per un periodo di tempo indefinito.
- Il sistema ERP di un'azienda deve interrogare periodicamente lo stato corrente di un caso per confrontarlo con l'assicuratore.
- I messaggi di conferma (conferme) inviati dal sistema destinatario devono pervenire al mittente entro un determinato tempo massimo ammesso.

4.3.2 Procedura di scambio messaggi Swissdec

Per poter creare un sistema in grado di conservare in modo affidabile i messaggi per poi tracciare integralmente un caso, occorre innanzitutto definire un meccanismo di comunicazione comune e uniforme indipendentemente dai processi che vi si dovranno eseguire. Il modello di comunicazione Swissdec previsto per lo Standard salari (ELM) e già utilizzato per lo Standard prestazioni (KLE) si può suddividere in due fasi:

1. inizializzazione di un evento
2. scambio di informazioni tecnico-specialistiche

Le due fasi dispongono di modelli di comunicazione caratteristici che si possono sintetizzare e descrivere come segue:
Fase 1 - 1:D:n: tipico modello per l'inizializzazione di un evento. L'azienda segnala un nuovo evento per uno o più sistemi di destinatari finali (1). Il distributore riceve la segnalazione e conferma la ricezione direttamente all'azienda. Il distributore elabora i dati relativi all'evento (2) e li distribuisce in base al numero dei sistemi di destinazione (3). Ognuno di questi sistemi conferma a sua volta la ricezione direttamente sul distributore. Nel frattempo il sistema ERP può interrogare il distributore per richiedere lo stato della distribuzione al destinatario finale (4). La richiesta può partire più volte [loop 1,n], finché non pervengono tutte le conferme e il distributore è in grado di notificare all'azienda, nelle proprie informazioni di stato, che la distribuzione è andata a buon fine.

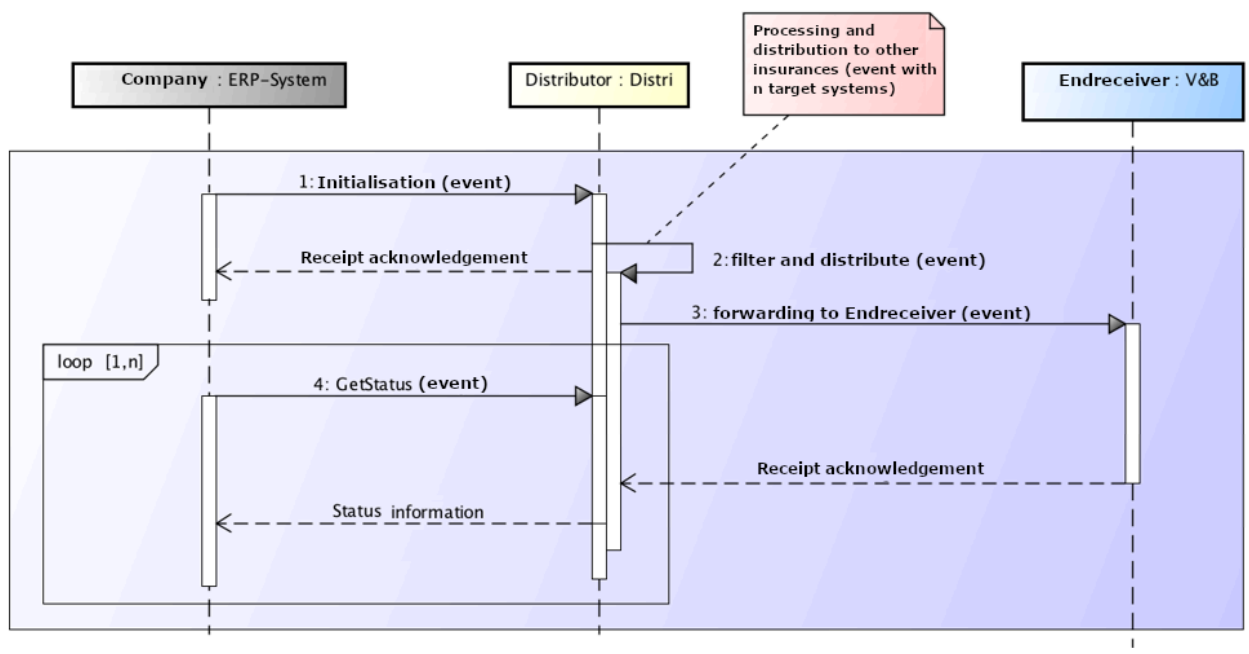

Fig. 7: Procedura di comunicazione relativa all'inizializzazione (1:D:n)

Fase 2 - 1:D:1: a seconda dello standard utilizzato (Standard salari o Standard prestazioni) e in base al caso specifico, il sistema ERP dell'azienda può interrogare indirettamente i singoli destinatari finali tramite il distributore circa lo stato o l'esito di un messaggio specifico (5). Il distributore inoltra la richiesta al sistema del destinatario finale interessato (6), che invia la risposta pertinente in base allo stato del processo. Questo messaggio può contenere una

richiesta di conferma (facoltativa) per il sistema ERP dell'azienda. Se il sistema destinatario richiede una conferma, il sistema ERP la fornisce in risposta al distributore (7), che a sua volta la inoltra (8). Infine il sistema destinatario attesta la ricezione della conferma. Questo flusso di messaggi può ripetersi più volte in base alla risposta e all'andamento del processo [loop 0,n].

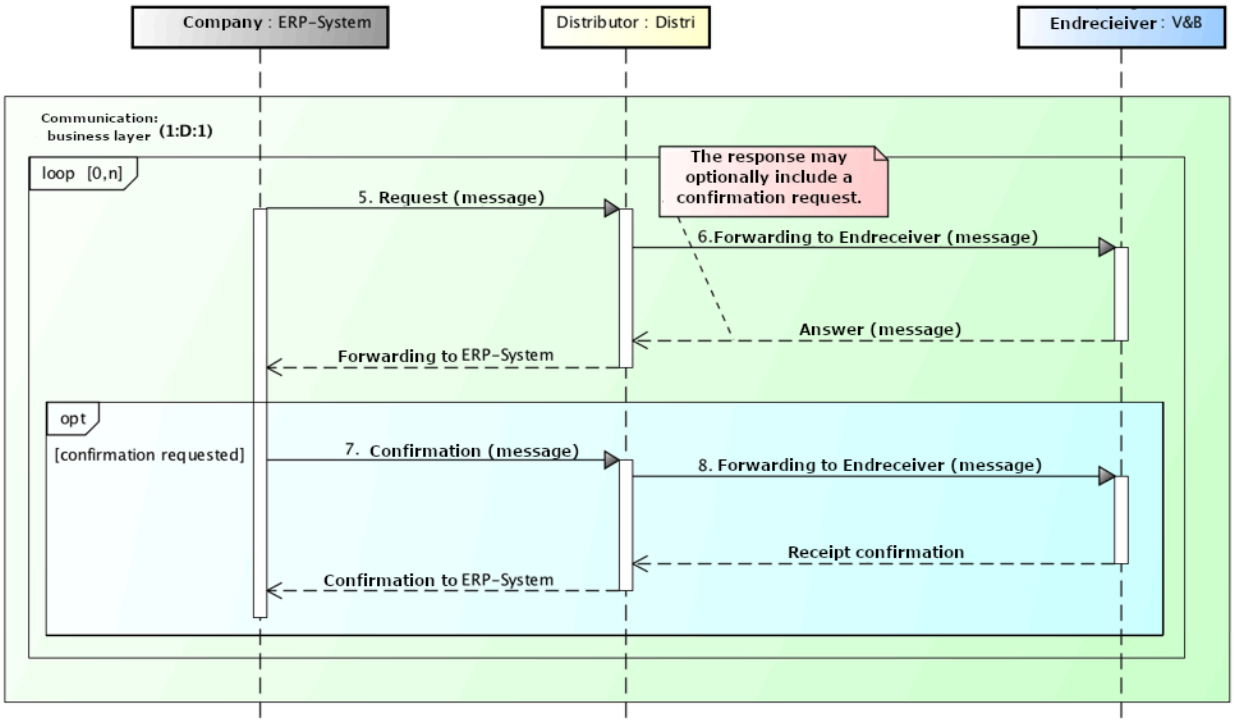

Fig. 8: Procedura di comunicazione relativa al flusso di messaggi tecnico-specialistici (1:D:1)

La tabella che segue riepiloga i requisiti relativi alla non disconoscibilità a livello tecnico-specialistico in un processo di comunicazione Swissdec. A tale proposito si tenga presente che è sempre e solo l'azienda a poter avviare lo scambio di comunicazioni.

	Azienda *(client)*	**Assicurazioni e autorità** *(server)*
Non disconoscibilità dell'origine dei dati (invio)	*Messaggio firmato*	*Messaggio firmato*
Non disconoscibilità della ricezione	*Conferma tecnico-specialistica*	*Conferma firmata*

4.3.3 Non disconoscibilità dell'origine dei dati

Per garantire la non disconoscibilità dell'origine dei dati vanno rispettati i seguenti requisiti:

- Ogni messaggio deve essere firmato da un sistema mittente (trasmettitore, distributore, destinatario finale) con un certificato IDI a livello SOAP, in modo da poterne attribuire correttamente l'origine a uno specifico mittente ed assicurarne l'integrità.
- Ogni sistema destinatario deve esaminare la firma IDI contenuta nell'header SOAP e confrontarla con la catena di certificati, fino al certificato radice.
- Se la verifica della firma IDI dà esito negativo, il messaggio ricevuto va respinto e deve essere generato un messaggio di errore da trasmettere al mittente.

4.3.4 Non disconoscibilità dell'avvenuta ricezione
Per garantire la non disconoscibilità della ricezione vanno rispettati i seguenti requisiti:

- Per i *sistemi server*: se la verifica del messaggio dà esito positivo, il destinatario (distributore, destinatario finale) lo deve confermare inviando un messaggio di risposta firmato (Response), che deve contenere la firma del messaggio ricevuto in origine dal mittente. Questo requisito si può implementare tecnicamente a livello di protocollo con una Web Service Security *Signature Confirmation*.
- Per i *sistemi client*: quando il sistema ERP di un'azienda conferma la ricezione di un messaggio, deve firmare e rispedire al mittente parti rilevanti del messaggio ricevuto. In questo caso la conferma deve avvenire a livello specialistico, in quanto non esiste una modalità tecnica a livello di protocollo.
- Il mittente del messaggio originale deve esaminare la firma IDI contenuta nella risposta (Response) e confrontarla con la catena di certificati, fino al certificato radice.
- Se la verifica della firma IDI dà esito negativo, la risposta ricevuta va respinta e deve essere generato un messaggio di errore.

4.3.5 *Prova di connessione:* affinché un sistema ERP possa dimostrare a posteriori di avere inviato un determinato messaggio in processi soggetti a vincoli temporali, tutti i pacchetti di richiesta inviati dal sistema ERP al distributore devono essere firmati e riconfermati dal distributore stesso.

4.3.6 Garanzia di trasparenza (tracciabilità)
Per poter garantire la trasparenza di un intero processo di comunicazione Swissdec (set di transazioni relative a un determinato caso) è necessario che il distributore, in qualità di intermediario, memorizzi tutte le informazioni di connessione (relazioni). In genere, durante lo scambio di informazioni tra i partner di comunicazione, il distributore elabora ancora i dati trasformandoli a livello di contenuti (mapping) e così facendo distrugge la firma del mittente originale. Di conseguenza anche lo stesso distributore dovrà firmare i pacchetti in uscita.
La firma di un messaggio Swissdec contiene sostanzialmente:

- un valore di hash del contenuto firmato;
- un riferimento al contenuto firmato nel corpo del messaggio;
- un timestamp basato sull'ora corrente del sistema;[4],
- informazioni chiave.

Il distributore deve memorizzare le seguenti informazioni relative a una procedura di comunicazione:

- numero di caso;
- firma di ogni messaggio ricevuto;
- firma di ogni messaggio trasformato e inviato;
- la versione del software del distributore;
- il modello di comunicazione (1:D:n, 1:D:1).

Il distributore **non** salva in modo permanente i contenuti dei messaggi: si limita a conservare per un breve periodo i contenuti della comunicazione nella sua «memoria di lavoro». Il contenuto dei messaggi deve quindi essere salvato autonomamente dai partner di comunicazione. A tal proposito vanno rispettate le seguenti linee guida:

- Ciascun mittente (azienda o assicuratore) memorizza il messaggio in chiaro dopo averlo firmato e prima di inviarlo, di modo che il messaggio in questione si possa di nuovo leggere in un momento successivo.
- Il destinatario (azienda o assicuratore) verifica la firma di un messaggio ricevuto e lo archivia non criptato secondo i propri regolamenti interni.

Per ricostruire integralmente un caso, è necessario mettere insieme i dati e le informazioni di tutti i partner coinvolti relativi al processo di comunicazione nonché i dati di connessione del distributore. In caso di controversia sarà quindi possibile tracciare un errore involontario o un comportamento errato.

[4] È consigliabile che i partecipanti Swissdec dispongano di una base temporale comune (server NTP)

5 Credenziali SUA

Per l'autentificazione delle aziende Swissdec è importante utilizzare certificati avanzati basati su specifiche proprie. Sebbene con ciò venga meno il fondamento giuridico della FiEle di cui al paragrafo 5.1.6, l'impiego di questi certificati «propri» risulta più flessibile e lascia maggiori margini di manovra.

5.1 Certificati IDI

5.1.1 Uso previsto dei certificati IDI
Dato che i certificati IDI si utilizzano sia per firmare che per cifrare i messaggi SOAP, sarebbe opportuno utilizzare due diversi certificati per tali applicazioni (uno per la crittografia e uno per l'autenticazione / firma). Ma poiché questi dati vengono criptati solo per il breve lasso di tempo necessario al trasporto e non devono essere salvati in forma criptata per poi essere decifrati in un secondo momento, non è necessario archiviare la chiave privata.
Di conseguenza, onde evitare inutili complicazioni nella gestione dei certificati IDI (soprattutto a carico dei sistemi ERP), non sono previste restrizioni d'uso e si utilizza *un* solo certificato per le operazioni di autenticazione, firma e cifratura.

5.1.2 Forme di emissione
In linea di massima i certificati IDI sono emessi come certificati software X.509[5] da una Certificate Authority (CA) incaricata a tal fine e trasmessi in modo sicuro ai sistemi destinatari, dove si installano automaticamente. Ove prescritto dai requisiti di sicurezza di un'azienda, è senz'altro possibile fornire il materiale chiave del certificato IDI su hardware certificato dell'impresa in questione. In tal caso il processo per la registrazione o l'emissione del certificato rimane invariato.

5.1.3 Gestione delle chiavi private
La coppia di chiavi per un certificato IDI viene generata nell'ambiente sicuro dell'azienda (sistema ERP o hardware specifico); di conseguenza non è possibile creare un backup della chiave privata, poiché né Swissdec né la CA emittente sono in possesso della chiave privata del certificato IDI. Ogni azienda dovrà quindi provvedere, tramite la propria infrastruttura, a conservare la chiave privata in un ambiente sicuro e fare in modo che le applicazioni autorizzate vi possano accedere in ogni momento. Per quanto riguarda i soft token, la chiave privata deve essere salvata in forma leggibile da un sistema ERP. Se invece i requisiti di sicurezza di un'azienda prescrivono l'emissione e l'archiviazione di chiavi private solo su hardware certificato (hard token, HSM), è necessario garantire che il sistema ERP sia sempre in grado di accedere al relativo materiale chiave salvato su tale hardware.

5.1.4 CP/CSP
Per i certificati IDI Swissdec la Certificate Authority emittente deve creare una Certificate Policy (CP) e un Certificate Practice Statement (CPS) secondo quanto previsto dall'RFC 7382[6].

5.1.5 Contenuto di un certificato IDI
A prescindere dal tipo di supporto, i certificati IDI devono contenere le seguenti informazioni:

Denominazione	Descrizione
Versione	Versione certificato (secondo RFC 5280: versione 3)
Serial Number	Identificazione univoca del certificato. Secondo le specifiche della CA emittente.
Certificate Signature Algorithm	Specifica dell'algoritmo di firma del certificato; segue lo standard attualmente più comune ed è armonizzato con la CA che emette il certificato. Requisito minimo: SHA256 with RSA Encryption (Key size 2048 bit)
Issuer	Informazioni sull'ente che emette il certificato (CA):

[5] Network Working Group, 2008. RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, online: https://www.ietf.org/rfc/rfc5280.txt (03.11.2015).

