Ministro per l'Innovazione e le Tecnologie

Piano Nazionale di e-Government

REGIONE DEL VENETO

e-goVernment Veneto

Direzione Sistema Informatico

SIRV-INTEROP

Sicurezza basata sui ruoli

Specifiche tecniche

(UML-A8.2-0)

Versione 1.0.0

06 ottobre 2004

Insiel

GRUPPO TELECOM ITALIA-FINSIEL

Approvazioni

Il presente documento è stato approvato da:

Storia delle Modifiche

Versione	Data	Descrizione

Riferimenti

Numero	Titolo	Prodotto da	Versione	Data

Sommario

1. Introduzione

In questo documento verranno analizzate le specifiche tecniche del sistema. Verranno innanzitutto esaminati i vari protocolli utilizzati nel sistema e l'uso che ne è stato fatto. Successivamente verrà data una descrizione generale della struttura del sistema. Poi verranno descritti i vari servizi messi a disposizione dal servizio di gestione e dal server SAML. In particolare per il server SAML verranno analizzati i trattamenti messi a disposizione delle porte.

Infine verranno descritti la struttura del repository xindice e l'architettura tecnologica del sistema.

2. Protocolli

Verrà fornita ora una descrizione generale dei protocolli utilizzati all'interno del sistema.

2.1 SOAP

Il SOAP (Simple Object Access Protocol) è un protocollo xml per la trasmissione di informazioni attraverso messaggi http. Nel nostro caso viene utilizzato dalle porte per comunicare tra di loro.

2.2 SAML (Security Assertion Markup Language)

Il SAML è un protocollo xml utilizzato per lo scambio di asserzioni di sicurezza. Esistono tre tipi di asserzione (di autenticazione, di attributo e di autorizzazione) ed ogni asserzione viene prodotta da un server specifico che risponde a delle richieste specifiche.

2.3 WSS

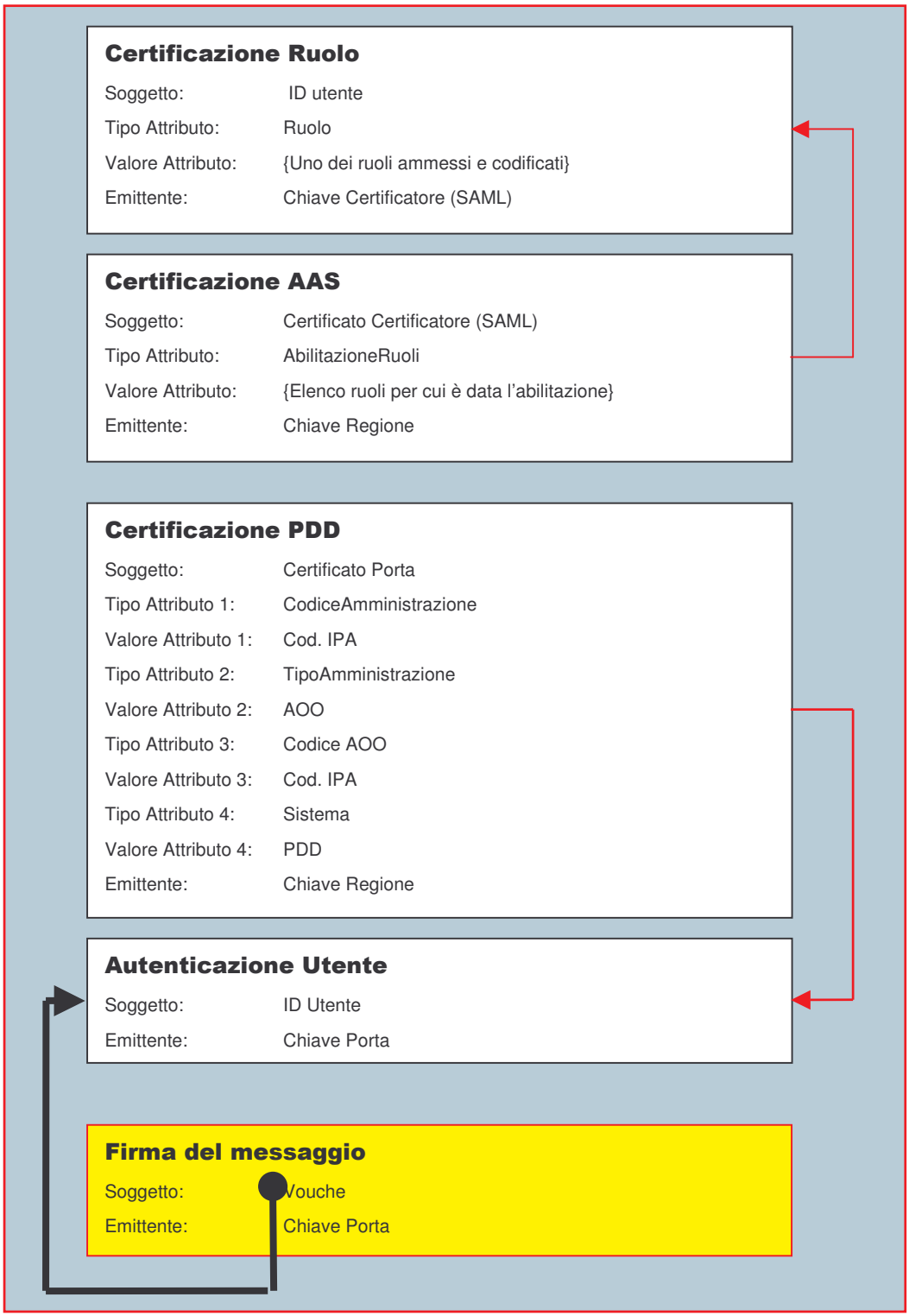
Il WSS (Web Services Security) è un protocollo che si occupa della trasmissione di asserzioni SAML per mezzo di un messaggio SOAP. Esso definisce la modalità con la quale queste asserzioni devono viaggiare attraverso il canale SOAP. Nel nostro caso il protocollo WSS viene utilizzato per trasferire le asserzioni necessarie dalla porta delegata alla porta applicativa.

