

Direttive Standard autenticazione delle aziende Swissdec CH (SUA)

Requisiti ricevitore finale

Le direttive per lo Standard autenticazione delle aziende Swissdec CH (SUA) sono state elaborate in collaborazione con:

- Suva
- Associazione Svizzera d'Assicurazioni

Editore

Swissdec
Fluhmattstrasse 1
6004 Lucerna
www.swissdec.ch

Indice

1.	Introduzione	6
1.1	Procedura semplificata per l'ottenimento del certificato	6
1.2	Istituzione e dominio	8
2.	Panoramica use case	10
2.1	Schemi d'insieme sugli use case	11
2.2	Spiegazioni sugli use case	12
2.3	Test	12
2.4	Sommario degli use case	12
2.4.1	UC001 Verifica del cliente / dell'azienda	12
2.4.2	UC002 Verifica della richiesta del cliente	12
2.4.3	UC003 Allestire l'esito della verifica	12
2.4.4	UC004 Contrassegno dei dati di test	12
2.4.5	UC005 Applicazione dei criteri di sicurezza	12
2.4.6	UC006 Verifica dell'accessibilità	12
2.4.7	UC007 Definizione delle finestre di manutenzione	12
2.4.8	UC008 Informazioni di supporto; esecuzione chiarimento manuale	12
2.4.9	UC009 Trattamento dei duplicati	13
2.5	Use case e operazioni correlate	13
3.	Use case	14
3.1	Use Case 001: Verifica del cliente / dell'azienda	14
3.2	Use case 002: Verifica della richiesta del cliente	15
3.2.1	Caso particolare: fiduciari	15
3.2.2	Caso particolare: nessun rapporto contrattuale in essere	15
3.3	Use case 003: Allestire l'esito della verifica	16
3.4	Use case 004: Contrassegno dei dati di test	16
3.5	Use case 005: Applicazione dei criteri di sicurezza	16
3.6	Use case 006: Verifica dell'accessibilità	17
3.7	Use case 007 Definizione delle finestre di manutenzione	17
3.8	Use case 008 Informazioni di supporto; esecuzione chiarimento manuale	18
3.9	Use case 009 Trattamento dei duplicati	18
4.	Requisiti supplementari	19
4.1	Creazione dei file di archivio	19
4.2	Versione SUA	19
4.3	Standard di comunicazione	19
4.4	Compressione facoltativa	19
4.5	Disponibilità	19
4.6	Intervalli di tempo definiti	20
4.7	Intervalli di valori definiti	20
4.8	Scalabilità	20
4.9	Modifiche all'interfaccia	20
4.10	Supporto e tempi di risposta	20
4.11	Prestazioni / rendimento	21
5.	Allegato	22
5.1	Riferimenti	22

Elenco delle figure

Fig. 1: Schema Registrazione / Configurazione SUA – 1° passo	7
Fig. 2: Schema Registrazione / Configurazione SUA – 2°, 3°, 4° e 5° passo	8
Fig. 3: Schema del processo Registrazione e Configurazione SUA	10
Fig. 4: Use case	11
Fig. 5: Diagramma di sequenza per l'ottenimento del certificato SUA	15

Elenco delle tabelle

Tabella 1: Carattere vincolante dei requisiti	5
Tabella 2: Use case e operazioni	13
Tabella 3: Use case 001 – Invio della notifica dei salari	14
Tabella 4: Use case 004 – Verifica dell'accessibilità	17
Tabella 5: Use case 007 – Definizione di finestre di manutenzione	17

Panoramica delle modifiche della versione 20190301

Direttive per lo Standard autenticazione delle aziende Swissdec CH (SUA) – Requisiti per il ricevitore finale, versione 20190301, edizione del 10.05.2021.

Capitolo	Modifica
Versione iniziale	

Convenzioni valide in questo documento

In questo documento sono usati i seguenti caratteri tipografici:

Text	Documentazione
Text	Codice
<Text>	Elemento XML
[TEXT]	Riferimento a un altro documento

Il carattere più o meno vincolante di ciascun requisito è espresso nel modo seguente:

Natura del vincolo	Forma di espressione
Obbligo	<i>deve</i>
Desiderio, auspicio	<i>dovrebbe</i>
Intenzione, proposito	<i>sarà</i>
Proposta	<i>può/è possibile</i>

Tabella 1: Carattere vincolante dei requisiti

Attenzione:

In alcuni casi gli schemi contenuti nel presente documento si riferiscono a versioni più datate, in quanto sufficienti per la comprensione degli aspetti concettuali; tuttavia, gli unici documenti sempre **vincolanti sono i file XML**¹ (ufficiali, ad es. Web Services Description Language (WSDL), XML Schema Definition (XSD), Extensible Stylesheet Language (XSL) Transformation e XML Instance Documents).

¹ www.swissdec.ch

1. Introduzione

Questo documento contiene i requisiti funzionali, tecnici e supplementari per il ricevitore finale (Endreceiver), che sono applicabili nel quadro dello Standard autenticazione delle aziende Swissdec CH (SUA), e precisamente i requisiti per l'ordine del certificato. La sicurezza del processo (autenticazione e carattere vincolante) nell'ambito dei processi Swissdec nei quali si applica l'autenticazione delle aziende Swissdec è descritta nelle specifiche dei processi interessati. Questo documento illustra invece gli aspetti tecnici dello standard e non la logica specialistica. Quando si ordina un certificato, il ricevitore finale è la parte che identifica l'azienda e verifica l'IDI dell'UST.

Una panoramica della procedura standardizzata è utile alla comprensione delle specifiche descritte nel seguito. Essa è fornita dal documento riepilogativo «OverviewUnternehmensAuthentifizierung.pdf» (OVOA, 2019) al quale questo documento fa riferimento.

1.1 Procedura semplificata per l'ottenimento del certificato

Per poter effettuare una registrazione è indispensabile avere un rapporto contrattuale in essere con un'assicurazione. Nel prosieguo i «ricevitori finali» sono assimilati ai «destinatari finali presso assicuratori e autorità (A&A)».

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 (IDI dell'UST, nome dell'azienda come risulta dall'iscrizione nel registro di commercio ecc.).