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

		commonName, organizationName, organizationalUnitName, countryName[7]
Validity		Periodo di validità del certificato: 1 anno
Subject		Informazioni sul titolare del certificato (vedi Tabella 2)
Subject Public Key Info		Informazioni sulla chiave del titolare del certificato
	Public Key Algorithm	Algoritmo Public key
	Subject's Public Key	Public key del titolare del certificato
Extensions:		
	Authority Key Identifier	Identificazione della public key in uso presso l'emittente del certificato
	Authority Information Access	URI per ulteriori informazioni relative all'emittente del certificato: OCSP, CA Issuers
	Certificate Policies	Riferimento (URI) a ulteriori requisiti (di natura tecnica, giuridica, processuale) da osservare per l'impiego del certificato rilasciato. Per accertare la necessità di tali requisiti ed eventualmente elaborarli si consulta il responsabile della protezione dei dati di Swissdec.
	CRL Distribution Points	URI riferito a una Certificate Revocation List (CRL) della Certificate Authority (CA) emittente
	Key Usage	Destinazione d'uso della chiave contenuta nel certificato: *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	Identificazione di un certificato con una specifica public key
Signature Algorithm		Specifica concernente l'algoritmo di firma del certificato
Signature Value		Firma del certificato

Tabella 1: Elementi di un certificato IDI

Le informazioni sul titolare del certificato sono ricavate, in parte automaticamente, dal registro d'identificazione delle imprese dell'UST. L'unità organizzativa (OrganizationalUnit, OU) può essere indicata liberamente dall'azienda. La tabella che segue illustra gli attributi relativi al titolare del certificato contenuti nel certificato stesso e la relativa origine.

[7] In questo punto (opzionale) può essere indicato anche il numero d'identificazione delle imprese dell'emittente del certificato, ad esempio IDI di Swissdec: Object Identifier (2 5 4 97) = NTRCH-CHE-113.865.903

Abbr.	Denominazione	Contenuto	Fonte	Priorità
CN	commonName	NTRCH-{UID-BFS}@swissdec.ch[8]	Registro d'identificazione delle imprese dell'UST	OBBLIGATORIO
O	organizationName	<Name> (nome) iscritto nel registro d'identificazione delle imprese dell'UST	Registro d'identificazione delle imprese dell'UST	OBBLIGATORIO
OU	organizationalUnitName	Sottounità dell'organizzazione, si può selezionare liberamente ed è collegabile in cascata	Input utente	FACOLTATIVO
L	localityName	Sede dell'azienda come risulta dal registro d'identificazione delle imprese, <town> (città) iscritta nel registro d'identificazione delle imprese	Registro d'identificazione delle imprese dell'UST	OBBLIGATORIO
ST	stateOrProvinceName	Cantone in cui ha sede l'azienda, <locality> (località) iscritta nel registro d'identificazione delle imprese	Registro d'identificazione delle imprese dell'UST	OBBLIGATORIO
C	countryName	<country> (Paese) iscritto nel registro d'identificazione delle imprese	Registro d'identificazione delle imprese dell'UST	OBBLIGATORIO
IDI	OID 2.5.4.97	OrganizationIdentifier: numero d'identificazione delle imprese iscritto nel registro d'identificazione delle imprese dell'UST, NTRCH-{UID-BFS}	Registro d'identificazione delle imprese dell'UST	OBBLIGATORIO
BC	OID 2.5.4.15	Business Category (Private Organization o Government Entity)[9]	Registro d'identificazione delle imprese dell'UST	FACOLTATIVO[10]

Tabella 2: Attributi del titolare del certificato (Subject)

A titolo facoltativo, è possibile inserire nel Subject del certificato IDI le informazioni relative all'indirizzo dell'impresa interessata, che si potranno verificare solo al momento dell'emissione del certificato. Non è obbligatorio inserirle in quanto possono subire variazioni durante il periodo di validità del certificato stesso.

Informazioni opzionali nel 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) → vedi ST
- OID 1.3.6.1.4.1.311.60.2.1.3: (Country) → vedi C
- OID 2.5.4.15 (BusinessCategory): indica il tipo di organizzazione. In linea di massima si può distinguere tra *Private Organization*, *Business Entity*, *Non-Commercial Entity* o *Government Entity*.

È anche possibile registrare le informazioni relative alla RA (Registration Authority) nella parte «Extensions» (Estensioni). Questa opzione, tuttavia, è opportuna solo se i certificati IDI devono essere utilizzati anche in contesti diversi da Swissdec.

[8] Conforme all'identificatore *legal person semantics identifier* di cui alla norma ETSI EN 319412-1, cap. 5.1. (http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.00_30/en_31941201v010100v.pdf)

[9] Qui si potrebbe anche riprendere la voce <legal Form> presente nel registro d'identificazione delle imprese dell'UST.

[10] Come convenuto con QuoVadis, nel certificato SUA non viene indicata la Business Category.

Informazioni facoltative per *Certificate Subject Alt Name*:

- Object Identifier (2 5 4 97) = {UID-BFS}
- Object Identifier (2 5 4 13) = IDI dell'UST dell'impresa (Enterprise)

Informazioni facoltative per *Certificate Issuer Alt Name*:

- Object Identifier (2 5 4 97) = {UID-BFS}
- Object Identifier (2 5 4 13) = validatore dell'IDI dell'UST dell'impresa

➔ L'Allegato A riporta un esempio di certificato IDI.

5.1.6 Impiego di certificati regolamentati per l'autentificazione delle aziende Swissdec

Da accertamenti con l'Ufficio federale delle comunicazioni (UFCOM) è risultato che la revisione completa della FiEle[11], l'Ordinanza relativa alla revisione della Legge federale sulla firma elettronica (OFiEle)[12] e gli emendamenti all'Ordinanza concernente dati ed informazioni elettronici (OeIDI)[13] non semplificherà per Swissdec la procedura di autentificazione delle aziende. La revisione completa della FiEle prevede, fra l'altro, la definizione dei formati dei certificati regolamentati per le seguenti applicazioni:

1. la firma elettronica di una persona fisica o il sigillo elettronico di un'unità IDI
2. l'identificazione elettronica di una persona fisica o unità IDI
3. il criptaggio di dati elettronici

Per quanto concerne l'utilizzo dei certificati di cui ai punti 2 e 3, i documenti summenzionati non contengono ulteriori indicazioni. A tal proposito le prescrizioni tecniche e amministrative (PTA) relative alla FiEle[14] rimandano alla norma europea (EN) ETSI 319 411, che prevede la possibilità di emettere un certificato avanzato utilizzato per l'identificazione elettronica anche sotto forma di «soft token». Ma come sottolineato nella presa di posizione di Swissdec del 28 luglio 2016 relativa alle versioni preliminari di FiEle, OFiEle e PTA, le condizioni quadro per l'utilizzo di certificati regolamentati per l'identificazione elettronica nella comunicazione da macchina a macchina non sono chiare. In particolare non è chiaro se l'emissione di questi certificati sia legata o meno a un token hardware, né come si debba svolgere il processo di registrazione e quali oneri comporterebbero i certificati emessi in questa forma.
Pertanto, indipendentemente dagli sviluppi a livello di certificati regolamentati sul mercato svizzero, per il momento Swissdec ha deciso di restare fedele al suo approccio originale che prevede l'impiego di certificati avanzati basati su specifiche proprie per l'*autentificazione delle aziende Swissdec*.

5.2 Certificate Signing Request (CSR)

Un CSP mette a disposizione un'interfaccia standardizzata (CSR o CMP[15]) che permette a Swissdec di elaborare automaticamente una richiesta (Request) con le informazioni sul titolare (Subject) secondo le indicazioni riportate qui di seguito nella Tabella 3. La struttura della richiesta di certificato elettronico da utilizzare è standardizzata ed nel formato PKCS#10[16]. Una CSR deve contenere le seguenti informazioni sul titolare (Subject) e sulla chiave:

Denominazione	Descrizione
Subject	Informazioni sul titolare del certificato, quali commonName (CN), organizationName (O), organizationalUnitName (OU), localityName (L), stateOrProvinceName (ST), countryName (C), oltre all'IDI dell'azienda (OID 2.5.4.97) → per maggiori dettagli vedi Tabella 2
PublicKey	Chiave pubblica del titolare del certificato (chiave RSA a 2048 bit)

Tabella 3: Attributi di una Certificate Signing Request (CSR)

[11] Revisione completa (FiEle)

[12] Revisione completa dell'ordinanza sulla firma elettronica (OFiEle)

[13] Adeguamento dell'ordinanza concernente dati ed informazioni elettronici (OeIDI)

[14] PTA: Prescrizioni tecniche e amministrative dell'UFCOM

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

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

5.3 Standard di crittografia

Si suppone che tutti i sistemi coinvolti utilizzino gli algoritmi crittografici e le dimensioni di chiave (key size) attualmente raccomandati. La selezione degli algoritmi crittografici in uso è affidata a un sistema differente in base alla sezione di comunicazione interessata (cfr. Fig. 5). A tale proposito si applica il seguente principio:

> Tutti i componenti coinvolti nella comunicazione (incluso il trasmettitore) devono supportare gli algoritmi previsti per la SUA.

Gli algoritmi e le dimensioni di chiave minimi ammessi devono soddisfare le seguenti raccomandazioni e direttive:

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

Inoltre, i gestori dei servizi di server web dovrebbero assicurare una configurazione del server web conforme alle raccomandazioni formulate dalla Internet Engineering Task Force (IETF) nell'RFC 7525.

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

5.4 Password SUA

Nei processi SUA descritti di seguito si utilizzano due diverse password: la password di registrazione e quella di blocco. Entrambe vengono inviate in forma scritta tramite lettera (ossia su un secondo canale non elettronico), dal distributore o da un'A&A all'azienda che richiede la registrazione.

5.4.1 Password di registrazione

La funzione principale della password di registrazione consiste nel garantire che un certificato firmato venga attribuito solo ed esclusivamente al destinatario corretto (sistema ERP). In altre parole, serve ad autenticare l'azienda. Si distinguono i seguenti scenari:

- Scenario 1: generazione di una coppia di chiavi (keypair) da parte del sistema ERP (vedi paragrafo 6.2.1)
  L'ERP genera una coppia di chiavi pubblica / privata (private / public key pair), e viene inviata al distributore una Certificate Signing Request (CSR) conforme al formato PKCS#10.
  In questo caso la password serve solo ad autenticare l'ERP nei confronti del distributore. Poiché l'autenticazione online avviene con l'invio della CSR, è possibile implementare una protezione efficace contro attacchi bruteforce sul lato del distributore (limitando il numero di tentativi ammessi, impostando timeout ecc.) .
- Scenario 2: hard token (vedi paragrafo 6.2.4)
  La coppia di chiavi con il relativo certificato viene consegnata all'azienda su un «hard token» con il relativo PIN. Per maggiori dettagli al riguardo si rimanda alla CA interessata. Il distributore è comunque coinvolto nel processo come istanza di autentificazione (Registration Authority).

5.4.2 Password di blocco

La password di blocco consente di autenticare l'azienda nel caso in cui intenda far bloccare un certificato emesso (vedi sezione 6.6). A tal fine dovrà trasmettere la password una sola volta a Swissdec, dopodiché il certificato verrà bloccato e quindi revocato presso la Certificate Authority (CA). In seguito sarà necessario avviare un nuovo processo di registrazione.

5.4.3 Requisiti per le password

Per la creazione delle password sono previsti i seguenti requisiti:

ID	Denominazione	Descrizione	Priorità
AP-01	Lunghezza password	Il più breve possibile e lunga quanto necessario.	OBBLIGATORIO
AP-02	Facilità d'uso	Dato che vengono consegnate in forma scritta tramite lettera, le password devono essere ben leggibili e semplici da digitare.	OBBLIGATORIO
AP-03	Checksum (somma di controllo)	Il checksum consente di controllare la correttezza nel momento in cui viene digitato.	OBBLIGATORIO
AP-04	Unicità	Un'entropia sufficientemente grande garantisce l'unicità delle password anche quando vengono emesse in grandi quantitativi.	OBBLIGATORIO

AP-05	Emissione	Per ogni singola azienda (IDI dell'UST) esiste una sola password di registrazione valida in un determinato momento.	OBBLIGATORIO
AP-06	Identificatore	La password contiene un componente liberamente definibile, ad es. per identificare l'emittente o la versione.	OBBLIGATORIO
AP-07	Cifratura	È garantita l'idoneità per la cifratura di formati di file per il trasporto di certificati e relativo materiale chiave.	FACOLTATIVO

Tabella 4: Requisiti per le password SUA

5.4.4 Creazione di password

Il processo di generazione delle password si articola come segue:

1. generazione di variabili casuali mediante un generatore di numeri pseudocasuali crittograficamente sicuro (CSPRNG[17])
2. mappatura della variabile casuale su un set di caratteri ridotto e creazione di una password della lunghezza predefinita (12 caratteri)
3. aggiunta di un identificatore (2 caratteri)
4. calcolo del checksum secondo ISO/IEC 7064, MOD 1271-36 (vedi esempio di codice) e aggiunta delle cifre di controllo (2 caratteri)
5. segmentazione in blocchi di quattro caratteri (vedi esempio)
6. memorizzazione in una banca dati mediante Key Derivation Function[18] (KDF)

Vanno inoltre rispettati i seguenti requisiti strutturali:

Set di caratteri ridotto	Numeri: 2345689 Lettere maiuscole: ABCDEFGHJKLMNPQRTUVWXYZ Sono esclusi: 1, 7, 0, O, S
Lunghezza password	12 caratteri (escl. cifre di controllo e identificatore)
Identificatore	2 caratteri
Cifre di controllo	Calcolo secondo ISO/IEC 7064, MOD 1271-36 2 caratteri
Segmentazione	Quattro blocchi da quattro caratteri, separati da un trattino, per un totale di 16 caratteri
Key Derivation Function	Argon2[19] (algoritmo vincitore del concorso «Password Hashing Competition»[20])

Tabella 5: Requisiti per la struttura delle password SUA

5.4.5 Esempio di password

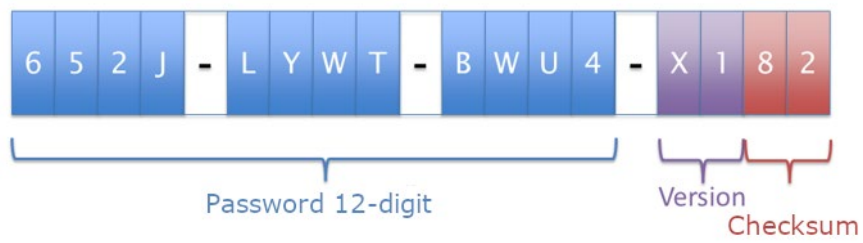

Fig. 9: Esempio di password SUA

5.4.6 Esempio di codice per l'implementazione

Al seguente link è possibile consultare un esempio di implementazione dello standard ISO/IEC 7064, MOD 1271-36 per ambiente Java:

[17] https://it.wikipedia.org/wiki/Generatore_di_numeri_pseudocasuali_crittograficamente_sicuro

[18] https://it.qaz.wiki/wiki/Key_derivation_function

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

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

https://github.com/danieltwagner/iso7064/blob/master/src/main/java/com/github/danieltwagner/iso7064/Mod1271_36.java

Ad ogni modo, in caso di riuso di un codice di terze parti occorre effettuare un rigoroso controllo per verificarne la correttezza. Bisogna inoltre tenere conto del copyright.

6 Processi SUA

Il processo globale di autentificazione delle aziende si articola in quattro fasi: registrazione, configurazione, esercizio e rinnovo / blocco (del certificato).
La Figura 10 qui di seguito mostra i due assi principali lungo i quali si sviluppa il processo, con i rispettivi componenti più importanti in ciascuna delle quattro fasi. Nei capitoli che seguono sono illustrate nei dettagli le singole fasi dei processi.

