REGIONE DEL VENETO

arsenàl.IT

GDL-O "Sicurezza"

Specifiche tecniche infrastruttura di sicurezza

FSEr FASCICOLO SANITARIO ELETTRONICO REGIONALE

Arsenàl.IT

Centro Veneto Ricerca e Innovazione per la Sanità Digitale

Informazioni preliminari

Contatti

Per ulteriori informazioni, si prega di contattare:

Dott. Mauro Zanardini

Project Engineer

Viale Oberdan, 5 – 31100 Treviso

Tel. 0422 216115 cell. 3346482818

e-mail: mzanardini@consorzioarsenal.it

Controllo del documento

N. documento:	Specifiche tecniche infrastruttura di sicurezza GDL-O Sicurezza v0.2
Stato di avanzamento:	Public Comment
Data di prima emissione:	09/05/13
Ultimo Aggiornamento:	13/09/13
Revisione:	versione 1.0
Numero di pagine:	
Responsabile del documento:	*Claudio Saccavini*
Coordinatore della stesura:	*Mauro Zanardini*
Autori:	*Mauro Zanardini*

Status del documento

Versione	Status	Data	Descrizione Modifica
0.1	**BOZZA**	**26/04/2013**	Versione 0.1 per revisione interna e gruppo ristretto
0.2	**BOZZA**	**10/05/2013**	pronto per revisione del GDL-O Sicurezza: • *Definizione di UTENTE e RESPONSABILE* • *Sistema richiedente di asserzioni sviluppa WS solo sincroni* • *eliminato l'utilizzo di* SPNameQualifier="farmaciaDiPippo" SPProvidedID="titolare" *sia in Subject che Issuer. (Il ruolo è un'informazione aggiunta SOLO dal provider di asserzioni ed è associata al processo di autenticazione).* • *modifica sequence diagram per descrivere i trigger event della richiesta di asserzione* • *aggiunta use-case Dematerializzazione. (Sequence Diagram)* • *creato nuovo actor diagram per lo use-case dematerializzazione* • *aggiunta una frase per specificare la gestione di errori in caso di utilizzo di token non validi sezione 3.2* • *aggiornamento Open Issues/Closed Issues*
1.0	**PUBLIC COMMENT version**	**12/06/2013**	pronto per public comment: • *Modifica/Chiusura Open Issues* • *Modifica Introduzione* • *Aggiunta di un cappello introduttivo destinato ai responsabili dei sistemi informativi (Summary)* • *aggiunta sezione specifica per i todo aziendali* • *definizione di una sezione relativa alla sincronizzazione dei sistemi* • *definizione infrastruttura Auditing* • *.completamento sezione sulla comunicazione sicura tra nodi della rete (mutua autenticzione dei nodi)* • *modifica parametri richiesta e asserzione* • *aggiunta specificazione dei controlli che deve svolgere l'attore Identity and Assertion Provider* • *aggiunta struttura Audit Messages RVE-1* • *aggiunta specificazione relativa alla struttura dei Fault per la richiesta di servizi con asserzione.* • *aggiunte appendici A e B (Appendice B vuota per ora)*
1.1	**review Public Comment**	**29/07/2013**	Review e integrazione commenti: • *Attore territoriale sincronazzato direttamente sul server di Galileo Ferraris e definita una frequenza minima di allineamento (10 minuti);.* • *Modifica TODO aziendali: gestione Certificati a*

			livello regionale e aggiornamento a cascata CRL aziendali. • *Definizione transazione RVE-2 Update Password* • *Aggiunta TODO aziendale gestione di un certificato "IDP.cer" per criptare il contenuto del tag newPassword per la transazione UpdatePassword [RVE-2]* • *Aggiunta contesto "Amministratore di sistema"* • *Correzione refusi figura 8, 9* • *Ristrutturati i contenuti del paragrafo 3.1* • *Aggiornamento tabella per Error Code Failed Authentication*

Indice

Indice delle Figure

Acronimi e definizioni

ATNA	Audit Trail and Node Authentication
ARR	Audit Record Repository
CF	codice fiscale
IHE	integrating the healthcare enterprise
LDAP	lightweight directory access protocol
NTP	Network Time Protocol
CT	Consistent Time
CRL	Certificate Revocation List
PHI	Protected Health Information
XUA	Cross-Enterprise User Assertions
XML	eXtensible Mark-up Language
XDS	Cross-Enterprise Document Sharing
SAML	Security Assertion Markup Language
SAR	Servizio di Accoglienza Regionale
PKI	Public Key Infrastructure
IETF	Informatic Enginneer Task Force
Utente	utilizzatore di un sistema applicativo che vuole accedere a determinati servizi.
Responsabile	possessore di credenziali conosciute da un Identity Provider in grado di asserire l'identità del responsabile stesso e di tutti gli utenti di cui questo responsabile è garante
TLS	Transport Layer Security
CA	Certification Authority

Introduzione

Il presente documento di specifiche tecniche è stato redatto all'interno del GDL-O "Sicurezza", gruppo di lavoro operativo del progetto Fascicolo Sanitario Elettronico Regionale.

L'obiettivo è quello di descrivere l'infrastruttura di sicurezza che gli attori dovranno implementare per autenticare gli utenti che avranno accesso ai servizi FSEr.

Il presente documento è diviso in due macro parti:

- descrizione dell'infrastruttura per la gestione dell'autenticazione per gli attori territoriali;
- descrizione dell'infrastruttura per la gestione dell'autenticazione per gli attori aziendali;

L'architettura del fascicolo sanitario elettronico regionale non prevede un unico servizio di autenticazone centralizzato, ma un'autenticazione federata. In tal senso tutti gli attori delle aziende sanitarie e del territorio si autenticheranno ai servizi del FSE-r tramite i sistemi di identity management (LDAP, IDentitiy provider, etc.,) delle aziende sanitarie di riferimento (quelle entro il cui territorio l'attore opera o con cui è convenzionato).

Il sistema di accesso ai servizi FSEr sarà declinato in 2 livelli. La autenticazione nel sistema, avverrà con credenziali di diverso tipo: passoword, certificati, o altri sistemi; a seguito di questo processo di autenticazione, l'attestazione di identità e dell'ambito d'uso, comporterà il rilascio di un token in grado di veicolare tutte le informazioni utili per verificare l'accessibilità ai servizi del FSEr. Questo token conterrà dunque il periodo di validità del token stesso, i dettagli sull'identità dell'utente, il suo ruolo, l'ambito d'uso dei servizi regionale.

Si precisa che la parte riguardante la gestione delle policies di visibilità per i servizi FSEr sarà descritta in un altro documento di specifiche tecniche, sempre a cura del GDL-O "Sicurezza".

Viene presentato di seguito l'iter di approvazione documentale a cui la documentazione redatta da Arsenàl.IT all'interno del progetto FSEr dovrà essere sottoposta.

Iter di approvazione documentale

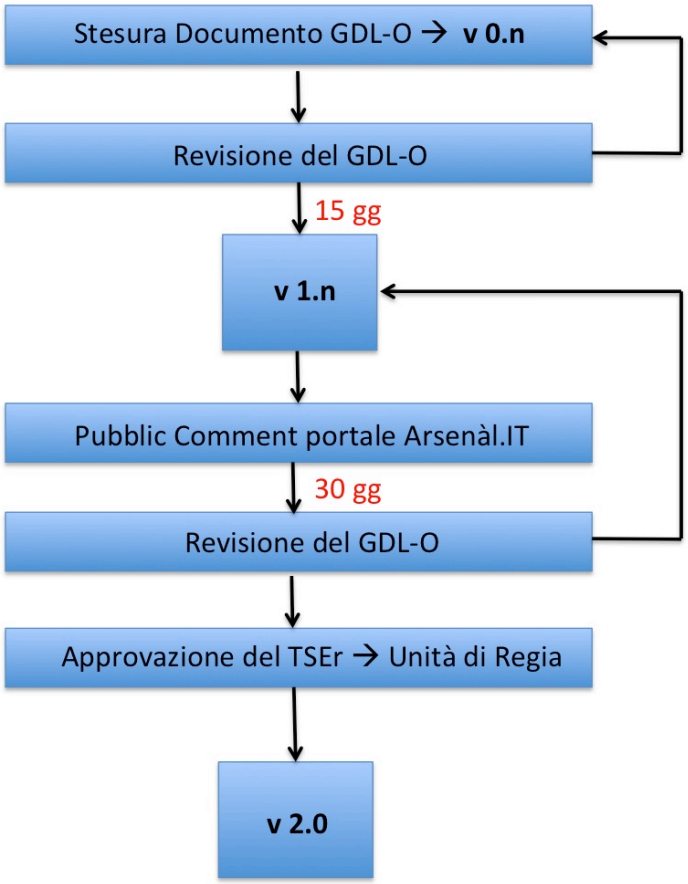


Figura 1 Iter di approvazione documentale

v 0.n → STATUS BOZZA → il documento è stato redatto all'interno del GDL-O di competenza, le modifiche e i commenti devono essere inviati all'indirizzo e-mail del coordinatore alla stesura del presente documento (riferimento paragrafo Informazioni generali – Contatti in incipit al presente documento) integrati i commenti e/o le eventuali modifiche del GDL-O vengono redatte le varie versioni v 0.n.

Una volta definita una v 0.n definitiva all'interno del GDL-O, questo ha **15 gg** per apportare ulteriori modifiche sempre inviandole all'indirizzo e-mail del coordinatore alla stesura.

v 1.n→ STATUS PUBBLIC COMMENT → il documento in formato PDF viene pubblicato sul sito di Arsenàl.IT e attraverso lo strumento del FORUM tutta la comunità di Arsenàl.IT può lasciare un proprio commento al documento pubblicato. I commenti saranno rilasciati seguendo delle specifiche istruzioni, disponibili sul sito di Arsenàl.IT.

Il periodo di *pubblic comment* durerà **30 gg.**

Durante il periodo di public comment Arsenàl.IT analizzerà i commenti rilasciati, proponendo una possibile soluzione. Ogni commento e la relativa risposta rimarranno visibili all'intera comunità che potrà intervenire nella discussione.

Alla fine del periodo di *pu*blic comment tutti i commenti analizzati da Arsenàl.IT verranno sottoposti al GDL-O di competenza. In caso di approvazione i cambiamenti verranno integrati al documento di riferimento.

Il GDL-O di competenza valuterà la rilevanza dei cambiamenti apportati al documento e deciderà l'eventuale pubblicazione dello stesso per un ulteriore periodo di *public comment* (pubblicazione v 1.n).

L'iter di pubblicazione e revisione si conclude nel momento in cui non sono apportati cambiamenti sostanziali al documento secondo decisione del GDL-O di competenza.

La versione definitiva andrà quindi in approvazione al TSE-R e all'Unità di Regia.

v 2.0 → APPROVATO → il documento in formato PDF approvato dall'Unità di Regia sarà reso pubblico.

Open Issues:

1. Da definire il servizio custom per l'update delle credenziali aziendali dei prescrittori (RVE-2).
2. Viene esclusa la possibilità di utilizzare un'asserzione ancora valida, ma in scadenza, per ottenere una nuova asserzione. Questa tipologia di servizio non sembra migliorare prestazioni o i livelli di sicurezza.
3. L'Infrastruttura per gli attori aziendali deve essere definita in un momento successivo.
4. Si chiede di valutare i contenuti delle tabelle di codifica presenti in Appendice A. Si propone di utilizzare il "codice" definito nelle tabelle in appendice all'interno dell'asserzione di identità.

Closed Issues:

-

Summary

Il primo obiettivo del seguente documento è descrivere i requisiti minimi di sicurezza che gli applicativi devono soddisfare per l'integrazione nei processi e servizi definiti nel Fascicolo Sanitario Elettronico regionale. Secondo obiettivo di questo documento è definire le specifiche tecniche per il processo di autenticazione degli utenti che necessitano di accedere ai servizi del Fascicolo Sanitario Elettronico regionale.

Il documento è strutturato in due sezioni che descrivono rispettivamente l'infrastruttura del sistema per gli attori territoriali (MMG, Farmacie, RSA, ecc.) e l'infrastruttura per gli attori aziendali.

Attori Territoriali:

Ogni attore coinvolto deve essere considerato un nodo sicuro. Per questo motivo le comunicazioni saranno permesse solo tra sistemi in grado di effettuare una mutua autenticazione attraverso verifica diretta della validità di certificati applicativi installati sugli applicativi. Questi certificati verranno rilasciati ad ogni main release dell'applicativo una volta superata la fase di labeling eseguita da consorzio Arsenàl.IT.

Una volta verificata l'attendibilità del certificato applicativo (attraverso l'utilizzo del protocollo TLS) viene aperto un canale di comunicazione sicuro attraverso il quale possono transitare le richieste di servizi. Ogni richiesta di servizi eseguita da uno specifico utente deve necessariamente essere corredata da un'asserzione d'identità (strutturata attraverso lo standard OASIS SAML 2.0). L'asserzione d'identità è creata dall'azienda sanitaria di competenza a seguito di una richiesta applicativa (Authentication Request) dell'attore territoriale. Tale richiesta deve veicolare le seguenti informazioni:

- le credenziali (user/password) di un utente "responsabile" della richiesta e conosciute dall'Identity Provider aziendale;
- il contesto clinico della richiesta (es. ricovero ordinario, screening ecc.);
- le modalità di autenticazione che l'utente ha eseguito sul client (es. User-Password, Smart Card, ecc.);
- il ruolo dichiarato dal responsabile delle credenziali (es. Medico, Infermiere, Tecnico, ecc.)
- un identificativo specifico per l'installazione dell'applicativo: (formato: ID_labeling^^^Main_Release^^^ID_installazione);
- Codice Fiscale del Responsabile delle Credenziali di autenticazione;
- Codice Fiscale dell'utente che sta effettuando la richiesta.

L'attore aziendale che riceve la richiesta di asserzione deve effettuare le seguenti verifiche prima di generare un asserzione di identità:

- Verificare in modo applicativo specifiche inibizioni associate al Client caratterizzato da uno specifico identificativo di installazione (black-list)
- Verificare la correttezza e la validità delle credenziali del responsabile utilizzate nella richiesta
- Verificare che il ruolo del responsabile coincide con il ruolo conosciuto dall'IDP
- Verificare che il contesto clinico dichiarato è tra i contesti clinici in cui può operare l'applicativo caratterizzato da uno specifico ID_labeling (questi contesti sono assegnati durante la fase di labeling)

L'asserzione d'Identità generata dall'attore aziendale conterrà le seguenti informazioni:

- Il contesto di autenticazione che ha determinato la generazione dell'asserzione
- Il codice fiscale dell'utente che ha effettuato la richiesta di asserzione
- Il codice fiscale del responsabile possessore delle credenziali utilizzate dall'utente
- il ruolo del responsabile delle credenziali di autenticazione
- il contesto clinico della richiesta
- il periodo di validità dell'asserzione di identità

L'asserzione d'identità cosi ottenuta deve essere veicolata all'interno dei messaggi di richiesta di servizi del Fascicolo Sanitario Elettronico regionale.

Attori Aziendali:

to be defined

Infrastruttura di Sicurezza (FSEr): Attori Territoriali

Questa sezione permette di descrivere l'Infrastruttura di Sicurezza ed autenticazione per gli attori territoriali che devono interfacciarsi ai servizi del Fascicolo Sanitario Elettronico regionale. Questa infrastruttura può essere applicata a Medici di base, farmacie, RSA, ecc.

TODO Aziendali:

- **Mantenere aggiornate la CRL dei sistemi aziendali allineandola periodicamente (ogni 10 minuti max) con la CRL gestita a livello regionale**
- **Integrazione dell'appliance dell'attore Identity and Assertion Provider**
  - **Definizione dei connettori necessari per autenticare un Responsabile dotato di credenziali direttamente nell'LDAP aziendale**
  - **Per garantire una gestione uniforme l'attore Identity and Assertion Provider gestirà delle tabelle di confine contenenti le informazioni utili per verificare l'appropriatezza della richiesta di asserzione. Tali informazioni**

devono essere mantenute aggiornate attraverso la configurazione di appositi connettori con i sistemi aziendali che tracciano queste informazioni:

- **ID_APPLICATIVO + CONTESTI ammessi (definiti a livello aziendale)**
- **CF_titolare + USER_ID**
- **CF_titolare + RUOLO**

Non è specificato se questo tipo di informazioni debba essere memorizzato all'interno dell'LDAP come attributi aggiuntivi allo schema esistente o attraverso altre modalità.