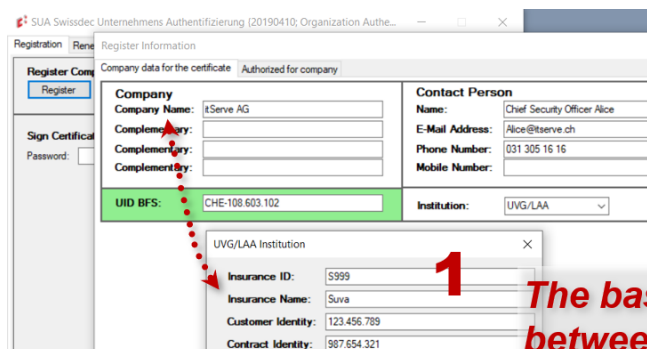
Nell'ambito della distribuzione o dell'ottenimento di un certificato SUA, si parla spesso di due fasi fondamentali, ossia:

- «ordine» mediante *registrazione* (RLOA, 2019)
- «attivazione» mediante *configurazione* (RLOA, 2019)

Schema Registrazione / Configurazione SUA – 1° passo:

Se un'azienda desidera registrarsi per ottenere il certificato SUA, un suo collaboratore seleziona nel sistema ERP un'assicurazione (destinatario finale A&A), che sarà utilizzata per identificare l'azienda in questione. Le informazioni necessarie per la registrazione (dati 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 per un determinato IDI dell'UST. Al sistema ERP viene comunicato l'esito della verifica mediante l'invio di un CertificateRequest-ID (CRID) appositamente generato, che identifica in modo univoco il sistema ERP e la richiesta (Request).



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

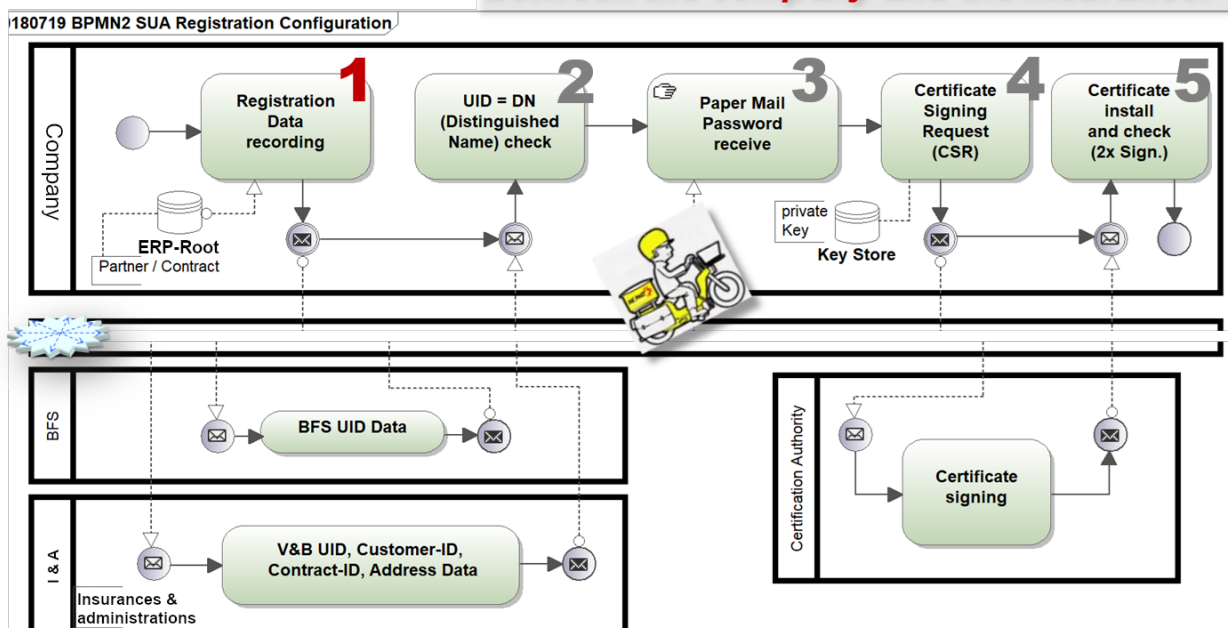


Fig. 1: Schema Registrazione / Configurazione SUA – 1° passo

Schema Registrazione / Configurazione SUA – 2° passo:

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'istituzione A&A selezionata in precedenza la quale verifica, con l'ausilio dei propri dati di base, la validità e la congruità dei dati 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).

Schema Registrazione / Configurazione SUA – 3° passo:

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 SUA.

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.

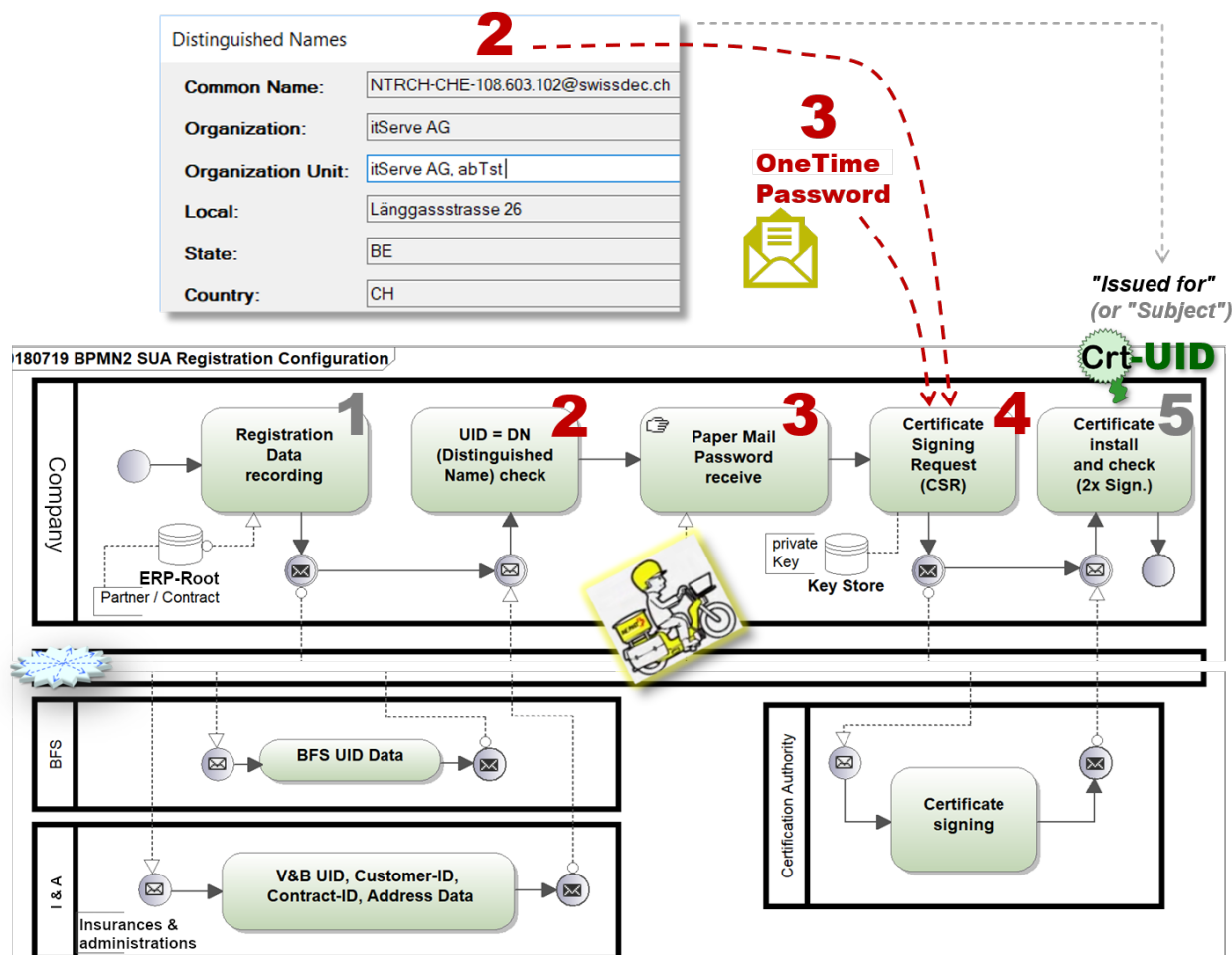


Fig. 2: Schema Registrazione / Configurazione SUA – 2°, 3°, 4° e 5° passo

Schema Registrazione / Configurazione SUA – 4° e 5° passo:

