

Direttive Swissdec Standard autenticazione delle aziende Swissdec CH (SUA)

Requisiti trasmettitore

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

Sommario

1.	Introduzione	6
1.1	Procedura semplificata per l'ottenimento del certificato	6
1.2	Istituzione e dominio	8
2.	Panoramica use case Trasmettitore	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 Ottenimento del certificato SUA	12
2.4.2	UC002 Ordine / Registrazione	12
2.4.3	UC003 Attivazione	12
2.4.4	UC004 Verifica dell'accessibilità	12
2.4.5	UC005 Verifica dell'interoperabilità (firma singola)	12
2.4.6	UC006 Rinnovo del certificato	12
2.4.7	UC007 Verifica dell'interoperabilità con Crt-IDI (firma doppia)	12
2.4.8	UC008 Contrassegno dei dati di test	13
2.4.9	UC009 Applicazione dei criteri di sicurezza	13
2.4.10	UC010 Informazioni di supporto; esecuzione chiarimento manuale	13
2.5	Use case e operazioni correlate	13
3.	Use case	14
3.1	Use case 001: Ottenimento del certificato SUA	14
3.2	Use case 002: Ordine / Registrazione	15
3.2.1	Ottenimento del certificato per fiduciari	15
3.2.2	Ottenimento del certificato in assenza di un rapporto contrattuale in essere	16
3.3	Use case 003: Attivazione	16
3.4	Use case 004: Verifica dell'accessibilità	17
3.5	Use case 005: Verifica dell'interoperabilità	18
3.5.1	Requisiti particolari	18
3.5.2	Prerequisiti	19
3.5.3	Post-condizioni	19
3.6	Use case 006: Rinnovo del certificato	20
3.7	Use case 007: Verifica dell'interoperabilità 2x	20
3.8	Use case 008: Contrassegno dei dati di test	20
3.9	Use case 009: Applicazione dei criteri di sicurezza	20
3.10	Use case 010 Informazioni di supporto; esecuzione chiarimento manuale	21
3.11	Requisiti particolari	21
3.11.1	Creazione dei file di archivio	21
4.	Allegato	22
4.1	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
Fig. 7: Use case 010 – Verifica dell'accessibilità	17
Fig. 8: Use case 11 – Verifica dell'interoperabilità	18

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 10 – Verifica dell'accessibilità	17
Tabella 5: Descrizione use case Verifica dell'interoperabilità	18
Tabella 6: Prerequisiti (trasmettitore)	19
Tabella 7: Analisi e risposta del distributore	19
Tabelle 8: Valutazione del trasmettitore	19

Panoramica delle modifiche della versione 20190301

Direttive per lo Standard autenticazione delle aziende Swissdec CH (SUA) – Requisiti per il trasmettitore, versione 1.0, edizione 20190301 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 su www.swissdec.ch

1. Introduzione

Questo documento contiene i requisiti funzionali, tecnici e supplementari per il trasmettitore, che sono applicabili contestualmente allo Standard autenticazione delle aziende Swissdec CH (SUA). Il trasmettitore viene utilizzato per gestire il certificato SUA (ossia per l'ottenimento, l'attivazione, la verifica e il rinnovo).

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.).

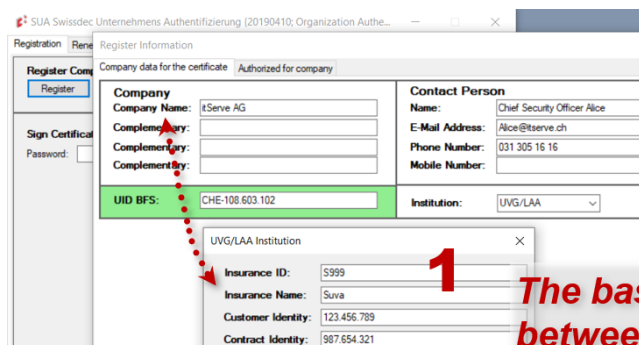
Nell'ambito della distribuzione o dell'ottenimento di un certificato SUA, si parla spesso di due fasi fondamentali, ossia:

- «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.

180719 BPMN2 SUA Registration Configuration

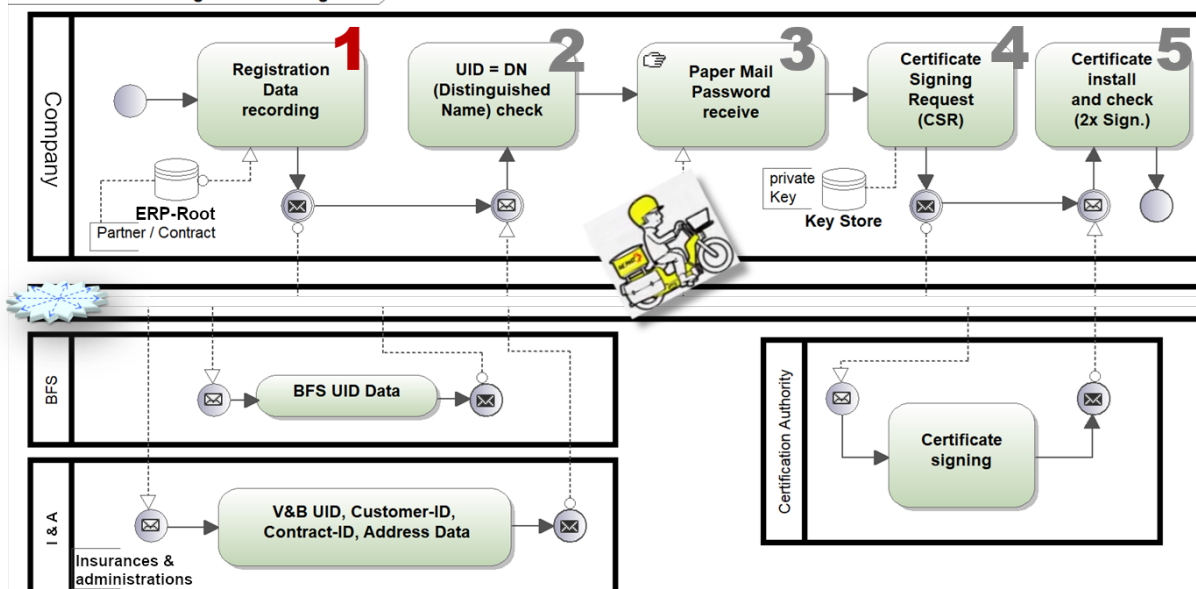


Fig. 1: Schema Registrazione / Configurazione SUA – 1° passo

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 responsa-

bile 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.