- **Gestione a livello di LDAP degli attori territoriali (MMG, titolari di farmacia) ai quali deve essere assegnata una USER_ID e una PASSWORD.**
- **L'azienda deve sincornizzare i propri sistemi con il Server NTP di Galileo Ferraris e dovrà esporre un servizio Server NTP per i propri sistemi interni.**
- **Garantire l'integrazione dell'LDAP aziendale con il servizio applicativo di rinnovo password (transazione [RVE-2])**
- **Implementazione di un ATNA Audit Record Repository**
- **Integrazione degli applicativi territoriali con i sistemi ATNA Audit Record Repository**

1 Use-case: Attori Territoriali

In questa sezione verrà descritto lo use-case di un utente territoriale che vuole autenticare la propria identità per accedere attraverso l'utilizzo di un applicativo locale (X-Service User) ai servizi del Fascicolo Sanitario Elettronico regionale (X-Service Provider). L'architettura del sistema di autenticazione degli utenti dovrà essere federata, in quanto l'Identity Provider dell'utente territoriale è generalmente non integrato al Service Provider dei servizi FSEr. I servizi verranno dunque esposti senza poter verificare direttamente l'identità dell'utente che richiede il servizio. L'Utente è l'utilizzatore di un sistema applicativo che vuole accedere a determinati servizi. Il Responsabile è un possessore di credenziali conosciute da un Identity Provider in grado di asserire l'identità del responsabile stesso e di tutti gli utenti di cui questo responsabile

è garante. L'utente di un sistema si autenticherà localmente all'interno del proprio applicativo utilizzando specifiche credenziali locali (UserPassword dell'utente, SmartCard, ecc...). Utilizzando le credenziali del proprio responsabile, l'utente eseguirà una richiesta di asserzione verso l'Identity and Assertion Provider di riferimento. La richiesta veicolerà ulteriori informazioni relative a contesto e motivazioni della richiesta, utili a valutare la richiesta stessa ed a strutturare l'asserzione di identità. La Response di questa richiesta conterrà un asserzione d'identità firmata digitalmente utilizzabile come ticket per accedere a servizi esposti dal FSEr..

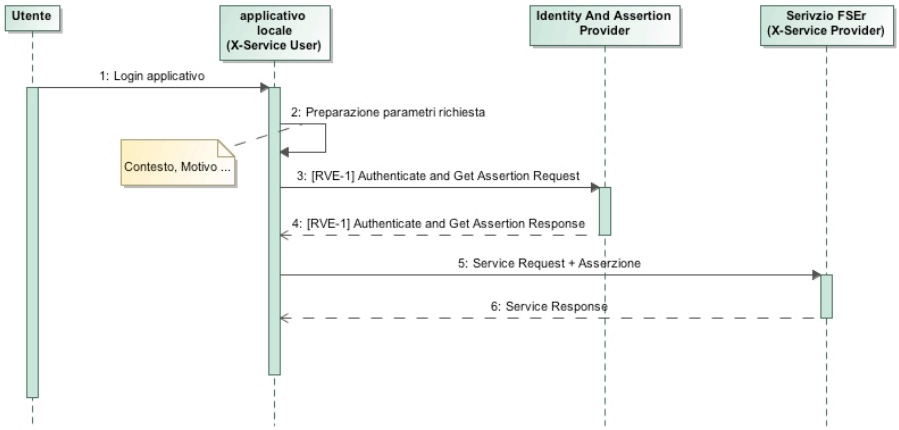


Figura 2 Use-case autenticazione FSEr

2 Sincronizzazione degli applicativi

Tutti i sistemi coinvolti all'interno dell'infrastruttura del Fascicolo Sanitario Regionale devono garantire la sincronia. Per questo motivo ogni sistema dovrà garantire i requisiti dell'attore Time Client come definito nel profilo di integrazione IHE Consistent Time (CT) IHE TF-ITI:1 sezione 7. La sincronizzazione è in questo modo garantita con un errore mediano minore di un secondo.

Un attore CT Time Client deve utilizzare il protocollo NTP (Network Time Protocol) definito nello standard RFC 1305 per la transazione [ITI-1] Maintain Time.

L'azienda garantirà la sincronizzazione dei propri sistemi interni, agendo da Time Client raggruppato con Time Server, allineando il proprio clock con il Time Server di Galileo Ferraris a questi NTP Server primario e secondario:

- **ntp1.inrim.it (193.204.114.232)**

- **ntp2.inrim.it (193.204.114.233)**

Gli attori territoriali in qualità di Time Client si allineeranno direttamente con il Time Server di Galileo Ferraris utilizzando la transazione [ITI-1] Maintain Time.

I dettagli implementativi della transazione sono descritti negli standard di riferimento e al seguente indirizzo: http://www.ntp.org .

Ogni sistema deve garantire l'allineamento del proprio clock con il Time Server effettuando la sincronizzazione **almeno ogni 10 minuti.**

In Figura 3 viene descritta l'infrastruttura per garantire la sincronizzazione dei sistemi coinvolti nel Fascicolo Sanitario Elettronico regionale.

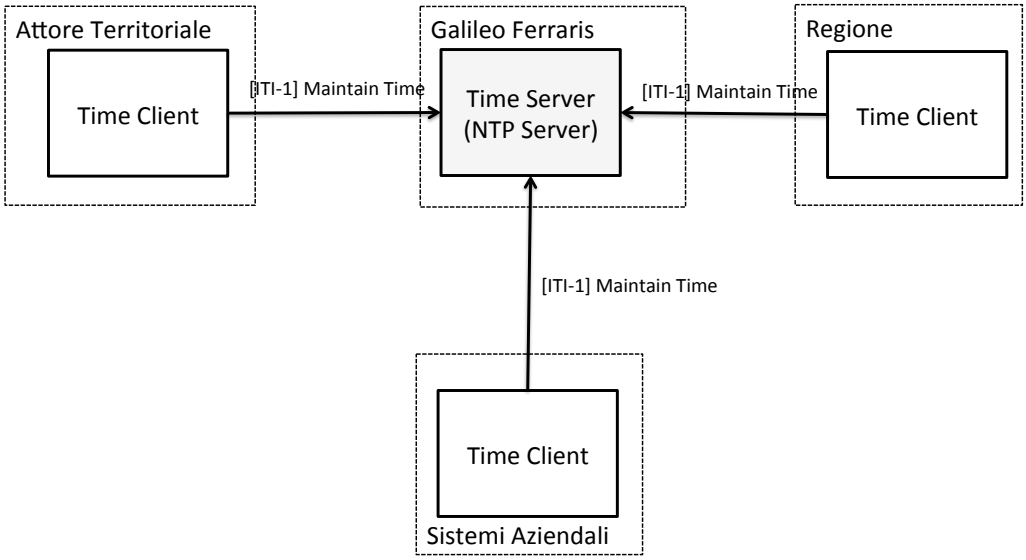


Figura 3: Sincronizzazione dei sistemi

3 Comunicazione sicura tra sistemi ([ITI-19] Authenticate Node):

Per garantire l'accessibilità ai servizi del Fascicolo Sanitario Elettronico regionale ai soli sistemi che hanno superato in modo proficuo una sessione di labeling il processo di connessione tra due applicativi avviene attraverso una mutua autenticazione dei sistemi coinvolti in ogni transazione (per ulteriori dettagli relativi al proceso di labeling si faccia riferimento alla documentazione di riferimento: "ref_labeling"). In questa sezione verranno individuate le principali caratteristiche che i sistemi coinvolti nella rete fascicolo dovranno implementare per garantire comunicazioni sicure. I nodi della rete individuati in via preliminare sono tre:

- Nodo Regionale
- Nodo Aziendale
- Nodo Territoriale (MMG, Farmacia ecc...)

Ogni nodo della rete dovrà considerarsi un nodo sicuro (Secure Node/Secure Application IHE). Un Secure Node locale dovrà presentare la propria identità al Secure Node remoto e dovrà a sua volta verificare l'identità Secure Node remoto. Dopo questa mutua autenticazione possono essere instaurate le successive comunicazioni sicure. Il requisito ulteriore di un Secure Node è quello di autenticare lo user che richiede all'accesso dei servizi al nodo stesso. Questo tipo di operazione verrà gestita solo a livello locale e non comporterà nessuna specifica comunicazione con il Secure Node remoto.

Le comunicazioni sicure e la mutua autenticazione devono avvenire in accordo con le linee guida specifiche del protocollo TLS v1.2 (standard IETF RFC5426) con verifica diretta del certificato applicativo installato sul Server e con verifica della firma di un certificato installato nell'applicativo Client. La firma del certificato Client deve essere effettuata con una chiave pubblica appartenente ad un elenco di CA trustabili.

L'infrastruttura creata per la verifica dell'identità dei nodi e l'apertura di canali sicuri è di tipo PKI: Public Key Infrastructure.

3.1 Creazione Certificati Applicativi Labeling

Al termine del processo di Labeling al software testato vengono associati:

- **ID_labeling**: uno specifico identificativo caratterizzante la main release del software che è stata testata;

- **Certificato applicativo** caratterizzante il prodotto e utilizzabile per garantire l'autenticazione dell'applicativo secondo protocollo TLS.

Ad ogni prodotto labellato è assegnata una CA riconosciuta su tutto il territorio regionale. La coppia (Chiave pubblica, Chiave Privata) viene generata dalla Regione del Veneto ed aggiunta alle liste di validità regionali ed aziendali Il certificato applicativo è self-signed, quindi firmato utilizzando la chiave privata assegnata allo prodotto e corrispondente alla chiave pubblica contenuta nel certificato. La connessione ai sistemi aziendali può avvenire solo da sistemi nei quali è installato un certificato applicativo contenente una chiave pubblica conosciuta (cioè presente nell'elenco delle chiavi pubbliche assegnate durante il processo di labeling) e firmato con una chiave privata associata alla stessa chiave pubblica. La gestione delle liste di revoca (o Certificate Revocation List (CRL)) è realizzata in accordo con lo standard IETF RFC5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". Al rilevamento di un'anomalia, i sistemi aziendali possono comunicare alla regione la necessità di revocare un certificato. Le CRL locali mantengono l'aggiornamento rispetto alla CRL regionale mediante un processo periodico di allineamento (10 minuti).

In Figura 4 è presentata una schematizzazione dell'Infrastruttura PKI concepita per il Fascicolo Sanitario Elettronico regionale.

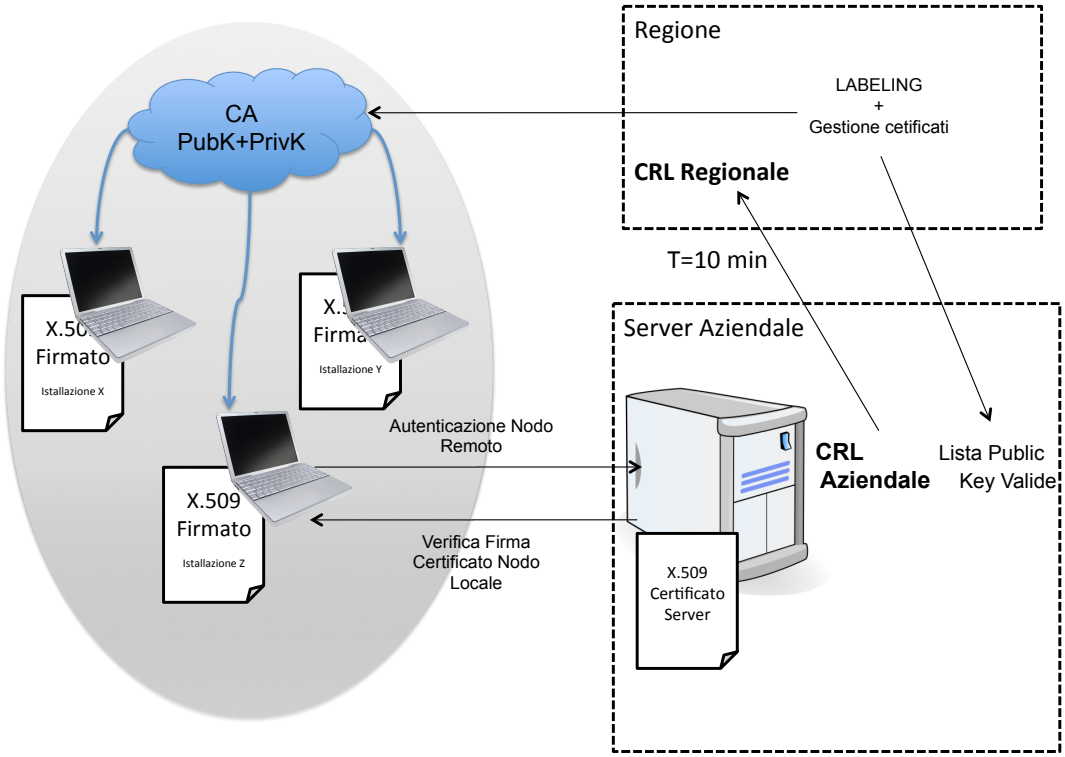


Figura 4: PKI Fascicolo Sanitario Elettronico regionale

Si sottolinea che questa modalità di inibizione di un applicativo dovrebbe essere utilizzata solo in caso di **GRAVE** malfunzionamento del software su più installazioni e viene quindi richiesto di ripetere il processo di labelling.

L'ID_labeling che viene definito in fase di labeling permette di svolgere un azione di controllo e filtro applicativo sui sistemi. Concatenando l'ID_labeling con un identificativo della "Minor Release" del software e con un identificativo definito per la specifica installazione, è possibile ottenere il codice "ApplicationID" che deve essere veicolato all'interno di una richiesta di autenticazione di un Utente (per i dettagli della transazione di autenticazione degli utenti si veda sezione 5.1). I sistemi aziendali possono quindi utilizzare questo parametro per verificare l'attendibilità o meno di una richiesta di autenticazione generata da uno specifico applicativo.

3.1.1 *Requisiti dei certificati*

Sono definiti i seguenti requisiti per i certificati applicativi:

- Non sono richiesti specifici attributi per il contenuto dei certificati
- Certificati per mutua autenticazione devono essere X509 basati su chiave RSA di lunghezza 2048-4096
- Tempo di scadenza dei certificati deve essere al massimo 2 anni
- **Non deve essere utilizzata l'autenticazione del sistema per gestire sistemi di accesso ai dati clinici (Access Policies basate sull'identità dell'utente NON sulla tipologia di prodotto utilizzato). La verifica delle policies di accesso ai dati clinici è garantito dall'asserzione di identità degli user**

3.2 Transazioni sicure tra WS: "WS-I Basic Security Profile"

Una associazione trusted tra due nodi deve essere stabilita utilizzando lo standard WS-I Basic Security Profile Version 1.1. Questa associazione deve essere utilizzata per tutte le transazioni sicure che devono avvenire tra i due nodi.

3.3 Standard di riferimento

- IETF-RFC2246: The TLS Protocol v. 1.0
- WS-I Basic Security Profile Version 1.1
- IHE ATNA profile

4 Audit degli Eventi ([ITI-20] Record Audit Event)

Questa sezione descrive le modalità per la generazione, e la memorizzazione degli Audit degli eventi di rilevanza dal punto di vista della sicurezza e tracciabilità del sistema. Verrà descritta la distribuzione degli ATNA Audit Record Repository e gli standard di riferimento utili per definire la struttura dei messaggi Syslog che devono essere generati dai sistemi coinvolti.

4.1 Infrastruttura Auditing

L'infrastruttura definita per la memorizzazione degli Audit applicativi è federata. Ogni sistema coinvolto all'interno del sistema Fascicolo Sanitario Elettronico regionale DEVE garantire le proprietà di un ATNA Secure Node o ATNA Secure Application (come descritto precedentemente e negli specifici standard di riferimento IHE ITI TF-1: sez. 9) Ogni azienda implementerà un ATNA Audit Record Repository (ARR) in accordo con lo standard ATNA. In questo modo ogni azienda sanitaria sarà responsabile dello storing di tutti gli Audit generati a seguito del tentativo di accesso ai propri sistemi ed al tentativo di consultare documenti o informazioni cliniche memorizzate nei repository aziendali.