A questo punto il collaboratore può prelevare il certificato generando una richiesta CSR (Certificate Sign Request) e utilizzando la password ricevuta dall'azienda tramite la lettera di cui sopra (3° passo), dopodiché può installarlo automaticamente in loco nel sistema ERP. Per completare il processo, il corretto funzionamento del nuovo certificato SUA sarà verificato almeno mediante l'operazione `Operation OrganizationAuthenticationRenewPort.CheckInteroperability()`, che richiede due firme.

Il processo di registrazione SUA si conclude nel momento in cui il trasmettitore riesce a eseguire correttamente una trasmissione con il certificato SUA.

Attenzione:

Il ricevitore finale è coinvolto solo nel 1° e 2° passo. I restanti passi, come ad esempio la verifica dei certificati, riguardano solo il trasmettitore e il distributore.

Per una descrizione dettagliata del processo rimandiamo alle direttive e al progetto di dettaglio (RLOA, 2019).

1.2 Istituzione e dominio

La SUA è applicabile a diversi processi di trasmissione Swissdec e sarà infatti impiegata in molteplici contesti. Tuttavia, poiché l'identificazione delle aziende è obbligatoria nell'ambito dello Standard prestazioni CH (KLE) ma attualmente facoltativa per lo Standard salari CH (KLE), gli esempi proposti qui di seguito si riferiscono soprattutto al primo. Ad ogni modo, le informazioni riportate di seguito si applicano a tutti gli standard Swissdec che consentono di utilizzare la SUA.

In questo documento si distingue fra il termine dominio e istituzione.

Dominio: ramo assicurativo in relazione al quale vengono trasmessi i dati. Lo Standard prestazioni CH (KLE) supporta i domini LAINF, LAINFC, AIC e IGM.

Istituzione: destinatario che riceve i dati. In questo caso si tratta di assicurazioni che appartengono ai rispettivi domini.

Un'impresa può pertanto entrare in contatto con diverse istituzioni all'interno di un dominio. Un'istituzione può altresì supportare più domini.

2. Panoramica use case

Lo schema seguente illustra una prima panoramica del processo completo che consente di ottenere un certificato SUA.

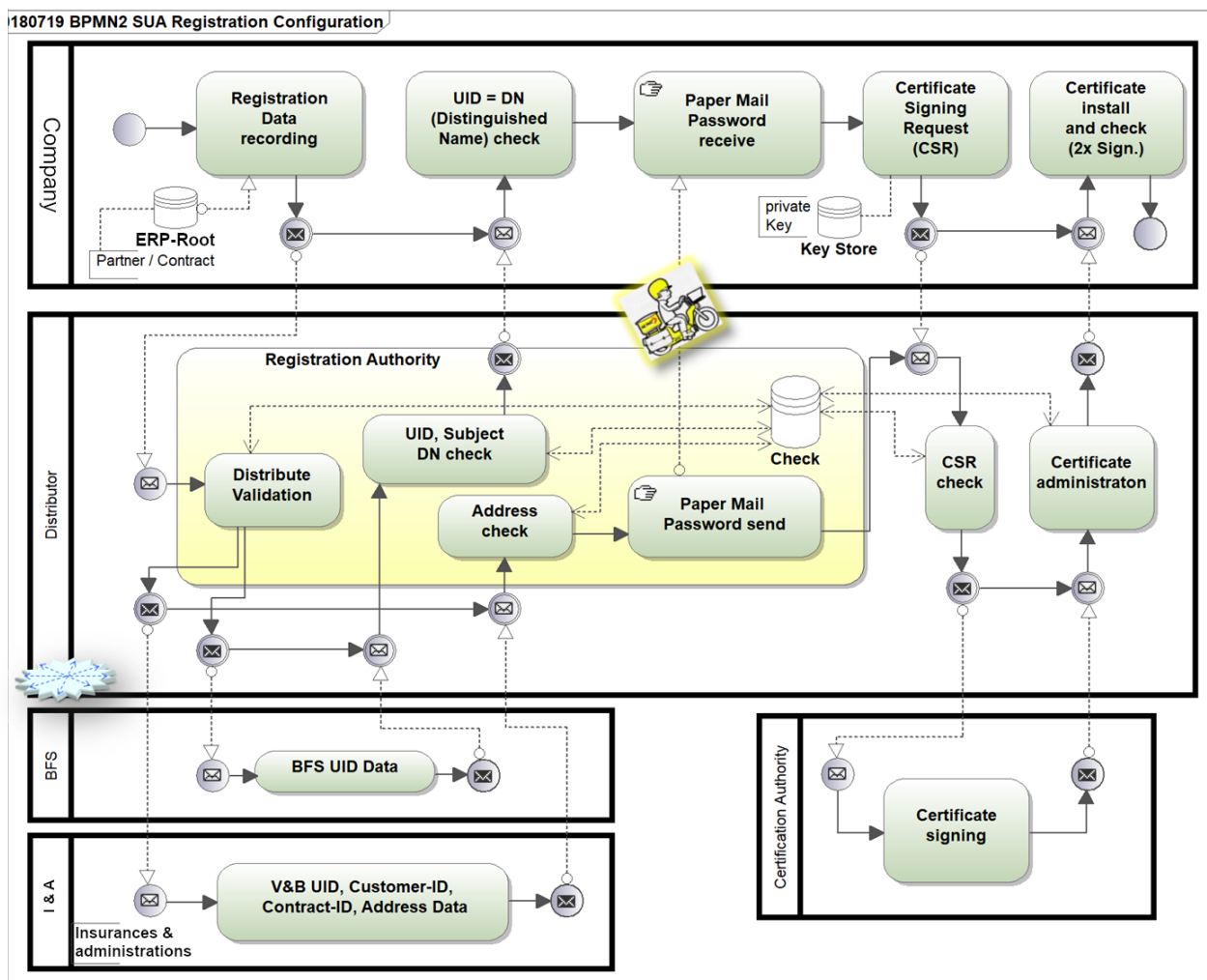


Fig. 3: Schema del processo Registrazione / Configurazione SUA

2.1 Schemi d'insieme sugli use case

Una parte degli use case è strutturata in modo analogo agli altri standard Swissdec. Per questo motivo, fra gli elementi dello schema XML è possibile trovare il concetto «IDI dell'UST», che coincide sostanzialmente con il termine IDI (nello storico o ad es. in DeclareSalary ... CompanyDescription/IDI-UST). Alla luce delle analogie esistenti fra i vari standard si è deciso di mantenere parte delle designazioni precedenti, in modo da semplificare l'implementazione del progetto.