Questo messaggio WSS può essere composto da un numero variabile di asserzioni; nel nostro caso le asserzioni sono due :

a) **Autenticazione Utente**, asserzione che indica chi è l'utente che ha richiesto il ruolo. Questa asserzione viene firmata con la chiave della porta. Inoltre questa asserzione contiene al suo interno un ulteriore asserzione (**Certificazione PDD**) che attesta che la

porta in questione è riconosciuta dalla Regione. In pratica questa seconda asserzione ha come soggetto il certificato della porta, e viene firmata con la chiave privata della regione. In fase di verifica si controllerà innanzitutto che l'Autenticazione Utente sia firmata in maniera corretta, e successivamente verrà verificato che il certificato di firma sia quello contenuto nel soggetto della **CertificazionePDD**.

b) **Certificazione Ruolo**, asserzione che indica la lista degli attributi, in questo caso ruoli, con cui l'utente indicato nel soggetto dell'asserzione intende presentarsi sul server di autorizzazione. Questa asserzione viene rilasciata dal SAML Attribute Server (AAS), il quale la firma col suo certificato ed inserisce all'interno della Certificazione Ruolo un'ulteriore asserzione CertificazioneAAS, la quale contiene come soggetto il certificato dell'AAS. La CertificazioneAAS, analogamente all'asserzione CertificazionePDD, viene firmata con la chiave privata della regione.


Certificazione Ruolo
Soggetto: ID utente
Tipo Attributo: Ruolo
Valore Attributo: {Uno dei ruoli ammessi e codificati}
Emittente: Chiave Certificatore (SAML)
Certificazione AAS
Soggetto: Certificato Certificatore (SAML)
Tipo Attributo: AbilitazioneRuoli
Valore Attributo: {Elenco ruoli per cui è data l'abilitazione}
Emittente: Chiave Regione
Certificazione PDD
Soggetto: Certificato Porta
Tipo Attributo 1: CodiceAmministrazione
Valore Attributo 1: Cod. IPA
Tipo Attributo 2: TipoAmministrazione
Valore Attributo 2: AOO
Tipo Attributo 3: Codice AOO
Valore Attributo 3: Cod. IPA
Tipo Attributo 4: Sistema
Valore Attributo 4: PDD
Emittente: Chiave Regione
Autenticazione Utente
Soggetto: ID Utente
Emittente: Chiave Porta
Firma del messaggio
Soggetto: Vouche
Emittente: Chiave Porta

Descrizione generale del sistema.