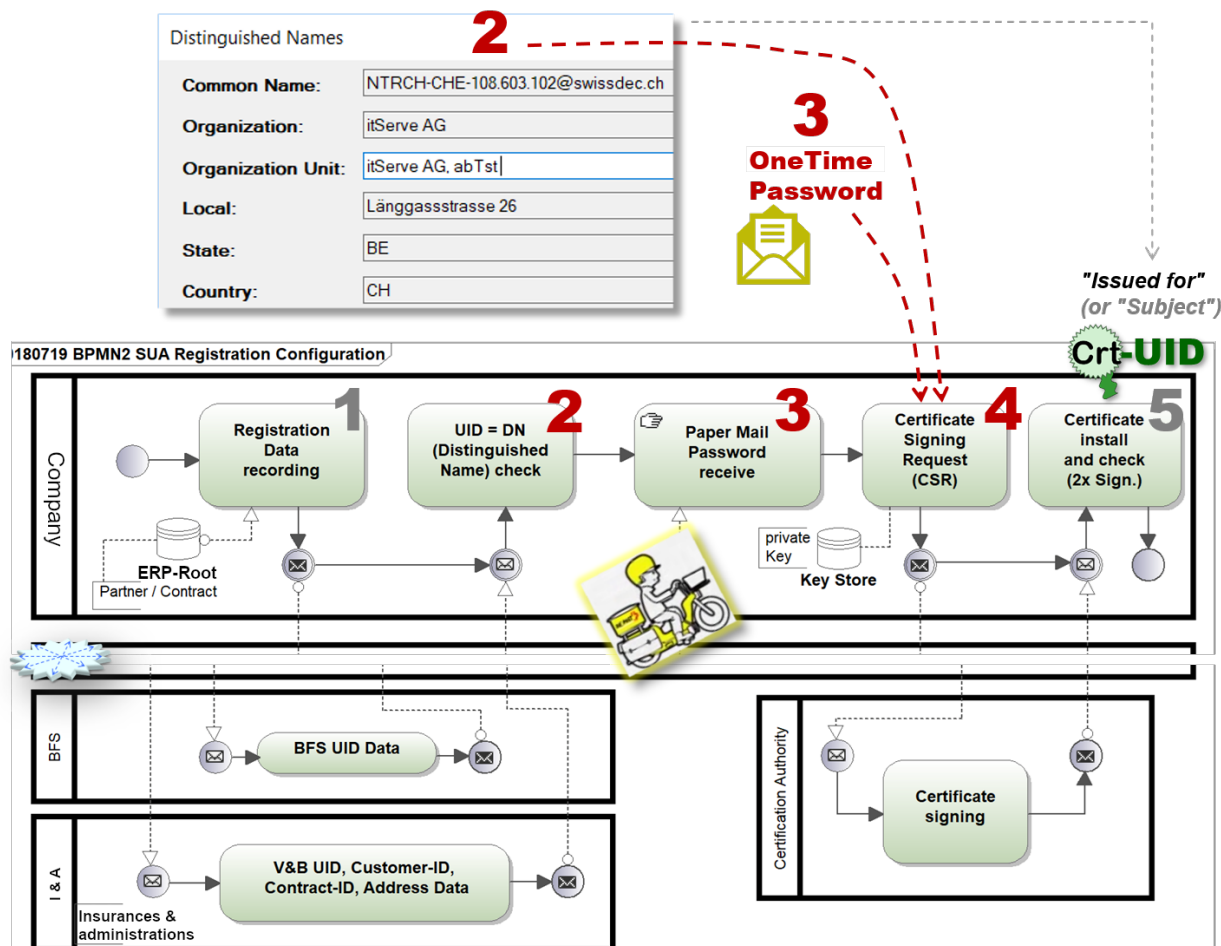


Fig. 2: Schema Registrazione / Configurazione SUA – 2°, 3°, 4° e 5° passo

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. Si potranno inoltre eseguire ulteriori test di trasmissione.

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

Per una descrizione dettagliata del processo rimandiamo alle direttive e alle specifiche dettagliate (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 Trasmettitore