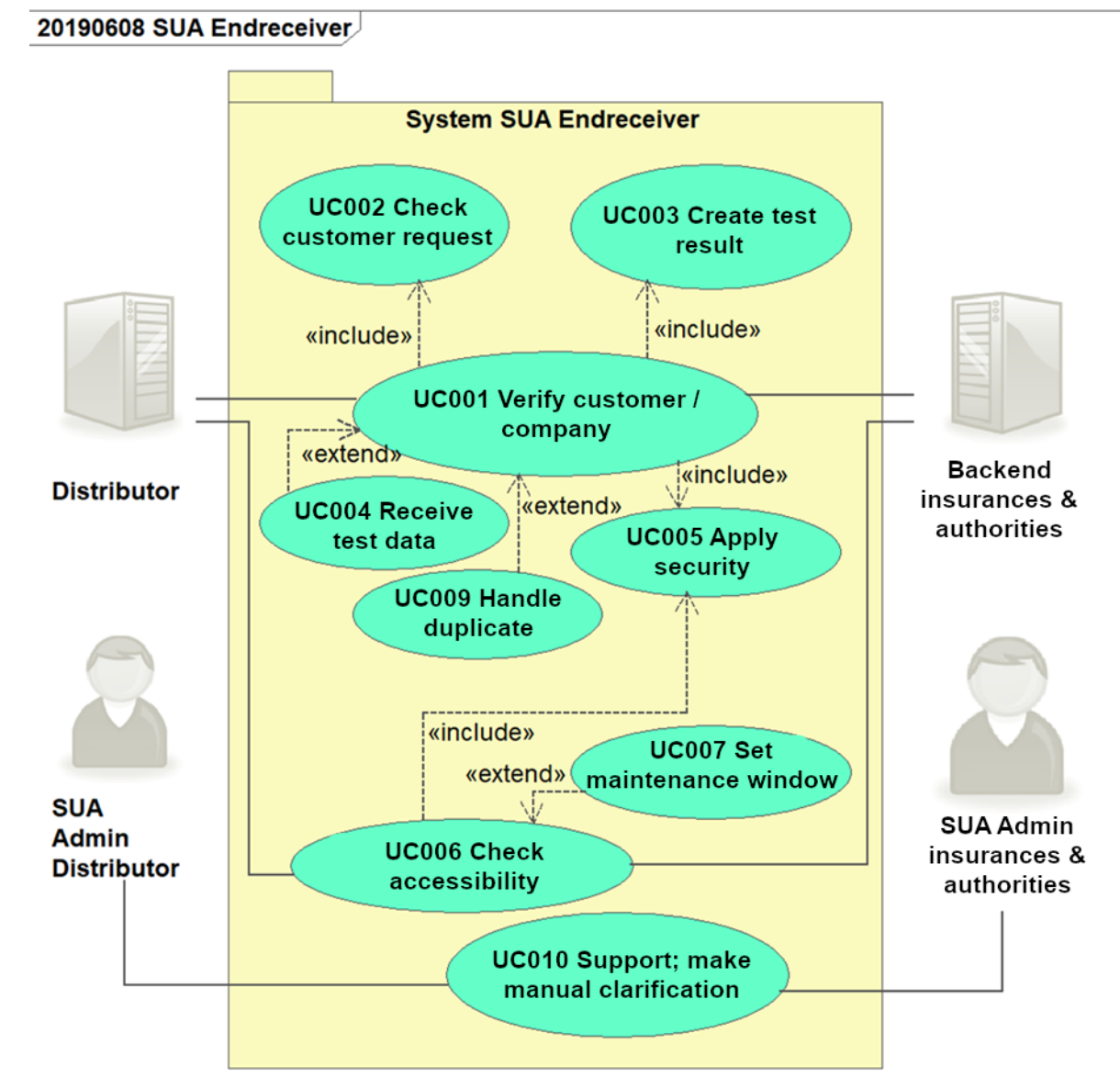


Fig. 4: Use case

2.2 Spiegazioni sugli use case

I requisiti illustrati come use case si riferiscono alla parte tecnica di un sistema del ricevitore finale, che riceve l'ordine di un certificato SUA e fornisce la relativa risposta.

Per il collaudo, un ricevitore finale *deve* soddisfare sempre i seguenti requisiti di sistema:

- UC001 Verifica del cliente / dell'azienda
- UC002 Verifica della richiesta del cliente
- UC003 Allestire l'esito della verifica
- UC004 Contrassegno dei dati di test
- UC005 Applicazione dei criteri di sicurezza
- UC006 Verifica dell'accessibilità
- UC007 Definizione delle finestre di manutenzione
- UC008 Informazioni di supporto; esecuzione chiarimento manuale
- UC009 Trattamento dei duplicati

La modalità di interazione fra utente e sistema dipende dalle scelte operate dal produttore del sistema e non è oggetto di queste specifiche.

2.3 Test

I test di collaudo si riferiscono agli use case. Insieme ai requisiti, essi contribuiscono alla comprensione complessiva del sistema previsto. I vari test sono generalmente delineati dallo sviluppatore stesso già durante la fase di sviluppo (Test Driven Development).

2.4 Sommario degli use case

2.4.1 UC001 Verifica del cliente / dell'azienda

Un nuovo certificato viene ordinato via distributore. L'assicuratore (A&A) deve verificare i dati relativi al contratto del cliente / dell'azienda. A tal fine si utilizzano altri use case: UC002, UC003, UC004 e UC005.

2.4.2 UC002 Verifica della richiesta del cliente

Con il processo di ordine / registrazione effettivo, il destinatario finale (A&A) verifica l'identità del richiedente. A tale scopo i dati forniti vengono confrontati con i dati relativi al contratto / dati di base presso l'A&A.

Nota: per motivi di sicurezza, il distributore non trasmette l'IDI dell'UST.

2.4.3 UC003 Allestire l'esito della verifica

Una volta condotta la verifica con esito positivo (UC002), tutti i dati vengono forniti contrassegnati con l'elemento <Success> (incl. IDI dell'UST).

2.4.4 UC004 Contrassegno dei dati di test

Qualsiasi messaggio può essere contrassegnato come caso di test. Un tale messaggio viene spedito attraverso il sistema produttivo, ma non elaborato in produzione dal ricevitore finale. Nel caso della SUA, la risposta del ricevitore finale è identica a prescindere dal fatto che si tratti di un caso di test o di un messaggio reale in ambiente produttivo.

2.4.5 UC005 Applicazione dei criteri di sicurezza

Ogni messaggio inviato deve essere firmato e crittografato.