Viene ora analizzata la struttura generale del sistema di gestione degli accessi ad un servizio.

Si deve innanzitutto distinguere fra il sistema vero e proprio, composto dalle porte di dominio e da uno o più server SAML, e il complesso di servizi dediti alla manutenzione dello stesso. Tutte le informazioni relative alla gestione degli accessi vengono memorizzate su un repository di tipo xml, ed è appunto su questo tipo di struttura che dovrà poggiare il server SAML ed i servizi di manutenzione.

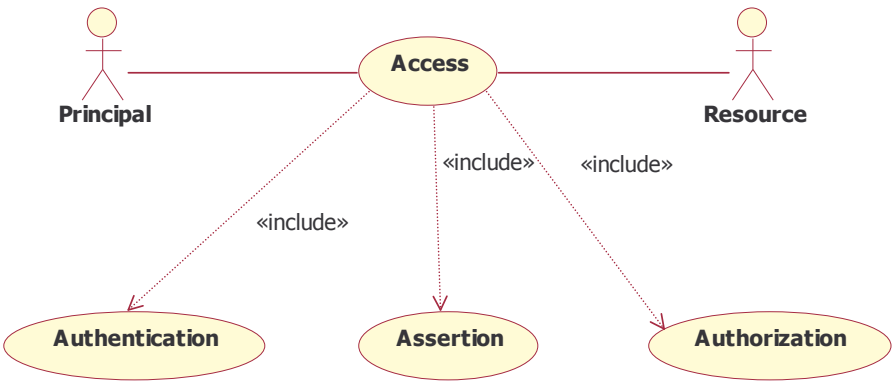
2.4 Server SAML

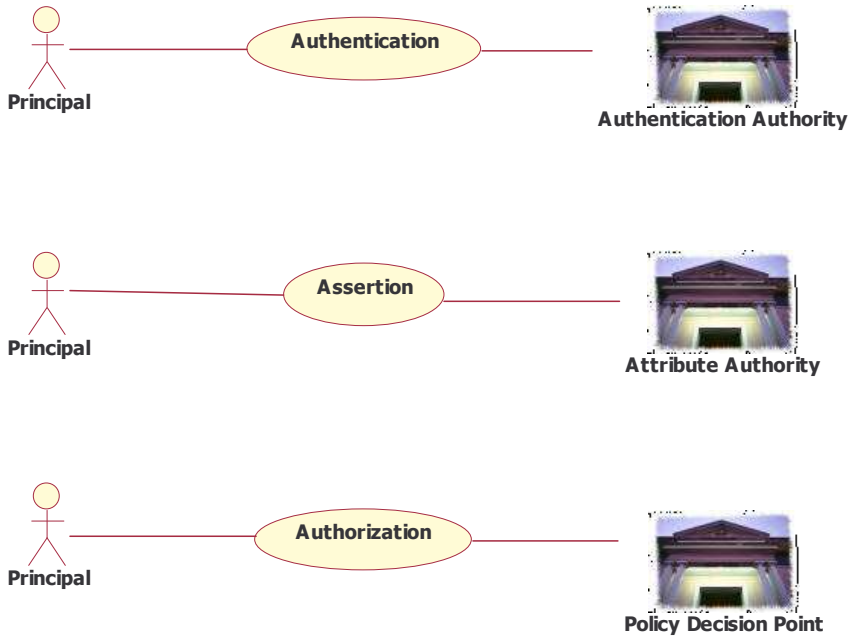
Il Server SAML è un server dedito al rilascio di asserzioni. Nel protocollo SAML sono definite tre tipi standard di asserzioni, la *Authentication Assertion* nella quale il server certifica che l'utente indicato nell'asserzione si è loggato precedentemente in qualche maniera (indicata nell'asserzione) sul sistema, la *Attribute Assertion* nella quale il server asserisce che il soggetto dell'asserzione è in possesso di determinati attributi, ed infine la *Authorization Assertion*, nella quale si autorizza o meno il soggetto dell'asserzione ad accedere ad una risorsa specificata nella richiesta. Il modello di funzionamento del server è molto semplice, in quanto ad una determinata tipo di richiesta esso risponde con la relativa asserzione.