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

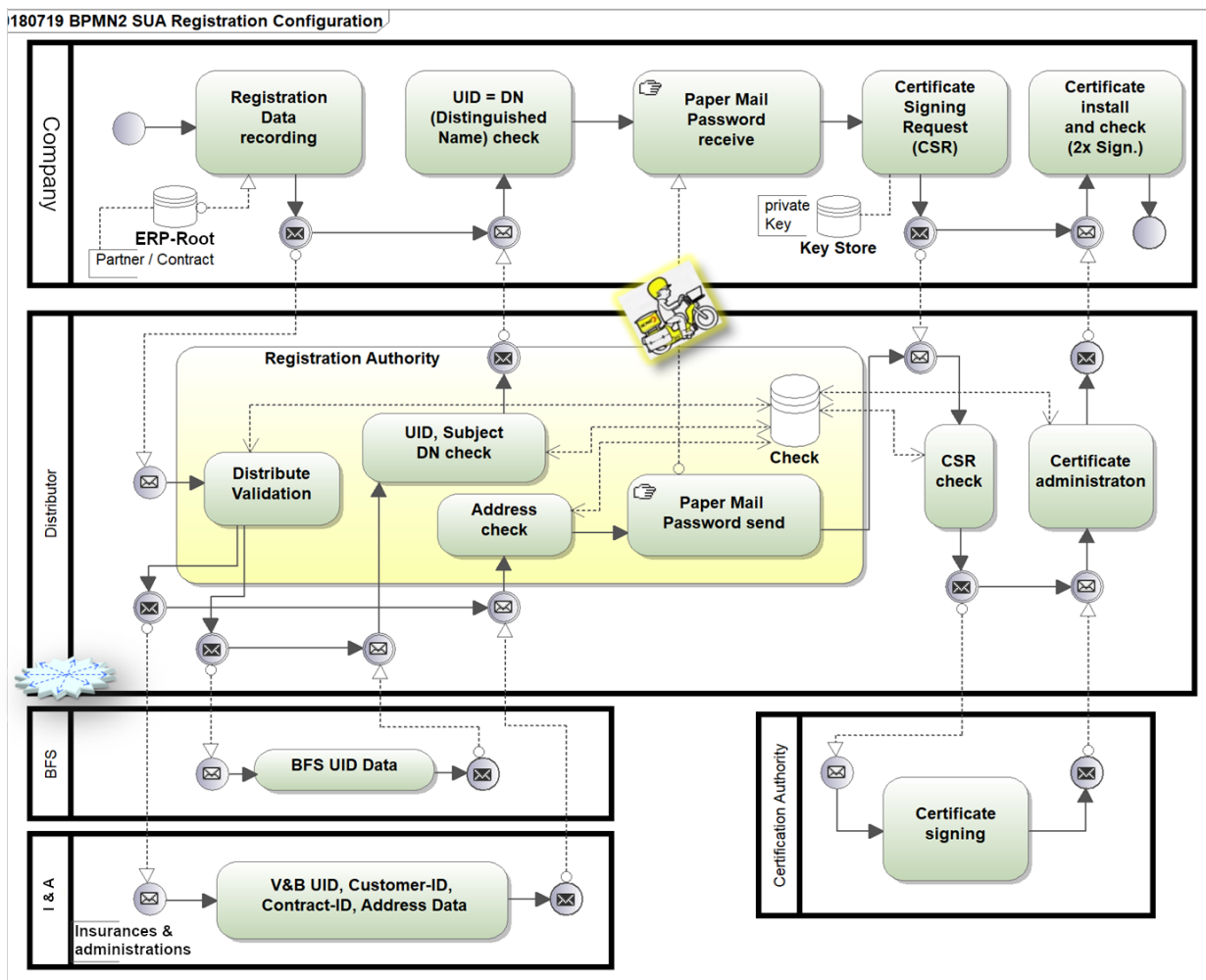


Fig. 3: Schema del processo Registrazione / Configurazione SUA

2.1 Schemi d'insieme sugli use case

Una parte degli use case è strutturata in modo analogo agli altri standard Swissdec. Le aziende che ne hanno già adottato uno possono utilizzare le stesse funzionalità anche per la SUA (ad es. accessibilità, interoperabilità).

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.