Deve essere realizzato anche un ARR a livello regionale in grado di tracciare ogni tentativo di accesso ai servizi regionali (Registry, SAR, ecc.). I flussi informativi vengono così distribuiti su un'architettura federata.

Per quanto riguarda gli attori territoriali, deve essere realizzata un'integrazione tra questi sistemi e l'ARR dell'azienda di riferimento.

Per ogni specifica transazione verrà definito, a seguito di un'analisi di risk assesment, se e in che modalità generare Audit messages. Non è obiettivo di questa documentazione tecnica definire la struttura di tutti gli audit messages generati a seguito delle specifiche transazioni di accesso ai servizi del FSEr.

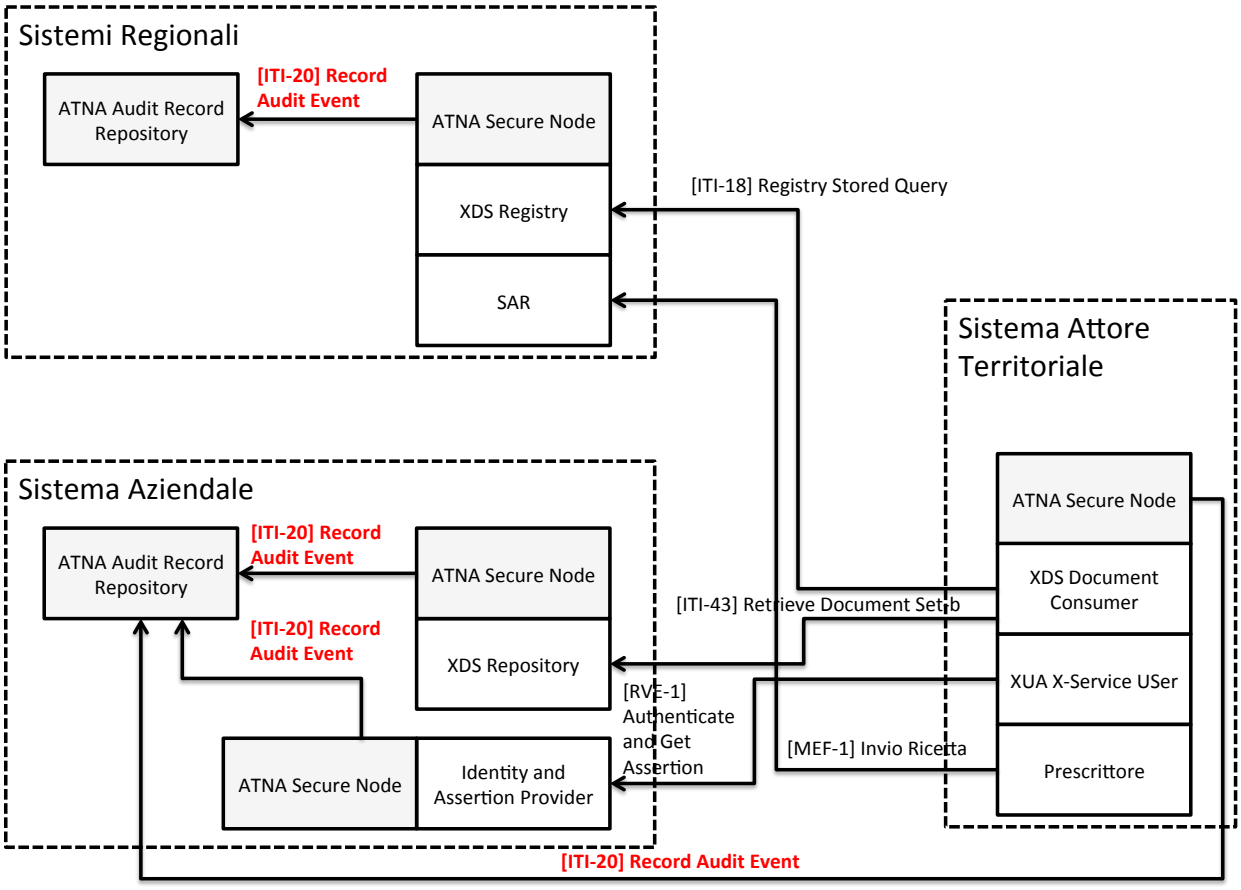


Figura 5: Infrastruttura Auditing FSEr

L'infrastruttura creata permette di verificare analizzando gli Audit memorizzati nel ARR Regionale tutti i tentativi di accesso ai documenti condivisi a livello di FSEr. Per verificare l'effettivo accesso a tali informazioni, è necessario interrogare gli specifici ARR aziendali che tracciano gli accessi ai Repository documentali.

Il processo di autenticazione di un attore territoriale è considerato step fondamentale per tutte le successive interazioni all'interno dei servizi del FSEr. Per questo motivo questo evento deve essere tracciato da una coppia messaggi di Audit:

- il primo inviato dall'applicativo dell'attore territoriale in corrispondenza della richiesta di autenticazione
- il secondo inviato dall'attore Identity and Assertion Provider in corrispondenza della creazione dell'asserzione di identità veicolata all'interno della Response

alla transazione [RVE-1]. (per i dettagli relativi alla transazione [RVE-1] ed al contenuto degli audit messages generati si faccia riferimento alla sezione 5.1 di questo documento di specifiche).

I messaggi di Audit sono strutturati come descritto in sezione 4.2. Questi messaggi sono inviati ad un attore ATNA ARR di riferimento attraverso l'utilizzo di una transazione [ITI-20] Record Audit Event descritta all'interno del documento: IHE ITI TF-2a: 3.20.

L'attore ARR può ricevere e memorizzare Audit messages relativi a diverse tipologie di eventi.

L'attore ARR può essere interrogato per ricevare le necessarie informazioni relative all'auditing. Le modalità di interrogazione sono definite in sezione 4.1.1. L'interfaccia dell'attore ARR permette di interrogare per eventi associati ad uno specifico paziente, ad uno specifico documento o associati ad uno specifico operatore sanitario.

4.1.1 *Interrogazione di un sistema di ARR federato*

to be defined: Fuori scopo per ora. Da definire nel 2014.

4.2 Struttura degli Audit messages

L'auditing degli eventi di rilevanza dal punto di vista della sicurezza è di fondamentale importanza. Per distribuire i carichi di comunicazione tra i sistemi si è concepita un infrastruttura di Audit Trail federata con più ARR (Audit Record Repository). La generazione di Audit Record avviene a livello di Secure Node/Secure Application. I messaggi di Audit sono generati secondo il protocollo Syslog (RFC-5424), veicolando all'interno del campo MSG la struttura XML definita dallo standard RFC-3881: "Security Audit and Access Accountability Message XML Data Definitions for Healthcare Application" in accordo con la transazione IHE ITI-20: Record Audit Event e lo standard DICOM: "Audit Trail Message Format Profile".

Ogni transazione standardizzata definisce in modo mandatorio la struttura di questa porzione XML in modo tale da poter veicolare le informazioni necessarie al Security Officer. Per le transazioni non standardizzate (transazioni MEF ciclo prescrittivo, RVE-1,

RVE-2, ecc...) verrà definita una specifica struttura dell'audit all'interno delle specifiche di riferimento.

I messaggi Syslog DEVONO essere inviati attraverso protocollo TLS garantendo la confidenzialità e l'autenticazione dei sistemi coinvolti. Le modalità per l'invio dei messaggi attraverso i protocolli sopracitati è definita negli standard IETF di riferimento: RFC5425 e RFC5426.

I principali set di informazioni che sono veicolati all'interno di un messaggio di audit sono:

1. **Event Identification**: informazioni che permettono di identificare lo specifico evento tracciato;
2. **Active Participant Identification**: informazioni relative all'utente che ha svolto l'evento. Veicola informazioni sull'identità che sono veicolate attraverso l'asserzione di identità.
3. **Network Access Point Identification:** identifica il punto di accesso alla rete da cui è stato eseguito l'evento
4. **Audit Source Identification:** individuazione della sorgente applicativa che ha generato l'Audit
5. **Participant Object Identification:** set di informazioni che permette di identificare i vari soggetti che partecipano all'evento o le varie istanze di dati coinvolte nell'evento tracciato.

4.3 Standard di riferimento

- IETF-RFC5424: The Syslog Protocol
- IETF-RFC5425: Transport Layer Security (TLS) Transport Mapping for Syslog
- IETF-RFC3881: Security Audit and Access Accountability Message XML Data Definitions for Healthcare Application
- DICOM Audit Trail Message Format Profile

- IHE ATNA profile

5 Federazione di Identity Provider: approccio SAML 2.0

Verrà definita un'infrastruttura per l'autenticazione degli user federata. In questo modo, un Service Provider potrà erogare servizi ad uno user non conosciuto sulla base di un'asserzione di identità (token SAML 2.0) creata da un Identity Provider Trusted. Gli attori Identiy Provider (Assertion Creator) sono localizzati a livello Aziendale, in quanto gli Active Directory aziendali gestiscono già le credenziali di autenticazione di medici aziendali ed MMG. Nello stesso modo dovranno essere gestite le credenziali rilasciate al titolare di ogni farmacia territoriale. Il sistema Identity Provider aziendale dovrà sviluppare due servizi:

1. Un servizio di autenticazione e richiesta asserzione (RVE-1: Authenticate and Get Assertion) che permetterà ad un qualsiasi attore X-Service User (Cross-Enterprise Service User) che vuole accedere a servizi regionali o extra aziendali, di richiedere un'asserzione di identità previa autenticazione mediante l'utilizzo delle credenziali fornite dall'identity provider (I dettagli della transazione sono descritti di seguito nella sezione 5.1).
2. Un servizio applicativo per l'aggiornamento periodico delle credenziali di autenticazione (RVE-2: Update Password, sezione 5.3)

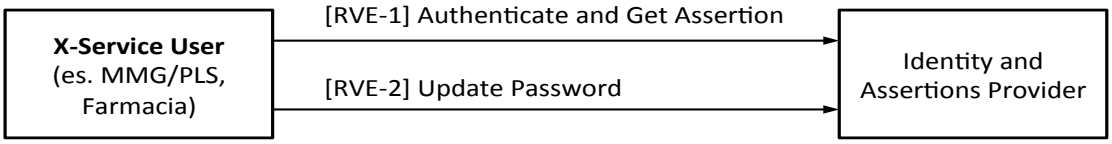


Figura 6: Transazioni Piattaforma di autenticazione federata FSEr

L'infrastruttura di Sicurezza è concepita in modo da poter essere integrata con il sistema di policy management che verrà creato a livello Regionale per garantire il controllo degli accessi ai PHI. Di seguito è presentato uno schema riassuntivo

rappresenta l'infrastruttura creata per la richiesta, la produzione e l'utilizzo del token SAML 2.0.

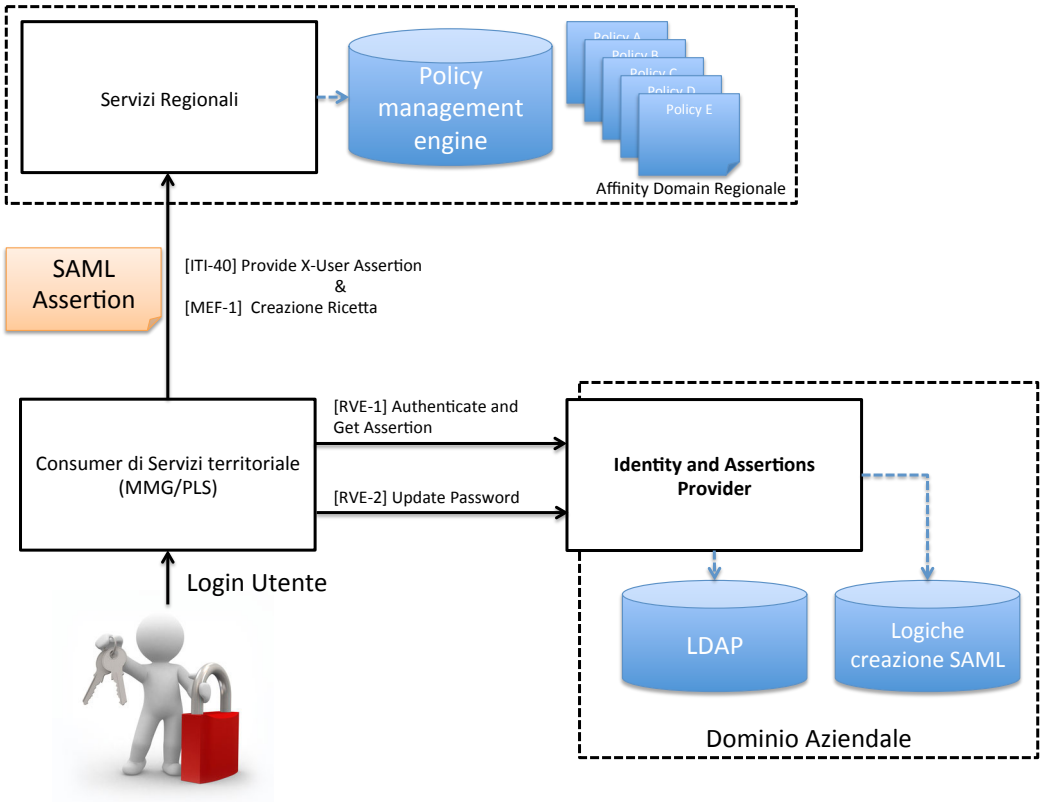


Figura 7: Infrastruttura per l'autenticazione degli utenti

Un utente che necessita di interfacciarsi sul sistema Fascicolo Sanitario Elettronico regionale dovrà autenticarsi nel proprio sistema locale secondo le regole impostate. L'applicativo utilizzato dall'utente richiederà allo Identity and Assertion Provider aziendale un'asserzione d'identità presentandosi con le credenziali aziendali di un responsabile (mappato quindi nell'LDAP aziendale). L'asserzione viene creata per lo specifico utente che ha eseguito la richiesta e conterrà informazioni relative al Ruolo, Contesto all'interno delle quali è stata realizzata la richiesta. L'asserzione firmata digitalmente (XML Signature) viene utilizzata come ticket per accedere ai servizi del

FSEr di interesse. L'attore X-Service Provider sarà caratterizzato da un sistema di policy management in grado di verificare l'accessibilità alle risorse richieste.

5.1 RVE-1: Authenticate and Get Assertion

Questa sezione descrive la transazione RVE-1 individuando scopo, semantica dei messaggi scambiati e Expected Actions degli attori coinvolti. Questa transazione è utilizzata dall'X-Service User e dall' Identity and Assertions Provider. Questa transazione non descrive come utilizzare l'asserzione generata dall'Identity and Assertions Provider. L'utilizzo dell'asserzione di identità per accedere a servizi regionali o extra-aziendali è descritto all'interno della transazione [ITI-40] Provide X-User Assertion profilata da IHE (si faccia riferimento alla sezione 5.2 di questo documento).

L'attore Identity and Assertion Provider si interfaccia direttamente con i sistemi aziendali. Il processo di autenticazione avviene all'interno dell'LDAP aziendale attraverso la configurazione di un connettore specifico. Le ulteriori informazioni necessarie per la verifica della richiesta di asserzione e per definire il contenuto informativo dell'asserzione stessa sono ricavati dall'attore Identity and Assertion Provider all'interno di opportune tabelle di confine configurate in modo tale da essere periodicamente aggiornate a seguito di un processo di query svolto sui sistemi aziendali. I connettori necessari per popolare le specifiche tabelle di frontiera sono configurati a livello aziendale.