Il protocollo di comunicazione è il SOAP; nel nostro caso quindi le porte dovranno costruire la richiesta apposita, creare la richiesta SOAP contenente la query ed inviarla al server. Questo dopo aver analizzato la richiesta provvederà a generare la risposta andando a verificare i dati contenuti all'interno del repository xml. Una volta ottenute le informazioni necessarie costruirà la risposta e la restituirà alla porta di dominio dempre attraverso il protocollo SOAP.

Le porte costruiscono ed interpretano questi messaggi per mezzo di appositi trattamenti che verranno analizzati in seguito.

Nel nostro caso avremo un generico utente o *principal*), in possesso di una *Authentication Assertion*, che vorrà accedere ad un servizio di suo interesse. Prima di tutto egli dovrà accedere ad un server SAML di competenza il quale dovrà erogare una *Attribute Assertion* contenente uno o più attributi di competenza dell'utente. Successivamente l'utente si presenterà al servizio di interesse con questa asserzione, ed un altro server SAML provvederà ad accertarsi che il soggetto in questione possa accedere al servizio richiesto (rilasciando una *AuthorizationAsserion*) o in base ad una autorizzazione individuale appositamente creata per l'utente (quindi basata sull'identità dell'utente stesso) oppure in base agli attributi in suo possesso. Ovviamente la seconda ipotesi sarà la più frequente, in quanto permette di gestire in maniera sicura e con il minimo dispendio di risorse il maggior numero di utenti.





3. architettura di gestione accessi

Nella logica federativa più sistemi concorrono a livello paritetico per generare nuovi e più potenti livelli di servizio. Gli standard, sia in termini applicativi che tecnologici costituiscono la lingua franca che consente ai sistemi ed alle applicazioni di interagire. Esistono poi delle componenti informative e di servizio condivise quali: i sistemi di Registry, gli Indici, i sistemi di gestione degli eventi ecc.. Questi sistemi anche se operano secondo una logica federativa sono visti come un'entità unica in rappresentanza di uno stesso livello di conoscenza e di servizio.

In quest'ottica deve anche essere vista la Gestione dei Diritti di Accesso. Un servizio da rendere disponibile a tutti in modo omogeneo ed al quale concorrono dinamicamente attori e ruoli diversi.

Il servizio di Gestione dei Diritti di Accesso è reso indispensabile dal contesto architetturale. Siamo infatti in presenza di servizi che integrano servizi erogati da altri domini ai quali l'utente può risultare completamente estraneo. In questa situazione i sistemi tradizionali di gestione degli utenti e dei diritti di accesso non sono sufficienti. Anche in termini di responsabilità non si può partire dal presupposto che ogni dominio gestisca il profilo di tutti i possibili utenti siano essi sistemi o individui.

Per gestire l'accesso ad un servizio (sia anche una semplice estrazione classificata di informazioni) occorre:

- Identificare in modo certo l'utente o il sistema richiedente

- Disporre di una politica di accesso per il servizio richiesto
- Appurare in modo certo gli attributi forniti dall'utente (o sistema) legati alla politica d'accesso del servizio

3.1 identificazione dell'utente

Per l'identificazione dell'utente si ipotizza l'uso delle tecniche attuali di autenticazione tramite firma digitale. E' dunque necessario che la richiesta di accesso ad un servizio sia accompagnata da un certificato di identità valido dell'utente. Per la validità a livello legale è necessario prevedere l'utilizzo di dispositivi (smart-card) di firma qualificati (norme AIPA).