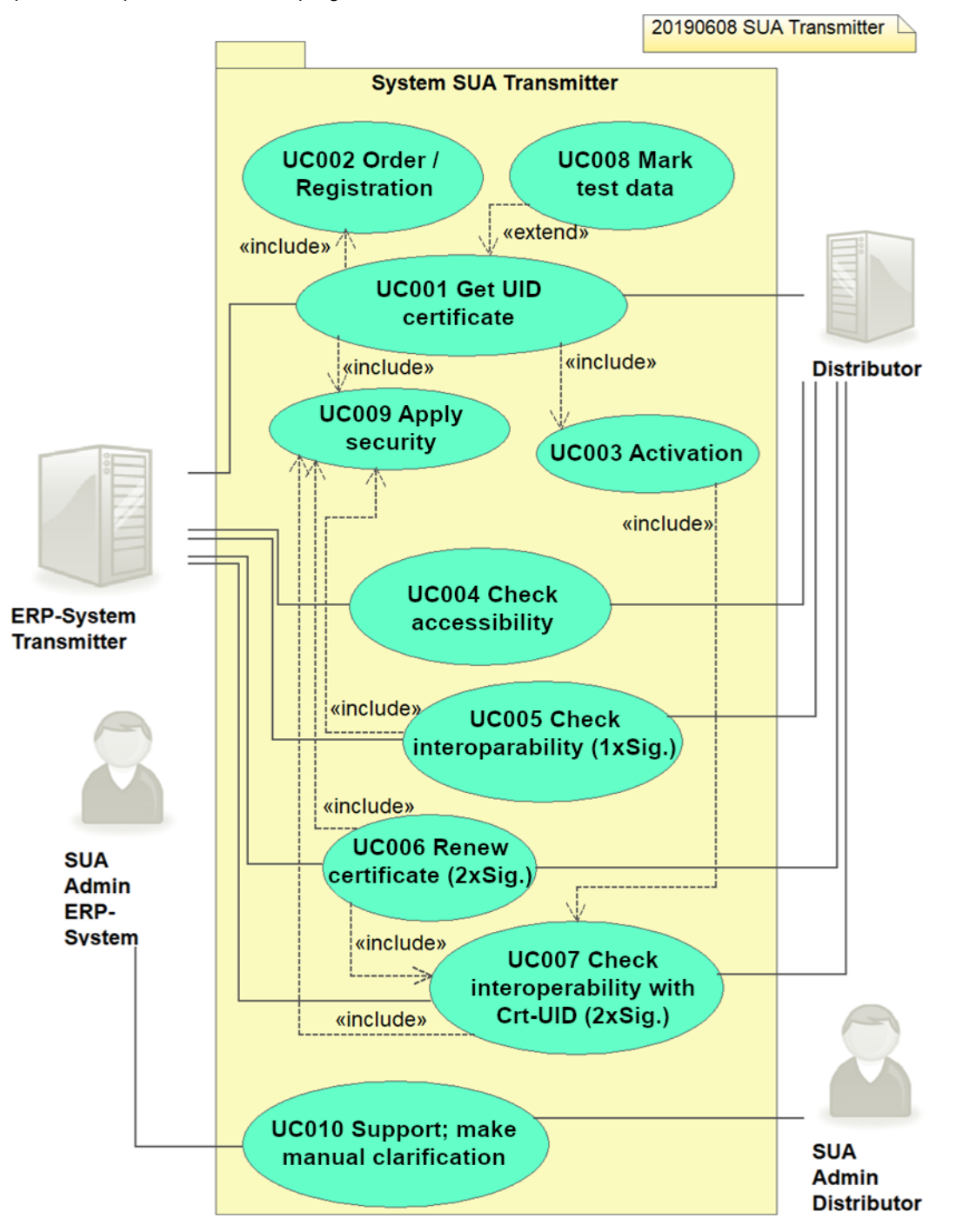


Fig. 4: Use case

2.2 Spiegazioni sugli use case

I requisiti illustrati come use case si riferiscono alla parte tecnica di un sistema costituito da un sistema ERP e un trasmettitore che gestisce l'elaborazione e la trasmissione elettronica dei dati per l'ottenimento di un certificato SUA.

Per la certificazione, un sistema ERP con trasmettitore *deve* soddisfare sempre i seguenti requisiti di sistema:

- UC001 Ottenimento del certificato
- UC002 Ordine / Registrazione
- UC003 Attivazione
- UC004 Verifica dell'accessibilità
- UC005 Verifica dell'interoperabilità (firma singola)
- UC006 Rinnovo del certificato
- UC007 Verifica dell'interoperabilità con Crt-IDI (firma doppia)
- UC008 Contrassegno dei dati di test
- UC009 Applicazione dei criteri di sicurezza
- UC010 Informazioni di supporto; esecuzione chiarimento manuale

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

2.3 Test

Nell'ambito della certificazione vengono eseguiti test che si riferiscono agli use case, rispettandone il più possibile anche la sequenza cronologica. 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 Ottenimento del certificato SUA

Un nuovo certificato viene acquistato via distributore. La risposta del distributore viene salvata (vedi cap. 3 «Use case»). A tal fine si utilizzano altri use case: UC002, UC003, UC009 e UC008.

2.4.2 UC002 Ordine / Registrazione

Con il processo di ordine / registrazione effettivo viene verificata l'identità del richiedente. Nello specifico, un destinatario finale (Assicuratore & Autorità) e il registro dell'UST verificano in particolare i dati IDI dell'UST.

In caso di esito positivo, il trasmettitore/sistema ERP riceve un CertificateRequest-ID e un X509Subject per il controllo. Inoltre, all'azienda viene inviata a mezzo posta una lettera contenente una password.

2.4.3 UC003 Attivazione

Una volta completata correttamente la registrazione (UC002) è possibile prelevare il certificato SUA utilizzando la password contenuta nella lettera (UC002). A questo punto il nuovo certificato SUA viene attivato nel sistema ERP e può essere sottoposto a una verifica dell'interoperabilità (UC007).

2.4.4 UC004 Verifica dell'accessibilità

Un messaggio speciale viene inviato via Internet al distributore per verificarne l'accessibilità.

2.4.5 UC005 Verifica dell'interoperabilità (firma singola)

Viene inviato al distributore uno speciale messaggio per verificare l'interoperabilità tra il trasmettitore e il distributore (ad es. codifica, marshalling, tempistica ecc.). La richiesta viene firmata solo con il certificato ERP.

2.4.6 UC006 Rinnovo del certificato

È possibile rinnovare un certificato SUA in qualsiasi momento. A tal fine viene inviata al distributore una richiesta CSR (Certificate Sign Request), e il trasmettitore riceve il nuovo certificato nella risposta (Response).

Per motivi di sicurezza il numero di rinnovi possibili è limitato (vedi specifiche dettagliate (RLOA, 2019)).

2.4.7 UC007 Verifica dell'interoperabilità con Crt-IDI (firma doppia)

Viene inviato al distributore uno speciale messaggio per verificare l'interoperabilità tra il trasmettitore e il distributore (ad es. codifica, marshalling, tempistica ecc.). La richiesta viene firmata due volte, con i certificati ERP e SUA.

2.4.8 UC008 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 (Endreceiver).

2.4.9 UC009 Applicazione dei criteri di sicurezza

Ogni messaggio inviato deve essere firmato almeno una volta (certificato ERP) e crittografato.

2.4.10 UC010 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.

2.5 Use case e operazioni correlate

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

Use case	Operazione / Elemento
	OrganizationAuthenticationService WSDL / XSD
UC001 Ottenimento del certificato SUA UC002 Ordine / Registrazione	<ul style="list-style-type: none">RegisterOrganizationRegisterOrganizationResponseGetResultFromRegisterOrganizationGetResultFromRegisterOrganizationResponseOrganizationAuthenticationFault
UC003 Attivazione	<ul style="list-style-type: none">SignCertificateSignCertificateResponseOrganizationAuthenticationFault
UC004 Verifica dell'accessibilità	<ul style="list-style-type: none">PingPingResponse
UC005 Verifica dell'interoperabilità	<ul style="list-style-type: none">CheckInteroperabilityCheckInteroperabilityResponse
	OrganizationAuthenticationService WSDL / XSD
UC006 Rinnovo del certificato	<i>Firma doppia (certificato ERP e SUA)</i> <ul style="list-style-type: none">RenewCertificateRenewCertificateResponseOrganizationAuthenticationFault
UC007 Verifica dell'interoperabilità	<i>Firma doppia (certificato ERP e SUA)</i> <ul style="list-style-type: none">CheckInteroperabilityCheckInteroperabilityResponse

Tabella 2: Use case e operazioni

3. Use case

3.1 Use case 001: Ottenimento del certificato SUA

Per il diagramma di questo use case, vedi Fig. 4: Use case a pagina 11.