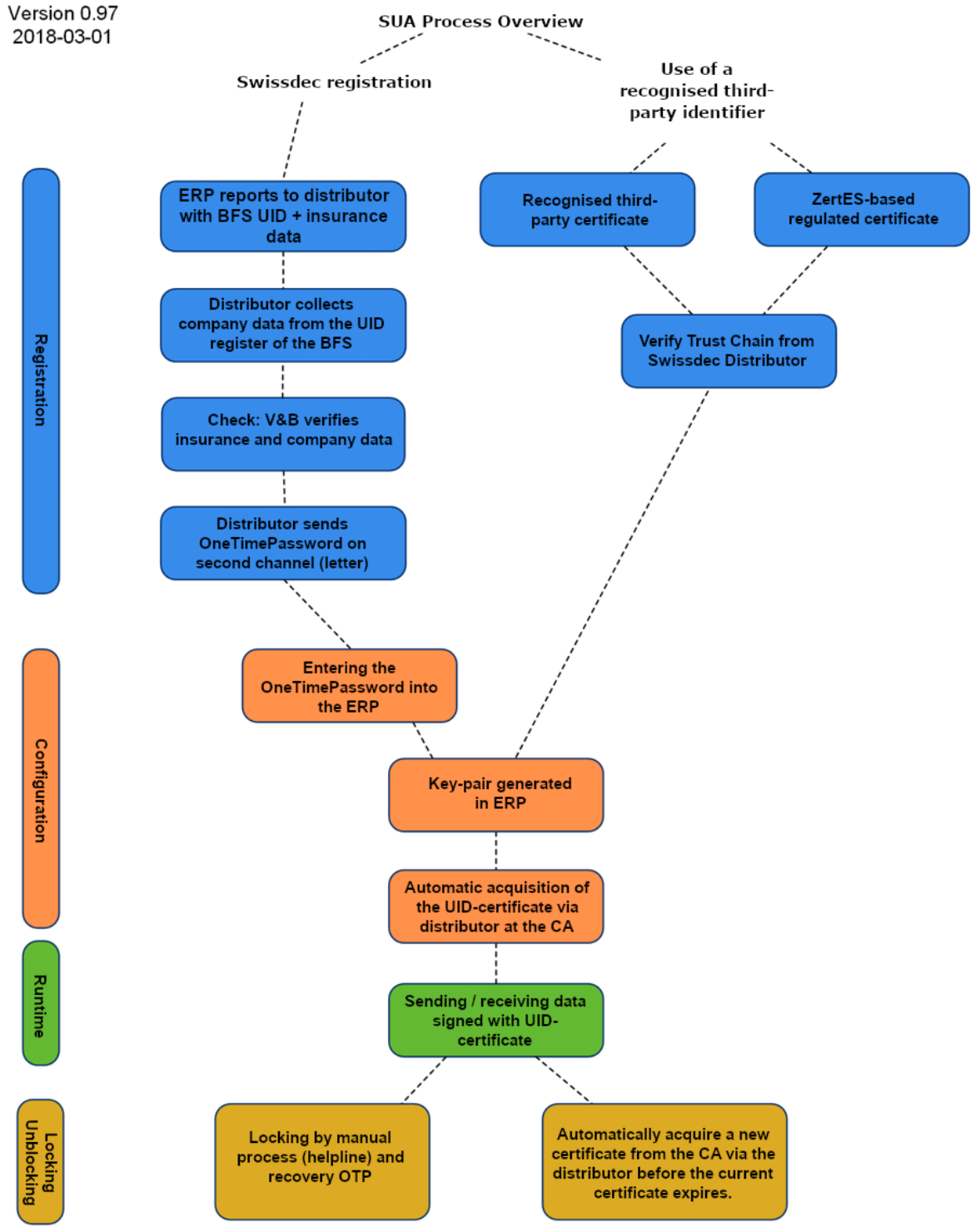

Fig. 10: Processo completo di autentificazione delle aziende Swissdec in quattro fasi

6.1 Processo di registrazione

Per la registrazione sono previste sostanzialmente due opzioni (vedi Fig. 10): la prima consiste nel registrarsi presso Swissdec, la seconda prevede una registrazione semplificata con l'ausilio di un identificativo terzo, come un certificato (regolamentato) ai sensi della FiEle.
Al momento si ritiene che, in futuro, la modalità più comune con cui le imprese gestiranno i processi aziendali sulla base dell'autentificazione delle aziende Swissdec sarà la registrazione diretta presso Swissdec. Man mano che si diffonderanno i certificati aziendali emessi secondo i requisiti della FiEle, il processo di registrazione verrà notevolmente semplificato.

6.1.1 Registrazione Swissdec
Per poter effettuare una registrazione è indispensabile avere un rapporto contrattuale in essere con un'assicurazione. Si suppone che l'assicurazione conduca i necessari accertamenti sull'azienda al momento della stipula del contratto e che disponga sempre, nelle proprie anagrafiche, di dati IDI aggiornati (numero d'identificazione delle imprese, nome dell'azienda come risulta dall'iscrizione nel registro di commercio ecc.).
Le aziende che non hanno un rapporto contrattuale in essere devono ottenere un certificato regolamentato (vedi paragrafo 6.1.2) per accedere alla registrazione diretta.
Anche i fiduciari che firmeranno in un secondo momento i dati delle aziende da loro amministrate con il proprio certificato IDI devono svolgere il normale processo di registrazione e configurazione. Si presume che anche i fiduciari siano aziende con rapporti contrattuali in essere con le A&A, e che sia possibile effettuare la registrazione sulla base di tali rapporti.
In linea di principio, la registrazione presso Swissdec può essere effettuata con due diverse modalità: in un caso sono le assicurazioni e autorità a entrare in contatto con le aziende, nell'altro le A&A delegano tale contatto a Swissdec. Il punto 6.1.1.1 descrive la procedura preferenziale, in cui il distributore Swissdec invia alle aziende le informazioni necessarie per la registrazione. Il successivo punto 6.1.1.2 illustra invece il processo di registrazione che prevede il contatto da parte di assicurazioni e autorità.
In entrambi i casi le informazioni per la configurazione iniziale risultanti dal processo di registrazione vengono inviate alle aziende tramite un secondo canale non elettronico. Per tale canale sono previsti i seguenti requisiti:

ID	Denominazione	Descrizione	Priorità
AB-01	Verifica dell'indirizzo	L'indirizzo (indirizzo e-mail, numero SMS, indirizzo postale) deve essere noto all'assicurazione presso la quale l'azienda si registra e deve essere verificato dall'assicurazione stessa.	OBBLIGATORIO
AB-02	Sicurezza	È necessario garantire che le informazioni giungano al destinatario e che non possano pervenire a persone non autorizzate.	OBBLIGATORIO
AB-03	Trasferibilità	Le informazioni trasmesse devono essere inoltrate alla persona competente (persona di contatto).	OBBLIGATORIO
AB-04	Semplicità di archiviazione	Dovrebbe essere possibile salvare e archiviare con semplicità le informazioni trasmesse.	FACOLTATIVO
AB-05	Durata	Le informazioni trasmesse devono giungere ai destinatari in tempi ragionevoli.	OBBLIGATORIO
AB-06	Contenuto	Le informazioni devono essere autoesplicative, in modo da innescare prontamente le azioni successive (inoltro alla persona di contatto).	OBBLIGATORIO
AB-07	Trasparenza	Deve essere possibile determinare la posizione, lo stato di invio e l'archiviazione delle informazioni inviate presso il destinatario.	OBBLIGATORIO
AB-08	Costi	I costi applicati dovrebbero essere adeguati.	FACOLTATIVO

Tabella 6: Requisiti per il canale non elettronico

La Tabella 7 illustra il grado di soddisfazione dei requisiti a seconda dei vari media utilizzati.

ID	Denominazione	E-mail	SMS	Lettera
AB-01	Verifica dell'indirizzo	Event. noto	Event. noto	L'indirizzo postale della direzione dell'azienda è noto (parte della relazione commerciale))
AB-02	Sicurezza	Ricezione relativamente certa (event. necessaria conferma di ricezione))	Ricezione non certa	Garantita da un operatore postale; in determinate circostanze è obbligatorio utilizzare la raccomandata.
AB-03	Trasferibilità	Semplice possibilità di inoltro (all'indirizzo e-mail della persona di contatto)	Semplice possibilità di inoltro, ma bisogna conoscere il numero di SMS	Consegna a mano o tramite posta interna in azienda
AB-04	Semplicità di archiviazione	Archiviazione / stampa e-mail	Non semplice	Direttamente possibile
AB-05	Durata	Tempi molto rapidi	Tempi in genere molto rapidi	Variabile in base al tipo di recapito (da 1 giorno a 1 settimana)

AB-06	Contenuto	Soddisf.	Troppo breve	Soddisf.
AB-07	Trasparenza	Difficile da tracciare, solo conferma di ricezione	No, impossibile	Possibile mediante Posta A Plus o raccomandata
AB-08	Costi	Nessuno	Costi contenuti	In base al tipo di recapito

Tabella 7: Soddisfazione dei requisiti previsti per il canale non elettronico in base ai media utilizzati

Come mostra la Tabella 7, al momento il canale che soddisfa al meglio i requisiti previsti è quello postale («Lettera»), che garantisce un equilibrio ottimale tra i criteri «sicurezza», «costi» e «durata». Il secondo canale non elettronico citato di seguito, pertanto, è la lettera raccomandata (o una spedizione mediante Posta A Plus).
Il processo di registrazione è rappresentato sia come diagramma BPMN, sia come diagramma di sequenza. In entrambi i grafici sono illustrati da un lato lo svolgimento del processo vero e proprio, e dall'altro le relazioni di comunicazione che si stabiliscono al suo interno.

6.1.1.1 Invio di una lettera all'azienda da parte del distributore

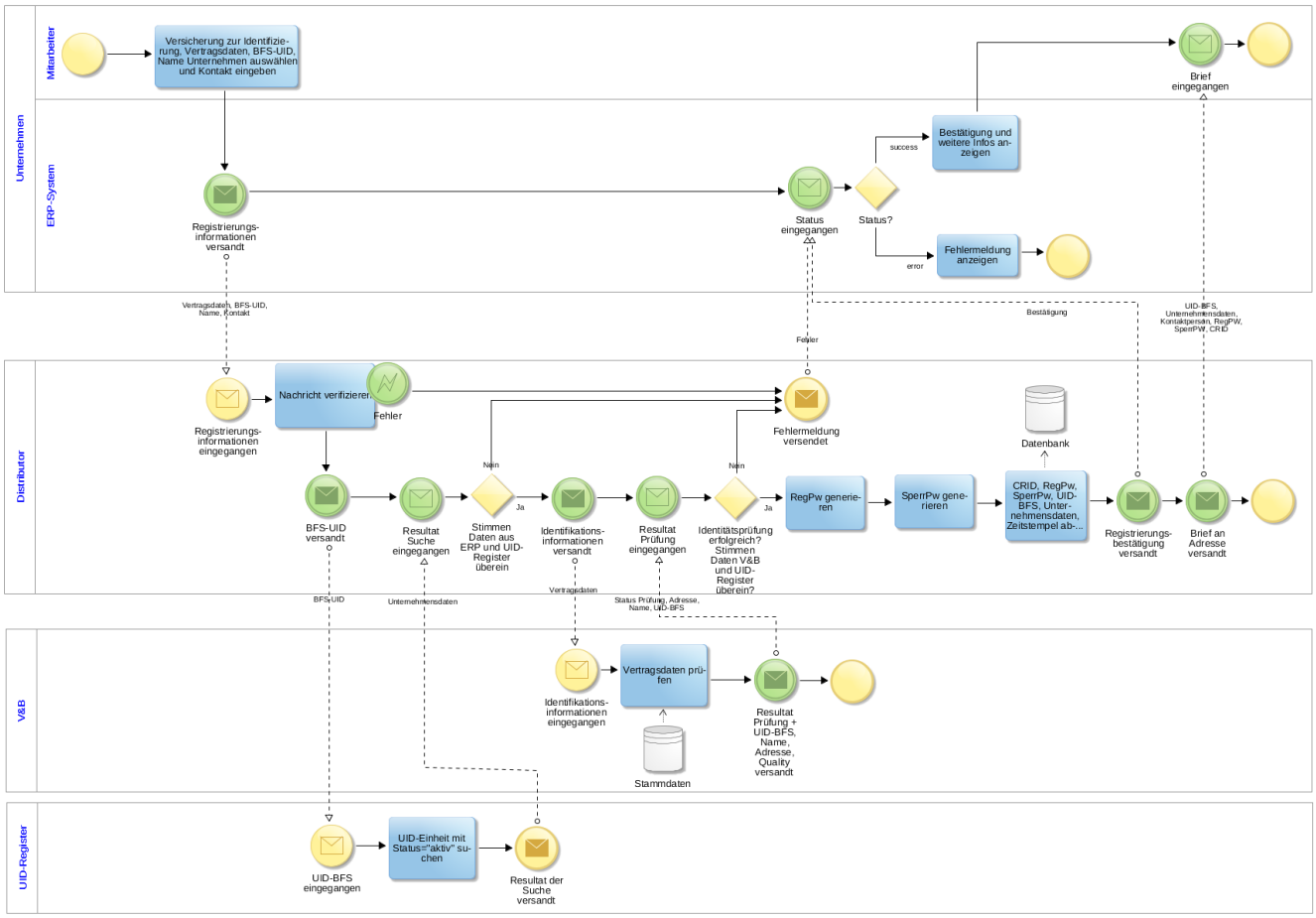

Fig. 11: Processo di registrazione

Se un'azienda desidera registrarsi per l'autentificazione delle aziende Swissdec, un suo collaboratore seleziona nel sistema ERP un'assicurazione che sarà utilizzata per identificare l'azienda in questione. Le informazioni necessarie per la registrazione (IData inerenti il contratto, IDI dell'UST, nome dell'azienda) vengono in gran parte allestite automaticamente dal sistema ERP e quindi inviate al distributore. Inoltre si deve selezionare, o inserire nel sistema, un interlocutore responsabile con sufficienti dati identificativi, come nominativo, e-mail, numero di telefono / cellulare, funzione / divisione.

Il distributore verifica il messaggio ricevuto e inoltre assicura che sia attivabile un numero limitato di richieste di registrazione (ad esempio, max. 5)[21] per un determinato IDI dell'UST. Al sistema ERP viene comunicato l'esito della verifica mediante l'invio di un *CertificateRequestID* (CRID) appositamente generato, che identifica in modo univoco il sistema ERP e la richiesta (Request).
Se la verifica condotta dal distributore sul messaggio è andata a buon fine, vengono richiamate le informazioni sull'azienda presenti nel registro d'identificazione delle imprese dell'UST. Con l'aiuto dell'IDI dell'UST il sistema ricerca un set di dati «attivo» riferito all'azienda, che viene raffrontato con i dati precedentemente ricevuti (nome iscritto nel registro di commercio).
Nel passo successivo, i dati del contratto vengono inoltrati dal distributore all'A&A selezionata in precedenza la quale verifica, con l'ausilio dei propri dati di base, la validità e la congruità dei dati (dati contrattuali) inviati dall'azienda.
L'esito della verifica viene quindi rispedito al distributore insieme alle informazioni tratte dai dati di base, ossia IDI, nome dell'azienda e informazioni di indirizzo (direzione).
Se l'esito inviato dall'A&A è negativo, il distributore segnala la circostanza al sistema ERP dell'azienda, che genera il relativo messaggio di errore per l'utente. A questo punto l'utente deve contattare direttamente l'A&A per un controllo incrociato dei dati relativi all'assicurazione e all'azienda.
Quindi il distributore verifica l'identità confrontando i dati ricevuti dall'A&A con quelli contenuti nel registro d'identificazione delle imprese. Oltre al numero d'identificazione delle imprese e al nome dell'azienda può confrontare anche i dati relativi all'indirizzo (in maniera automatica o manuale).
Se la verifica dell'identità dà esito positivo, il distributore genera una password di registrazione e una di blocco, che vengono salvate insieme all'IDI dell'UST, ai dati tratti dal registro d'identificazione delle imprese dell'UST, al CRID e a un timestamp. La password di registrazione servirà per la configurazione successiva e ha una validità limitata di 30 giorni. Il distributore invia una conferma di avvenuta identificazione dell'azienda al sistema ERP, che la mostra all'utente. La conferma contiene una serie di informazioni, tra cui i dati dell'azienda tratti dal registro d'identificazione delle imprese dell'UST utilizzati per allestire il certificato IDI.
Il distributore, o una terza parte incaricata a tal fine da Swissdec, crea una lettera (raccomandata o Posta A Plus) indirizzata al recapito indicato dall'A&A (direzione) e contenente le password di registrazione e di blocco, il CRID, l'IDI dell'UST, i dati dell'azienda tratti dal registro d'identificazione delle imprese dell'UST e la persona di contatto responsabile dell'azienda, oltre a una serie di altre informazioni (ad es. sul processo di configurazione). In tal modo le informazioni vengono recapitate alla persona responsabile dell'azienda tramite un secondo canale non elettronico, il che migliora ulteriormente la qualità dell'identificazione. Secondo gli standard di autenticazione correnti (Regolamento eIDAS dell'UE, eCH-0170v2, NIST SP 800-63 e ISO 29115), questa procedura è conforme a un livello elevato di verifica del destinatario alla consegna di un mezzo di autentificazione.
Inoltre, il distributore può anche trasmettere all'azienda lo stato della lettera spedita (ad es. in preparazione, inviata, pervenuta) se la parte terza supporta questa funzionalità.
L'intero processo di registrazione è vincolante e si applicano, in aggiunta, i requisiti previsti al capitolo 2.
Per garantire il corretto svolgimento delle procedure di registrazione e, successivamente, di configurazione (vedi sez. 6.2), bisognerebbe poterle eseguire in modalità di prova. Nella **modalità di prova** non vengono spedite lettere né vengono emessi certificati. L'interrogazione al registro d'identificazione delle imprese e la verifica da parte dell'A&A si svolgono come in una registrazione «reale». Ciò consente di gestire senza difficoltà i casi in cui le informazioni contenute nel registro non siano aggiornate e vadano corrette prima di procedere con la registrazione.

[21] Un'azienda può avere più richieste di registrazione attive, ad esempio per diversi sistemi ERP. Limitando il numero di richieste possibili si dovrebbe impedire che l'azienda invii nuove richieste prima che si riescano a completare quelle già attive (la spedizione della lettera può richiedere 1-2 giorni). Questo per evitare richieste eccedenti al registro d'identificazione delle imprese dell'UST e spedizioni superflue di lettere, che potrebbero comportare costi aggiuntivi.