E' comunque possibile prevedere, anche per l'identificazione, una modalità di riconoscimento indiretta. Nella modalità indiretta è l'Amministrazione accedente che si assume l'incarico e l'onere di riconoscere l'utente avvallandolo ai terzi. In questo modo è possibile realizzare l'integrazione di servizi anche in back-end ad applicazioni tradizionali che identificano ad esempio l'utente con login e password. E' ovvio che in questo caso, anche per l'identificazione, la responsabilità viene assunta dall'Amministrazione che ne avvalla l'autenticità.

3.2 politiche di accesso.

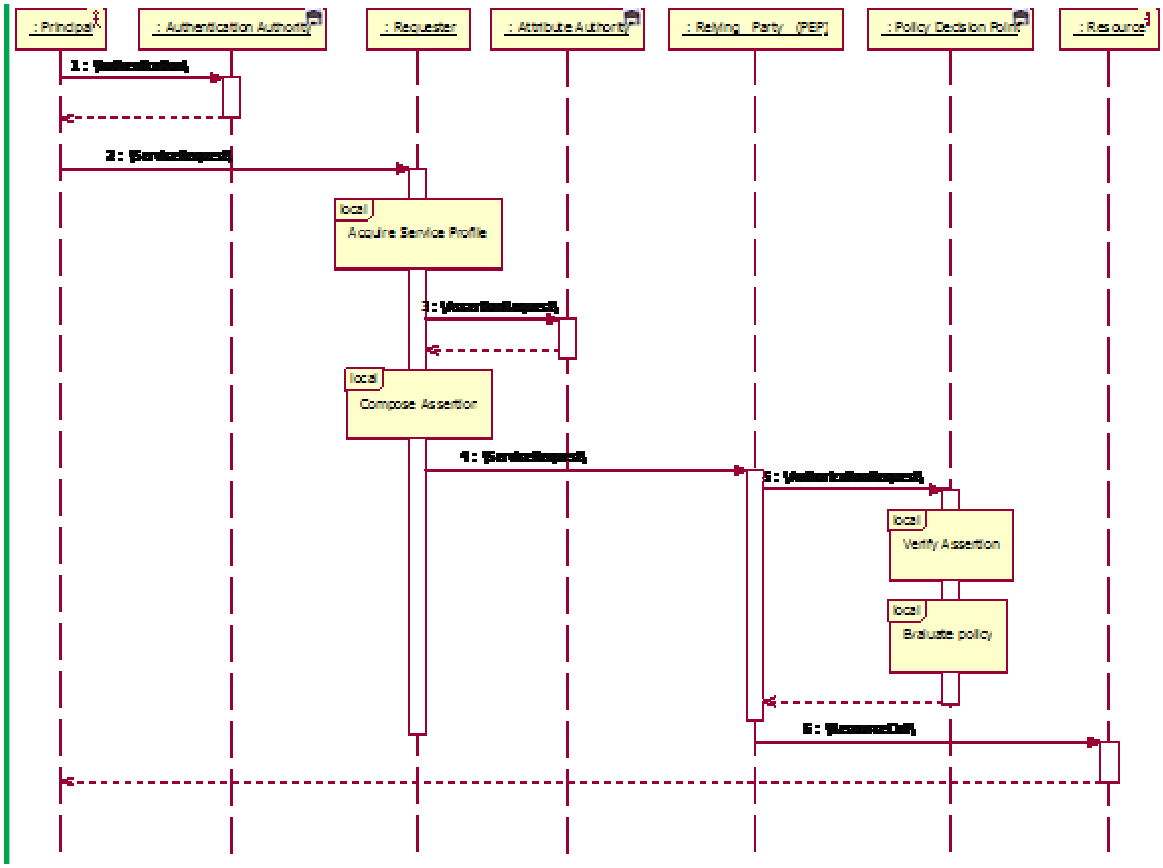
Ogni servizio può avere una diversa politica d'accesso. Di seguito si elencano alcune tipologie elementari di politiche d'accesso:

- per iscrizione ad un albo professionale
- per appartenenza un'Amministrazione specifica
- per un ruolo all'interno di una tipologia di Amministrazioni
- per autorizzazione personale

Se poi consideriamo le diverse tipologie di interdipendenza tra informazioni, servizi e individui, la casistica diventa molto più ampia.