Breve descrizione	<p>Un nuovo certificato SUA viene acquistato via distributore.</p> <p>Le risposte del distributore vengono analizzate e archiviate. Viene salvato anche un file di archivio del messaggio inviato.</p>
Attori	Sistema ERP, distributore, ricevitore finale
Fattore scatenante	Un impiegato dell'azienda (addetto alla sicurezza) desidera acquistare un certificato SUA.
Prerequisiti	Il sistema ERP è in grado di trasmettere e ricevere messaggi relativi a eventi comunicati in forma elettronica ed è in possesso di un certificato ERP.
Post-condizioni	<ul style="list-style-type: none"> ▪ L'ottenimento del certificato SUA è stato completato correttamente ▪ Il certificato SUA è stato attivato e testato con successo <p>In caso di errore:</p> <ul style="list-style-type: none"> ▪ Messaggio di errore
Use case inclusi	<p>UC002 Ordine / Registrazione</p> <p>UC003 Attivazione</p> <p>UC007 Verifica dell'interoperabilità con Crt-IDI (firma doppia)</p> <p>UC009 Applicazione dei criteri di sicurezza</p>
Procedura standard	<ol style="list-style-type: none"> 1. UC002: il certificato viene ordinato presso il distributore. A tal fine occorre indicare un'assicurazione in essere e il relativo rapporto contrattuale. Il messaggio viene firmato una volta (UC009). 2. Il relativo risultato viene recuperato in modo asincrono e verificato. Il messaggio viene firmato una volta (UC009). A questo punto X509Subject corrisponde alla richiesta di certificato e <i>deve</i> essere verificato dal richiedente. 3. Si attende la lettera contenente la OneTimePassword, spedita per posta. 4. UC003: viene creata una richiesta CSR, che viene comunicata al distributore insieme alla OneTimePassword. Il messaggio viene firmato una volta (UC009). Tutti i dati <i>devono</i> essere identici a quelli contenuti in X509Subject (2° passo). L'unico dato modificabile è quello relativo alla OU (Organization Unit) in DistinguishedNames. La chiave privata (Key) rimane presso il trasmettitore. Nella risposta il trasmettitore riceve il certificato SUA. 5. Il certificato SUA viene installato e attivato. In seguito si <i>deve</i> verificare il tutto mediante UC007. <p><i>Dovrebbero</i> inoltre seguire ulteriori trasmissioni di prova con standard Swissdec esistenti.</p>
Procedura alternativa	<p>{UC008} Invio di dati come dati di test</p> <p>Come da procedura standard, dal 1° al 4° passo, vedi schema</p> <p>Ma con le seguenti differenze:</p> <p>Nel 3° passo non viene inviata alcuna lettera. La OneTimePassword è contenuta in <code>GetResultFromOrganizationRegistrationResponse ... Success/Comment</code></p> <p>Nel 4° passo, nella risposta non viene consegnato alcun certificato SUA.</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 durante la firma o la crittografia. ▪ Il ricevitore finale non è raggiungibile. ▪ Il messaggio allestito dal sistema ERP non corrisponde allo schema (validità non data).

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

I 20190531 SUA Certificate distribution (1:D:1)

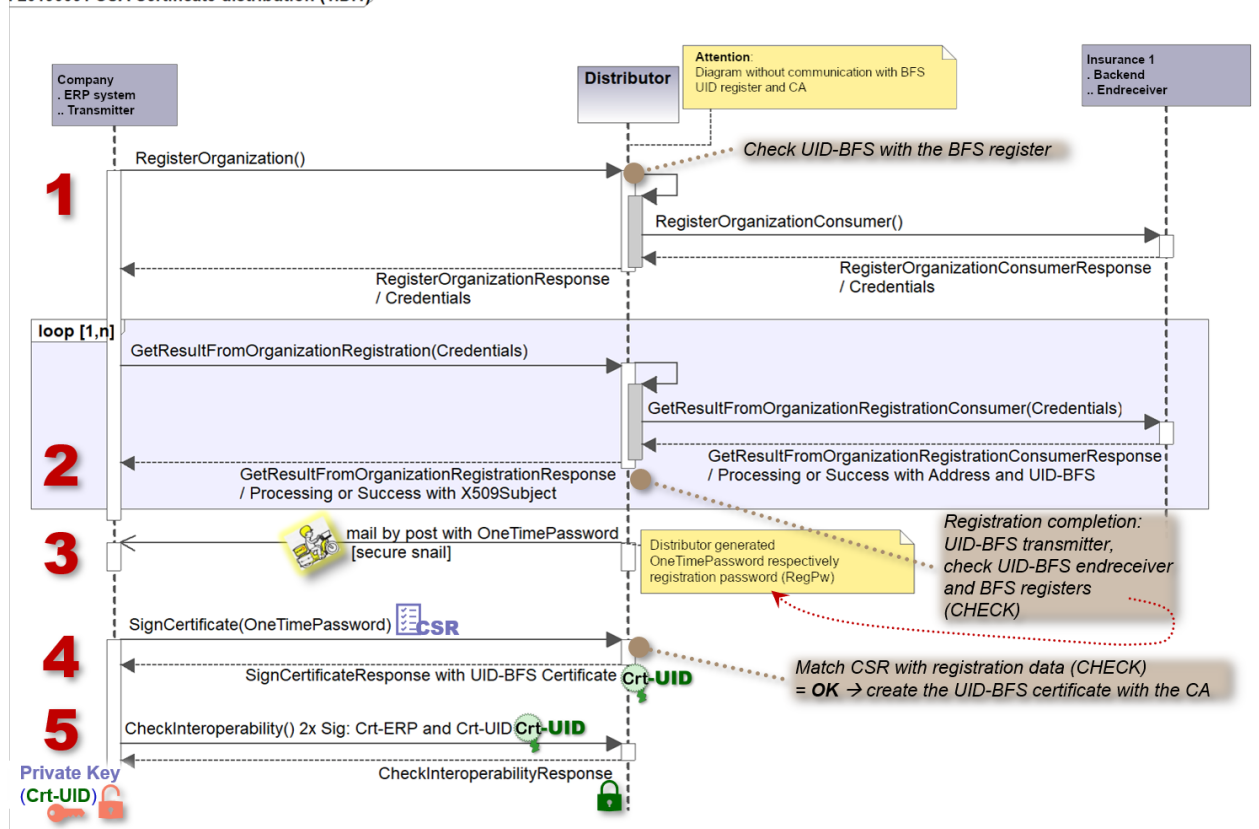


Fig. 5: Diagramma di sequenza per l'ottenimento del certificato SUA

3.2 Use case 002: Ordine / Registrazione

Innanzitutto l'azienda deve richiedere il certificato (vedi UC001). Ecco come procedere:

L'acquisto del certificato si avvia tramite `RegisterOrganization`. L'azienda invia le informazioni necessarie per la creazione del certificato al distributore, il quale comunica la richiesta al destinatario finale.