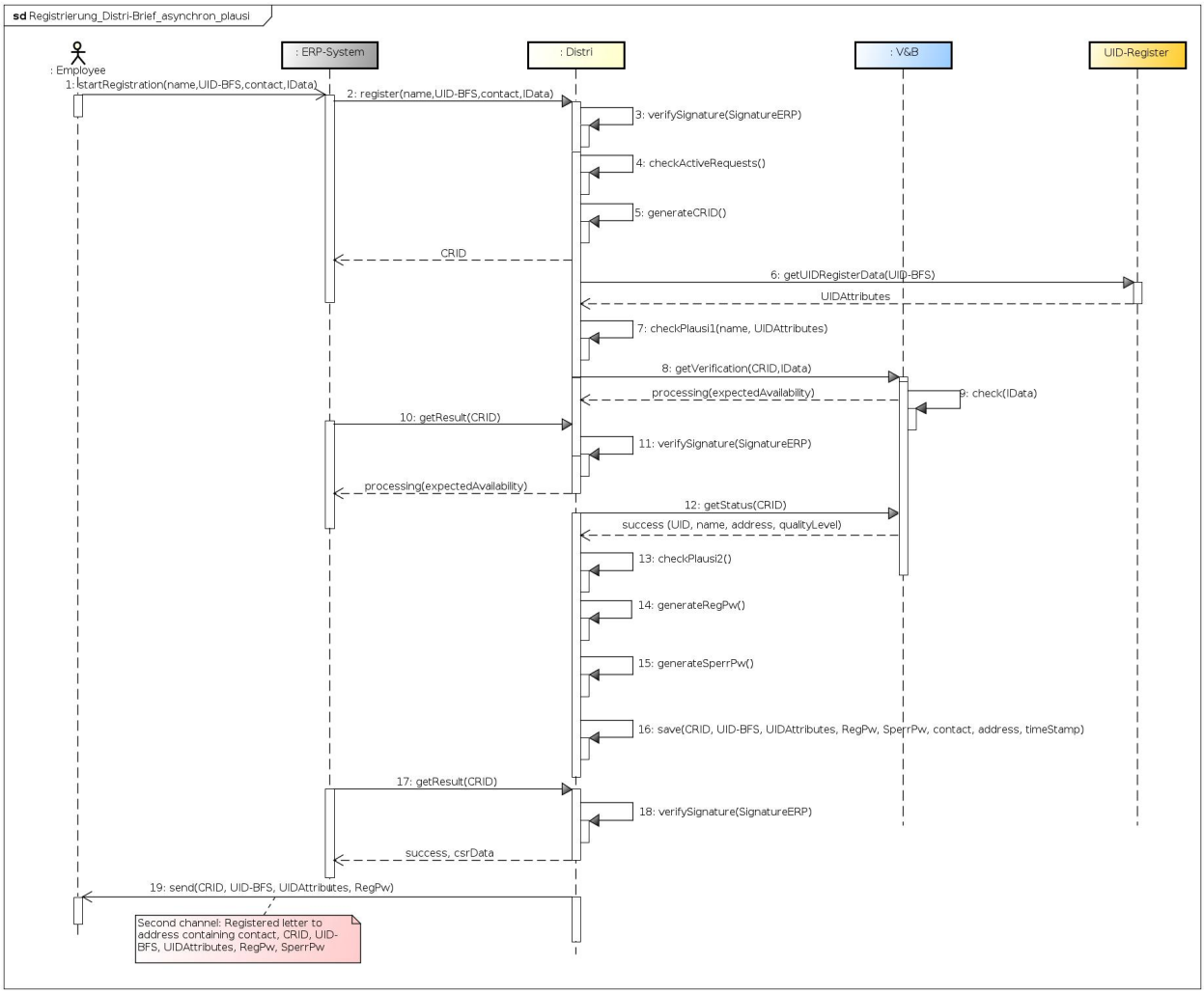

Fig. 12: Diagramma di sequenza del processo di registrazione

In genere la comunicazione fra l'ERP e il distributore è asincrona: in altre parole, il risultato della chiamata al registro (sincrona) che restituisce il CRID viene recuperato mediante richieste ripetute getResult (sincrone). Tra il registro d'identificazione delle imprese dell'UST e i sistemi dell'A&A si ha invece comunicazione sincrona.

Tabella 8: Descrizione delle singole fasi del processo di registrazione

N.	Descrizione
1	**startRegistration(name, UID-BFS, contact, IData)**: L'utente seleziona il nome (name) iscritto nel registro di commercio e l'IDI dell'UST della propria azienda, nonché il relativo rapporto contrattuale con un'assicurazione registrato nel sistema ERP per l'identificazione dell'azienda stessa. Le informazioni necessarie sull'assicurazione vengono prelevate dal sistema ERP. Inoltre l'utente inserisce una persona di contatto con le relative informazioni identificative. IData: dati relativi all'assicurazione (insurance data), informazioni sul rapporto contrattuale. Devono contenere i seguenti attributi: • numero assicuratore / InsuranceID, per identificare il destinatario finale • numero cliente / CustomerIdentity • numero contratto / subnumero / ContractIdentity contact: informazioni identificative relative alla persona responsabile. Dovrebbe contenere i seguenti attributi:

	• nome completo • e-mail • numero di telefono / cellulare • reparto / funzione
2	**register(name, UID-BFS, contact, IData):** Il sistema ERP trasmette al distributore i dati relativi all'assicurazione, all'azienda (IDI dell'UST) e al fiduciario, nonché i dati di contatto.
3	**verifySignature(SignatureERP)** Il distributore controlla la validità della firma del messaggio e verifica la compatibilità con la versione dello standard SUA.
4	**checkActiveRequests()** Il distributore verifica che il numero massimo ammesso di richieste di registrazione per una IDI dell'UST non sia stato superato. In caso contrario il processo di registrazione viene interrotto e, alla successiva richiesta getResult(), l'ERP riceve in risposta lo stato di errore.
5	**generateCRID()** Il distributore genera un CRID (CertificatRequestID) per il caso specifico, che identifica in modo univoco il processo di registrazione del sistema ERP.
<--	Il distributore invia al sistema ERP una conferma di ricezione del messaggio: CRID: ID generato per il caso; permette di recuperare l'esito della verifica d'identità e identifica il sistema ERP nonché la rispettiva richiesta (Request).
6	**getUIDRegisterData(UID-BFS)** Il distributore invia una richiesta sincrona con l'IDI dell'UST dell'azienda al registro d'identificazione delle imprese dell'UST.
<--	Il distributore riceve in risposta gli attributi necessari (UIDAttributes) per verificare la richiesta CSR dell'azienda, e precisamente:[22] [23]: • Nome: <root>/eCH-0108:organisation/eCH-0098:organisationIdentification/eCH-0097:organisationName • Paese: <root>/eCH-0108:organisation/eCH-0098:contact/eCH-0046:address[eCH-0046:otherAddressCategory/text()='main']/eCH-0046:postalAddress/eCH-0010:addressInformation/eCH-0010:country • Città: <root>/eCH-0108:organisation/eCH-0098:contact/eCH-0046:address[eCH-0046:otherAddressCategory/text()='main']/eCH-0046:postalAddress/eCH-0010:addressInformation/eCH-0010:town • Località (Cantone)[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 (forma giuridica)[25]: <root>/eCH-0108:organisation/eCH-0098:organisationIdentification/eCH-097:legalForm • PublicStatus[26]: <root>/eCH-0108:uidregInformation/eCH-0108:uidregPublicStatus

[22] Fonte: Ufficio federale di statistica UST, 2015. Registro d'identificazione delle imprese – Interfaccia webservice 3.0. Online: https://www.bfs.admin.ch/bfs/it/home/registri/registro-imprese/numero-identificazione-imprese/registro-idi/interfacce-idi.assetdetail.1760903.html (20.2.2018).

[23] Gli standard eCH su cui si basa l'interfaccia del registro d'identificazione delle imprese dell'UST sono stati aggiornati nel 1° trimestre 2018, per cui non si esclude una modifica dell'interfaccia legata a tali sviluppi.

[24] La località è un'informazione facoltativa nel registro d'identificazione delle imprese dell'UST.

[25] La forma giuridica è un'informazione facoltativa nel registro d'identificazione delle imprese dell'UST. Si utilizza una nomenclatura a due cifre (01, 02, 03) o a quattro cifre secondo lo standard eCH-0097 (https://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0097&documentVersion=4.0), che deve poi essere convertita al momento della trasmissione nel certificato.

[26] `PublicStatus` indica se i dati di un'azienda iscritti nel registro d'identificazione delle imprese possano o meno essere resi accessibili al pubblico su Internet. Vedi anche la sezione 9.6.

	In questo caso l'IDI dell'UST consultato deve essere contrassegnato come «Attivo»: se così non fosse, non si potrebbe presumere che gli attributi siano aggiornati e/o corretti. Stato IDI: <root>/eCH-0108:uidregInformation/eCH-0108:uidregStatusEnterpriseDetail
7	**checkPlausi1(name,UIDAttributes)** Il distributore verifica i dati tratti dal registro d'identificazione delle imprese dell'UST e li confronta con i dati dell'azienda di cui al n. 2. Se i dati non coincidono, il processo di registrazione viene interrotto e compare un messaggio di errore.
8	**getVerification(CRID, IData)** Il distributore invia il CRID e i dati inerenti il rapporto contrattuale all'A&A selezionata in precedenza.
9	**check(IData)** L'A&A procede alla verifica del rapporto contrattuale dell'azienda con l'ausilio dei propri dati di base. Il raffronto può essere svolto in modo automatizzato o manuale da parte di un collaboratore. La verifica dell'identità dà esito positivo se c'è una perfetta corrispondenza fra i due set di dati. Se i dati inviati non coincidono con i dati di base dell'A&A, non è possibile confermare l'identità dell'azienda.
<--	**processing(expectedAvailability)** L'A&A conferma che il processo di elaborazione è iniziato e comunica al distributore un intervallo di tempo previsto per il completamento.
10	**getResult(CRID)** Dopo che il distributore ha ricevuto la conferma (CRID), il sistema ERP richiede lo stato dell'elaborazione corrente. A tal fine il sistema ERP invia al distributore il CRID corrispondente in una richiesta (Request) firmata con il certificato ERP.
11	**verifySignature(SignatureERP)** Vedi n. 3
<--	**processing(expectedAvailability)** Il distributore risponde al sistema ERP che l'elaborazione è ancora in corso e comunica l'intervallo di tempo presumibilmente necessario per completare l'operazione.
12	**getStatus(DID)** Trascorso l'intervallo di tempo definito dall'A&A, il distributore richiede lo stato dell'elaborazione corrente inviando una richiesta in merito (Request).
<--	**success(BFS_UID, name, address, qualityLevel, contact)** L'assicuratore invia in risposta al distributore l'esito della verifica. In caso di esito positivo, la risposta (Response) contiene i seguenti elementi: • success: identità confermata correttamente • IDI dell'UST: il numero d'identificazione delle imprese contenuto nei dati di base dell'A&A • name: nome dell'azienda • address: dati relativi all'indirizzo dell'azienda del cliente, comprensivi di nome dell'azienda (direzione), casella postale, via, numero civico, NPA, località • qualityLevel: qualità del controllo dei dati (ad es. 0 – automatico, 10 – manuale, 100 – secondo FiEle) • contact: persona di contatto presso l'A&A che ha svolto la verifica e alla quale bisogna rivolgersi per eventuale supporto In caso di esito negativo viene inviato un errore: • error: errore nella verifica dell'identità In questo caso, i passi riportati qui di seguito relativi al distributore non vengono eseguiti.
13	**checkPlausi2()** A questo punto il distributore confronta le informazioni dell'A&A con i dati ricevuti in precedenza e tratti dal registro d'identificazione delle imprese. In questa fase vengono confrontati, in modo manuale o automatico (ad es. con metodi fuzzy basati sull'intelligenza artificiale), i numeri d'identificazione delle imprese, i nomi dell'azienda e i dati relativi all'indirizzo. Se i dati provenienti dalle due fonti coincidono, la registrazione va a buon fine e può proseguire con i passi successivi.

14	**generateRegPw()** Se la verifica dell'identità dà esito positivo (success) il distributore genera una password di registrazione (RegPw) conformemente ai requisiti applicabili (vedi sezione 5.4).
15	**generateSperrPw()** Inoltre il distributore genera anche una password di blocco (SperrPw) secondo i requisiti illustrati alla sezione 5.4. Quest'ultima viene utilizzata nel processo di blocco (vedi sezione 6.6)
16	**save(CRID, UID-BFS, UIDAttributes, RegPw, SperrPw, contact, address, timeStamp)** Il distributore salva la RegPw e la SperrPw insieme all'IDI dell'UST, ai dati relativi all'azienda tratti dal registro d'identificazione delle imprese (UIDAttributes), al CRID, ai dati di contatto (contact), ai dati relativi all'indirizzo (address) e a un timestamp (timeStamp). La password di registrazione (RegPw) ha una validità massima di 30 giorni.
17	**getResult(CRID)** Trascorso l'intervallo di tempo previsto (expectedAvailability), il sistema ERP richiede al distributore lo stato dell'elaborazione corrente. A tal fine il sistema ERP invia al distributore il CRID corrispondente in una richiesta (Request) firmata con il certificato ERP.
18	**verifySignature(SignatureERP)** Vedi 3
<--	Quando il distributore ha disponibile l'esito della verifica d'identità (success | error), lo invia al sistema ERP sotto forma di risposta (Response). Insieme all'esito success invia anche l' IDI dell'UST confermato e le informazioni necessarie per creare una richiesta CSR (informazioni sul titolare [Subject]).
19	**send(CRID, UID-BFS, UIDAttributes, RegPw, SperrPw)** Se la verifica dell'identità dell'azienda è andata a buon fine (success), il distributore - o una terza parte incaricata a tal fine da Swissdec - invia una lettera (secondo canale non elettronico) alla direzione aziendale (address), indicando la persona di contatto ricevuta (contact). A tal fine vengono usati i dati di contatto trasmessi dall'ERP e i dati relativi all'indirizzo contenuti nell'anagrafica clienti dell'A&A. La lettera deve riportare le seguenti informazioni minime, necessarie per la configurazione: • CRID per l'identificazione del processo di registrazione specifico. • IDI dell'UST e UIDAttributes dell'azienda che intende registrarsi • RegPw per la configurazione • SperrRW per bloccare il certificato IDI • validità della RegPW.

Se la verifica dell'identità eseguita dall'A&A va a buon fine, dopo avere completato correttamente la registrazione il collaboratore incaricato riceve le informazioni sull'azienda prelevate dal registro d'identificazione delle imprese dell'UST (in formato elettronico, sotto forma di risposta a una richiesta getResult(), oppure tramite lettera).

6.1.1.2 Spedizione di una lettera all'azienda da parte dell'A&A

Questa procedura è sostanzialmente analoga al processo di registrazione in cui il distributore invia una lettera all'azienda.

Dopo avere verificato con successo le informazioni di registrazione inviategli dal sistema ERP, il distributore provvede a generare la password di registrazione e quella di blocco. Ora, a differenza della procedura precedente, insieme alle informazioni rilevanti per l'identificazione dell'azienda (profilo assicurativo, IDI dell'UST) vengono inviate all'A&A anche le password.

L'A&A verifica, con l'ausilio dei propri dati di base, la validità e la congruità delle informazioni di registrazione fornite dall'azienda. Quindi invia in risposta l'esito della verifica d'identità.

Se la verifica dell'identità va a buon fine, l'A&A invia una lettera (raccomandata o Posta A Plus), indirizzata alla direzione aziendale con indicazione della persona di contatto (contact) e contenente la password di registrazione con la relativa validità, la password di blocco, il CRID, l'IDI dell'UST, oltre a una serie di altre informazioni (ad es. sul processo di configurazione).

Questo processo di registrazione è un'opzione possibile, ma per il momento è esclusa. Si potrebbe però concepire una procedura alternativa in cui l'A&A avvia la registrazione con una circolare (invio di massa) contenente solo le istruzioni di registrazione indicate al punto 6.1.1.1.

6.1.2 Registrazione con certificato regolamentato secondo FiEle

La descrizione dettagliata del processo di registrazione con certificati regolamentati ai sensi della FiEle è stata scorporata in un documento a parte intitolato «Autentificazione delle aziende Swissdec – Specifica dettagliata – Informazioni supplementari sulla registrazione con certificati FiEle» [1].

6.1.3 Vantaggi e svantaggi dei vari processi di registrazione

Tabella 9: Vantaggi e svantaggi delle singole varianti del processo di registrazione

Processo	Vantaggi	Svantaggi
Invio lettera da parte del distributore	• Spedizione centralizzata e armonizzata delle lettere da parte di Swissdec • Nessuna necessità di inoltrare le informazioni all'A&A • Opzionale: nessuna necessità di trasmettere le informazioni relative all'indirizzo del cliente[27]	• Informazioni di contatto relative al cliente trasmesse al distributore ed eventualmente a una parte terza • Nessun contatto diretto tra l'A&A e il cliente
Invio della lettera da parte dell'A&A	• Contatto diretto fra l'A&A e il cliente • Rapporto di fiducia tra cliente e fornitore	• Necessità che l'A&A definisca il processo per la spedizione delle lettere • Processo di registrazione che vede direttamente coinvolte numerose organizzazioni di diverso genere • Possibilità che la lettera contenente la password di registrazione (RegPw) vada persa nella corrispondenza di natura assicurativa
Registrazione con certificato secondo FiEle	• Possibilità di eseguire registrazione e configurazione in un'unica fase (senza necessità di lettera) • Registrazione per aziende senza un rapporto contrattuale in essere con A&A • Identificazione delle aziende conforme ai requisiti della FiEle • Autorità di registrazione accreditata ai sensi della FiEle • Utilizzo della struttura di certificazione già presente • Nessuna necessità di coinvolgere l'A&A	• Costi molto elevati a carico delle aziende per l'ottenimento di un certificato ai sensi della FiEle • Diffusione dei certificati ai sensi della FiEle piuttosto scarsa e limitata alle grandi aziende

6.2 Registrazione di fiduciari

Un fiduciario deve registrarsi per ottenere un certificato SUA solo se intende inviare dati ad A&A in nome e per conto di un'azienda e non effettua tale operazione direttamente dall'ERP dell'azienda interessata (nel qual caso tutti i messaggi sarebbero firmati con il certificato SUA dell'impresa). In questa fattispecie, il rapporto di delega viene regolamentato dall'azienda a livello organizzativo e non occorre depositare una procura scritta presso l'assicurazione.