In Figura 8 è descritto il comportamento dell'attore Identity and Assertion Provider, individuando:

- i parametri forniti all'interno della richiesta
- i parametri inseriti all'interno dell'asserzione di identità
- le modalità di interfacciamento con i sistemi aziendali

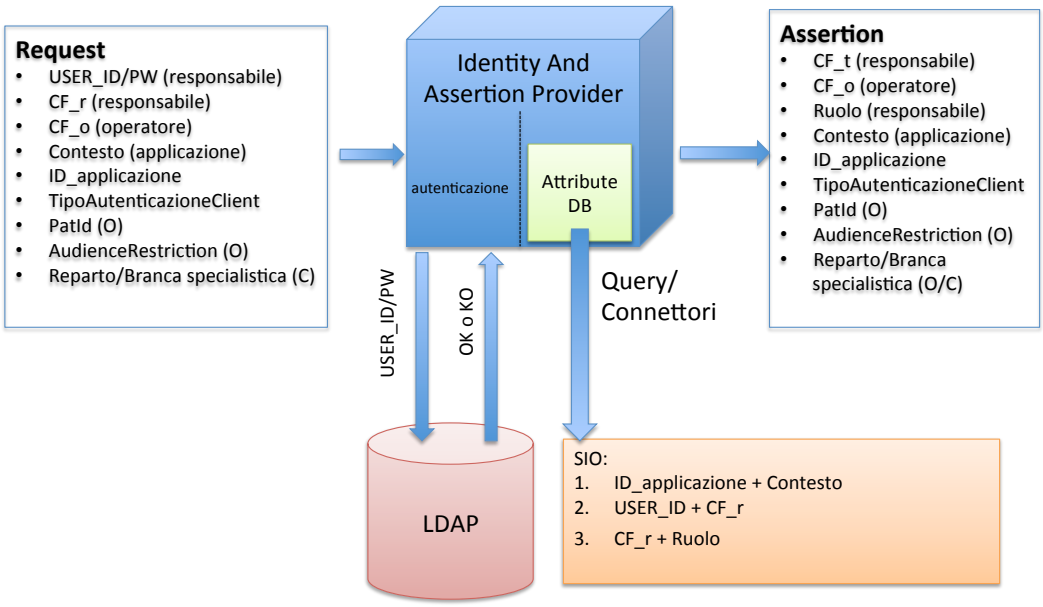


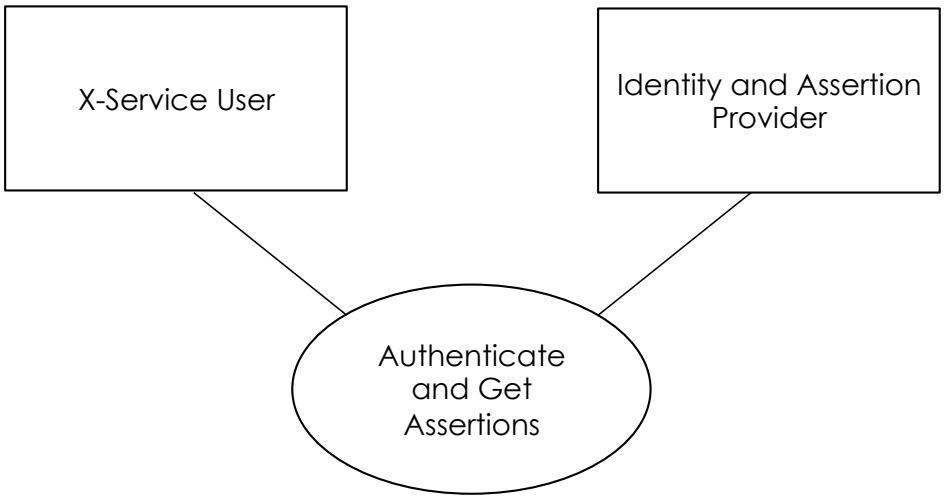
Figura 8: Comportamento dell'Attore Identity and Assertion Provider

5.1.1 *Scopo*

Questa transazione è utilizzata dall'X-Service User, ovvero un attore che deve accedere a servizi regionali o extra aziendali senza potersi autenticare direttamente all'X-Service Provider. Per questo motivo l'X-Service User richiede al proprio Identity and Assertions Provider di produrre un token SAML 2.0 che asserisca l'identità ed il ruolo dell'utente che si è autenticato sul proprio sistema. Come definito in precedenza: una richiesta di asserzione è caratterizzata da un UTENTE che rappresenta l'effettivo richiedente e il RESPONSABILE, ovvero il detentore delle credenziali di autenticazione che sono utilizzate dall'utente per richiedere l'asserzione. L'utente è autenticato sul sistema client (X-Service User) utilizzando delle proprie credenziali. Il sistema X-Service User effettua una richiesta di asserzione presentando le credenziali di autenticazione (Username e Password) del responsabile. Queste due figure possono coincidere o meno a seconda dello use-case in esame (es. nel caso della farmacia territoriale, il responsabile è sempre il titolare della farmacia stessa, mentre i vari operatori che possono partecipare al processo di erogazione farmaceutica costituiscono i vari utenti)

5.1.2 *Attori e ruoli*

Actor:	X-Service User
Role:	Richiede la creazione di un'asserzione di identità utilizzando delle credenziali di un responsabile conosciuto dall'identity provider.
Actor:	Identity and Assertion Provider
Role:	Verifica l'identità dell'utente (e del responsabile) dell'attore X-Service User e sulla base di logiche interne crea un'asserzione valida o genera una risposta di errore.



5.1.3 *Standard di riferimento*

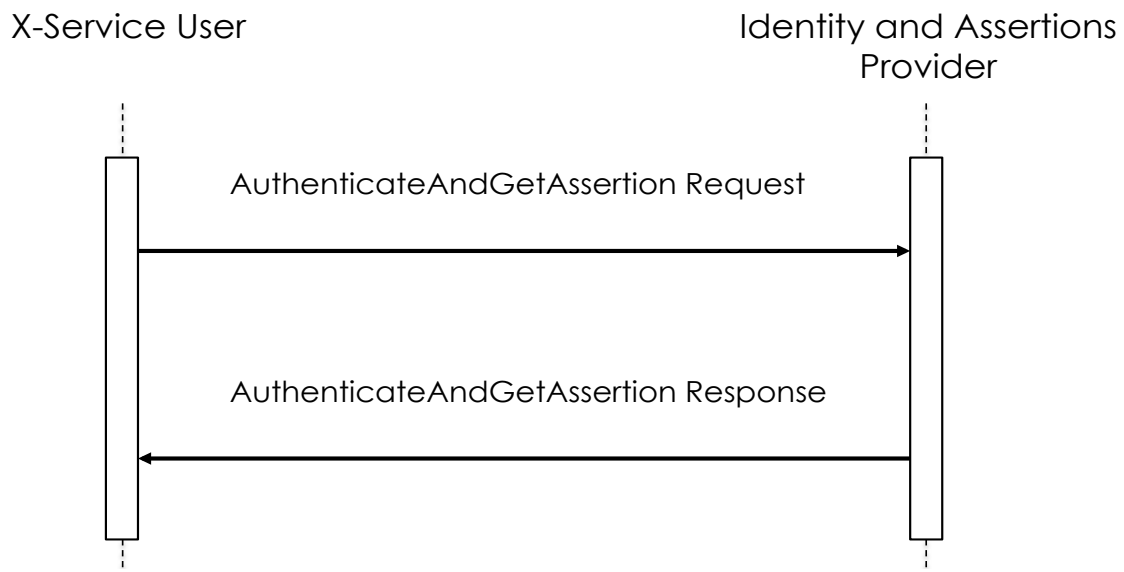
585

- W3C WS-Addressing 1.0 – SOAP Binding
- OASIS WS-Security
- OASIS WS-UsernameToken Profile
- OASIS SAML family spec.

590

- IHE ITI TF-2x: Appendix V
- IHE ITI TF-2b

5.1.4 *Interaction Diagram*



595

5.1.4.1 AuthenticateAndGetAssertion Request

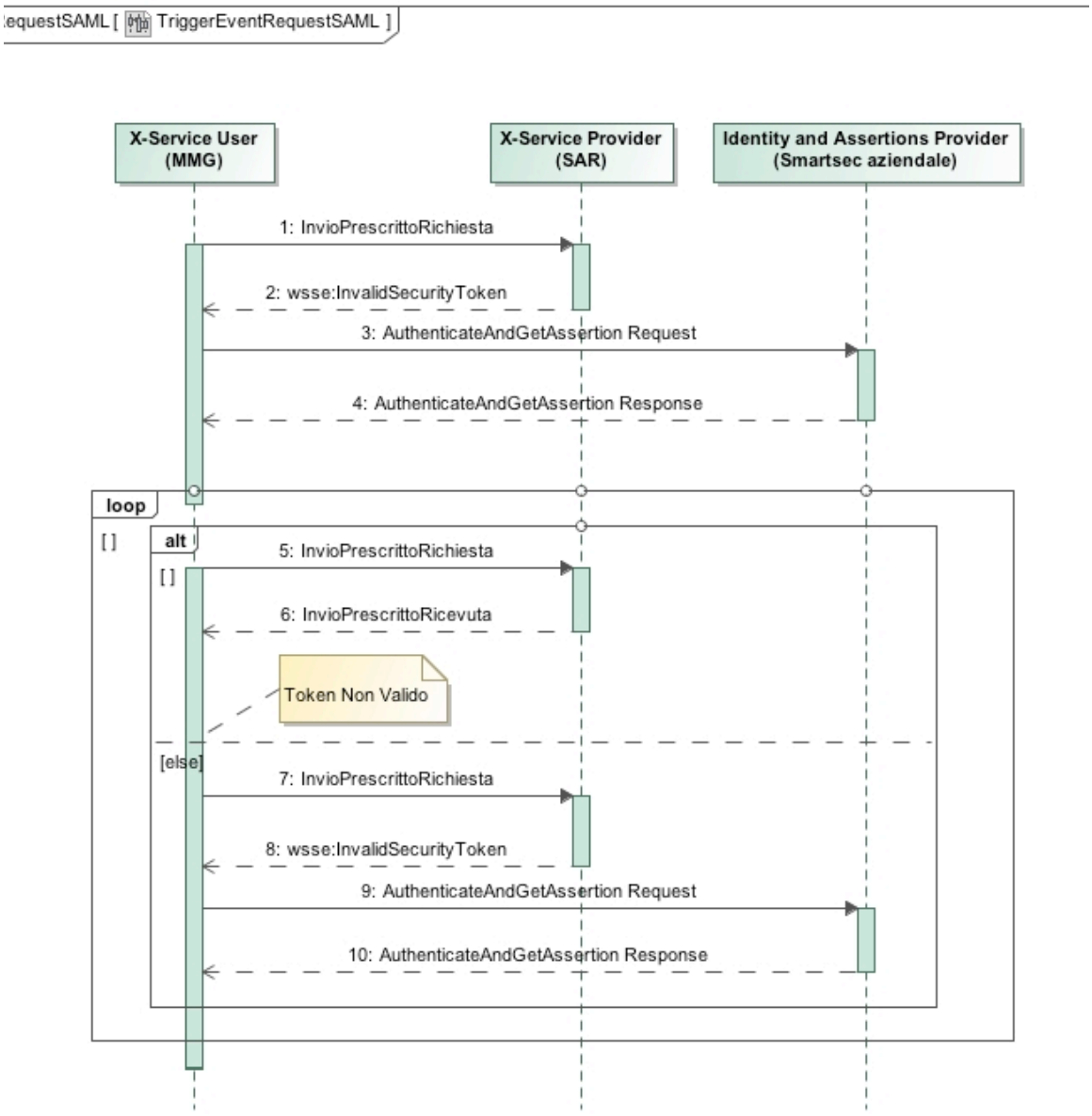
Lo stesso Server (Identity And Assertion Provider) può essere invocato da tutti i client afferenti al suo dominio di autenticazione (tutti gli invocatori di servizi X-Service User).

600

5.1.4.1.1 Trigger Events

Il trigger events che determina la richiesta di una nuova asserzione d'identità è l'impossibilità di accedere ad un servizio esposto da un attore X-Service Provider a causa dell'utilizzo di un'asserzione non valida (vedi figura Figura 9). Oppure l'X-Service User è dotato di un servizio di keep-alive dell'asserzione in modo da poter riconoscere se l'asserzione sta per scadere o meno.

605



610 **Figura 9: Trigger Richiesta asserzione**

5.1.4.1.2 Message Semantics

Il messaggio creato dovrà essere un messaggio SOAP e quindi rispettare lo schema definito da http://schemas.xmlsoap.org/soap/envelope/.

L'Header del messaggio SOAP conterrà le informazioni relative all'autenticazione dello user Client. Si farà riferimento per questo elemento allo standard OASIS WS-Security ed in particolare allo UsernamePassword Token Profile.

Il Body conterrà la porzione di messaggio necessaria per effettuare la richiesta di asserzione.

5.1.4.1.2.1 SOAP Header

La struttura dell'Header DEVE essere conforme alle specifiche WS-Addressing 1.0 SOAP Binding redatte dal W3C (http://www.w3.org/2005/08/addressing nelle specifiche il namespace di riferimento sarà **wsa**). Queste specifiche permettono di individuare all'interno del messaggio scambiato il destinatario del messaggio stesso. Ogni messaggio NON DEVE contenere più di un elemento delle tipologie seguenti:

- **<wsa:To>** = indirizzo URI del destinatario ultimo del messaggio
- **<wsa:Action>** = URI che identifica la semantica attesa nel body ("urn:rve:AuthenticateAndGetAssertionRequest" identifica che il messaggio veicola una richiesta di autenticazione e una richiesta di asserzione asserzione)
- **<wsa:MessageID>** = identificativo univoco del messaggio

L'Header del messaggio SOAP deve anche contenere la porzione legata all'autenticazione dello responsabile, possessore delle credenziali (Username e password) necessarie per richiedere l'asserzione di identità per l'utente al Identity and Assertions Provider. Questa porzione è strutturata mediante l'utilizzo dello standard WS-Security: SOAP Message Security Version 1.1.1 (namespace di riferimento **wsse**). Accoppiando questo standard con il profilo WS Security UsernameToken Profile 1.0 (namespace di riferimento associato al WS-Utility profile: **utp**) è possibile definire come l'X-Service User deve utilizzare il token Username e Password per autenticare l'identità del responsabile attraverso l'Identity and Assertions Provider.

L'elemento UserNameToken, contenuto all'interno di un elemento Security DEVE contenere:

- **<wsse:Username>** = l'identificativo del responsabile conosciuto dall'Identity and Assertions Provider
- **<wsse:Password>** = non DEVE contenere la password in clearText.. Questo elemento deve essere valorizzato con il digest della password (password/@type=Password_Digest) definito come di seguito concatenando password, nonce ed un time stamp.
- **<wsse:Nonce>** = valore random creato dall'inviante per ogni UserNameToken. Il Server deve mantenere l'elenco dei nonce utilizzati (accopiando il nonce con il creation time wsu:Created si può limitare il dispendio di risorse del server limitando la cache ai nonce più recenti).
- **<utp:Created> =** il time stamp di creazione dello usernameToken e coincide con l'istante di creazione del messaggio di richiesta. E' strutturato secondo il formato UTC.

Sia <wsse:Nonce> che <wsu:Created> DEVONO essere presenti e DEVONO essere inclusi nel digest della password:

Pasword_Digest = Base64 (SHA-1 (nonce + created + password))

la funzione di hash deve essere applicata alla concatenazione dei tre elementi descritti precedentemente. Il valore del campo created deve essere concatenato nella propria codifica UTF-8.