2.4.6 UC006 Verifica dell'accessibilità

Viene inviato un messaggio a intervalli regolari per verificare l'accessibilità del ricevitore finale e le eventuali finestre di manutenzione pianificate.

2.4.7 UC007 Definizione delle finestre di manutenzione

Occorre configurare una finestra temporale e una notifica per i lavori di manutenzione, da poter fornire come risposta (Response) alla richiesta (Request) del distributore.

2.4.8 UC008 Informazioni di supporto; esecuzione chiarimento manuale

Tutte le informazioni di supporto (notifiche, segnalazioni di guasti) devono essere presentate in modo chiaramente comprensibile per l'utente finale. L'utente deve sapere da dove proviene il messaggio e come rispondere. Quando un'azienda richiede supporto, deve essere possibile fornirle informazioni.

2.4.9 UC009 Trattamento dei duplicati

I duplicati di richieste (Request) complete sono contrassegnati dal distributore. Le eventuali informazioni contenute nel duplicato non ancora elaborate o alle quali non è ancora stata data una risposta vanno trattate. Ulteriori duplicati devono poter essere riconosciuti e trattati sia nella fase `RegisterOrganizationConsumer`, sia nella fase `GetResultFromOrganizationRegistrationConsumer`.

2.5 Use case e operazioni correlate

Il modello sottostante è un sistema Client-Server dove il distributore è il Client. Vengono impiegati gli standard WSDL e XML Schema. Le seguenti operazioni ed elementi si trovano nel file WSDL associato (WSDL0A, 2019) e nello schema descrittivo (XS0A, 2019). La procedura e il protocollo sono illustrati in (RLOA, 2019).

Use case	Operazione / Elemento
	<i>OrganizationAuthenticationService WSDL / XSD</i>
UC001 Verifica del cliente / dell'azienda UC002 Verifica della richiesta del cliente UC003 Allestire l'esito della verifica UC004 Contrassegno dei dati di test UC005 Applicazione dei criteri di sicurezza	<ul style="list-style-type: none">▪ <code>RegisterOrganizationConsumer</code>▪ <code>RegisterOrganizationConsumerResponse</code>▪ <code>GetResultFromRegisterOrganizationConsumer</code>▪ <code>GetResultFromRegisterOrganizationConsumerResponse</code>▪ <code>OrganizationAuthenticationConsumerFault</code>
UC006 Verifica dell'accessibilità UC007 Definizione delle finestre di manutenzione	<ul style="list-style-type: none">▪ <code>PingConsumer</code>▪ <code>PingConsumerResponse</code>▪ <code>OrganizationAuthenticationConsumerFault</code>

Tabella 2: Use case e operazioni

3. Use case

3.1 Use Case 001: Verifica del cliente / dell'azienda

Breve descrizione	Un nuovo certificato SUA viene ordinato via distributore. L'assicuratore (A&A) deve verificare i dati relativi al contratto del cliente / dell'azienda.
Attori	Distributore, ricevitore finale
Fattore scatenante	Un dipendente dell'azienda (addetto alla sicurezza) desidera acquistare un certificato SUA e il distributore riceve la relativa richiesta.
Prerequisiti	Il sistema ERP è in grado di trasmettere e ricevere messaggi SUA comunicati in forma elettronica ed è in possesso di un certificato ERP.
Post-condizioni	<ul style="list-style-type: none"> La verifica sui dati dell'azienda ha dato esito positivo I dati corrispondenti (incl. IDI dell'UST) sono stati recuperati. <p>In caso di errore:</p> <ul style="list-style-type: none"> Messaggio di errore
Use case inclusi	UC002 Verifica della richiesta del cliente UC003 Allestire l'esito della verifica UC004 Contrassegno dei dati di test UC005 Applicazione dei criteri di sicurezza
Procedura standard	<p>1. UC002: Con il processo di ordine / registrazione effettivo, ossia l'operazione <code>RegisterOrganizationConsumer</code>, il destinatario finale (A&A) verifica l'identità del richiedente. A tale scopo i dati forniti vengono confrontati con i dati relativi al contratto / dati di base presso l'A&A. Nota: per motivi di sicurezza <i>non</i> viene trasmesso l'IDI dell'UST.</p> <p>2. Una volta condotta la verifica con esito positivo (UC002), tutti i dati <i>devono</i> essere forniti contrassegnati con l'elemento <code><Success></code> (incl. IDI dell'UST). Il risultato viene quindi recuperato in modo asincrono con l'operazione <code>GetResultFromOrganizationRegistrationConsumer</code>. Se nell'operazione iniziale <code>RegisterOrganizationConsumer</code> è presente l'attributo <code>WithDelegate</code>, significa che la richiesta proviene da un «fiduciario» (). In tal caso, nella fase <code>GetResultFromOrganizationRegistrationConsumer</code> <i>devono</i> essere forniti anche tutti i delegati.</p>
Procedura alternativa	<p>{UC008} I dati vengono riconosciuti come dati di test Come da procedura standard, dal 1° al 2° passo</p> <p>{1° passo: Finestra / servizio di manutenzione non disponibile} L'informazione sulla finestra di manutenzione (da-a) è già stata trasmessa al distributore mediante UC006 «Verifica dell'accessibilità». Durante le finestre di manutenzione, il distributore restituisce i messaggi di risposta con l'informazione indicante l'interruzione direttamente al sistema ERP richiedente.</p> <p>{1° passo: Interruzione non prevista / servizio non disponibile} In questo caso il distributore invia direttamente al sistema ERP richiedente un messaggio d'errore, vedi (ACKNSwissdec, 2020). Il distributore riceve un messaggio di errore.</p> <p>{1° passo: Rilevamento di un doppione, procedura UC009 «Trattamento dei duplicati»}</p> <p>{1° passo: Criteri di sicurezza non soddisfatti, respingimento del messaggio}</p>
Elenco degli errori	<p>Errori tecnico-specialistici:</p> <ul style="list-style-type: none"> Il messaggio viola le regole di plausibilità. <p>Errori tecnici:</p> <ul style="list-style-type: none"> Errore di firma / cifratura / decodifica. Il messaggio allestito dal distributore non corrisponde allo schema (validità non data).