Il destinatario finale verifica la validità della richiesta e trasmette la propria risposta al distributore.

A questo punto, con il comando `GetResultFromRegisterOrganization`, l'azienda può recuperare dal distributore le informazioni inviate dal destinatario finale.

Per poter ordinare un certificato è necessario un rapporto contrattuale in essere fra l'azienda e il destinatario finale. L'unica eccezione in tal senso è rappresentata dai fiduciari (vedi paragrafo 3.2.1).

Un'azienda può avere più richieste di registrazione attive in uno stesso momento, ad esempio se dispone di più sistemi ERP differenti. Attualmente esiste un limite massimo di cinque richieste attivabili contemporaneamente, in modo da non sovraccaricare il registro d'identificazione delle imprese dell'UST ed evitare inutili spedizioni di lettere. L'invio di informazioni a mezzo posta può infatti richiedere 1 o 2 giorni: limitando il numero di richieste si intende evitare che, in questo lasso di tempo, l'utente ne presenti altre per lo stesso numero d'identificazione delle imprese (IDI) con il medesimo sistema ERP.

3.2.1 Ottenimento del certificato per fiduciari

Se un'impresa è amministrata da un fiduciario vanno rispettate le seguenti indicazioni:

Tra il fiduciario e il destinatario finale 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». Il destinatario finale 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 SUA per fiduciari, con cui firmerà tutti i messaggi che invierà a nome dell'azienda da lui amministrata.

Per garantire la sicurezza del processo, il destinatario finale non riceve i dati completi del fiduciario ma solo l'informazione <WithDelegate>, che dovrà utilizzare per risalire alle proprie informazioni sull'azienda; dovrà quindi inviare al distributore i suoi dati sul fiduciario collegati a tali informazioni. Il certificato viene emesso soltanto se le informazioni di entrambe le parti coincidono.

3.2.2 Ottenimento del certificato in assenza di un rapporto contrattuale in essere

Al momento le aziende che non hanno un rapporto contrattuale in essere non possono ottenere un certificato utilizzando la procedura SUA convenzionale. Tuttavia, poiché in futuro si intende implementare lo Standard SUA in un numero crescente di processi Swissdec, anche queste aziende ne avranno necessità a breve. Sono allo studio varianti che prevedono un controllo da parte dell'autorità fiscale, con la quale l'azienda interessata deve comunque essere legata da un rapporto in essere.

3.3 Use case 003: Attivazione

Una volta ricevute le informazioni necessarie per attivare il certificato in suo possesso, l'azienda può compiere il passo successivo. Crea quindi una richiesta CSR e la invia al distributore insieme alla OneTimePassword ricevuta per posta.

Non essendo ancora disponibile un certificato SUA valido, il messaggio viene sottoscritto con firma semplice (UC009). In questa fase tutti i dati devono essere identici a quelli della registrazione originale, contenuti in X509Subject. L'unico dato modificabile è quello relativo alla OU (Organization Unit) in DistinguishedNames.

In tal modo la chiave privata (Key) può rimanere presso il trasmettitore, così da garantire la sicurezza del certificato.

Nella risposta a questa richiesta, il trasmettitore riceve il certificato SUA valido, che ora si può utilizzare per la doppia firma / crittografia. Il certificato deve essere installato e attivato, dopodiché si potrà verificare il tutto mediante UC007.

3.4 Use case 004: Verifica dell'accessibilità

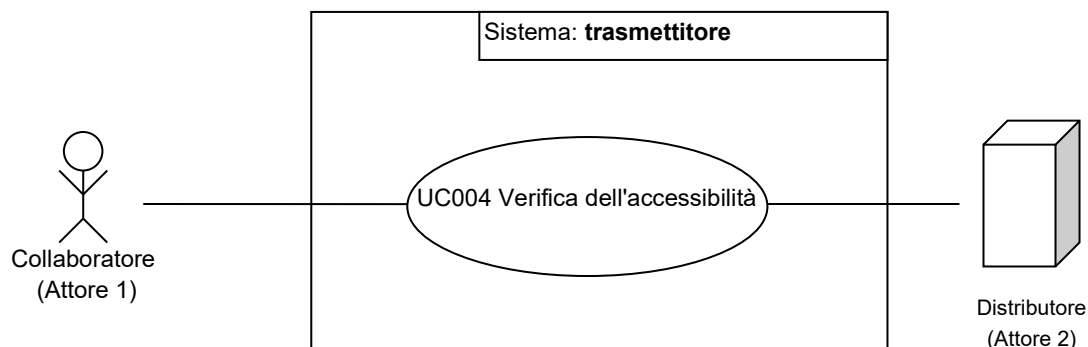


Fig. 6: Use case 010 – Verifica dell'accessibilità

Breve descrizione	<i>Deve essere verificata l'accessibilità del distributore. A questo scopo viene inviata una normale richiesta (WSDLOA, 2019) al distributore. La risposta del distributore conferma l'accessibilità.</i>
Attori	Attore 1: collaboratore, Attore 2: distributore
Fattore scatenante	Dovrebbe essere verificata l'accessibilità del distributore.
Prerequisiti	Nessuno
Post-condizioni	<ul style="list-style-type: none"> La risposta del distributore include un timestamp che indica l'ora di sistema presso il distributore stesso (XSDOA, 2019). <p>In caso di errore:</p> <ul style="list-style-type: none"> Distributore non accessibile: messaggio di errore Contenuti divergenti (XSDOA, 2019) (ACKNSwissdec, 2018): messaggio di errore
Use case inclusi	-
Procedura standard	<ol style="list-style-type: none"> L'attore avvia la verifica. Il trasmettitore invia una normale richiesta al server (ping) avente come target l'indirizzo del distributore. Il trasmettitore esamina la risposta ricevuta dal distributore.
Procedura alternativa	<p>Distributore non accessibile</p> <p>{dopo passo 1}</p> <ol style="list-style-type: none"> Viene visualizzato un messaggio di errore. <p>{fine}</p>
Elenco degli errori	<p>Errori tecnici:</p> <ul style="list-style-type: none"> Il distributore non è accessibile. Il distributore invia una risposta errata.