Di seguito è presentato un esempio di SOAP Header per il messaggio AuthenticateAndGetAssertion Request:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ soap.xsd">
   <soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.w3.org/2005/08/addressing ws-addr.xsd">
      <wsa:Action> urn:rve:AuthenticateAndGetAssertionRequest </wsa:Action>
      <wsa:MessageID>urn:uuid:9376254e-da05-41f5-9af3-ac56d63d8ebd</wsa:MessageID>
      <wsa:To>http://identityAndAssertionsProvider</wsa:To>
      <wsse:Security
         xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd oasis-200401-wss-wssecurity-secext-1.0.xsd">
         <wsse:UsernameToken
            xmlns:utp="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
            <wsse:Username>PIPPO</wsse:Username>
            <wsse:Password
Type="wsse:PasswordDigest">weYI3nXd8LjMNVksCKFV8t3rgHh3Rw==</wsse:Password>
            <wsse:Nonce>WScqanjCEAC4mQoBE07sAQ==</wsse:Nonce>
            <utp:Created>2003-07-16T01:24:32Z</utp:Created>
         </wsse:UsernameToken>
      </wsse:Security>
   </soap:Header>
   <soap:Body>
      ... <!—qua va il body con la richiesta di asserzione-->
   </soap:Body>
</soap:Envelope>
```

5.1.4.1.2.2 SOAP Body

Il body del messaggio SOAP deve essere strutturato in accordo con il protocollo SAML definito nelle specifiche "Assertions and Protocols for the OASIS SAML V2.0" e fa riferimento al namespace: **samlp**="urn:oasis:names:tc:SAML:2.0:protocol".

La richiesta di asserzione è costituita da un elemento **<samlp:AuthnRequest>** che possiede i seguenti attributi obbligatori:

- **ID:** è l'identificativo univoco della richiesta. Tipo di dato "ID" e corrisponde all'identificativo univoco contenuto nell'elemento del Header SOAP <wsa:MessageID> privato dei caratteri "urn:uuid:" (il dataType ID non permette l'utilizzo del carattere ":").

es:

header/MessageID=urn:uuid:9376254e-da05-41f5-9af3-ac56d63d8ebd

body/ AuthnRequest/@ID=9376254e-da05-41f5-9af3-ac56d63d8ebd

- **Version:** deve essere valorizzato con "2.0".
- **IssueInstant:** istante in cui è creata la richiesta in formato UTC.

All'interno dell'elemento <samlp:AuthnRequest> sono contenuti una serie di sotto-elementi che permettono di identificare l'attore che sta effettuando la richiesta, il soggetto per il quale DEVE essere creata l'asserzione ed il motivo. Il processo di autenticazione DEVE avvenire a seguito dell'analisi del contenuto dell'elemento UsernameToken contenuto nell'Header SOAP e quindi prima della lettura dell'elemento <samlp:AuthnRequest>.

I sotto elementi contenuti (riferimento al namespace **saml**=" urn:oasis:names:tc:SAML:2.0:assertion") sono:

- **<saml:Issuer>:** elemento che permette di identificare il **responsabile** che effettua la richiesta (tipo di dato complesso NameIDType). Questo elemento deve veicolare le stesse informazioni utilizzate per effettuare l'autenticazione attraverso il blocco WS-Security contenuto nel SOAP Header. Questo elemento contiene una stringa con il CODICE FISCALE del responsabile della richiesta. **Conseguentemente l'Issuer sarà sempre un attore conosciuto dall'attore Identity and Assertions Provider (soggetto presente nell'LDAP aziendale)**.
- **<samlp:Extensions>:** è l'elemento che permette di veicolare verso l'attore Identity and Assertions Provider informazioni aggiuntive utili per creare l'asserzione stessa. L'elemento Extensions contiene un set di attributi, forniti dal sistema cient, che poi comporranno l'asserzione. PUO' quindi contenere solamente un elemento **<AttributeStatment>**.
    - **<AttributeStatment>:**questo elemento contiene molteplici elementi
        - **<Attribute>:** è l'elemento che descrive l'attributo della richiesta di asserzione. Sono attesi almeno tre elementi

Attribute all'interno di un messaggio AuthenticateAndGetAssertion Request:

1. **UserClientAuthentication**: descrive la tipologia di autenticazione eseguita dall'utente per accedere ai servizi del sistema X-Service User. I codici da utilizzare per questo attributo sono definiti in Appendice A: CodeSystems.

2. **RequestContext**: descrive il contesto all'interno del quale si è resa necessaria la richiesta di servizio. Questo attributo può essere valorizzato con i codici definiti in Appendice A: CodeSystems.

3. **ApplicationID**: definisce l'ID dell'applicativo che esegue la richiesta di asserzione il formato dell'ID è: [ID_labeling]^[minor_release]^[installazione] dove "ID_labeling" è l'ID associato al prodotto software che ha superato la fase di labeling, "minor_release" rappresenta la versione successiva del software non labellata, "istallazione" rappresenta un identificativo univoco per la specifica installazione del software labellato.

4. **PatienID**: rappresenta l'identificativo univoco del paziente nei confronti del quale l'utente sta agendo con il contesto dichiarato. L'opzionalità di questo attributo è dipendente dalla tipologia di servizio al quale si vuole accedere.

5. **Reparto_Branca**: attributo che permette di veicolare le informazioni relative al reparto o la branca specialistica dal quale è effettuata la richiesta di autenticazione.

- **<saml:Subject>**: specifica l'utente che effettua la richiesta. Esistono vari use-case per i quali il Subject di un'asserzione è diverso dall'Issuer della richiesta, in quanto una richiesta può essere effettuata solo presentando UsernameToken di responsabili accreditati dall'attore Identity and Assertions Provider. Per esempio:

a) richiesta effettuata per un operatore di una farmacia diverso dal titolare:

UsernameToken= titolare , *Issuer* = titolare , *Subject* = operatore.

b) richiesta effettuata da un medico sostituto con credenziali dell'MMG:

UsernameToken= MMG , *Issuer* = MMG , *Subject* = sostituto.

L'identità dell'utente è tracciata all'interno di un elemento di tipo NameIDType:

- **<NameID>** : DEVE contenere il **codice fiscale** del soggetto per cui viene richiesta l'asserzione. Questo utente deve essere caratterizzato anche dallo userID utilizzato per autenticarsi all'interno del client e dall'individuazione del provider che ha autenticato l'utente. Queste informazioni sono veicolate attraverso l'utilizzo dei seguenti attributi:
  - **SPNameQualifier**: il provider che qualifica il name (es. la farmacia)
  - **SPProvidedID**: l'ID utilizzato dallo user all'interno della struttura

- **<saml:Conditions>**: è l'elemento che permette di veicolare le condizioni SAML che l'X-Service User si aspetta di ottenere all'interno dell'asserzione per limitarne la validità e l'utilizzo. **L'attore Identity and Assertions Provider può modificare queste condizioni se necessario**. L'elemento <saml:Conditions> può contere i seguenti attributi:
  - **NotBefore:** specifica il primo istante di tempo per cui l'asserzione è valida
  - **NotOnOrAfter**: specifica l'istante di tempo in cui l'asserzione scade

All'interno dell'elemento <saml:Conditions> è possibile aggiungere un elemento <AudienceRestriction>:

- **<AudienceRestriction>:** è un elemento opzionale che permette di specificare il Serivizio regionale o extra-aziendale a cui si cercherà di accedere utilizzando l'asserzione richiesta. Per ogni destinatario individuato viene aggiunto un elemento:
  - **<Audience>:** che contiene l'URL del servizio a cui si cercherà di accedere utilizzando l'asserzione prodotta (questo servizio corrisponde all'attore X-Service Provider, vedi sezione 5.2)

Di seguito è presentato un esempio di SOAP body per un messaggio AuthenticateAndGetAssertion Request:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ soap.xsd">
   <soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.w3.org/2005/08/addressing ws-addr.xsd">
.... <!—qua va l'header con la richiesta di asserzione-->
   </soap:Header>
   <soap:Body xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:protocol saml-schema-protocol-2.0.xsd">
      <samlp:AuthnRequest ID="9376254e-da05-41f5-9af3-ac56d63d8ebd" Version="2.0"
         IssueInstant="2003-07-16T01:24:32Z">
         <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">CF_Pippo</Issuer>
         <samlp:Extensions>
            <AttributeStatement xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
               <Attribute Name="UserClientAuthentication">
                  <AttributeValue>A.1</AttributeValue>
               </Attribute>
               <Attribute Name="ApplicationID ">
                  <AttributeValue>1.2.3.4.5.6^0.4^00023</AttributeValue>
               </Attribute>
               <Attribute Name="PatientID">
                  <AttributeValue>TRMLRA56L50F382V</AttributeValue>
               </Attribute>
               <Attribute Name="RequestContext">
                  <AttributeValue>C.1.1</AttributeValue>
               </Attribute>
            </AttributeStatement>
         </samlp:Extensions>
         <Subject xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
            <NameID>ZNRMRA86L11B157N</NameID>
         </Subject>
         <Conditions xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
            NotBefore="2003-07-16T01:24:32Z" NotOnOrAfter="2003-07-17T01:24:32Z">
            <AudienceRestriction>
               <Audience>http://X-ServiceProvider</Audience>
            </AudienceRestriction>
         </Conditions>
      </samlp:AuthnRequest>
   </soap:Body>
</soap:Envelope>
   </soap:Body>
</soap:Envelope>
```

5.1.4.1.3 Expected Actions

Il messaggio AuthenticateAndGetAssertion Request prevede due azioni consecutive:

- richiesta di autenticazione di un responsabile;
- richiesta di un'asserzione di identità per un utente.

Il processamento dell'header permette di eseguire l'autenticazione dello user. Se Lo usernameToken viene processato in modo corretto l'attore Identity and Assertions Provider riconosce l'identità del responsabile della richiesta. L'attore Identity and Assertions Provider DEVE:

- rigettare token creati che non utilizzano wsse:Nonce e wsu:Created.
- rigettare token con time stamp troppo datati (un intervallo di tempo indicativo di 5 minuti)
- tenere memoria dei nonce utilizzati all'interno del time limit impostato.

In caso di errore nel processo di autenticazione, l'attore Identity and Assertions Provider deve generare un messaggio di Response che veicola l'errore in accordo con le specifiche definite all'interno dello standard WS-Security section 12 "Error Handling" (la struttura di un messaggio di Response generato a seguito del fallimento de processo di autenticazione è definito in sezione 5.2.1):

- **<wsse:FailedAuthentication>**: Se il security Token non può essere autenticato o autorizzato. (Le specifiche tipologie di errore associate a questa classe di errore sono definite in appendince A, sezione A.4.5).

Se l'attore Identity and Assertions Provider è in grado di processare in modo corretto il body SOAP del messaggio AuthenticateAndGetAssertion Request, DEVE creare un messaggio di risposta AuthenticateAndGetAssertion Response contentente un'asserzione di identità per il <Subject> individuato nella richiesta. Se l'attore Identity and Assertions Provider ritiene una richiesta NON valida secondo la sintassi SAML o non ritiene di poter asserire l'identità dell'utente definito nell'elemento <Subject>, DEVE creare un messaggio di Response con al suo interno un elemento **<StatusCode>** che descrive la condizione di errore. Di seguito sono presentate le varie condizioni di errore che devono essere utilizzate all'interno dell'attributo **value**:

- *urn:oasis:names:tc:SAML:2.0:status:Requester*: la richiesta non è stata completata in quanto si è individuato un errore dal lato del client

- *urn:oasis:names:tc:SAML:2.0:status:Responder*: la richiesta non è stata completata in quanto si è individuato un errore dal lato del server
- *urn:oasis:names:tc:SAML:2.0:status:InvalidAttrNameOrValue*: contenuto non atteso o non valido è individuato negli attributi della richiesta
- *urn:oasis:names:tc:SAML:2.0:status:RequestDenied*: il server è riuscito a processare la richiesta ma ha scelto di non rispondere con un successo.
- *urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported*: il server non supporta la richiesta

L'elemento <statusCode> può contenere altri sottoelementi che permettono di dettagliare la condizione di errore:

- **<StatusMessage>**: permette di veicolare all'operatore una stringa contenente maggiori informazioni sulla condizione di errore verificatosi.

5.1.4.1.3.1 Controlli eseguiti sui parametri della richiesta

In questa sezione verrano descritti i controlli mandatori e quelli opzionali che l'attore Identity and Assertion Provider deve eseguire sui parametri della richiesta di autenticazione. La gestione e il mantenimento dei flussi informativi necessari per effettuare la verifica è in carico all'azienda sanitaria di riferimento, la quale dovrà predisporre degli specifici connettori verso l'attore Identity and Assertion Provider.

Le principali verifiche mandatorie che l'attore deve garantire sono:

- Verificare che il contesto dichiarato dall'applicativo sia tra i contesti che l'azienda ha abilitato per quel determinato ID_labeling:

  contesto dichiarato ∈ (contesti + ID_labeling)

- Verificare che il CF del responsabile coincida con il CF memorizzato nei sistemi aziendali:

  CF_r == CF conosciuto in azienda

Le verifiche opzionali che deve effettuare l'attore Identity and Assertion Provider sono presentate di seguito. L'opzionalità può essere legata a policy aziendali o a specificità legate al servizio a cui l'attore X-Service User cercherà di accedere utilizzando l'asserzione di identità. In questo caso DOVREBBE essere veicolato all'interno dei

parametri della richiestal'elemento AudienceRestriction specificante l'url del X-Service Provider (vedere sezione 5.2 per i dettagli):

- Verificare che l'ApplicationID non sia tra le istallazioni o tra le minor release "bannate" dall'azienda:

  ApplicationID ∉ applicativi Bannati Aziendali

- Verificare che lo specifico paziente (PatientID) sia nella relazione dichiarata (contesto) con l'utente che esegue la richiesta:

  PatientID ∈ (contesto + PatientID)

- Verificare che la tipologia di autenticazione eseguita sul Client sia tra le tiplogie di autenticazione ammesse:

  UserClientAuthentication ∈ UserClientAuthentication ammessi

5.1.4.2 AuthenticateAndGetAssertion Response

Questo messaggio veicola verso l'attore X-Service User l'asserzione di identità necessaria per invocare successivi servizi regionali o extra-aziendali

5.1.4.2.1 Trigger Events

Il messaggio di Response contenente l'asserzione viene generato in risposta ad un messaggio di Request.

5.1.4.2.2 Message Semantics

5.1.4.2.2.1 SOAP Header e Body

Il messaggio di response è un messaggio SOAP che descrive una **<soap:Action>** del tipo *urn:rve:AuthenticateAndGetAssertionResponse*. E' necessario tracciare nell'Header del messaggio SOAP l'identificativo del messaggio di Request che ha determinato la generazione della Response attraverso l'elemento **<wsa:RelatesTo>**.

Il SOAP Body contiene un elemento <samlp:Response> che DEVE contenere al suo interno:

- **<samlp:Status>** elemento obbligatorio che contiene a sua volta una serie di elementi:
  - **<samlp:StatusCode>:** Elemento obbligatorio che permette di veicolare un codice che descrive lo stato di attività della risposta alla richiesta corrispondente. Questo elemento DEVE contenere un attributo:
    - **Value**: valorizzato con *"urn:oasis:names:tc:SAML:2.0:status:Success"* in caso di successo, o con una condizione di errore descritta in "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0" , sezione 45.
  - **<samlp:StatusMessage>**: elemento opzionale che permette di veicolare un messaggio all'utente che richiede un'asserzione
- **<saml:Assertion>:** se la richiesta è stata processata in modo corretto (Status di successo), l'elemento Response deve contenere un elemento assertion che permette di strutturare l'asserzione in accordo con lo schema "urn:oasis:names:tc:SAML:2.0:assertion".

Di seguito viene presentato un esempio di messaggio SOAP per il messaggio AuthenticateAndGetAssertion Response (il contenuto dell'asserzione è descritto nella sezione 5.1.4.2.2.2).