Tabella 3: Use case 001 – Invio della notifica dei salari

20190531 SUA Certificate distribution (1:D:1)

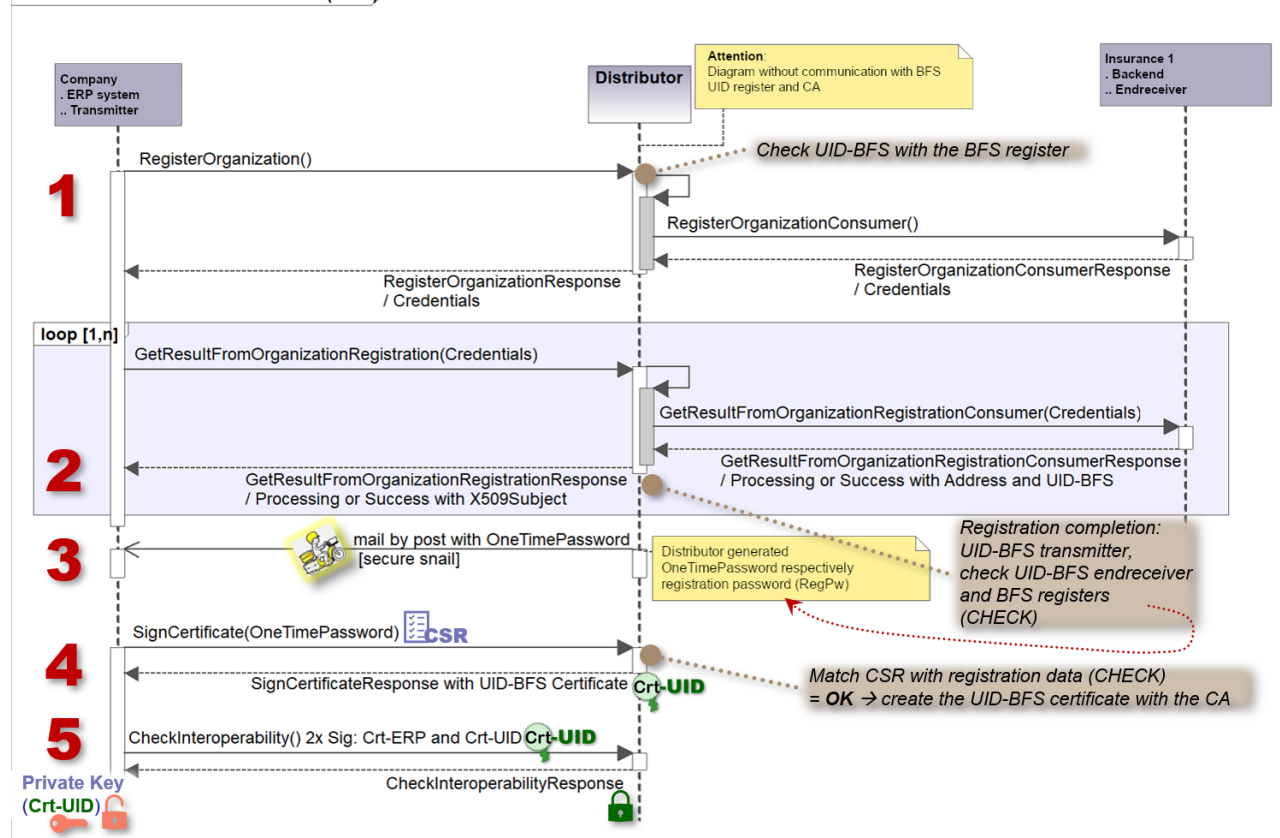


Fig. 5: Diagramma di sequenza per l'ottenimento del certificato SUA

3.2 Use case 002: Verifica della richiesta del cliente

Il destinatario finale confronta i dati ricevuti dal distributore con quelli relativi al contratto e/o con i dati di base, quindi li ritrasmette al distributore. Si precisa tuttavia che, per motivi di sicurezza, l'IDI dell'UST non viene inviato.

A questo punto il destinatario finale può autorizzare la prosecuzione del processo SUA oppure interromperlo, garantendo così l'emissione di certificati SUA esclusivamente per rapporti contrattuali validi.

3.2.1 Caso particolare: fiduciari

Se un'azienda è assistita da un fiduciario, quest'ultimo può richiedere un certificato SUA a favore dell'impresa, a condizione che il fiduciario sia noto al destinatario finale.

In questo caso sarà il fiduciario a comunicare al distributore le informazioni sull'azienda necessarie per richiedere il certificato SUA. Inoltre fornirà, sempre al distributore, anche informazioni sul proprio conto.

A&A non ricevono dal distributore informazioni dettagliate sul fiduciario, ma solo l'attributo `WithDelegate`.

A questo punto il destinatario finale verifica se sono noti uno o più fiduciari presso l'azienda. In caso affermativo, trasmette al distributore le informazioni sui fiduciari noti per l'azienda in questione. Il distributore confronta le informazioni così ricevute con quelle del trasmettitore e valuta se coincidono almeno per uno dei fiduciari, in modo da poter autorizzare l'emissione di un certificato SUA. In caso contrario, il processo viene interrotto. A questo punto l'azienda e A&A dovranno chiarire e aggiornare le informazioni sui fiduciari, dopodiché occorrerà avviare un nuovo processo.

3.2.2 Caso particolare: nessun rapporto contrattuale in essere

In rari casi eccezionali, può capitare che un'azienda e A&A debbano scambiarsi informazioni sebbene non siano legate da alcun rapporto contrattuale. Ad esempio se, nell'ambito dello Standard prestazioni CH (KLE), si verifica una ricaduta di un paziente che nel frattempo ha cambiato posto di lavoro e assicurazione.

Al momento lo standard non prevede una soluzione per simili casistiche, ma in futuro, con una prossima versione, si intende consentire l'identificazione IDI tramite un raffronto con i dati delle autorità fiscali, in modo da poter eseguire il processo di registrazione SUA.

3.3 Use case 003: Allestire l'esito della verifica

Una volta appurata con successo la corrispondenza tra le informazioni, il destinatario finale mette a disposizione i dati in suo possesso, che si potranno recuperare dal distributore con il comando `GetResultFromRegisterOrganizationConsumer`.

A questo punto, se la verifica ha dato esito positivo, il destinatario finale trasmette la risposta al distributore mediante `GetResultFromRegisterOrganizationConsumerResponse`.

In caso di errore (tecnico o tecnico-specialistico), il destinatario finale può interrompere il processo generando una segnalazione in tal senso (`OrganizationAuthenticationConsumerFault`).

3.4 Use case 004: Contrassegno dei dati di test

Quando si ordina un certificato SUA, è possibile contrassegnarlo come caso di test. Questo avviene inserendo l'elemento `<TestCase>` in posizione appropriata nell'istanza XML (in base allo schema). L'evento viene elaborato normalmente dal distributore, ma viene trattato come caso di test dal destinatario finale.

Questo use case serve a individuare eventuali problemi nella catena di trasmissione produttiva. I messaggi dell'impresa dovrebbero attraversare l'intera catena automatizzata dei sistemi coinvolti (ERP, trasmettitore, distributore, ricevitore finale) e dei loro componenti senza avviare una transazione effettiva. **Non vengono creati certificati.**

Qualsiasi altra azione relativa a questa procedura *deve* parimenti essere contrassegnata come caso di test.

Non ci devono essere forme miste nella trasmissione: ciò che inizia come caso di test *deve* anche terminare come caso di test.

Questo use case andrebbe utilizzato solo in casi eccezionali. *Non* deve essere utilizzato a scopi di dimostrazione o di sviluppo. Per questi scopi sono disponibili un'applicazione di riferimento o uno showcase.