Tabella 4: Use case 10 – Verifica dell'accessibilità

Con il ping viene trasmessa l'ora del sistema, il che permette di confrontare gli orari del distributore e del mittente. Ciò consente di scoprire problemi di timestamp.

Il trasmettitore *deve* confrontare l'ora del sistema ricevuta dal distributore con la propria e avvisare l'utente qualora vi sia uno scostamento significativo tra i due valori. Lo scostamento massimo ammesso corrisponde a 1 minuto di ritardo e 2 minuti di anticipo.

Questo use case serve per assicurare la qualità in fase di installazione e sviluppo.

3.5 Use case 005: Verifica dell'interoperabilità

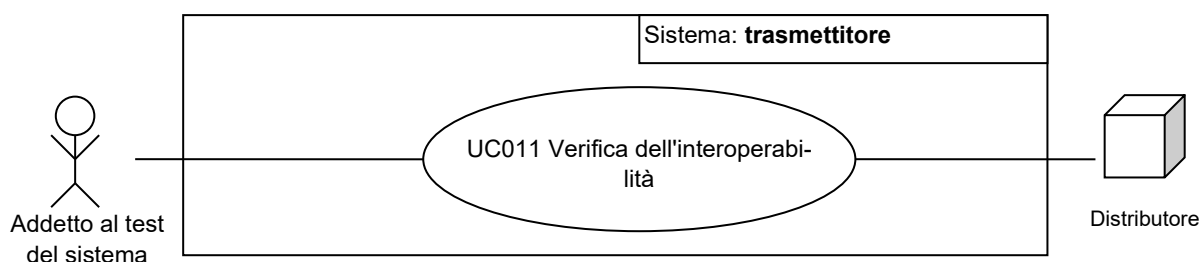


Fig. 7: Use case 11 – Verifica dell'interoperabilità

Breve descrizione	Per verificare l'interoperabilità tra un trasmettitore e il distributore, il trasmettitore <i>deve</i> essere in grado di emettere una <code>CheckInteroperabilityRequest</code> (WSDLID, 2018).
Attori	Addetto al test del sistema, distributore
Fattore scatenante	L'installazione dovrebbe essere testata.
Prerequisiti	Nessuno
Post-condizioni	La trasmissione ha avuto successo e i risultati rispondono alle attese.
Use case inclusi	-
Procedura standard	<ol style="list-style-type: none"> 1. L'attore avvia la verifica dell'interoperabilità e inserisce i valori per l'operando 2. 2. L'attore avvia l'invio dei dati. 3. Il trasmettitore prepara la richiesta al server. 4. Il messaggio è firmato con la chiave privata / certificato del produttore e con l'identificazione dell'azienda, come da specifica (SECTID, 2018). 5. Il trasmettitore invia al distributore la richiesta server con cifratura ssl. 6. Il distributore elabora i dati inviati (trasformazione UmlautString, calcolo «FirstOperand +- SecondOperand») e invia la risposta al trasmettitore. 7. Il trasmettitore analizza la risposta ricevuta dal distributore. 8. Il trasmettitore visualizza la risposta ricevuta dal distributore.
Elenco degli errori	<p>Errori tecnico-specialistici:</p> <ul style="list-style-type: none"> ▪ L'interoperabilità non è data. <p>Errori tecnici:</p> <ul style="list-style-type: none"> ▪ Errore durante la firma. ▪ Errore di codifica / decodifica. ▪ Il distributore non è accessibile.

Tabella 5: Descrizione use case verifica dell'interoperabilità

3.5.1 Requisiti particolari

Il test di interoperabilità è utilizzato a fini di sviluppo e durante l'installazione per garantire l'interoperabilità tra un trasmettitore e il distributore.

Le maggiori difficoltà si incontrano nella codifica delle stringhe di caratteri (encoding) e nell'interpretazione dei numeri in virgola mobile.

Il test di interoperabilità consente anche lo svolgimento di un controllo di sicurezza semplice e veloce. Entrambi i sistemi (trasmettitore e distributore) devono effettuare determinate analisi per poter stabilire, in caso di errore, la causa.

I parametri nelle seguenti tabelle sono descritti in (WSDLID, 2018).

3.5.2 Prerequisiti

Il trasmettitore invia i seguenti dati:

Nome del parametro	Valore	Osservazioni
UmlautString	ÄÖÜÄÉÓÚÄÊËÛ	valore fisso
FirstOperand	999000000000.00	valore fisso, 999 miliardi
SecondOperand	nessun valore predefinito	qualsiasi numero in virgola mobile
SystemDateTime	Data e ora del trasmettitore	Data e ora del sistema

Tabella 6: Prerequisiti (trasmettitore)

3.5.3 Post-condizioni

Analisi e risposta del distributore:

Nome del parametro	Analisi / calcolo	Osservazioni
UmlautStringIsCorrect	$UmlautString_{TRANS} = \text{ÄÖÜÄÉÓÚÄÊËÛ}$	Valore restituito: true / false
FirstOperandIsCorrect	$FirstOperand_{TRANS} = 999000000000.00$	Valore restituito: true / false
UmlautString	äöüäéóúäêëû	Valore restituito: UmlautString _{DISTRI} lettere da maiuscole a minuscole.
AdditionResult	$AdditionResult_{DISTRI} = FirstOperand_{TRANS} + SecondOperand_{TRANS}$	Valore restituito: valore calcolato AdditionResult _{DISTRI}
SubtractionResult	$AdditionResult_{DISTRI} = FirstOperand_{TRANS} + SecondOperand_{TRANS}$	Valore restituito: valore calcolato SubtractionResult _{DISTRI}
SystemDateTime	Data e ora del distributore	Valore restituito: data e ora del sistema