Se il fiduciario dispone di un proprio sistema ERP in cui gestisce i dati delle aziende amministrate (diversi fiduciari), allora dovrà ottenere un certificato SUA.

[27] Le informazioni relative all'indirizzo non vengono messe a disposizione dall'A&A, bensì ottenute direttamente dal registro d'identificazione delle imprese dell'UST (come illustrato nel passaggio alternativo 9 della Tabella 8) e quindi utilizzate per la spedizione della lettera.

Per la registrazione dei fiduciari si distinguono due diversi casi:

a) Il fiduciario, come altre aziende, ha già un rapporto contrattuale in essere con un assicuratore o un'autorità di registrazione (A&A) in base al quale si può eseguire una registrazione SUA. In questo caso deve seguire il normale processo di registrazione (vedi paragrafo 6.1.1).

b) Tra il fiduciario e l'A&A non esiste un rapporto diretto in base al quale si possa eseguire una registrazione SUA. In tal caso si può utilizzare la relazione contrattuale in essere tra il fiduciario e un'azienda amministrata dallo stesso. A tale scopo il fiduciario deve avviare un processo di registrazione nel proprio sistema ERP, inserendo i dati relativi al contratto dell'azienda e i propri dati (nome del fiduciario, IDI, informazioni di contatto ecc.): fungerà da cosiddetto «delegato». L'A&A che effettua la registrazione controlla i dati dell'azienda e del fiduciario e verifica l'esistenza di una procura. A differenza di quanto avviene con il «normale» processo di registrazione, a questo punto la lettera contenente la password per la registrazione viene spedita al fiduciario, il quale provvede a configurare e salvare nel proprio sistema ERP il certificato IDI per fiduciari, e quindi firmerà con il proprio certificato SUA tutti i messaggi che invierà a nome dell'azienda da lui amministrata.

6.3 Processo di configurazione iniziale

6.3.1 Configurazione iniziale previa registrazione

Il processo di configurazione iniziale si avvia dall'ERP selezionando una procedura di registrazione (inserire CRID e IDI dell'UST) per una registrazione eseguita in precedenza (ancora in corso o già completata correttamente). L'ERP mostra al collaboratore competente le informazioni sul titolare (Subject) per il certificato IDI contenute nella conferma di registrazione.

Il collaboratore verifica le informazioni e, se la procedura di registrazione selezionata è già stata completata e il collaboratore ha già ricevuto la lettera con la password di registrazione, è possibile proseguire con la configurazione.

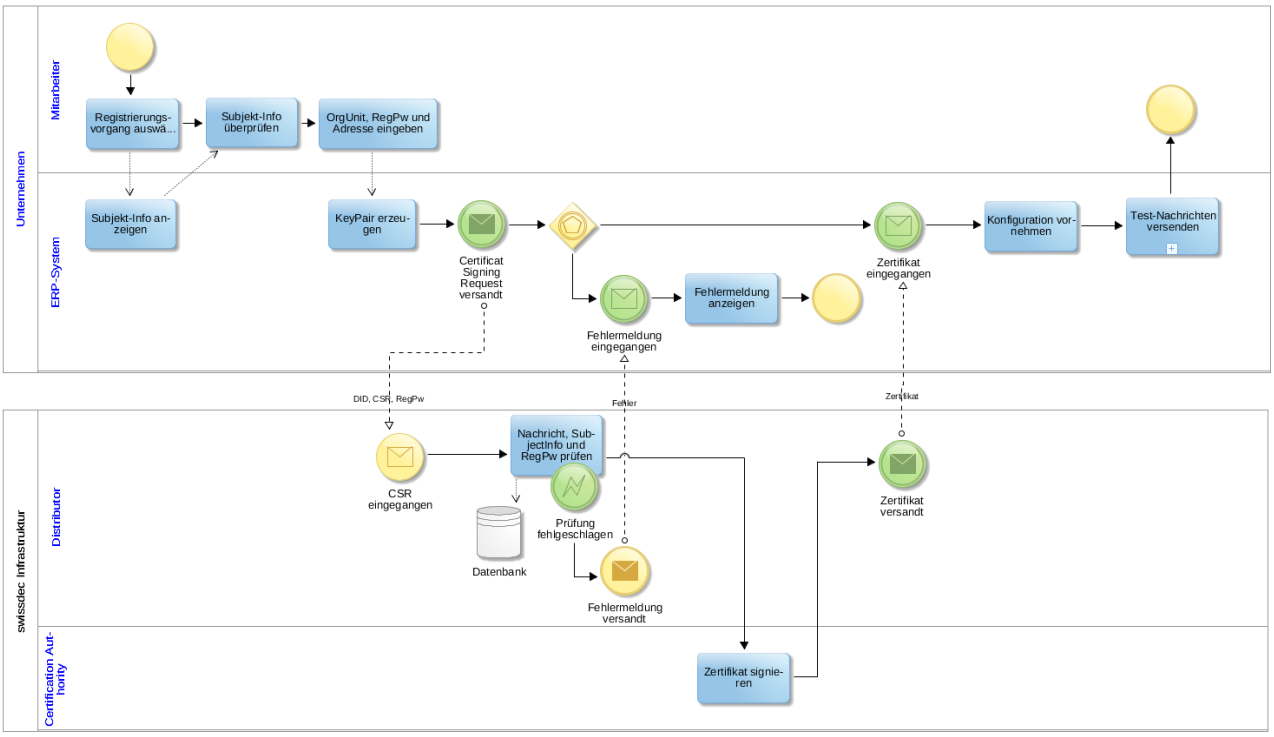

Fig. 13: Processo di configurazione iniziale

Nella fase successiva il collaboratore competente deve indicare la password di registrazione ricevuta. Inoltre può completare le informazioni sull'azienda per il certificato IDI indicando una sottounità (vedi anche Tabella 2).

Il sistema ERP genera la coppia di chiavi (KeyPair) e quindi invia al distributore una Certificate Signing Request (CSR) unitamente alla password di registrazione, al CRID e all'IDI dell'UST.

Il distributore controlla che il messaggio ricevuto sia valido (firma certificato ERP), completo (informazioni necessarie per la creazione del certificato) e conforme (struttura della richiesta CSR), e verifica la password di registrazione fornita in combinazione con il numero di registrazione. A questo punto le informazioni sul titolare (Subject) contenute nella

CSR vengono confrontate con i dati relativi all'azienda salvati in fase di registrazione. Se questi controlli non vanno a buon fine, il sistema ERP riceve immediatamente un messaggio di errore e il processo viene interrotto.
Se il distributore ha ricevuto una CSR valida la trasmette direttamente alla Certification Authority (CA), che firma automaticamente il certificato e lo rispedisce al distributore.
A questo punto il distributore invia il certificato firmato al sistema ERP che provvede a integrarlo.
Una volta che il certificato IDI è integrato nel sistema ERP, è possibile controllarne il corretto funzionamento mediante messaggi di verifica dell'interoperabilità (CheckInteroperability). Se il test va a buon fine, la password di registrazione utilizzata viene annullata.

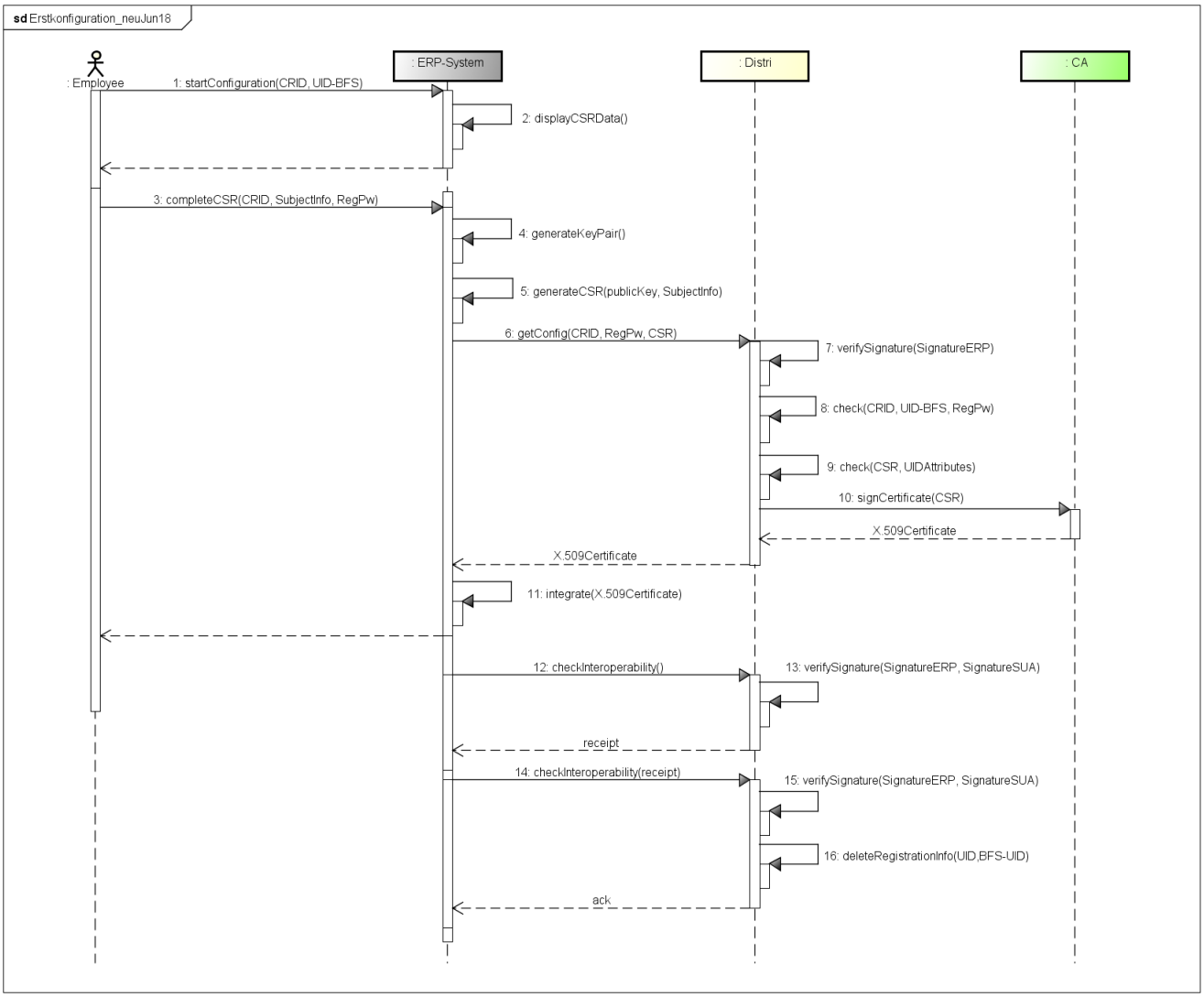

Fig. 14: Diagramma di sequenza del processo di configurazione iniziale

Tabella 10: Descrizione delle singole fasi del processo di configurazione iniziale

N.	Descrizione
1	**startConfiguration(CRID, UID-BFS)** Il processo di configurazione si attiva direttamente dal sistema ERP. Un collaboratore responsabile seleziona nel sistema ERP il CRID e l'IDI dell'UST in relazione ai quali è presente una registrazione completata correttamente.
2	**displayCSRData()** Il sistema ERP mostra all'utente le informazioni ricevute in relazione alla richiesta CSR.
<--	L'ERP mostra all'utente lo stato ricevuto.
3	**completeCSR(CRID, SubjectInfo, RegPw)** L'utente trasmette le informazioni integrate sul titolare (Subject) (i dati sono tratti dal registro

	d'identificazione delle imprese dell'UST ed è possibile compilare solo la sottounità dell'organizzazione, vedi anche Tabella 2) unitamente alla password di registrazione (RegPw).
4	**generateKeyPair()** Il sistema ERP genera la coppia di chiavi (pubblica e privata) come indicato nella sezione 5.3.
5	**generateCSR(publicKey, SubjectInfo)** Il sistema ERP genera una CSR (Certificate Signing Request) come indicato nella Tabella 3.
6	**getConfig(CRID, RegPw, CSR)** Il sistema ERP invia al distributore una richiesta (Request) contenente il CRID, la richiesta CSR e la RegPw.
7	**verifySignature(SignatureERP)** Il distributore controlla la validità della firma del messaggio e verifica la compatibilità con la versione dello standard SUA.
8	**check(CRID, UID-BFS, RegPw)** Il distributore verifica la validità della RegPw in combinazione con la rispettiva IDI dell'UST e il CRID mediante i dati contenuti nella banca dati.
9	**check(CSR, UIDAttribute)** Viene verificata la conformità strutturale della CSR generata dal sistema ERP con i requisiti dello standard SUA (paragrafo 5.1.6). A ciò si aggiunge un confronto fra le informazioni sul titolare (Subject) contenute nella CSR e quelle presenti nella banca dati del distributore. In caso di non conformità ai requisiti o discrepanze rispetto alle informazioni salvate nel distributore, il sistema ERP riceve un messaggio di errore.
10	**signCertificate(CSR)** Il distributore invia la richiesta CSR alla CA. La struttura di questa interfaccia e il formato dei dati trasmessi vanno convenuti con la CA prescelta.
<--	La CA invia in risposta il certificato X.509 firmato.
<--	Il distributore invia una risposta (Response) al sistema ERP con il certificato firmato (X.509Certificate) in formato di certificato con codifica Base64 (PEM).
11	**integrate(X.509Certificate)** Il sistema ERP integra il certificato X.509.
12	**checkInteroperability()** Dopo avere integrato correttamente il certificato, il sistema ERP invia al distributore un messaggio per la verifica dell'interoperabilità (checkInteroperability).
13	**verifySignature(SignatureERP, SignatureSUA)** Il distributore controlla le firme del messaggio, che deve essere correttamente firmato con i certificati ERP e IDI come previsto dai requisiti relativi a firma e cifratura.
<--	Se il controllo eseguito sul messaggio dà esito positivo, il distributore invia una conferma al sistema ERP (receipt).
14	**checkInteroperability(receipt)** Affinché il distributore possa verificare che il sistema ERP è in grado non solo di inviare ma anche di ricevere, il sistema ERP restituisce al distributore, con un secondo messaggio, la conferma appena ricevuta (receipt).
15	**verifySignature(SignatureERP, SignatureSUA)** Vedi n. 13.
16	**deleteRegistrationInfo(CRID, UID-BFS, RegPw)** Dopo avere verificato con esito positivo il secondo messaggio di prova, il distributore cancella dalla banca dati tutte le informazioni relative alla procedura di registrazione (tra cui la RegPw).
<--	**ack** Il distributore conferma al sistema ERP la ricezione del secondo messaggio di prova.

6.3.2 Opzione: generazione della coppia di chiavi e del certificato da parte del distributore
Durante l'elaborazione della presente specifica dettagliata è stata concepita un'opzione che permetterebbe al distributore di generare il materiale chiave e creare il certificato IDI a livello centrale qualora l'ERP non fosse in grado di provvedervi per motivi tecnici. In tal caso il certificato IDI verrebbe inviato in formato elettronico al sistema ERP e semplicemente integrato in loco. Per maggiori dettagli in merito si rimanda al documento supplementare «Autentificazione delle aziende Swissdec – Specifica dettagliata – Generazione della coppia di chiavi e del certificato da parte del distributore».
Il fatto che il materiale chiave e soprattutto la chiave privata siano generati esternamente al sistema destinato al loro utilizzo comporta notevoli svantaggi in termini di sicurezza:

- Il materiale chiave deve essere trasmesso in formato elettronico.
- Il materiale chiave e il certificato vanno archiviati in un adeguato «formato contenitore» e protetti dall'accesso non autorizzato.
- La password di registrazione viene utilizzata sia per l'autentificazione nell'ambito del processo di configurazione, sia per la cifratura del file-contenitore, il che comporta requisiti aggiuntivi per le sue caratteristiche.
- La gestione e la memorizzazione temporanea (cashing) del file-contenitore comporta ulteriori rischi a livello di sicurezza, che andranno mitigati con misure non solo tecniche ma anche organizzative.

Inoltre, considerando che i framework standard in uso nella grande maggioranza dei sistemi ERP supportano la generazione di coppie di chiavi e la creazione di una corrispondente richiesta CSR, l'implementazione da parte dei sistemi ERP risulta piuttosto semplice. È anche possibile agevolare il processo mettendo a disposizione appositi codici sorgente (code sample).