3.5 Use case 005: Applicazione dei criteri di sicurezza

Ad eccezione del test di accessibilità, ogni trasmissione e ogni risposta *devono* essere firmate e crittografate. Per maggiori informazioni sono disponibili i documenti sulla sicurezza dal lato destinatario (vedi SECER, 2020)).

3.6 Use case 006: Verifica dell'accessibilità

Lo use case «Verifica dell'accessibilità» presuppone la cifratura SSL a 2 vie. La richiesta e la risposta sono firmate e i dati XML cifrati come indicato in (SECER, 2020).

Breve descrizione	L'accessibilità del ricevitore finale dovrebbe essere verificata a partire dal distributore. Allo scopo è sufficiente l'invio di una semplice richiesta PingConsumerRequest come indicato in (WSDLOA, 2019) al ricevitore finale, il quale a sua volta confermerà l'accessibilità con la risposta PingConsumerResponse.
Attori	Distributore, operatore del distributore
Fattore scatenante	Verifica ciclica da parte del distributore, dell'operatore (Operator) in caso di malfunzionamento
Prerequisiti	Nessuno
Post-condizioni	Nessuna
Use case inclusi	UC005 Applicazione dei criteri di sicurezza
Procedura standard	<ol style="list-style-type: none"> 1. Il distributore invia la richiesta al ricevitore finale. In aggiunta viene comunicato l'intervallo del polling. Intervallo: attualmente 30 minuti (anche durante una finestra di manutenzione; l'intervallo è pertanto dinamico) 2. Verifica della sicurezza UC005. 3. Il ricevitore finale risponde con il suo timestamp attuale, vedi <PingConsumerResponse>.
Procedura alternativa	{3° passo: facoltativamente può essere comunicata al distributore una finestra di manutenzione pianificata (non disponibilità da x a y) mediante UC007 «Definizione delle finestre di manutenzione». Questa funzione <i>deve</i> essere implementata.}
Elenco degli errori	Errori tecnici: <ul style="list-style-type: none"> ▪ Messaggio non valido. ▪ Il messaggio non può essere decifrato.

Tabella 4: Use case 004 – Verifica dell'accessibilità

3.7 Use case 007 Definizione delle finestre di manutenzione

Breve descrizione	Estensione di UC006 «Verifica dell'accessibilità». Il ricevitore finale <i>deve</i> implementare una funzionalità che permetta di inserire i dati inerenti alle finestre di manutenzione e comunicarli al distributore nella risposta a UC006 «Verifica dell'accessibilità».
Attori	Amministratore tecnico del ricevitore finale
Fattore scatenante	Verifica ciclica da parte del distributore, dell'operatore in caso di malfunzionamento
Prerequisiti	Nessuno
Post-condizioni	Nessuna
Use case inclusi	Nessuno
Procedura standard	<ol style="list-style-type: none"> 1. L'amministratore tecnico del ricevitore finale inserisce i dati riguardanti la finestra di manutenzione. 2. La risposta del ricevitore finale (PingConsumerResponse) al distributore contiene i dati inseriti relativi alla finestra di manutenzione.
Procedura alternativa	Nessuna
Elenco degli errori	Errori tecnici: <ul style="list-style-type: none"> ▪ Messaggio non valido.

Tabella 5: Use case 007 - Definizione di finestre di manutenzione

3.8 Use case 008 Informazioni di supporto; esecuzione chiarimento manuale

Quando un'azienda richiede supporto in relazione all'ordine di un certificato, deve essere possibile fornirle informazioni in merito. Il collaboratore (lato destinatario) deve quindi essere in grado di individuare l'origine dei problemi consultando i file di log e i messaggi di errore. Ad esempio, anche le richieste (Request) non andate a buon fine devono comunque comparire nei log ed essere tracciabili in base agli ID utilizzati.

3.9 Use case 009 Trattamento dei duplicati

I duplicati di una richiesta `RegisterOrganization` sono individuati dal distributore tecnicamente (bit identici) e marcati con l'elemento `<Duplicate>` in `DistributorRequestContext`. Ciò tuttavia implica che il distributore può individuare univocamente un duplicato, per cui nella prassi non si utilizza più l'elemento `<Duplicate>`.

Di conseguenza non esisteranno più duplicati, in quanto il distributore assegna un nuovo `CertificateRequest-ID` a ogni richiesta. Pertanto, ad ogni richiesta `RegisterOrganization` relativa a un'azienda, anche se ripetuta, deve essere data una normale risposta.

4. Requisiti supplementari

4.1 Creazione dei file di archivio

Questo requisito garantisce il backup di una copia di ciascun messaggio inviato e ricevuto. I dati devono essere allestiti in forma di richiesta SOAP e archiviati come documento di istanza XML. I file di archivio devono essere firmati, ma non devono essere crittografati.

4.2 Versione SUA

Lo schema contiene l'elemento `<RequestContext/UserAgent/StandardVersion>`, che identifica la versione in uso dello Standard autenticazione delle aziende Swissdec CH (SUA). Questa indicazione è necessaria in ragione degli adattamenti svolti nelle varie versioni che non si riferiscono allo schema ma esclusivamente al contenuto degli elementi; vale a dire che, a seconda della versione dello Standard autenticazione delle aziende Swissdec CH (SUA), il contenuto degli elementi può essere definito in modo differente.

4.3 Standard di comunicazione

La connessione con lo Standard *deve* avvalersi della tecnologia web service (SOAP² versione 1.1, WSDL³ versione 1.1 e WSS⁴ versione 1.0). I dati *devono* essere cifrati sia nel layer HTTPS⁵ (two-way SSL/TLS), sia a livello SOAP in base a WSS (SECER, 2020).

4.4 Compressione facoltativa

È facoltativa la compressione delle richieste (Request) e delle risposte (Response). In ragione della grande quantità di informazioni ridondanti, i dati XML possono essere compressi fortemente. L'esperienza suggerisce un tasso di compressione di circa il 50 per cento. Per consentire lo smistamento, per il tramite del distributore, di notifiche di eventi voluminose e risparmiare larghezza di banda per tutti i partecipanti, vi è la possibilità di comprimere le richieste in uscita dal distributore su base GZIP. L'eventuale compressione viene stabilita al momento della connessione.

In caso di compressione GZIP del corpo (body) del messaggio, le richieste in uscita dal distributore possiedono almeno i seguenti campi nell'intestazione http:

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

Le risposte compresse provenienti dai ricevitori finali *devono* contenere, qualora sia stata applicata la compressione, il campo seguente:

- Content-Encoding: gzip

Ulteriori informazioni sono disponibili all'indirizzo seguente <http://www.ietf.org/rfc/rfc1952.txt>

4.5 Disponibilità

L'unità di riferimento comprende il distributore e tutti i ricevitori finali con cui è stata stabilita una connessione: ciò significa che, per l'azienda (fonte dei dati relativi all'evento), l'intero sistema è come una singola unità. Se il ricevitore finale non dovesse operare al livello di qualità atteso, finirebbe col ridurre l'affidabilità dell'intero sistema. Tutti i partecipanti devono pertanto concordare un'affidabilità **minima**.