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ soap.xsd">
   <soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.w3.org/2005/08/addressing ws-addr.xsd">
      <wsa:Action>urn:rve:AuthenticateAndGetAssertionResponse</wsa:Action>
      <wsa:MessageID>urn:uuid:4532254e-fe54-56g8-2xf3-cc5cf6ac8eb1</wsa:MessageID>
      <wsa:To>http://X-ServiceUser</wsa:To>
      <wsa:RelatesTo>urn:uuid:9376254e-da05-41f5-9af3-ac56d63d8ebd</wsa:RelatesTo>
   </soap:Header>
   <soap:Body xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:protocol saml-schema-protocol-2.0.xsd">
      <samlp:Response ID="dhdeieiwlls2344ere" InResponseTo="anfd4n3jf893329dnnnf" Version="2.0"
IssueInstant="2003-07-16T01:25:40Z">
         <samlp:Status>
            <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode>
         <samlp:StatusMessage>Tutto OK!</samlp:StatusMessage>
         </samlp:Status>
         <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" ID="
assertion_2.16.840.1.113883.2.9.2.50112_anfd4n3jf893329dnnnf " IssueInstant="2003-07-16T01:25:40Z">
            <!—Qui va il contenuto dell'Asserzione-->
         </Assertion>
      </samlp:Response>
   </soap:Body>
</soap:Envelope>
```

5.1.4.2.2.2 Struttura dell'Asserzione d'identità

L'elemento **<saml:Assertion>** DEVE contenere i seguenti attributi:

- **Version**: deve essere "2.0"
- **ID**: identificativo univoco dell'asserzione creata dall'Identity and Assertions Provider. Questo identificativo DEVE essere necessariamente univoco a livello regionale. Per questo motivo si suggerisce di strutturare l'ID in questo modo:

  ID = "assertion" +"_"+ [OID_azienda]+"_"+[AuthnRequest/@ID]

es. un'asserzione generata dalla ULSS 12 di Mirano a seguito della richiesta con ID "erbtgfvcsaewc":

assertion_2.16.840.1.113883.2.9.2.50112_erbtgfvcsaewc

- **IssueInstant**: istante temporale in cui è stata creata l'asserzione

L'elemento <saml:Assertion> contiene i seguenti elementi:

- **<saml:Issuer>:** elemento obbligatorio che descrive il creatore dell'Asserzione. Dovrebbe essere valorizzato con l'url dell'attore Identity and Assertions Provider che ha creato l'asserzione

- **<ds:Signature>:** Questo elemento è OBBLIGATORIO e permette di firmare l'asserzione con un XML signature autenticando l'attore Identity and Assertions Provider. Questa firma è eseguita in accordo alle specifiche definite dal namespace **ds:** "http://www.w3.org/2000/09/xmldsig#". L'elemento <ds:Signature> DEVE contenere due elementi **<ds:SignedInfo>** e **<ds:SignatureValue>**. <ds:SignatureInfo> permette di definire i parametri dell'algoritmo di firma utilizzato utilizzando i seguenti elementi obbligtori:

  - **<ds:CanonicalizationMethod>**: l'attributo **Algorithm** contiene la definizione dell'algoritmo di canonicalizzazione. Un applicativo conforme a SAML 2.0 dovrebbe utilizzare un algoritmo di canonicalizzazione esclusiva [Excl-C14N] definita dal seguente uri "http://www.w3.org/2001/10/xml-exc-c14n#".

  - **<ds:SignatureMethod>**: l'attributo **Algorithm** contiene la definizione dell'algoritmo di firma utilizzato (XML Signature con utilizzo di algoritmo RSA): "http://www.w3.org/2000/09/xmldsig#rsa-sha1"

  - **<ds:Reference>**: deve essere UNICO e deve contenere l'attributo **URI** che fa riferimento all'attributo Assertion/@**ID** contenuto nell'asserzione preceduto da "#". Questo elemento DEVE contenere i seguenti elementi:

    - **<ds:DigestMethod>**: l'attributo **Algorithm** contiene la definizione dell'algoritmo utilizzato per creare il Digest. Deve essere "http://www.w3.org/2000/09/xmldsig#sha1"

- **<ds:DigestValue>**: questo elemento contiene il valore del Digest in formato base64

Il secondo elemento <ds:SignatureValue> veicola la firma dell'asserzione in formato base64.

- **<saml:Subject>:** questo elemento DEVE essere presente e DEVE riportare le stesse informazioni contenute le <saml:Subject> della richiesta (rappresenta dunque l'utente per cui è creata l'asserzione di identità).

- **<saml:Conditions>:** definisce le condizioni di validità dell'asserzione. Possono essere ereditate dal messaggio di Request o possono essere sovrascritte dall'attore Identity and Assertions Provider, in accordo con le policy di accesso ai servizi definite a livello regionale. L'elemento <saml:Conditions> DEVE avere valorizzati i seguenti attributi:

  - **NotBefore** : istante di inizio della validità dell'asserzione
  - **NotOnOrAfter** : istante di fine validità dell'asserzione

Questo elemento PUO' contenere un elemento **<saml:AudienceRestriction>** (con zero o più sotto elementi **<saml:Audience>** valorizzati con l'url di un servizio) per individuare il o gli attori X-Service Provider che possono accettare l'asserzione di identità.

- **<saml:AttributeStatment>**: sezione che permette di veicolare gli attributi dell'asserzione che sono associati allo user richiedente dall'attore Identity and Assertions Provider. Queste sono le informazioni che verranno analizzate dall'attore X-Service Provider per valutare l'accessibilità o meno ai propri servizi. Questo elemento contiene una serie di elementi **<saml:Attribute>**. Certi elementi <saml:Attribute> sono ereditati dal messaggio di Request (**ApplicationID, PatientID, RepartoBranca, RequestContext, UserClientAuthentication**) altri sono definiti direttamente dall'attore Identity and Assertions Provider:

  1. **Role:** permette di definire il ruolo associato allo user autenticato attraverso l'asserzione di identità. Il codeSystem per questo attributo è definito in Appendice A: CodeSystems

2. **ResponsibleParty:** permette di veicolare all'interno dell'asserzione il Codice Fiscale del Responsabile **(il codice fiscale dell'Issuer del messaggio di richiesta)**

- **<saml:AuthnStatment>:** Elemento creato dall'attore Identity and Assertions Provider per veicolare all'interno dell'asserzione i dettagli del processo di autenticazione che ha portato alla creazione dell'asserzione stessa. Contiene un attributo **authnInstant**, che traccia l'istante a cui è avvenuta l'autenticazione ed un elemento **<saml:AuthnContext>** che descrive le modalità di autenticazione. Questo elemento contiene una serie di sottoelementi:

  - **<saml:AuthnContextClassRef>:** contiene l'URI che descrive le modalità di autenticazione: "urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword"

  - **<saml:AuthenticatingAuthority>:** l'url del servizio che ha eseguito l'autenticazione

Di seguito è presentato un esempio completo di messaggio SOAP AuthenticateAndGetAssertion Response che veicola un'asserzione di identità.

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ soap.xsd">
   <soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.w3.org/2005/08/addressing ws-addr.xsd">
      <wsa:Action>urn:rve:AuthenticateAndGetAssertionResponse</wsa:Action>
      <wsa:MessageID>urn:uuid:4532254e-fe54-56g8-2xf3-cc5cf6ac8eb1</wsa:MessageID>
      <wsa:To>http://X-ServiceUser</wsa:To>
      <wsa:RelatesTo>urn:uuid:9376254e-da05-41f5-9af3-ac56d63d8ebd</wsa:RelatesTo>
   </soap:Header>
   <soap:Body xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:protocol saml-schema-protocol-2.0.xsd">
      <samlp:Response ID="dhdeieiwlls2344ere" InResponseTo="anfd4n3jf893329dnnnf" Version="2.0"
IssueInstant="2003-07-16T01:25:40Z">
         <samlp:Status>
            <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode>
         <samlp:StatusMessage>Tutto OK!</samlp:StatusMessage>
         </samlp:Status>
         <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" ID="sdd343nfnd"
IssueInstant="2003-07-16T01:25:40Z">
            <Issuer
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://IdentityAndAssertionsProvider</Issuer>
            <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"> <!-- firma per autenticare Issuer  -->
               <SignedInfo>
                  <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                  <Reference URI="#sdd343nfnd">
                     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                     <DigestValue></DigestValue> <!-- digest di asserzione in base64 -->
                  </Reference>
               </SignedInfo>
               <SignatureValue>yhtgrewstret</SignatureValue> <!-- firma in base64 -->
               <!--  <KeyInfo/> -->
            </Signature>
            <Subject xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
               <NameID>ZNRMRA86L11B157N</NameID>
            </Subject>
            <Conditions xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
               NotBefore="2003-07-16T01:24:32Z" NotOnOrAfter="2003-07-17T01:24:32Z">
               <AudienceRestriction>
                  <Audience>http://X-ServiceProvider</Audience>
               </AudienceRestriction>
            </Conditions>
            <AttributeStatement>
               <Attribute Name="UserClientAuthentication">  <!-- custom -->
                  <AttributeValue>A.1</AttributeValue>
```

```
                </Attribute>
                 <Attribute Name="ApplicationID ">
                   <AttributeValue>1.2.3.4.5.6^0.4^00023</AttributeValue>
                </Attribute>
                 <Attribute Name="PatientID">
                   <AttributeValue>TRMLRA56L50F382V</AttributeValue>
                </Attribute>
                <Attribute Name="RequestContext"> <!-- custom -->
                   <AttributeValue>C.1.1</AttributeValue>
                </Attribute>
                <Attribute Name="Role" NameFormat="urn:oasis:names:tc:xacml:2.0:subject:role">
                   <AttributeValue>A.1</AttributeValue>
                </Attribute>
                <Attribute Name="ResponsibleParty">
                   <AttributeValue>CF_pippo</AttributeValue>
                </Attribute>
             </AttributeStatement>
             <AuthnStatement AuthnInstant="2003-07-16T01:25:40Z" >
                <AuthnContext>
                   <AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassw
                      ord</AuthnContextClassRef>
<AuthenticatingAuthority>http://IdentityAndAssertionsProvider</AuthenticatingAuthority>
                </AuthnContext>
             </AuthnStatement>
          </Assertion>
       </samlp:Response>
    </soap:Body>
</soap:Envelope>
```

985 **5.1.4.2.3 Expected Actions**

In caso di errore l'X-Service User può tentare di creare una nuova Request in funzione degli errori ricevuti.

Se il messaggio di Response ha veicolato correttamente un'Asserzione di identità,
990 questo token verrà utilizzato dal X-Service User per richiedere l'accesso a ulteriori servizi Regionali o extra aziendali in accordo alla transazione [ITI-40] Provide X-User Assertion descritta in sezione 5.2.

5.1.4.2.4 Security e Audit Considerations

L'evento associato alla richiesta di autenticazione ed asserzione è un evento di rilevanza dal punto di vista della sicurezza del sistema. Per questo motivo l'evento DEVE essere tracciato attraverso messaggi di Audit Record generati dagli attori coinvolti.

5.1.4.2.4.1 Audit Identity and Assertions Provider

Di seguito è presentata la struttura dell'Audit Message che deve essere inviato all'Audit Record Repository aziendale una volta che l'attore Identity and Assertions Provider ha risposto all'attore X-Service User che ha effettuato una richiesta di autenticazione tramite l'utilizzo di una transazione [RVE-1] Authenticate and Get Assertion. La struttura di questo Audit è creata in accordo allo standard DICOM "Security and System Management Profiles". ("M" = elemento mandatorio, "U" elemento opzionale, "Not specialized" = la specifica implementazione può valorizzare questo elemento a proprio piacimento)

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110114, DCM,"User Authentication")
	EventActionCode	M	**E=Execute**
	EventDateTime	M	Ora della creazione del messaggio di Response alla richiesta di autenticazione e di asserzione
	EventOutcomeIndicator	M	*not specialized*
	EventTypeCode	M	EV("RVE-1", "Transactions", "Authenticate and Get Assertion")
Source (X-Service User) (1)			
Human Requestor (1)			
Destination (Identity and Assertions Provider) (1)			
Assertion (1)			
Patient (0..1)			
Source: **AuditMessage/ ActiveParticipant**	UserID	M	Il valore del ApplicationID
	AlternativeUserID	M	not specialized
	UserName	*U*	*not specialized*
	UserIsRequestor	*M*	"true"
	RoleIDCode	M	EV (110153, DCM, "Source")
	NetworkAccessPointTypeCode	U	deve essere "2" identifica il fatto che che è un indirizzo IP
	NetworkAccessPointID	U	Indirizzo IP del X-Service User

Destination: **AuditMessage/ ActiveParticipant**	UserID	M	Identity and Assertion Provider SOAP URI
	AlternativeUserID	U	not specialized
	UserName	U	not specialized

(1)	UserIsRequestor	M	"false"
	RoleIDCode	M	EV (110152, DCM, "Destination")
	NetworkAccessPointTypeCode	U	"1" per il nome (DNS) "2" per l'indirizzo IP
	NetworkAccessPointID	U	Il nome del servizio (DNS) o l'indirizzo IP

Human Requestor (1)	UserID	M	CF del Responsabile (contenuto dell'attributo ResponsibleParty)
	AlternativeUserID	U	userID dell'utente nell'enterprise che lo autenitca (valore dell'attributo Subject/NameID/@ SPProvidedID)
	UserName	U	CF dell'utente
	UserIsRequestor	M	not specialized
	RoleIDCode	M	Il ruolo del responsabile
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	

1010

Assertion (1) **(AuditMessge/ParticipantObjectIdentification)**	ParticipantObjectTypeCode	M	**"4" (Other)**
	ParticipantObjectTypeCodeRole	M	not specialized
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	V(12, RFC-3881, "URI")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	l'identificativo univoco dell'asserzione Assertion/@ID
	ParticipantObjectName	*M*	*"Assertion"*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*M*	*Contesto della richiesta di asserzione*

Patient **(AuditMessge/ParticipantObjectIdentification)**	ParticipantObjectTypeCode	M	**"1" (Person)**
	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	V(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	PatientID
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

5.1.4.2.4.2 Audit X-Service User

Di seguito viene presentato l'Audit Message che deve essere creato dal Richiedente di asserzione in corrispondenza del'invio del messaggio di richiesta della transazione [RVE-1] Authenticate and Get Assertion:

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110114, DCM,"User Authentication")
	EventActionCode	M	**E=Execute**
	EventDateTime	M	Ora della creazione del messaggio di Response alla richiesta di autenticazione e di asserzione
	EventOutcomeIndicator	M	*not specialized*
	EventTypeCode	M	EV("RVE-1", "Transactions", "Authenticate and Get Assertion")
Source (X-Service User) (1)			
Human Requestor (1)			
Destination (Identity and Assertions Provider) (1)			
AuthnRequest (1)			
Patient (0..1)			

Source: AuditMessage/ ActiveParticipant	UserID	M	Il valore del ApplicationID
	AlternativeUserID	M	not specialized
	UserName	*U*	*not specialized*
	UserIsRequestor	*M*	"true"
	RoleIDCode	M	EV (110153, DCM, "Source")
	NetworkAccessPointTypeCode	U	deve essere "2" identifica il fatto che che è un indirizzo IP
	NetworkAccessPointID	U	Indirizzo IP del X-Service User

Destination: AuditMessage/ ActiveParticipant (1)	UserID	M	Identity and Assertion Provider SOAP URI
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV (110152, DCM, "Destination")
	NetworkAccessPointTypeCode	U	"1" per il nome (DNS) "2" per l'indirizzo IP
	NetworkAccessPointID	U	Il nome del servizio (DNS) o l'indirizzo IP

Human	UserID	M	CF del Responsabile (contenuto dell'attributo ResponsibleParty)

	AlternativeUserID	U	userID dell'utente nell'enterprise che lo autenitca (valore dell'attributo Subject/NameID/@ SPProvidedID)
	UserName	U	CF dell'utente
	UserIsRequestor	M	not specialized
	RoleIDCode	M	not specialized
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	

AuthnRequest (1) **(AuditMessge/ParticipantObjectIdentification)**	ParticipantObjectTypeCode	M	**"4" (Other)**
	ParticipantObjectTypeCodeRole	M	not specialized
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	V(12, RFC-3881, "URI")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	l'identificativo univoco della richiesta AuthnRequest/@ID
	ParticipantObjectName	*M*	*"Authentication Request"*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*M*	*Contesto della richiesta di asserzione*

Patient **(AuditMessge/ParticipantObjectIdentification)**	ParticipantObjectTypeCode	M	**"1" (Person)**
	ParticipantObjectTypeCodeRole	M	"1" (Patient)
	ParticipantObjectDataLifeCycle	*U*	*not specialized*
	ParticipantObjectIDTypeCode	M	V(2, RFC-3881, "Patient Number")
	ParticipantObjectSensitivity	*U*	*not specialized*
	ParticipantObjectID	M	PatientID
	ParticipantObjectName	*U*	*not specialized*
	ParticipantObjectQuery	*U*	*not specialized*
	ParticipantObjectDetail	*U*	*not specialized*

5.1.5 Sintesi scambio informativo transazione [RVE-1]

In questa sezione viene presentata una rappresentazione tabellare per descrivere dove deve essere veicolato il contenuto informativo in fase di Request e Response, specificando l'opzionalità (R: Required, O: Optional) dei parametri forniti dal richiedente, quali sono ereditati (dalla richiesta) e/o controllati (sulla base delle informazioni possedute dall'attore IAP, vedi sezione 5.1.4.1.3.1), quali sono aggiunti dall'attore Identity and Assertion Provider:

Tabella 1: Contenuto informativo transazione [RVE-1]

Parametro	Request		Asserzione		Ereditato	Controllato	Aggiunto
	elemento	opt	elemento	opt			
CF_responsabile	Issuer	R	attribute ResponsibleParty	R	SI	SI	NO
CF operatore	Subject/NameID	R	Subject/NameID	R	SI	NO	NO
contesto clinico della richiesta	attribute RequestContext	R	attribute RequestContext	R	SI	NO	NO
Applicazione che effettua la richiesta	attribute ApplicationID	R	attribute ApplicationID	R	SI	SI	NO
Il paziente nei confronti del quale si vuole intervenire	attribute PatientID	O	attribute PatientID	O	SI	NO	NO
Servizio al quale si accederà/potrà accedere usando l'asserzione	AudienceRestriction/ Audience	O	AudienceRestriction/ Audience	O	SI (attore IAP crea un'asserzione solo per la risorsa specificatain richiesta)	SI (attore IAP verifica accessibilità ad una risorsa)	SI (attore IAP concede accesso solo ad una specifica risorsa)
userID operatore	Subject/NameID/@SPProvidedID	O	N/A	-	NO	NO	NO
ruolo del responsabile	N/A	-	attribute Role	R	NO	NO	SI
modalità di autenticazione sul dispositivo Client	attribute AuthorClientAuthentication	R	attribute AuthorClientAuthentication	R	SI	NO	NO
modalità di autenticazione eseguita dall'attore IAP	N/A	-	authnContext	R	NO	NO	SI
credenziali di autenticazione del responsabile	usernameToken	R	N/A	-	NO	SI	NO

1035

5.2 Richiesta Servizi: [ITI-40] Provide X-User Assertion

Questa transazione descrive come un attore X-Service User deve utilizzare un'asserzione di identità ottenuta dall'attore Identity and Assertions Provider per ottenere l'erogazione di servizi applicativi da parte di un attore X-Service Provider (fornitore di servizi Regionale o extra-aziendale). Gli attori coinvolti rispettano le specifiche tecniche definite da IHE nel profilo XUA (IHE-ITI-TF-1 sezione 13), e la transazione di riferimento è la [ITI-40] Provide X-User Assertion, descritta (IHE-ITI-TF-2b sezione 3.40).