6.3.3 Opzione: configurazione con registrazione automatica (invio di massa)
È stata inoltre elaborata e testata un'altra opzione, che consiste in una registrazione automatica tramite l'invio di massa di lettere di registrazione da parte dell'A&A. I relativi risultati sono raccolti in un documento separato intitolato «Autentificazione delle aziende Swissdec - Specifica dettagliata relativa all'invio di massa».
Si è comunque deciso di accantonare questa opzione in quanto ritenuta inadeguata per i seguenti motivi:

- Per ragioni di sicurezza, la richiesta di partecipare all'autentificazione delle aziende e di ricevere una password di registrazione deve sempre partire da un'azienda, e quindi da un sistema ERP: in tal modo si può presupporre che i responsabili presso l'azienda interessata siano adeguatamente informati e preparati in merito allo svolgimento del processo di registrazione e configurazione.
- Se non è l'azienda a registrarsi per la SUA di propria iniziativa, non è possibile prevedere quando utilizzerà effettivamente la password di registrazione che le viene trasmessa. La RegPW così inviata dovrebbe quindi avere una validità di durata maggiore, il che a sua volta aumenterebbe il rischio di abuso.
- Se l'A&A spedisce le password di registrazione con un invio di massa, non è possibile escludere che una stessa azienda riceva più lettere validevalide contenenti diverse password. Tuttavia, come illustrato alla sezione 5.4, in ogni momento esiste una sola password di registrazione valida per una specifica azienda / uno specifico IDI dell'UST.

6.3.4 Opzione: configurazione con «hard token»
Poiché la coppia di chiavi per un certificato IDI viene sempre generata da parte dell'azienda, il certificato Swissdec viene salvato come «soft token» nell'ambiente sicuro del sistema ERP oppure viene creato e archiviato su un componente hardware certificato (token crittografico o modulo di sicurezza hardware [HSM]). Queste due metodologie non comportano differenze sostanziali nel processo di registrazione dal punto di vista di Swissdec e della CA emittente.
L'emissione, la revoca e il rinnovo di un certificato IDI Swissdec competono alla Certificate Authority. Se si utilizza un hard token, bisogna chiarirne le caratteristiche concrete e le relative modalità di implementazione con la CA responsabile. Qualunque sia la forma di token prescelta, Swissdec agisce in veste di Registration Authority e il processo di registrazione va preventivamente completato secondo una delle varianti illustrate nella sezione 6.1.
Dato che l'impiego di un hard token assicura un livello di sicurezza più elevato, è possibile estendere la validità del certificato che vi è incorporato. Se un certificato software prevede un triplice rinnovo automatico per un anno, con un hard token il certificato si dovrebbe poter utilizzare fino a tre anni. Trascorso tale periodo, si richiederà anche in questo caso la verifica dell'identità dell'azienda, che dovrà effettuare una nuova registrazione.
Il processo di configurazione è quindi molto simile a quello descritto al paragrafo 6.2.1, con la differenza che in questo caso la CA invia l'hard token all'azienda, che dovrà poi renderlo disponibile per un sistema ERP. Per controllare la corretta configurazione del sistema ERP è possibile utilizzare i messaggi di verifica dell'interoperabilità (checkInteroperability) illustrati al paragrafo 6.2.1 , Tabella 10, n. 12-16. Scambiando questi messaggi si conclude il processo e si conferma anche la corretta installazione dell'hard token.

Questa stessa procedura funziona anche per i token nei moduli HSM; in questo caso l'azienda ha la responsabilità di assicurare che il sistema ERP acceda al materiale chiave.
I vantaggi e gli svantaggi di questa variante sono riportati nella Tabella 11.

Tabella 11: Vantaggi e svantaggi dell'hard token

Vantaggi	Svantaggi
• Memorizzazione del certificato e quindi delle chiavi su un dispositivo hardware sicuro • Autentificazione a due fattori (token + PIN) • Emissione e gestione dell'hard token di competenza esclusiva della CA	• I sistemi ERP devono supportare l'hard token (interfaccia fisica, ERP su cloud). • Inserimento del PIN a ogni utilizzo di certificato o memorizzazione temporanea (caching)

6.4 Processi di runtime in base allo Standard prestazioni CH (KLE)

Si riporta qui di seguito l'utilizzo del certificato IDI prendendo come esempio i processi di runtime dello Standard prestazioni CH (KLE).

6.4.1 Notifica di un evento

L'azienda comunica un evento (Incident) a un'assicurazione e autorità competente. La notifica viene effettuata direttamente dal sistema ERP. È possibile indirizzare la notifica a più assicurazioni e autorità facendo pervenire a ciascuna di esse le informazioni necessarie.
Il diagramma di sequenza riportato di seguito illustra la procedura di notifica di un evento in base allo Standard prestazioni CH. Si precisa che sia la rappresentazione grafica sia la descrizione successiva si concentrano sugli aspetti rilevanti nel contesto dell'autentificazione delle aziende Swissdec, mentre per le informazioni tecnico-specialistiche relative al processo si rimanda alla documentazione dedicata allo Standard prestazioni CH.

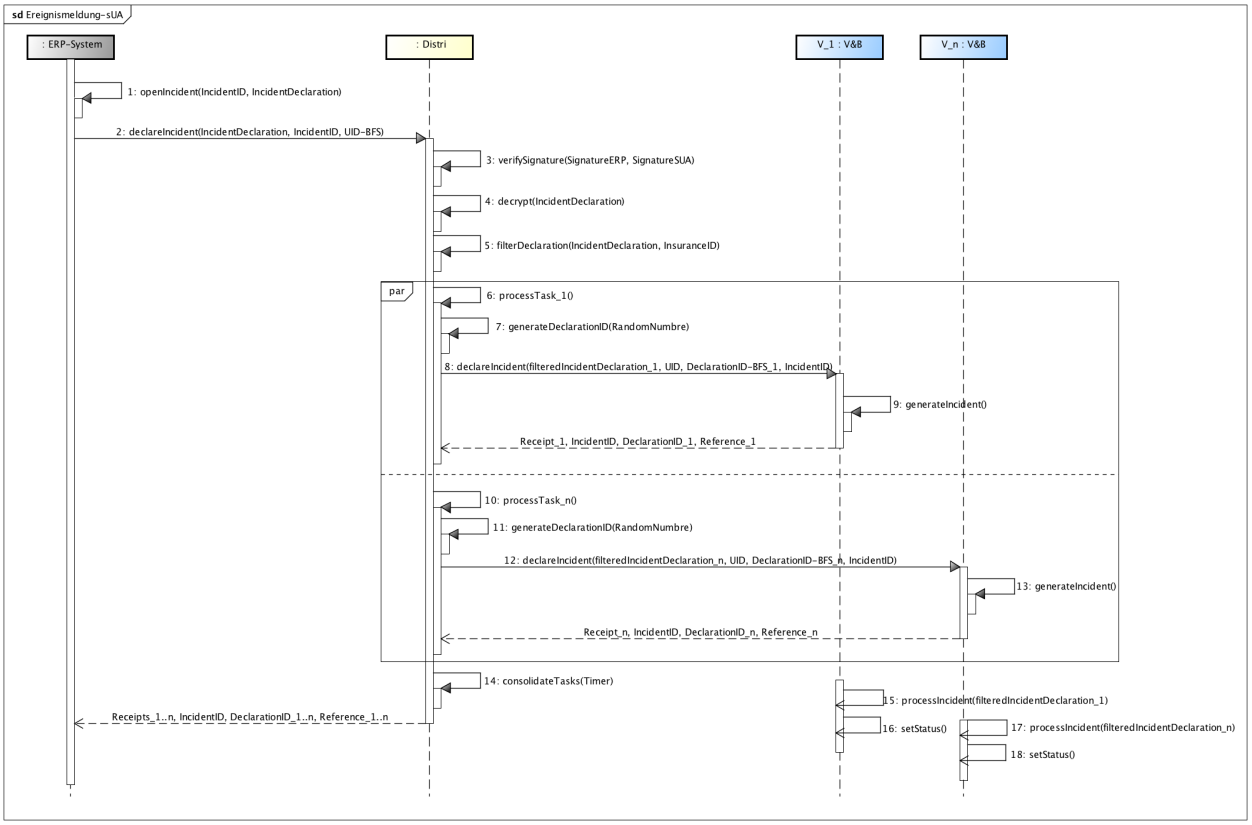

Fig. 15: Notifica di eventi nello Standard prestazioni CH (KLE) con la SUA

Tabella 12: Descrizione delle singole fasi di una notifica di eventi nello Standard prestazioni CH con la SUA

N.	Descrizione
1	**openIncident(IncidentID, IncidentDeclaration)** Nel sistema ERP viene aperto un nuovo evento, al quale viene assegnato il rispettivo numero di identificazione (IncidentID). Le informazioni rilevanti per l'A&A vengono registrate in una IncidentDeclaration.
2	**declareIncident(IncidentDeclaration, IncidentID, UID-BFS)** Una volta completata la IncidentDeclaration, il sistema ERP può trasmetterla tramite il distributore alle assicurazioni e autorità indicate come destinatari. Vengono trasmessi anche l'IncidentID e l'IDI dell'UST.
3	**verifySignature(SignatureERP, SignatureSUA)** Il distributore controlla le firme del messaggio, che deve essere correttamente firmato con i certificati ERP e IDI come previsto dai requisiti relativi a firma e cifratura.
4	**decrypt(IncidentDeclaration)** Il distributore decifra il contenuto del messaggio inviato.
5	**filterDeclaration(IncidentDeclaration, InsuranceID)** Per evitare ridondanze nella comunicazione, i dati vengono inviati una sola volta nella IncidentDeclaration. Il distributore prepara i dati individualmente per i singoli destinatari, in modo da inoltrare a ciascuno di essi solo le parti di messaggio pertinenti. In questo processo, l'InsuranceID identifica i singoli destinatari finali della IncidentDeclaration inviata.
6 / 10	**processTask()** Dal distributore si avvia un task separato per ogni messaggio da inoltrare. Il numero di task dipende dal numero di destinatari finali registrati nella IncidentDeclaration.
7 / 11	**generateDeclarationID(RandomNumber)** Per ogni messaggio da inviare, il distributore genera un numero di identificazione individuale e univoco nell'ambito dei processi di business Swissdec, denominato DeclarationID.
8 / 12	**declareIncident(filteredIncidentDeclaration_1..n, UID-BFS, DeclarationID_1..n, IncidentID)** Le informazioni raccolte per i singoli destinatari finali (filteredIncidentDeclaration) vengono inviate a ciascuno di essi insieme all'IDI dell'UST dell'azienda, al relativo DeclarationID e all'IncidentID. Il messaggio viene firmato dal distributore e criptato con la public key del destinatario finale.
10 / 13	**generateIncident()** L'assicuratore o l'autorità elabora il messaggio ricevuto.
<--	In risposta invia una conferma (receipt) contenente l'IncidentID, il DeclarationID e un numero di riferimento (reference). • Reference numero di caso dell'assicuratore o autorità.
14	**consolidateTasks(Timer)** Se una IncidentDeclaration ha dato origine a più task, il distributore riceverà diverse singole risposte dai destinatari finali coinvolti e provvederà a raggrupparle, a condizione però che gli pervengano entro una finestra temporale prestabilita (timer). Se le risposte non giungono al distributore nei tempi previsti, il processo viene interrotto con conseguente invio di un messaggio di errore al sistema ERP. In tal caso si dovrà trasmettere di nuovo la notifica di evento.

N.	Descrizione
<--	Il distributore rispedisce al sistema ERP tutte le conferme (receipt), l'IncidentID, i DeclarationID e i numeri di riferimento (reference) ricevuti. In questo modo viene confermato il corretto completamento della notifica di evento. Il messaggio viene firmato dal distributore e criptato con la public key del sistema ERP (certificato IDI).
15 / 17	**processIncident(filteredIncidentDeclaration)** A prescindere dalla notifica di evento, si prosegue con l'elaborazione dell'incident aperto presso ciascuno dei destinatari finali.
16 / 18	**setStatus()** Nel prosieguo dell'elaborazione dell'Incident, l'assicurazione o l'autorità possono impostare uno degli stati predefiniti. Lo stato viene notificato al sistema ERP dell'azienda, dopo che quest'ultimo avrà avviato una richiesta di comunicazione.

6.4.2 Polling

Una volta completata con successo una notifica di evento, l'ulteriore elaborazione dell'Incident prosegue utilizzando un flusso di comunicazione one-to-one tra il sistema ERP dell'azienda e il rispettivo destinatario finale (A&A): tutte le comunicazioni passano sempre per il distributore, ma il sistema ERP si rivolge a un solo destinatario finale per volta. A tal fine si utilizza una procedura di polling[28], come previsto nello Standard prestazioni CH (KLE). In questo processo il distributore funge da cosiddetto «security endpoint» nei confronti delle varie A&A, ovvero autentifica ogni singolo messaggio inviato da un'azienda mediante la firma del certificato IDI ed è responsabile, nei confronti delle aziende, della crittografia dei messaggi di risposta inviati dalle A&A.

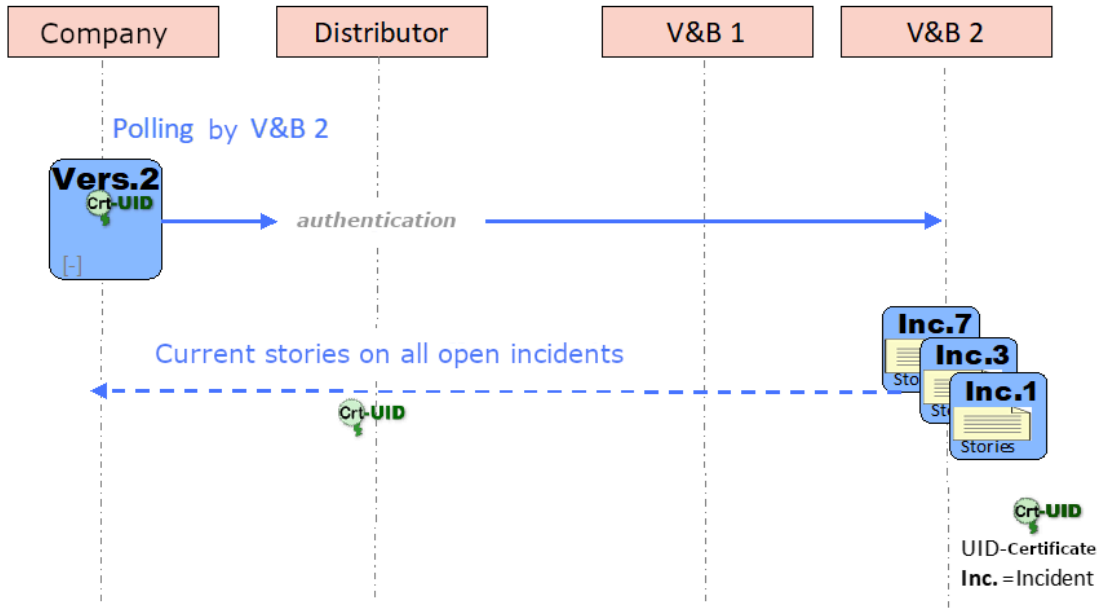

Fig. 16: Procedura di polling (rappresentazione schematica)

Il processo di autentificazione delle aziende Swissdec consente di garantire che le aziende siano sempre identificabili in modo univoco come mittenti nella comunicazione tra il sistema ERP e l'A&A, permettendo così di configurare la comunicazione nel modo più efficiente possibile. Ad esempio, un utente può richiedere attraverso il sistema ERP (tramite Request) che gli siano inviati in risposta (Response) dei dati relativi a diversi Incident attivi presso un

[28] La struttura di comunicazione di Swissdec si basa su una duplice comunicazione client-server (ERP -> distributore e distributore -> A&A) che per sua natura non permette all'A&A di avviare uno scambio di messaggi. Affinché i messaggi dell'A&A possano giungere al sistema ERP, quest'ultimo (così come il distributore) contatta i sistemi dell'A&A mediante polling a intervalli regolari.

destinatario finale. Dopodiché, nel sistema ERP, è possibile elaborare direttamente le informazioni o i requisiti nel contesto dei rispettivi Incident.

6.4.3 Delega

Secondo i requisiti definiti nell'ambito del progetto di soluzione per l'autentificazione delle aziende Swissdec, deve essere ammessa la facoltà di delega di un'azienda, ad esempio a un fiduciario (A-13). Inoltre, già nel progetto di soluzione il requisito 14 (A-14) stabiliva che la verifica della validità della delega, nell'ambito della comunicazione tra il sistema ERP e il destinatario finale, compete all'A&A.
Di conseguenza la delega non incide sui processi di registrazione e configurazione iniziale di cui sopra. Un delegato si registra con il proprio IDI dell'UST seguendo il normale processo, e dopo la configurazione può inviare dati a un'A&A, tramite il distributore, a nome di un'altra azienda. L'A&A dovrà accertare, in base ai contenuti e al mittente dei dati, se sussista o meno una delega legittima e se i dati possano quindi essere ulteriormente elaborati.