Requisiti emananti dallo Standard prestazioni CH

- Tutte le trasmissioni m2m (da macchina a macchina) avvengono in **«tempo reale» (disponibilità Internet 7 giorni su 7, 24 ore su 24)**

Questo requisito comporta quanto segue per il destinatario:

- Anche le istituzioni e i loro ricevitori finali **devono** offrire al minimo **un servizio di ricezione dei dati su base 7x24**.
- **Le interruzioni pianificate⁶ (ad. es. finestre di manutenzione)** *devono* essere svolte in fasce orarie a traffico ridotto e *devono* essere annunciate in anticipo (vedi Use case UC003: «Verifica dell'accessibilità»).
- A seguito di un'**interruzione non pianificata**, le imprese interessate da un trasferimento dati fallito *dovrebbero* essere informate del ripristino della disponibilità del destinatario.
- Qualora i servizi interni preposti alla verifica dell'accettazione **non dovessero essere disponibili**, *può* comunque essere confermata l'accettazione. Ciò *dovrebbe* essere comunicato al mittente con un'allerta / avviso nella conferma.

² SOAP (originariamente Simple Object Access Protocol)

³ Il Web Services Description Language (WSDL) è una specifica XML neutrale, non legata quindi a nessuna piattaforma, linguaggio di programmazione o protocollo per la descrizione dei servizi di rete (web services) preposti allo scambio di informazioni.

⁴ Web Services Security (WSS) della Organization for the Advancement of Structured Information Standards (OASIS)

⁵ http 1.0 o 1.1; almeno TLS 1.2 con chiave minima di sessione a 256 bit

⁶ Si applica ai normali interventi di manutenzione, ad eccezione di hot fix e patch

Se un controllo successivo dei dati porta al rifiuto del messaggio, la segnalazione al cliente di questa fattispecie avviene al di fuori di queste specifiche.

Approccio orientato all'obiettivo a riguardo della disponibilità:

Vogliamo adottare una **visione orientata al cliente**. Le disponibilità dei sistemi vanno intese come **valori target futuri**. Ciò motiva le aziende a inoltrare le notifiche in forma elettronica. Riguardo alla disponibilità non sono previsti controlli. Pertanto, in questo documento sono stabiliti solo dei valori di riferimento, mentre per i rispettivi fondamenti si rimanda all'allegato.

4.6 Intervalli di tempo definiti

- Orari di operatività dell'intero sistema (distributore, comunicazione e ricevitore finale, tragitto m2m, fino alla risposta di conferma all'impresa)
 - 7 giorni la settimana per 24 ore al giorno
 - Fasce orarie di punta: tranne che nei fine settimana, tutti i giorni dalle ore 06:00 alle 20:00 (il tempo rimanente è fascia oraria ridotta)
- Finestre di manutenzione per correzioni e aggiornamenti
 - 10 ore alla settimana
 - Al di fuori degli orari di punta, possibilmente tra le ore 02:00 e le 05:00
- Orario di servizio e supporto per i partecipanti al sistema (distributore e rispettivi ricevitori finali)
 - Orario d'ufficio abituali
 - Supporto per finestre di manutenzione annunciate

4.7 Intervalli di valori definiti

L'obiettivo è di disporre di una soluzione pragmatica = «lightweight construction» e «best effort»

- Durante gli **orari di punta** la disponibilità del ricevitore finale (m2m) **dovrebbe** essere almeno del 99,52%.
- Nelle **fasce orarie ridotte** la disponibilità del ricevitore finale (m2m) **dovrebbe** essere almeno del 93,00%.

4.8 Scalabilità

I sistemi del destinatario finale dovrebbero essere in grado di scalare in base ai carichi previsti. È ipotizzabile iniziare con una soluzione minimale, che potrà essere potenziata in base alla crescita delle esigenze per garantire il livello di disponibilità e di prestazioni richieste.

4.9 Modifiche all'interfaccia

- Qualora modifiche apportate allo Standard autenticazione delle aziende Swissdec CH (SUA) venissero attivate anche presso il ricevitore finale, *deve* essere adattata l'intera connessione (da parte del distributore e del ricevitore finale).
- Se nessuna delle modifiche dello Standard autenticazione delle aziende Swissdec CH (SUA) deve essere attivata presso il ricevitore finale, il distributore *può* trasformare la struttura dati esistente (mappatura), a condizione che ciò sia possibile in termini di contenuto («firewall di progettazione»).

Il distributore trasmetterà sempre dati definiti in modo chiaro dal punto di vista tecnico-specialistico. Al momento non è prevista alcuna soluzione generica.

4.10 Supporto e tempi di risposta

Per quanto riguarda le attività di supporto, sono stabiliti unicamente gli aspetti tecnici; vale a dire che in questa sede vengono definite solo le infrastrutture informative per tutti i sistemi nella catena di processo.

Il supporto *deve* essere fornito in tedesco, francese e italiano per i seguenti settori o attori:

- Le imprese e i loro produttori ERP
- Le istituzioni destinatarie finali (ricevitori finali)

Ciò significa che anche i messaggi di errore devono essere visualizzati, almeno in parte, nelle lingue di destinazione previste. Vedi il messaggio:

.../RequestContext/LanguageCode

Per determinare i tempi di reazione vengono definite le seguenti **classi di errore**

- Critical = 15 min.

- Medium = 4 ore
- Uncritical = 1 giorno

Queste classi di errore vengono usate in vari sistemi (applicazioni, file di log, strumenti di monitoraggio ecc.). Inoltre, il supporto di 2° livello *deve* essere coordinato con gli sviluppatori dell'applicazione.

4.11 Prestazioni / rendimento

- La quantità massima di dati deve essere stabilita da ciascun ricevitore finale; i sistemi vanno pertanto dimensionati (scalati) di conseguenza.
- Tempo di risposta (tutte le operazioni): l'intera trasmissione dovrebbe avvenire «in tempo reale». Il tempo di trasmissione o di smistamento dovrebbe essere **inferiore a un minuto**. Per il ricevitore finale ciò significa che:

- il tempo di elaborazione dipende dal ricevitore finale, dal volume di dati e dalla capacità della linea;
- la risposta *dovrebbe* arrivare entro 20 secondi;
 - il distributore stabilisce inoltre un tempo di attesa massimo per ogni ricevitore finale (timeout: valore di default attuale = 60 secondi).

5. Allegato

5.1 Riferimenti

I seguenti riferimenti possono essere scaricati, in parte raggruppati in file zip, da Internet. I file index.html in essi contenuti permettono di accedere a informazioni, alla panoramica e a singoli documenti.

ACKNSwissdec, S. (2020). AcknowledgementNotification. Bern, Schweiz.

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

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

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

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