Tabella 7: Analisi e risposta del distributore

Valutazione del trasmettitore:

Nome del parametro	Analisi / calcolo	Osservazioni
UmlautStringIsCorrect	$UmlautStringIsCorrect = true$	deve essere 'true'
FirstOperandIsCorrect	$FirstOperandIsCorrect = true$	deve essere 'true'
UmlautString	$UmlautString_{DISTRI} = \text{äöüäéóúäêëû}$	deve essere 'äöüäéóúäêëû'
AdditionResult	$FirstOperand_{TRANS} + SecondOperand_{TRANS} = AdditionResult_{DISTRI}$	Calcolo e confronto, grado di precisione 2 posizioni decimali
SubtractionResult	$FirstOperand_{TRANS} - SecondOperand_{TRANS} = AdditionResult_{DISTRI}$	Calcolo e confronto, grado di precisione 2 posizioni decimali
SystemDateTime	$ SystemDateTime_{DISTRI} - SystemDateTime_{TRANS} < 1 \text{ ora}$	La differenza di tempo dovrebbe essere < 1 ora

Tabella 8: Valutazione del trasmettitore

3.6 Use case 006: Rinnovo del certificato

Di norma un certificato SUA ha una durata di un anno.

Decorso tale periodo è possibile rinnovarlo un numero limitato di volte mediante il processo SUA², dopodiché è necessario ottenere un nuovo certificato. Il limite al numero di rinnovi serve a garantire la costante attualità delle informazioni relative al certificato SUA depositato (attualità e autenticità).

Non appena la validità residua del certificato SUA scende sotto i 30 giorni, dovrebbe attivarsi automaticamente il processo di rinnovo. Per tale processo si utilizzano il certificato SUA esistente e la password ricevuta al momento della registrazione iniziale.

Il processo di rinnovo si avvia con l'operazione `RenewCertificate`. Il distributore verifica la validità della richiesta ed esegue un confronto con il registro d'identificazione delle imprese dell'UST per controllare l'attualità dei dati relativi all'azienda. Se i dati del registro d'identificazione delle imprese non coincidono con quelli del vecchio certificato SUA, la richiesta viene annullata e l'azienda, anziché procedere con un rinnovo, deve di nuovo eseguire l'intero processo per ottenere il certificato.

Se invece i dati coincidono, il distributore provvede a ottenere un nuovo certificato SUA con validità rinnovata di un anno e lo consegna all'azienda. A questo punto l'azienda deve trasmettere un messaggio di test per verificare il nuovo certificato.

3.7 Use case 007: Verifica dell'interoperabilità 2x

Questo use case è pressoché identico al numero 005: Verifica dell'interoperabilità 1x. L'unica differenza consiste nel fatto che in questo caso si firma anche con il certificato SUA oltre che con il certificato ERP. In tal modo l'utente può testare la validità e la corretta installazione del certificato SUA.

3.8 Use case 008: 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. Analogamente, una registrazione eseguita come produttiva non può essere proseguita 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.

3.9 Use case 009: Applicazione dei criteri di sicurezza

Ad eccezione del test di accessibilità, ogni trasmissione deve essere firmata e crittografata. Per maggiori informazioni sono disponibili i documenti sulla sicurezza dal lato trasmettitore (vedi (SECTR)).

² La frequenza con cui sarà possibile rinnovare la certificazione sarà definita dopo avere acquisito le prime esperienze con il processo di produzione.

3.10 Use case 010 Informazioni di supporto; esecuzione chiarimento manuale

Breve descrizione	Gli errori, le avvertenze e le informazioni illustrati in (ACKNSwissdec, 2018) <i>devono</i> essere analizzati e mostrati all'utente e/o comunicati al destinatario finale. È <i>obbligatorio</i> utilizzare gli ID.
Attori	Applicazione contabilità salari, trasmettitore, distributore
Fattore scatenante	È stato inviato un messaggio o una richiesta via distributore a un ricevitore finale. La risposta perviene via distributore.
Prerequisiti	<ul style="list-style-type: none">Il distributore invia una risposta
Post-condizioni	<ul style="list-style-type: none">Gli errori, le avvertenze e le informazioni contenuti nella risposta vengono allestiti e mostrati all'utente in modo completo e comprensibile.Le informazioni non rilevanti per l'utente finale devono essere disponibili per il supporto tecnico (StackTrace, Fault Detail ecc.).Le note all'attenzione del ricevitore finale devono essere inviate a quest'ultimo sotto forma di notifica.In caso di errore: Distributore non accessibile: messaggio di errore
Use case inclusi	-
Elenco degli errori	<p>Errori tecnici:</p> <ul style="list-style-type: none">Errore durante la firma.Il distributore non è accessibile.Il messaggio allestito dalla contabilità salariale non corrisponde allo schema (validità non data).Errore di codifica / decodifica. <p>Errori tecnico-specialistici:</p> <ul style="list-style-type: none">Come da (RLID, 2018)

3.11 Requisiti particolari

3.11.1 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. Allegato

4.1 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. (2018). AcknowledgementNotification. Bern, Schweiz.

OVID, S. (2018). IncidentOverview. Bern, Schweiz.

OVOA, S. (2019). Overview Unternehmens-Authentifizierung SUA. Bern, Schweiz.

RLID, S. (2018). Richtlinien für den Leistungsstandard-CH. Bern, Schweiz.

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

SECTID, S. (2018). ID_SecurityTransmitter. Bern, Schweiz.

SECTR, S. (kein Datum). SecurityTransmitter. Bern, Schweiz.

WSDLID, S. (2018). IncidentDeclarationService. Bern, Schweiz.

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

XSDID. (2018). IncidentDeclarationServiceTypes.xsd. Bern, Schweiz.

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