6.5 Rinnovo

Il processo di rinnovo dei certificati IDI (solo «soft token») si svolge in modo analogo al processo di configurazione iniziale (paragrafo 6.2.1), con alcune piccole differenze che spieghiamo qui di seguito:

- Il processo non va avviato inserendo una password di registrazione, bensì si attiva automaticamente non appena la validità residua del certificato IDI in uso scende sotto i 30 giorni. Il sistema ERP avvia il processo più volte, finché non viene emesso e integrato un nuovo certificato valido.
- La password di blocco ricevuta inizialmente rimane valida anche dopo il rinnovo del certificato IDI, per cui il distributore non invia un'altra lettera con una nuova password di blocco.
- Per l'intera comunicazione nell'ambito del processo di rinnovo viene utilizzato il materiale chiave ancora valido (certificato IDI). Solo una volta completata la configurazione con il nuovo certificato emesso viene inviato un messaggio di prova con quest'ultimo certificato, che si dovrà utilizzare per tutte le comunicazioni successive.
- Per accertare che non siano intervenute modifiche nei dati relativi all'azienda (nome, Paese, città) così come riportati nel certificato IDI, il distributore interroga anche il registro d'identificazione delle imprese dell'UST inviandogli l'IDI dell'UST dell'azienda in questione. Se i dati iscritti nel registro non coincidono con quelli del vecchio certificato IDI, il processo di rinnovo viene interrotto con un messaggio di errore ed è necessario avviare un nuovo processo di registrazione (vedi sezione 6.1).

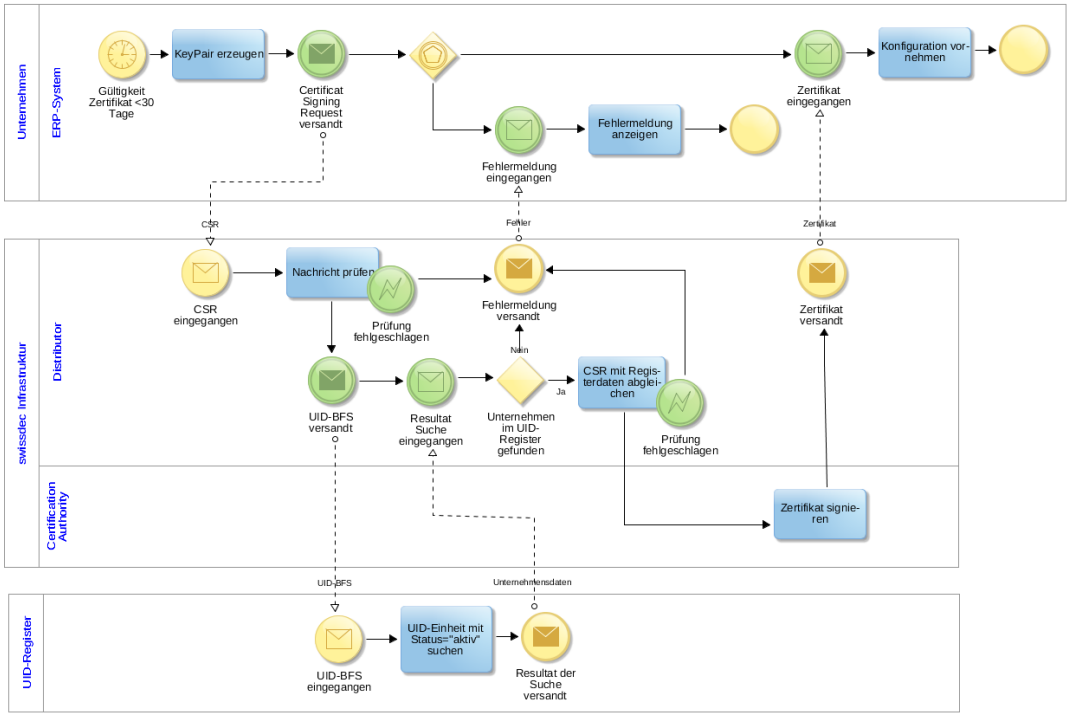

Fig. 17: Processo di rinnovo

Trattandosi di un processo automatizzato, è necessario che l'attualità e l'autenticità dell'azienda vengano periodicamente verificate. Per questo motivo è previsto un numero limitato di rinnovi automatici (nello specifico tre) per

il certificato IDI: quando il sistema ERP ha ottenuto automaticamente un nuovo certificato per tre volte, viene richiesto all'azienda di avviare un nuovo processo di registrazione e di far confermare la propria identità da un'A&A in virtù di un rapporto contrattuale in essere.

Quando un certificato SUA viene sostituito possono verificarsi problemi nei processi a lungo termine, ad esempio con lo Standard prestazioni (KLE). Poiché il certificato deve essere sostituito periodicamente, può capitare che i risultati relativi a una notifica di evento debbano essere criptati con materiale chiave più recente rispetto a quello richiesto dal messaggio originale. Il distributore deve essere in grado di gestire situazioni di questo tipo.

6.6 Blocco

In caso di abuso accertato o presunto di un certificato IDI, è possibile bloccarlo. A tal fine si utilizza la password di blocco inviata all'azienda nell'ambito del processo di registrazione.
In genere è lo stesso titolare a bloccare il certificato IDI. In casi eccezionali può provvedervi anche Swissdec, qualora intenda escludere una determinata azienda dalle funzionalità Swissdec prima che scada il periodo di validità ordinario.
La procedura di blocco si svolge in due fasi. In primo luogo, per avviare il blocco del certificato IDI, il collaboratore dell'azienda in questione deve autenticarsi presso Swissdec. Swissdec verifica la richiesta e, se il controllo va a buon fine, blocca immediatamente il certificato IDI sul distributore. Solo in una seconda fase la richiesta di blocco viene inoltrata alla CA di competenza.
Poiché il blocco del certificato sul distributore comporta l'interruzione immediata di tutte le funzioni Swissdec autentificate, non è richiesto un controllo dello stato («Certificate Revocation List» o «Online Certificate Status Protocol») da parte dei partecipanti.

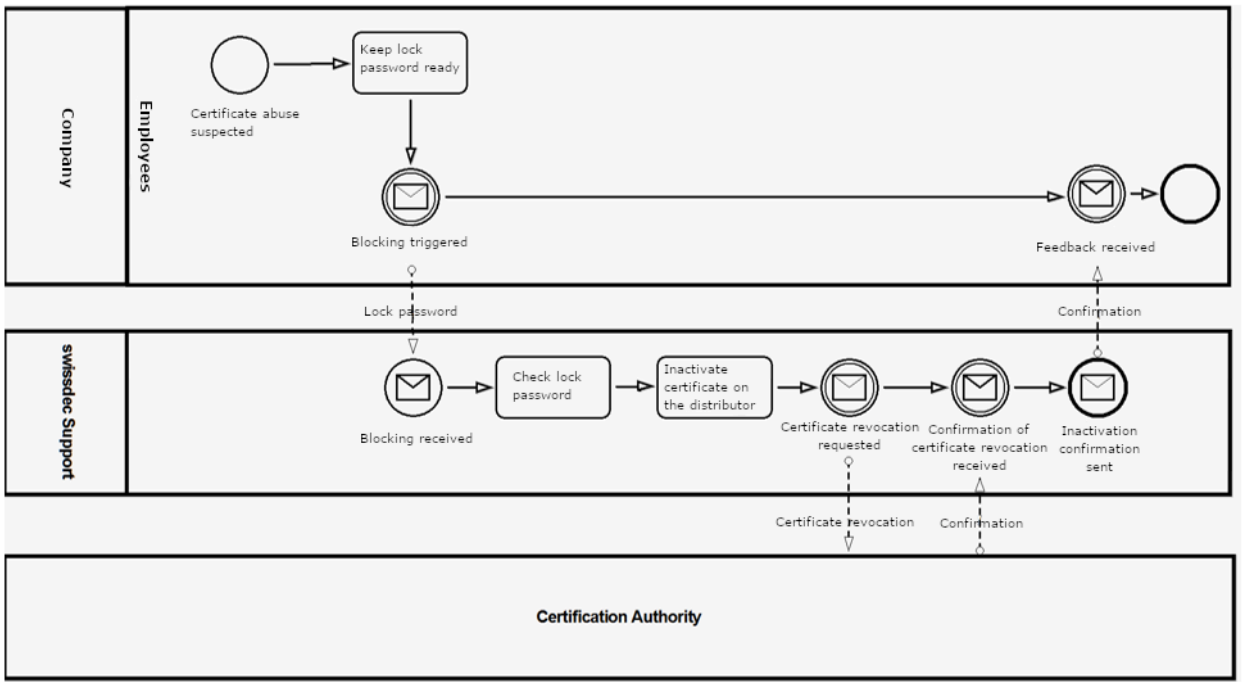

Fig. 18: Processo di blocco

Il collaboratore autorizzato di un'azienda avvia il processo di blocco contattando il Supporto Swissdec e fornendo la password di blocco per l'identificazione. Il Supporto verifica la password di blocco indicata e fornisce assistenza all'azienda. Se effettivamente si presume un abuso del certificato, il Supporto lo disattiva / blocca direttamente sul distributore e attiva la procedura di revoca del certificato presso la CA. In seguito conferma al collaboratore dell'azienda che il certificato in questione è stato revocato.
Se l'azienda non dispone più della password di blocco o non vi ha accesso, occorre innanzitutto accertare la legittimazione del collaboratore. A tal fine si verifica caso per caso, sulla scorta di un'apposita autocertificazione e coinvolgendo un'A&A, se la persona richiedente sia o meno autorizzata a bloccare il certificato a nome dell'azienda in questione.
Si tenga presente che il blocco di un certificato è un processo irreversibile. Una volta eseguito, per poter tornare a comunicare con il distributore l'azienda deve effettuare una nuova registrazione (come indicato nella sezione 6.1).

6.7 Gestione di errori ed eccezioni

Il capitolo 6 descrive il processo SUA con una serie di diagrammi di sequenza in cui le procedure si svolgono sostanzialmente senza intoppi. Le relative rappresentazioni con diagrammi BPMN mostrano casi di errori che si possono generare nell'ambito del processo, ma non riflettono problematiche di natura tecnica. In questa sezione illustriamo quindi brevemente la gestione di errori ed eccezioni nel contesto dei processi SUA.
Ogni fase del processo e ogni singola comunicazione, in teoria, sono passibili di errori o possono sfociare in esiti o stati diversi da quelli auspicati. In tal caso, tutti i partecipanti alla comunicazione coinvolti nel processo di autentificazione delle aziende SUA sono tenuti a rispondere con un'eccezione (Exception) al mittente di una richiesta (Request). L'eccezione contiene le informazioni relative all'errore che si è verificato e può essere rilevata e gestita correttamente dagli altri partner di comunicazione.

7 Componenti dinamici della specifica

Pur essendo stati definiti nella specifica, diversi elementi delle credenziali SUA (capitolo 5) e dei processi SUA (capitolo 6) hanno sostanzialmente natura dinamica. La Tabella 13 riportata di seguito ne fornisce un elenco, illustrando il contesto in cui trovano applicazione e le caratteristiche attualmente definite. Poiché queste ultime si basano sulle conoscenze odierne, sarà opportuno riesaminarle nell'ambito della fase pilota a valle della specifica e alla luce della successiva implementazione. Sarà quindi possibile modificarle periodicamente in base alle nuove conoscenze acquisite con l'attuazione e l'utilizzo dell'autentificazione delle aziende Swissdec nella prassi.

Tabella 13: Elementi dinamici nella specifica

Contesto	Elemento	Caratteristiche
Certificato IDI	Certificato algoritmo crittografico	SHA256 with RSA Encryption
	Dimensione della chiave (key size)	2048 bit
	Periodo di validità del certificato	1 anno Con hard token: 3 anni
Password di registrazione	Lunghezza password	12 caratteri + 2 caratteri per l'identificatore + 2 caratteri cifre di controllo
	Periodo di validità della RegPW	Massimo 30 giorni
Password di blocco	Lunghezza password	12 caratteri + 2 caratteri per l'identificatore + 2 caratteri cifre di controllo
	Periodo di validità della SperrPw	Illimitato
Processo di rinnovo	Periodo antecedente la scadenza del certificato a partire dal quale il sistema ERP avvia la procedura di rinnovo.	30 giorni
	Numero di rinnovi automatici possibili	3
Processo di registrazione	Numero di richieste di registrazione attive	5
Processo di registrazione	Secondo canale non elettronico	Lettera raccomandata / Posta A Plus

8 Conformità ai requisiti del progetto di soluzione

Nell'ambito del progetto di soluzione per l'autentificazione delle aziende Swissdec sono stati definiti alcuni requisiti formali che la presente specifica dettagliata osserva nella misura più ampia possibile.
La Tabella 14 riportata di seguito fornisce una panoramica dei requisiti previsti dal progetto di soluzione. L'ultima colonna precisa se i singoli requisiti sono stati o meno contemplati nella specifica. Il segno di spunta «✓» indica la completa attuazione, lo stesso simbolo fra parentesi «(✓)» indica che il requisito è stato considerato solo in parte o non esplicitamente, mentre una «x» sta a significare che non è stato possibile contemplare il requisito in questione.

Tabella 14: Progetto di soluzione SUA – Requisiti

ID	Denominazione	Descrizione	Priorità	
A-01	Emissione certificato IDI	Per le aziende identificate in modo univoco, la Certification Authority (CA) emette certificati in base al numero d'identificazione delle imprese (IDI).	OBBLIGATORIO	✓
A-02	Emissione certificato del produttore	Il distributore verifica la capacità di un sistema ERP di supportare il processo di business mediante un certificato specifico per il produttore ERP.	OBBLIGATORIO	✓
A-03	Certification Authority (CA)	Per garantire l'affidabilità dei certificati utilizzati, la Certification Authority (CA) assicura che la qualità dei propri certificati e processi sia adeguata ai processi di business.	OBBLIGATORIO	✓
A-04	Assegnazione certificato IDI	Ogni certificato IDI contiene un solo numero d'identificazione delle imprese (IDI).	OBBLIGATORIO	✓
A-05	Certificati per singolo IDI	A un IDI possono essere assegnati più certificati. (Rinnovo certificato, più istanze ERP)	OBBLIGATORIO	✓
A-06	Durata certificato IDI	I certificati IDI emessi dalla CA hanno una validità di durata limitata (min. 1 anno).	OBBLIGATORIO	✓
A-07	Rinnovo certificato IDI	Alla scadenza del certificato il sistema ERP ottiene automaticamente un nuovo certificato presso la CA.	OBBLIGATORIO	✓
A-08	Revoca certificato IDI	In caso di abuso, la CA revoca il certificato con effetto immediato.	OBBLIGATORIO	✓
A-09	Istanza di registrazione	Le aziende si registrano presso una delle istanze autorizzate da Swissdec.	OBBLIGATORIO	✓
A-10	Identificazione univoca dell'azienda	Le aziende che desiderano registrarsi vengono identificate in modo univoco dall'istanza autorizzata da Swissdec secondo un processo predefinito.	OBBLIGATORIO	✓
A-11	Identificazione ad opera dell'istanza autorizzata	L'istanza autorizzata da Swissdec identifica l'azienda sulla base di un'apposita autocertificazione o mediante un secondo canale sicuro.	OBBLIGATORIO	✓
A-12	Identificazione mediante terzi (Third Party)	L'azienda viene identificata tramite terzi affidabili (Trusted Third Party).	FACOLTATIVO	✓
A-13	Delega (ad es. fiduciario)	Il delegato deve registrarsi ed essere in grado di autenticarsi presso il distributore con il proprio numero d'identificazione delle imprese (IDI).	OBBLIGATORIO	✓
A-14	Verifica delega	In qualità di destinatario finale di un messaggio, l'assicurazione o l'autorità verifica un'eventuale delega.	OBBLIGATORIO	✓
A-15	Configurazione automatica del sistema ERP	Una volta concluso correttamente il processo di registrazione, il sistema ERP ottiene automaticamente il certificato IDI (opzionale: con chiave privata) e altre informazioni di configurazione dal distributore e/o dalla CA, e in pochi minuti è operativo.	OBBLIGATORIO	✓
A-16	Autorizzazione del sistema ERP	Quando il sistema ERP invia un messaggio, deve ottenere dal distributore l'autorizzazione necessaria per i processi aziendali Swissdec.	OBBLIGATORIO	✓
A-17	Autenticazione dell'azienda	Quando il sistema ERP invia un messaggio, lo firma con un certificato IDI.	OBBLIGATORIO	✓
A-18	Verifica del sistema ERP	Quando riceve un messaggio, il distributore verifica l'autorizzazione del sistema ERP e i processi di business Swissdec.	OBBLIGATORIO	✓
A-19	Autentificazione dell'azienda	Quando riceve un messaggio, il distributore verifica le firme, elabora le informazioni e trasmette i dati sull'identità ai destinatari.	OBBLIGATORIO	✓
A-20	Trasparenza	Il flusso di messaggi deve essere tracciabile dall'azienda / sistema ERP, dal distributore e dalle assicurazioni e autorità.	OBBLIGATORIO	✓
A-21	Facilità d'uso	Sia la messa in funzione che l'utilizzo del sistema sono concepiti per risultare agevoli per gli utenti.	OBBLIGATORIO	(✓)
A-22	Semplice messa in funzione	Per configurare un sistema ERP non occorre rivolgersi a un tecnico specializzato.	OBBLIGATORIO	✓
A-23	Rapida messa in funzione	Se l'azienda ha già un rapporto in essere con un'assicurazione o un'autorità, il processo di registrazione (inclusa la configurazione del sistema ERP) richiede al massimo 10 minuti.	OBBLIGATORIO	✓
A-24	Accesso a un portale tramite browser	Il sistema ERP consente di accedere a un portale (ad es. A&A) utilizzando un browser.	OBBLIGATORIO	(✓)

A-25	Plausibilizzazione dei messaggi	Quando riceve un messaggio, il distributore verifica se il numero d'identificazione dell'azienda ivi contenuto corrisponde a quello riportato nel certificato.	OBBLIGATORIO	✓
A-26	Infrastruttura utilizzata per il certificato	L'infrastruttura a chiave pubblica (public key infrastructure) utilizzata per la creazione dei certificati digitali si basa sullo standard RFC-5280 X.509 (attuale versione: 3).	OBBLIGATORIO	✓
A-27	Riservatezza a livello di messaggi	Per poter proteggere in modo ancor più efficace le informazioni trasmesse contro vettori di attacchi nonostante l'uso di un canale sicuro, i contenuti inviati devono essere criptati per il rispettivo destinatario.	OBBLIGATORIO	✓

Nell'ambito della specifica dettagliata sono stati contemplati tutti i requisiti definiti nel progetto di soluzione. Tuttavia, alcuni di essi sono stati inclusi solo in parte nella specifica o non vengono menzionati esplicitamente:

- A-21 Facilità d'uso:
  La facilità d'uso è stata contemplata in fase di sviluppo e definizione delle specifiche dei processi SUA. Ad esempio, si è fatto il possibile per rendere le password semplici da digitare e per consentire al sistema ERP di riconoscere direttamente un errore di inserimento da parte dell'utente (cifre di controllo). Nell'ambito dell'elaborazione dei requisiti per la certificazione, sarà necessario definire ulteriori specifiche per determinati componenti – soprattutto a livello dei sistemi ERP e della struttura dell'interfaccia utente – o implementarli d'intesa con i produttori ERP interessati. Anche in questo caso la facilità d'uso è un criterio molto importante da considerare.
- A-24 Accesso a un portale tramite browser:
  Lo Standard salari CH (ELM)[29] prevede la possibilità di accedere tramite browser, direttamente dal sistema ERP, a portali web di determinate A&A e questa funzionalità è già adeguatamente supportata. A tale proposito la specifica dettagliata SUA non fornisce indicazioni approfondite: al momento non è ancora chiaro se in futuro la SUA potrà o dovrà essere utilizzata anche per l'autenticazione dei portali web delle A&A.