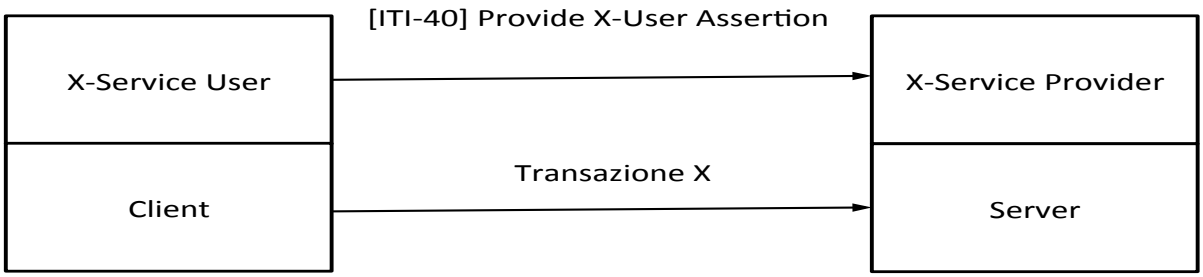


Figura 10 Raggruppamento tra attori per l'utilizzo di SAML token

Questa transazione permette di descrivere come un Client di servizi DEVE utilizzare un'asserzione di identità di cui dispone per invocare altri servizi applicativi (es. Un medico prescrittore MMG utilizzerà una Asserzione ricevuta dalla propria azienda di riferimento per invocare i servizi di Prescrizione sviluppati a livello regionale).

I messaggi applicativi verranno veicolati utilizzando l'imbustamento SOAP. L'asserzione di identità deve essere veicolata all'interno dell'header di un messaggio di richiesta di servizi applicativi utilizzando l'elemento **<wss:Security>**.

Di seguito è presentato un esempio di header che veicola un'asserzione SAML 2.0:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"  xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
    <wsa:To env:mustUnderstand="1">https://ser-healthcare1:8443/dx4-ihe-
xds/ws/iti18Service</wsa:To>
    <wsa:Action env:mustUnderstand="1">urn:ihe:iti:2007:RegistryStoredQuery</wsa:Action> <!-- il
messaggio SOAP è una query ITI-18 -->
    <wsa:MessageID>uuid:6662eab5-2ac2-4ad4-8c87-e8c468a623af</wsa:MessageID>
    <wsa:ReplyTo>
<addressing:Address>http://www.w3.org/2005/08/addressing/anonymous</addressing:Address>
    </wsa:ReplyTo>
    <wsse:Security>
      <saml:Assertion ID="_437640c5-3f0b-417c-93ff-11e573adc343" IssueInstant="2013-04-
16T14:39:41.107Z" Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
   <!-- qui va l'asserzione ottenuta da un Identity and Assertions Provider -->
      </saml:Assertion>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <!-- Qui il body di richiesta del servizio di Query (sintassi standard) -->
  </soap:Body>
</soap:Envelope>
```

5.2.1 *Gestione delle condizioni di Errore (Fault)*

Se la validazione del token SAML fallisce, l'attore raggruppato con l'entità X-Service Provider DEVE ritornare un codice di errore come descritto nelle specifiche tecniche WS-Sercurity section 12 "Error Handling" usando il meccanismo SOAP Fault.

Le classi di fault che possono essere generati da un attore X-Service Provider sono descritti di seguito:

- **wsse:FailedCheck**: La firma utilizzata per verificare la validità dell'asserzione non è corretta
- **wsse:SecurityTokenUnavailable**: La richiesta di servizio non veicola all'interno della porzione WS-Security un'asserzione di identità SAML 2.0
- **wsse:MessageExpired**: Intervallo di validità dell'asserzione non corretto
- **wsse:InvalidSecurityToken:** se parte del contenuto dell'asserzione non è conforme ai requisiti necessari per accedere al Servizio richiesto.

- **wsse:FailedAuthentication**: Non è possibile autenticare l'utente o l'asserzione di identità.

La struttura del messaggio di Risposta veicolante una condizione di errore deve essere conforme allo standard SOAP (permette di individuare la classe di errore) e dallo standard WS-BaseFault 1.1 (che permette di dettagliare la condizione di errore).

L'Header del messaggio di risposta veicolerà le informazioni che permettono di associare la Response contenente il Fault al messaggio di Request che non è stato possibile processare.

La classe del Fault generato è descritta all'interno del body del messaggio SOAP attraverso l'utilizzo dei seguenti elementi:

- **<faultcode>**: veicola uno dei codici di fault descritti precedentemente che descrivono la classe di errore.
- **<faultstring>**: stringa che descrive la condizione di errore (si propone di utilizzare per questo campo la definizione descritta precedentemente in corrispondenza dello specifico codice di errore)
- **<faultactor>**: definisce l'url del X-Service Provider che ha rigettato l'asserzione di identità;
- uno specifico elemento, del tipo BaseFault, caratterizzante la specifica tipologia di errore (es. <wsse:FailedCheck>). Questo elemento contiene una serie di sotto-elementi definiti dallo standard WS-BaseFault:
  - **< wsrf-bf:Timestamp>**: istante temporale in cui si è generato l'errore
  - **<wsrf-bf:ErrorCode>**: elemento che contiene lo specifico codice di errore definito in accordo con il vocabolario degli errori definito per il progetto FSEr di Regione del Veneto (**@dialect**="RVE:FSE"). < wsrf-bf:Description>: una descrizione dettagliata per l'errore

  Si faccia riferimento alla sezione A.4 Error Codes, dialect RVE:FSE in Appendice A di questo documento per la definizione dei codici di errore che possono essere generati e le relative description

Di seguito è presentato un esempio di messaggio SOAP veicolante una condizione di Fault.

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ soap.xsd">
   <soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"  >
      <wsa:To>https://X-ServiceUser</wsa:To>
      <wsa:Action>urn:ihe:iti:2007:RegistryStoredQuery</wsa:Action> <!-- il messaggio SOAP di richiesta ERA una query ITI-18 -->
      <wsa:MessageID>uuid:6662eab5-2ac2-4ad4-8c87-e8c468a623af</wsa:MessageID>
      <wsa:RelateTo>uuid:1232ffb5-2qq1-8id4-78ui-efkr679566at</wsa:RelateTo>
   </soap:Header>
   <soap:Body>
      <soap:Fault xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd oasis-200401-wss-wssecurity-secext-1.0.xsd">
         <faultcode>wsse:InvalidSecurityToken</faultcode>
         <faultstring>Parte del contenuto dell'asserzione non è conforme ai requisiti necessari per accedere al Servizio richiesto </faultstring>
         <faultactor>http://X-ServiceProvider</faultactor>
         <detail>
            <wsse:InvalidSecurityToken xmlns:wsrf-bf="http://docs.oasis-open.org/wsrf/bf-2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://docs.oasis-open.org/wsrf/bf-2 bf-2.xsd">
               <wsrf-bf:Timestamp>2005-05-04T20:18:44.970Z</wsrf-bf:Timestamp>
               <wsrf-bf:ErrorCode dialect="RVE:FSE">ERR_00041</wsrf-bf:ErrorCode>
               <wsrf-bf:Description> Il valore dell'attributo RequestContext non permette l'accesso al servizio </wsrf-bf:Description>
            </wsse:InvalidSecurityToken>
         </detail>
      </soap:Fault>
   </soap:Body>
</soap:Envelope>
```

1105

5.3 RVE-2 Update Password

Lo use-case di riferimento per questa transazione è rappresentato dalla necessità di un applicativo territoriale (e quindi non direttamente integrato con LDAP aziendale) di

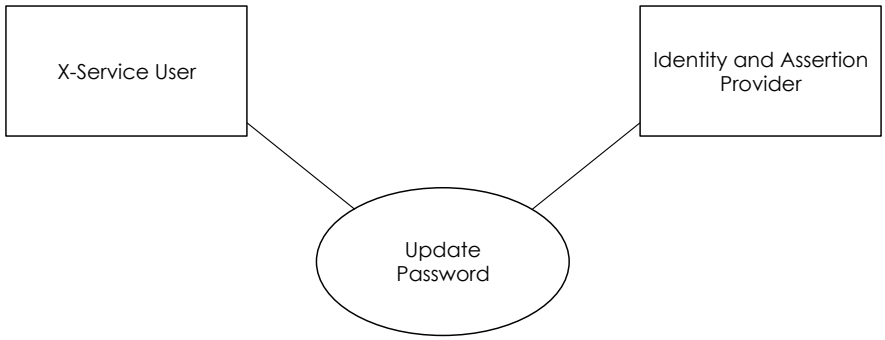
aggiornare le credenziali di accesso conservate dall'azienda.

5.3.1 *Scopo*

La transazione [RVE-2] Update Password permette ad un attore territoriale X-Service User di aggiornare, in modo applicativo, la password (gestita dall'azienda di riferimento) utilizzata per richiedere asserzioni di identità. Questa operazione viene effettuata a seguito di un autenticazione dell'utente.

5.3.2 *Attori e Ruoli*

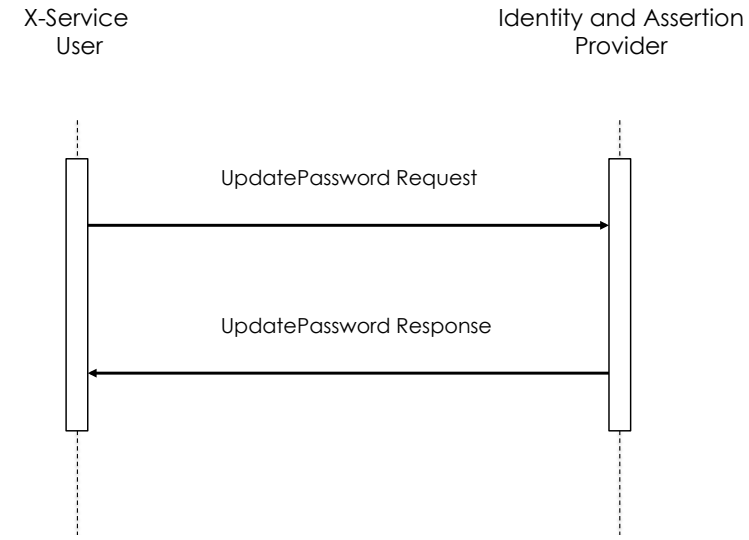
Actor:	X-Service User
Role:	Richiede l'aggiornamento della password gestita dall'identity provider di riferimento.
Actor:	Identity and Assertion Provider
Role:	Riceve una richiesta di aggiornamento di password e restituisce conferma o meno dell'avvenuta operazione.



5.3.3 *Standard di Riferimento*

- W3C WS-Addressing 1.0 – SOAP Binding
- OASIS WS-Security
- OASIS WS-UsernameToken Profile

5.3.4 *Interaction Diagram*



5.3.4.1 PasswordUpdate Request message

5.3.4.1.1 Trigger Events

Questo messaggio viene generato a seguito della necessità di rinnovare delle credenziali scadute o in scadenza. Quindi può essere generato a seguito della ricezione di un messaggio di errore di classe FailedAuthentication del tipo ERR_00056 "Password Scaduta", o a seguito di un meccanismo di monitoraggio della validità delle credenziali stesse (questo periodo di validità è gestito dall'azienda di riferimento ed è restituito come informazione nella Response di ogni transazione di aggiornamento password).

5.3.4.1.2 Message Semantic

Il messaggio creato dovrà essere un messaggio SOAP e quindi rispettare lo schema definito da http://schemas.xmlsoap.org/soap/envelope/.

Si farà riferimento per questo elemento allo standard OASIS WS-Security ed in particolare ad un estensione del UsernamePassword Token Profile.

Il Body del messaggio SOAP veicola la richiesta di aggiornamento della password.

La struttura dell'Header DEVE essere conforme alle specifiche WS-Addressing 1.0 SOAP Binding permettendo il corretto instradamento e processamento del messaggio di richiesta.

- **<wsa:To>** = indirizzo URI del destinatario ultimo del messaggio
- **<wsa:Action>** = URI che identifica la semantica attesa nel body ("urn:rve:UpdatePasswordRequest" identifica che il messaggio veicola una richiesta di aggiornamento password)
- **<wsa:MessageID>** = identificativo univoco del messaggio

L'operazione di aggiornamento password è simile al processo di autenticazione, per questo motivo l'Header del messaggio SOAP è strutturato mediante l'utilizzo dello standard WS-Security: SOAP Message Security Version 1.1.1 (namespace di riferimento **wsse**). Accoppiando questo standard con una specifica estensione del profilo WS Security UsernameToken Profile 1.0 (namespace di riferimento associato al WS-Utility profile: **utp**) è possibile utilizzare il token Username e Password per aggiornare le credenziali dell'utente che gestisce l'attore X-Service User attraverso l'Identity and Assertions Provider. Il processo di autenticazione precedente all'agigornamento password deve infatti essere eseguito garantendo i massimi livelli di sicurezza.

L'elemento UserNameToken, contenuto all'interno di un elemento Security DEVE contenere:

- **<wsse:Username>** = l'identificativo del responsabile conosciuto dall'Identity and Assertions Provider;
- **<wsse:Password>** = non DEVE contenere la password in clearText.. Questo elemento deve essere valorizzato con il digest della password (password/@type=Password_Digest) definito come di seguito concatenando password, nonce ed un time stamp.
- **<wsse:Nonce>** = valore random creato dall'inviante per ogni UserNameToken. Il Server deve mantenere l'elenco dei nonce utilizzati (accopiando il nonce con il creation time wsu:Created si può limitare il dispendio di risorse del server limitando la cache ai nonce più recenti).
- **<utp:Created> =** il time stamp di creazione dello usernameToken e coincide con l'istante di creazione del messaggio di richiesta. E' strutturato secondo il formato UTC.

- **<rve-h:NewPassword>** = questo elemento (definito per estendere lo standard UsernameToken profile) deve contenere la nuova password criptata con un certificato IDPX.cer (dove X rappresenta l'ULSS di riferimento).