[29] Swissdec (2015). Direttive, online: https://www.swissdec.ch/it/release-e-aggiornamenti/direttive-elm/ (2.12.2015).

9 Punti in sospeso

Nella presente specifica dettagliata non è stato possibile definire in via risolutiva alcuni punti, che saranno però ripresi ed eventualmente rivalutati o precisati in maggiore dettaglio in base al livello di informazione corrente in occasione di revisioni successive o con la messa a punto di ulteriori documenti rilevanti ai fini della certificazione.

9.1 Processi e requisiti per Certificate Authority (CA)

In vista dell'implementazione dell'autentificazione delle aziende Swissdec si intende individuare una Certificate Authority accreditata con cui collaborare. In questo contesto si cercherà di chiarire se esistano fornitori di CA meno sofisticati (ad es. Let's Encrypt[30]) in grado di offrire servizi di qualità analoga. In fase di selezione della CA si dovrà tenere conto dei requisiti qui esposti in relazione ai processi e alle caratteristiche dell'infrastruttura del certificato. In ogni caso, nelle procedure operative di creazione del certificato e anche per quanto riguarda le sue caratteristiche formali, bisognerà valutare i dettagli con il fornitore di CA prescelto e all'occorrenza adeguarli.
Un dettaglio ancora da chiarire riguarda l'uso della Business Category (BC), che corrisponde alla forma giuridica presente nel registro d'identificazione delle imprese dell'UST: mentre nel registro si utilizzano i valori numerici previsti dallo standard eCH-0097[31] , nelle linee guida per certificati Extended Validation[32] del Cab Forum si impiegano solo quattro valori.

9.2 Autenticazione Client TLS

Come illustrato nel presente documento, l'autentificazione del mittente viene accertata con la creazione di un canale sicuro per mezzo di un certificato Client TLS. Tale verifica dovrebbe essere svolta utilizzando un certificato IDI. Durante la fase pilota bisognerà chiarire come supportare la procedura con i framework standard esistenti e se si possa o meno disporre di semplici codici sorgenti (code sample) per le principali piattaforme. Inoltre bisognerà coinvolgere il provider dell'infrastruttura di Swissdec per stabilire, in una fase successiva, come passare dal processo di autenticazione TLS unilaterale attualmente utilizzato a un'autenticazione Client TLS basata su certificato.

9.3 Processi SUA e guida interattiva per l'utente nei diversi sistemi ERP

Nel definire i processi e gli elementi di sicurezza si è cercato di garantire la massima facilità d'uso sia nella fase di impostazione che in quella operativa. Tuttavia, in vista dell'implementazione effettiva dei processi SUA nei sistemi ERP, bisognerà contattare i produttori interessati e definire all'occorrenza regole specifiche per uniformare il più possibile la rappresentazione dei processi e quindi la navigazione nei vari sistemi.

9.4 Collegamento a servizi postali

Nel processo di registrazione, di regola, l'identità dell'azienda deve essere verificata inviando una lettera (raccomandata o Posta A Plus) a una persona responsabile dell'impresa mediante un secondo canale non elettronico. La lettera andrebbe consegnata a mano. Al momento bisogna ancora chiarire con i servizi postali competenti le condizioni generali, i processi e i costi relativi a questa tipologia di consegna per una lettera del genere.
In alternativa, per completare la registrazione delle imprese con un livello di sicurezza sufficientemente elevato basterebbe anche una lettera raccomandata recante le informazioni di contatto personali ma SENZA consegna a mano.
Che tipo di accordo si potrebbe stipulare a tal fine con la Posta? La Posta offre già un servizio che permette al distributore di delegare la spedizione di una lettera raccomandata con i dati necessari?

9.5 Registrazione di aziende senza un rapporto contrattuale in essere con A&A

Al momento, per poter effettuare una registrazione SUA è indispensabile avere un rapporto contrattuale in essere con un'assicurazione o disporre di un certificato regolamentato. Se si intende adottare la SUA per altri processi, come l'imposta alla fonte, è necessario testare altre opzioni di registrazione, basate ad esempio su un rapporto in essere con un'autorità fiscale.

[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 Capitolo 9.2.4, pagina 11

9.6 Interrogazione registro IDI dell'UST

L'accesso alle iscrizioni nel registro d'identificazione delle imprese può essere bloccato per il pubblico ma non per l'amministrazione (vedi standard eCH-0108 relativo ai dati del Registro delle imprese, punto 3.2.2.2, disponibile in tedesco e francese). Su questo fronte bisognerebbe chiarire con l'UST se Swissdec possa agire in qualità di amministratore (ad es. in vece dell'Ufficio federale di statistica) per avere pieno accesso ai dati del registro.
In alternativa, ai fini del confronto dei dati in fase di registrazione (vedi par. 6.1.1), l'azienda può anche presentare un estratto scritto del registro d'identificazione delle imprese.

9.7 Rinnovo del certificato nel corso di processi a lungo termine

La sostituzione di un certificato può comportare problemi in caso di processi a lungo termine, ad esempio con lo Standard prestazioni (KLE). Per quanto riguarda la verifica delle firme, si potrebbe in parte evitare il problema allegando il certificato SUA a ogni messaggio firmato, in modo da consentire al destinatario di aggiornare il materiale chiave. Per quanto riguarda invece la cifratura dei messaggi, il rischio aumenta se il mittente non è in grado di aggiornare il materiale chiave da utilizzare e cripta una risposta utilizzando chiavi ormai «obsolete». A seconda dei processi interessati è necessario definire misure per risolvere questi problemi, ad esempio prevedendo che a ogni tentativo di polling sia inviato anche il certificato.

10 Elenco delle figure

11 Elenco delle tabelle

12 Glossario

Ufficio federale di statistica (UST)
Autorità federale della Confederazione Svizzera con sede a Neuchâtel.

Certification Authority (CA)
Organizzazione abilitata a emettere certificati digitali. Un certificato digitale consente di associare una determinata chiave pubblica a una persona o a un'organizzazione.[33]

Certificate Chain
Serve a verificare un certificato digitale; la CA che lo emette funge da «àncora di fiducia» (trust anchor) per la verifica della gerarchia del certificato in questione. In tal modo è possibile controllare l'affidabilità del relativo emittente.[34]

Certificate Signing Request (CSR)
Formato standard utilizzato per richiedere un certificato digitale. La CSR contiene la chiave pubblica di una coppia di chiavi (key pair) e la sua autenticità deve essere verificata dall'autorità di registrazione.[35]

Credenziali
Per credenziali (in inglese: credentials) si intende un insieme di strumenti utilizzato per confermare a un sistema l'identità di un altro sistema o di un utente. Il loro impiego presuppone la presenza di un'identità nota nel sistema. In genere, l'identità viene comprovata indicando un identificativo e un elemento di autenticazione.[36]

Declaration-ID
Numero identificativo già in uso nel sistema attuale e appartenente a un determinato caso. Il trasmettitore non invia una Declaration-ID nella sua richiesta iniziale (Initial Request). È il distributore a inserire una Declaration-ID nei suoi messaggi per agevolare eventuali richieste di informazioni all'assistenza.

OeIDI
Ordinanza del DFF concernente dati ed informazioni elettronici.

Sistema ERP
Software applicativo complesso o insieme di applicazioni software o di sistemi informatici in comunicazione fra loro, che vengono impiegati per supportare la pianificazione delle risorse a livello di intera azienda.[37]

OCSP
Il protocollo **Online Certificate Status Protocol** (**OCSP**) permette di consultare lo stato di certificati X.509 presso un servizio di convalida. Vedi anche RFC 6960.

Privacy Enhanced Mail (PEM) – Formato di file
Formato di file molto diffuso per l'archiviazione di materiale chiave e certificati X.509 con il sistema di codifica Base64.[38]

Conferma tecnico-specialistica
Forma di conferma a livello tecnico-specialistico e di contenuto tra mittente e destinatario. Dipende dal processo interessato e può svolgersi in un arco di tempo piuttosto lungo.

Password di registrazione (RegPw)
La funzione principale della password di registrazione consiste nel garantire che un certificato firmato, eventualmente con la rispettiva coppia di chiavi pubblica / privata (private / public key pair), venga attribuito solo ed esclusivamente al destinatario corretto (sistema ERP). In altre parole, serve ad autenticare l'azienda.

Request for Comments (RFC)
Le Request for Comments (acronimo RFC; in italiano: richieste di commenti) sono una serie di documenti di carattere tecnico e organizzativo riguardanti Internet (in origine Arpanet) e pubblicati dall'RFC Editor a partire dal 7 aprile 1969.[39]

RSA
La sigla RSA (acronimo di Rivest, Shamir e Adleman) indica un algoritmo di crittografia asimmetrica che si può utilizzare sia per criptare informazioni che per la firma digitale.[40]

[33] https://it.wikipedia.org/wiki/Certificate_authority
[34] https://it.qaz.wiki/wiki/Chain_of_trust
[35] http://en.wikipedia.org/wiki/Certificate_Signing_Request
[36] https://en.wikipedia.org/wiki/Credential
[37] https://it.wikipedia.org/wiki/Enterprise_resource_planning
[38] https://en.wikipedia.org/wiki/Privacy-enhanced_Electronic_Mail
[39] https://it.wikipedia.org/wiki/Request_for_Comments
[40] https://it.wikipedia.org/wiki/RSA_(crittografia)

SHA256
SHA-2 (in inglese, acronimo di secure hash algorithm, algoritmo hash sicuro) è un termine che comprende le quattro funzioni crittografiche di hash SHA-224, SHA-256, SHA-384 e SHA-512, pubblicate come standard nel 2001 dall'istituto statunitense NIST e destinate a sostituire l'algoritmo SHA-1.[41]

SOAP
SOAP (inizialmente acronimo di Simple Object Access Protocol) è un protocollo di rete che consente di scambiare dati fra sistemi e di eseguire chiamate di procedura remota (remote procedure call). È uno standard industriale ufficializzato dal World Wide Web Consortium (W3C).[42]

Sicurezza a livello di trasporto (canale sicuro)
La sicurezza a livello di trasporto prevede la trasmissione dei dati su un canale sicuro TLS (HTTPS). I sistemi mittente e destinatario si sono preventivamente autenticati e hanno concordato una chiave di sessione con cui vengono autenticati e criptati i dati da trasmettere.

Sicurezza a livello di messaggio
La sicurezza a livello di messaggio riguarda un'ulteriore autenticazione e cifratura dei dati (nella fattispecie del carico utile) su un canale sicuro. Nel caso di Swissdec, i messaggi SOAP sono protetti con lo standard Web Service Security.

Password di blocco (SperrPw)
La password di blocco consente di autenticare l'azienda qualora intenda bloccare un certificato emesso.

Subject Information
Si tratta delle informazioni contenute in un certificato X.509 relative all'organizzazione per la quale è stato emesso il certificato.

Autentificazione delle aziende Swissdec (SUA)
La SUA indica l'insieme dei processi e il requisito tecnico per l'identificazione univoca delle imprese nell'ambito dei processi di business Swissdec.

Conferma transazione
Questo tipo di conferma attesta semplicemente il trasferimento di un messaggio. Il sistema destinatario controlla la forma del messaggio inviato (sintassi, firma, semantica ecc.) e la include nella conferma, mentre il contenuto viene verificato nell'ambito della conferma tecnico-specialistica. La conferma di transazione deve quindi pervenire entro un certo lasso di tempo. In caso contrario, il mittente può ritenere che il messaggio non sia stato consegnato e quindi inviarlo di nuovo.

Trasmettitore
Il trasmettitore è l'interfaccia tra il sistema ERP e Swissdec. Il sistema ERP prepara i dati da inviare e li trasmette alla componente del trasmettitore che poi li invia al distributore tramite un canale sicuro, conformemente alle direttive Swissdec. In questa fase il trasmettitore convalida le dichiarazioni XML del sistema ERP in relazione a un determinato processo in base allo schema di convalida XSD ufficiale fornito da Swissdec. I dati vengono poi trasferiti in sicurezza (firmati e criptati) dal trasmettitore attraverso il canale sicuro (HTTPS). Al trasmettitore competono inoltre il processo globale di gestione degli errori (error handling), la ricezione delle risposte del distributore e il controllo della conferma di transazione. Infine, il trasmettitore provvede all'archiviazione e alla registrazione (logging) dei messaggi.

Transport Layer Security (TLS) / Secure Sockets Layer (SSL)
Transport Layer Security (TLS), meglio noto con il nome del suo predecessore Secure Sockets Layer (SSL), è un protocollo crittografico ibrido che permette il trasferimento sicuro dei dati in Internet.[43]

Numero d'identificazione delle imprese (IDI dell'UST)
Numero d'identificazione univoco che l'Ufficio federale di statistica (UST) assegna, dal gennaio 2011, a ogni impresa attiva in Svizzera; permette alle aziende di identificarsi ad ogni contatto con le autorità.[44]

Registro d'identificazione delle imprese dell'UST
Registro pubblico della Confederazione in cui sono iscritte tutte le imprese attive, identificate da un numero univoco. Sito Internet: https://www.uid.admin.ch

Uniform Resource Identifier (URI)
Per Uniform Resource Identifier (acronimo: URI, termine inglese traducibile con «identificatore universale e univoco di una risorsa») si intende un identificativo costituito da una sequenza di caratteri che identifica una risorsa fisica o astratta.[45]

[41] https://en.wikipedia.org/wiki/SHA-2
[42] https://it.wikipedia.org/wiki/SOAP
[43] https://it.wikipedia.org/wiki/Transport_Layer_Security
[44] https://www.bfs.admin.ch/bfs/it/home/registri/registro-imprese/numero-identificazione-imprese.html
[45] https://it.wikipedia.org/wiki/Uniform_Resource_Identifier

A&A
Assicurazioni e autorità sono le istanze che ricevono le informazioni e i dati trasmessi dalle aziende nell'ambito dei processi di business Swissdec.

Profilo assicurativo (VProfil)
Informazioni sui rapporti contrattuali in essere fra un'azienda e un'assicurazione.

OFiEle
Ordinanza sui servizi di certificazione nel campo della firma elettronica e di altre applicazioni di certificati digitali del 23.11.2016

WS-Security (WSS)
Web Services Security (WS-Security, WSS) è sostanzialmente un'estensione del protocollo SOAP per estendere la sicurezza ai servizi web.

Certificato X.509
Standard che definisce l'infrastruttura a chiave pubblica (public key infrastructure) per la creazione di certificati digitali; è profilato nello standard RFC-5280.

FiEle
Legge sulla firma elettronica del 18.3.2016 (Stato 1.1.2017)

13 Riferimenti

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

14 Controllo versione

Versione	Data	Descrizione	Autore
1.0	20.7.2018	Versione 1.0 della Specifica dettagliata	Annett Laube
1.1	8.11.2018	Aggiornamento / adeguamento WSDL	Annett Laube
1.2	31.1.2019	Scorporo processo di registr. / config. FiEle	Annett Laube
1.3	4.4.2019	Descrizione della registrazione di fiduciari	Annett Laube
1.4	26.4.2019	Adeguamento cert. SUA, formattazione	Annett Laube
1.5	10.5.2019	Adeguamento contenuto cert. SUA, requisito CSR ed esempio di certificato in allegato	Gerhard Hassenstein

Allegato A

Esempio di certificato IDI:

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 = Divisione finanze
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