Il body del messaggio contiene l'elemento vuoto **<rve:UpdatePasswordRequest>.**

Di seguito è presentato un esempio SOAP per il messaggio UpdatePassword Request:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ soap.xsd">
   <soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.w3.org/2005/08/addressing ws-addr.xsd">
      <wsa:Action>urn:rve:UpdatePasswordRequest</wsa:Action>
      <wsa:MessageID>urn:uuid:9376254e-da05-41f5-9af3-ac56d63d8ebd</wsa:MessageID>
      <wsa:To>http://identityAndAssertionsProvider</wsa:To>
      <wsse:Security
         xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd oasis-200401-wss-wssecurity-secext-1.0.xsd">
         <wsse:UsernameToken
            xmlns:utp="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd">
            <wsse:Username>PIPPO</wsse:Username>
            <wsse:Password
Type="wsse:PasswordDigest">weYI3nXd8LjMNVksCKFV8t3rgHh3Rw==</wsse:Password>
            <wsse:Nonce>WScqanjCEAC4mQoBE07sAQ==</wsse:Nonce>
            <utp:Created>2003-07-16T01:24:32Z</utp:Created>
            <rve-h:NewPassword>sfw4DTYgejowwo2odt0fem</ rve-h:NewPassword> <!-- nuova password
criptata-->
         </wsse:UsernameToken>
      </wsse:Security>
   </soap:Header>
   <soap:Body>
      <rve:UpdatePasswordRequest/>
   </soap:Body>
</soap:Envelope>
```

5.3.4.1.3 Expected Actions

Se il messaggio è processato correttamente e la Password specificata è corretta viene creato un messaggio di PasswordUpdate Response che attesta il corretto aggiornamento della password. In caso contrario il messaggio di Response veicola un fault SOAP (come descritto in sezione 5.2.1).

5.3.4.2 PasswordUpdate Response message

5.3.4.2.1 Trigger Events

Questo messaggio viene generato a seguito della ricezione di un messaggio PasswordUpdate Request.

5.3.4.2.2 Message Semantic

Questo messaggio è strutturato secondo lo standard SOAP envelope. Il messaggio di Response DEVE contenere nell'header l'elemento action al quale è associato l'urn: **urn:rve:UpdatePasswordResponse**. Se la richiesta di aggiornamento puo' essere processata, Il messaggio restituisce all'attore X-Service User il periodo di validità delle nuove credenziali aggiornate. L'header del messaggio SOAP non veicola specifiche informazioni. Il body del messaggio SOAP deve essere strutturato in accordo allo schema rve-b: "rve-body.xsd":

- **<rve-b:UpdatePasswordResponse>:** elemento strutturato che notifica l'avvenuto aggiornamento della password e il periodo di validità delle nuove credenziali;
    - **<rve-b:expirationDate>:** elemento che veicola la data di scadenza delle credenziali in formato UTC. Questa durata viene definita dalle policy aziendali.

In caso di errore il Body del messaggio SOAP veicola un fault appartenente alle seguenti classi:

- **wsse:FailedAuthentication:** se la password utilizzata non è valida o se la newPassword non rispetta i requisiti aziendali.

- **wsse:FailedCheck:** se la password utilizzata non è criptata con il certificato corretto

Di seguito è presentato un esempio di messaggio SOAP PasswordUpdate Response:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ soap.xsd">
  <soap:Header xmlns:wsa="http://www.w3.org/2005/08/addressing"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.w3.org/2005/08/addressing ws-addr.xsd">
    <wsa:Action>urn:rve:UpdatePasswordResponse</wsa:Action>
    <wsa:MessageID>urn:uuid:6541239o-er56-78y8-6ty4-hy56d63d8ebd</wsa:MessageID>
    <wsa:To>http://X-ServiceUser</wsa:To>
    <wsa:RelatesTo>urn:uuid:9376254e-da05-41f5-9af3-ac56d63d8ebd</wsa:RelatesTo>
  </soap:Header>
  <soap:Body>
    <rve-b:UpdatePasswordResponse>
      <rve-b:expirationDate>2013-11-05T13:15:30Z</rve-b:expirationDate>
    </rve-b:UpdatePasswordResponse>
  </soap:Body>
</soap:Envelope>
```

5.3.4.2.3 Expected Actions

Una volta ricevuto il messaggio di Response contenente l'elemento <rve-b:UpdatePasswordResponse> l'attore X-ServiceUser deve memorizzare le nuove credenziali in modo da poterle usare nel messaggio di Request della transazione Authenticate and Get Assertion [RVE-1] (vedi sezione 5.1).

Se il messaggio di Response veicola un SOAP Fault, la transazione non è andata a buon fine e deve essere ripetuta per poter accedere ai servizi del FSEr.

5.3.4.3 Security and Audit Considerations

La transazione Update Password è caratterizzata da un elevato livello di rischio. Per questo motivo si richiede di definire a livello aziendale un certificato (file ULSSX.cer) da utilizzare per criptare mediante algoritmo RSA il contenuto del campo NewPassword.

Si ritiene non necessario criptare la vecchia password, in quanto non può ulteriormente essere utilizzata per accedere ai servizi FSEr.

Si ritiene necessario tracciare il cambiamento di password con una copia di Audit messages generati dagli attori Identity and Assertion Provider e X-Service User

5.3.4.3.1 Audit Identity and Assertion Provider

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110114, DCM,"User Authentication")
	EventActionCode	M	**E=Execute**
	EventDateTime	M	Ora della creazione del messaggio di Response alla richiesta di aggiornamento della password
	EventOutcomeIndicator	M	*not specialized*
	EventTypeCode	M	EV("RVE-2", "Transactions", "Update Password")
Source (X-Service User) (1)			
Human Requestor (0..1)			
Destination (Identity and Assertions Provider) (1)			
Source: AuditMessage/ ActiveParticipant	UserID	M	Il valore del ApplicationID
	AlternativeUserID	M	not specialized
	UserName	*U*	*not specialized*
	UserIsRequestor	*M*	"true"
	RoleIDCode	M	EV (110153, DCM, "Source")
	NetworkAccessPointTypeCode	U	deve essere "2" identifica il fatto che che è un indirizzo IP
	NetworkAccessPointID	U	Indirizzo IP del X-Service User
Destination: AuditMessage/ ActiveParticipant (1)	UserID	M	Identity and Assertion Provider SOAP URI
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV (110152, DCM, "Destination")
	NetworkAccessPointTypeCode	U	"1" per il nome (DNS) "2" per l'indirizzo IP
	NetworkAccessPointID	U	Il nome del servizio (DNS) o l'indirizzo IP
Human Requestor (0..1)	UserID	M	CF del Responsabile
	AlternativeUserID	U	Not specialized
	UserName	U	Not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	Not specialized
	NetworkAccessPointTypeCode	NA	-
	NetworkAccessPointID	NA	-

5.3.4.3.2 Audit X-Service User

Real World Entities	Field Name	Opt.	Value Constraints
Event	EventID	M	EV (110114, DCM,"User Authentication")
	EventActionCode	M	**E=Execute**
	EventDateTime	M	Ora della creazione del messaggio di Response alla richiesta di aggiornamento della password
	EventOutcomeIndicator	M	*not specialized*
	EventTypeCode	M	EV("RVE-2", "Transactions", "Update Password")
Source (X-Service User) (1)			
Human Requestor (0..1)			
Destination (Identity and Assertions Provider) (1)			
Source: AuditMessage/ ActiveParticipant	UserID	M	Il valore del ApplicationID
	AlternativeUserID	M	not specialized
	UserName	*U*	*not specialized*
	UserIsRequestor	*M*	"true"
	RoleIDCode	M	EV (110153, DCM, "Source")
	NetworkAccessPointTypeCode	U	deve essere "2" identifica il fatto che che è un indirizzo IP
	NetworkAccessPointID	U	Indirizzo IP del X-Service User
Destination: AuditMessage/ ActiveParticipant (1)	UserID	M	Identity and Assertion Provider SOAP URI
	AlternativeUserID	U	not specialized
	UserName	U	not specialized
	UserIsRequestor	M	"false"
	RoleIDCode	M	EV (110152, DCM, "Destination")
	NetworkAccessPointTypeCode	U	"1" per il nome (DNS) "2" per l'indirizzo IP
	NetworkAccessPointID	U	Il nome del servizio (DNS) o l'indirizzo IP

Human Requestor (1)	UserID	M	CF del Responsabile
	AlternativeUserID	U	Not specialized
	UserName	U	Not specialized
	UserIsRequestor	M	not specialized
	RoleIDCode	M	Not specialized
	NetworkAccessPointTypeCode	NA	
	NetworkAccessPointID	NA	

Infrastruttura di sicurezza (FSEr): Attori Aziendali

work in progress

Appendice A: CodeSystems

A.1 CodeSystem Ruoli (attributo "Role")

Di deguito è presentata una tabella che rappresenta i Ruoli possibili per gli operatori in grado di accedere ai servizi del Fascicolo Sanitario Elettronico regionale.

Tabella 2: CodeSystem Ruoli

Gruppo	Sottogruppo	Ruolo	Codice
SANITARI	Personale ad alta specializzazione	medico	R.1.1
		biologo	R.1.2
		farmacista	R.1.3
		chimico	R.1.4
		veterinario	R.1.5
		psicologo	R.1.6
		fisico	R.1.7
		odontoiatra	R.1.8
		direzione professioni sanitarie	R.1.9
	Personale infermieristico	infermiere	R.1.10
		infermiere pediatrico	R.1.11
		ostetrico	R.1.12
	Personale di riabilitazione	fisioterapista	R.1.13
		logopedista	R.1.14
		ortottrista	R.1.15
		podologo	R.1.16
		educatore professionale	R.1.17
		terapista della neuro e psicomotricità dell'età evolutiva	R.1.18
		tecnico dell'educazione e riabilitazione psichitrica e psico-sociale	R.1.19
		terapista occupazionale	R.1.20
	Personale tecnico-sanitario (area tecnico-assistenziale)	dietista	R.1.21
		igienista dentale	R.1.22
		tecnico audio-protesista	R.1.23
		tecnico di fisiopatologia cardiocircolatoria e perfusione cardiovascolare	R.1.24

		tecnico ortopedico	R.1.25
	Personale tecnico-sanitario (area tecnico-diagnostica)	tecnico audiometrista	R.1.26
		tecnico di neurofisiopatologia	R.1.27
		tecnico sanitario di laboratorio biomedico	R.1.28
		tecnico sanitario di radiologia medica	R.1.29
	Area prevenzione	tecnico della prevenzione negli ambienti e nei luoghi di lavoro	R.1.30
		assistente sanitario	R.1.31
PROFESSIONALI		Professionale	R.2.1
		Direzione Ruolo Professionale	R.2.2
TECNICI		Tecnico	R.3.1
		Direzione Ruolo Tecnico	R.3.2
AMMINISTRATIVI		Amministrativo	R.4.1
		Direzione Ruolo Amministrativo	R.4.2

A.2 CodeSystem Contesti Clinici (attributo "RequestContext")

Di seguito è presentata la tabella di codifica per i vari contesti clinici all'interno dei quali può essere richiesto l'accesso ai servizi del Fascicolo Sanitario Elettronico regionale da parte di un operatore.

Tabella 3: CodeSystem Contesti

Macro-attività	Contesto	Codice
Continuità di cura	Assistenza Primaria (MMG, PLS)	C.1.1
	Medicina di Gruppo (UTAP sostituzione)	C.1.2
	Continuità Assistenziale (guardia medica/turistica)	C.1.3
Attività specialistico/diagnostica	per interni	C.2.1
	per esterni	C.2.2
	per esterni in day-service	C.2.3
Ricovero	Ricovero	C.3.1
Pronto Soccorso – Emergenza Sanitaria 118	Pronto Soccorso – Emergenza Sanitaria 118	C.4
Attività Erogativa Farmaceutica	Ospedaliera	C.5.1
	Terirtoriale	C.4.2
Attività amministrative	Prentazioni CUP	C.6.1
	Ritiro Referti	C.6.2
	Attività Amministrative Generiche	C.6.3
	Marketing	C.6.4
Servizi	Medicina legale -fiscale	C.7.1
	Invalidi civili	C.7.2

	Assistenza Protesica	C.7.3
	Assistenza domiciliare integrata	C.7.4
	Vaccinazioni – medicina scolastica	C.7.5
	Sert/Tossicodipendenze	C.7.6
	Consultori – Adozioni	C.7.7
	Neuropsichiatria infantile	C.7.8
	Donazione organi – Dichiarazioni di volontà	C.7.9
	Igiene e sanità pubblica (SISP)	C.7.10
	Igiene alimenti e nutrizione	C.7.11
	Prevenzione igiene e sicurezza sul luogo del lavoro	C.7.12
	Salute mentale	C.7.13
	Screening	C.7.14
	Assciazioni di volontariato	C.7.15
	Autorità giudiziaria	C.7.16
RSA	RSA	C.8
Reti di Patologia	Reti di Patologia	C.9
Attività di Ricerca	Attività di Ricerca	C.10
Amministratore di Sistema	Amministratore di Sistema	C.11

A.3 CodeSystem UserClientAuthentication

Di seguito è definita la tabella di codifica per le modalità di autenticazione degli utenti all'interno degli applicativi Client che si vogliono autenticarsi con un Identity and Assertion Provider aziendale.

Tabella 4: Modalità di autenticazione

Tipologia Autenticazione	Codice
User e Password	A.1
Strong Authentication con Card	A.2
Strong Authentication con Token	A.3

A.4 Error Codes, dialect RVE:FSE

In questa sezione sono definiti gli specifici errori generati dall'attore X-Service Provider che rifiuta l'erogazione di un servizio applicativo. Questi errori sono classificati in funzione della classe di Fault alla quale appartengono. Le classi di Fault sono definite e descritte in sezione 5.2.1.

A.4.1 wsse:FailedCheck

La firma utilizzata per verificare la validità dell'asserzione non è corretta

ErrorCode	Description
ERR_00011	mismatch tra firma e chiave pubblica
ERR_00012	firma digitale strutturata in modo non corretto
ERR_00013	NewPassword criptata utilizzando un certificato non corretto

A.4.2 wsse:SecurityTokenUnavailable

La richiesta di servizio non veicola all'interno della porzione WS-Security un'asserzione di identità SAML 2.0

ErrorCode	Description
ERR_00021	Assenza del Security token
ERR_00022	Assenza del token di Asserzione
ERR_00023	il token SAML utilizzato non è well-formed e non può essere riconosciuto
…	

A.4.3 wsse:MessageExpired

Intervallo di validità dell'asserzione non corretto

ErrorCode	Description
ERR_00031	Il valore dell'attributo NotBefore è posteriore all'istante di utilizzo dell'asserzione
ERR_00032	Il valore dell'attributo NotOnOrAfter è precedente all'istante di utilizzo dell'asserzione
ERR_00033	L'intervallo temporale dell'asserzione non è conforme alle policy regionali
…	

A.4.4 wsse:InvalidSecurityToken

1285 Il contenuto dell'asserzione non è conforme ai requisiti necessari per accedere al Servizio richiesto

ErrorCode	Description
ERR_00041	Il valore dell'attributo RequestContext non permette l'accesso al servizio
ERR_00042	Il valore dell'attributo Role non permette l'accesso al servizio
ERR_00043	Il valore dell'attributo ClientUserAuthentication non permette l'accesso al servizio
ERR_00044	Il valore dell'elemento AudienceRestriction non permette l'accesso al servizio
ERR_00045	Il valore dell'elemento ApplicationID non permette l'accesso al servizio
…	

A.4.5 wsse:FailedAuthentication

Non è possibile autenticare l'utente o l'asserzione di identità.

ErrorCode	Description

ERR_00051	Il firmatario dell'asserzione non è un attore trustabile
ERR_00052	Il responsabile o l'utente non possono accedere al servizio
ERR_00053	L'asserzione di identità non è firmata
ERR_00054	Credenziali Errate
ERR_00055	Data e Ora disallineate
ERR_00056	Password Scaduta
ERR_00057	Password che non rispetta le policy aziendali

1290

Appendice B: WSDL dei servizi definiti

to be defined

BIBLIOGRAFIA

DA COMPLETARE, I RIFERIMENTI SI TROVANO ANCHE ALL'INTERNO DEL DOCUMENTO