E' importante che le politiche siano definibili senza ambiguità. Ogni dominio deve prevedere un'infrastruttura in grado di gestire e verificare le politiche d'accesso per tutti i servizi erogati dal dominio. Anche in questo caso parliamo di un'infrastruttura che può essere solo virtualmente unica e risultare invece dalla federazione di più sistemi indipendenti seppur interni al dominio. Quest'ultima esigenza sarà soprattutto funzionale alla distribuzione delle responsabilità per l'accesso ai vari servizi.

La responsabilità del servizio di gestione delle policy è comunque direttamente legata ad uno o più amministratori ed è in questo senso che va impostata la struttura (derivata in genere dall'organigramma dell'Amministrazione). Il sistema che eroga il servizio è così svincolato dalla responsabilità di verifica dei diritti d'accesso, suo onere solo quello di archiviare (sottoforma di documento elettronico) l'autorizzazione rilasciata dal policy-manager.



3.3 verifica degli attributi

Le politiche d'accesso si possono basare su più tipologie d'informazione legate alla richiesta del servizio, tra queste:

- il servizio
- l'oggetto del servizio
- l'Amministrazione richiedente
- gli attributi dell'Amministrazione richiedente
- il richiedente
- gli attributi del richiedente

Per alcuni di questi attributi è necessaria un verifica di autenticità. Sicuramente è necessario appurare l'autenticità degli attributi: Amministrazione richiedente e richiedente. Già nell'identificazione dell'utente abbiamo visto come vengono prodotti, la verifica consisterà nel appurare la validità delle certificazioni attraverso le infrastrutture PKI interne ed esterne al dominio.

Per gli altri attributi può essere necessario avvalersi di altre autorità di certificazione. Nella pratica attuale ad esempio, quando è necessario dimostrare un ruolo: un'iscrizione ad un albo, un incarico ecc. l'interessato di norma si fa rilasciare dall'organismo preposto a tale dichiarazione un attestato

da esibire o comunque da rilasciare all'Amministrazione cui si rivolge. All'Amministrazione che riceve l'attestato è riservato l'onere della sua gestione ed anche la responsabilità della decisione che ne consegue. Questa pratica, oltre ad essere piuttosto onerosa può avere numerosi inconvenienti, il primo tra tutti la validità nel tempo. Possono venir concesse autorizzazioni su attestazioni non più valide solo per l'impossibilità di verificarne la validità di volta in volta. Ed anche qui si pone il problema della responsabilità.

La soluzione è quella di verificare sempre l'attributo specifico, verifica che deve essere eseguita richiedendone l'autenticazione a chi ne ha la responsabilità di gestione (ordine professionale, Amministrazione ecc.). Se dunque, all'interno di un dominio, un'Amministrazione deve attestare il ruolo ricoperto da una persona del suo organico (es. Tribunale, Giudice) dovrà disporre di un servizio in grado di rilasciare attestati in tal senso (**asserzioni**), ogni qual volta un sistema esterno ne faccia richiesta.

L'attestato elettronico potrà avere una validità temporale e potrà essere utilizzato anche più volte. L'attestato potrà essere allegato direttamente alla richiesta oppure potrà essere preteso al momento dell'accesso ad un servizio dallo stesso provider ecc.

3.4 integrazione nell'infrastruttura di cooperazione applicativa

Il sistema di Gestione Accessi si integra nella struttura di cooperazione applicativa attraverso le porte di dominio. In questo modo il sistema risulta completamente trasparente alle applicazioni e quindi ad i SI. L'unico flusso informativo richiesto al livello applicativo verticale o di supporto è l'identificazione dell'utente. L'infrastruttura a supporto di questa architettura si basa su tre classi di sistemi:

- Identity server
- Policy Manager
- Assertion Server

L'Identity server produce le attestazioni di identità. Come si diceva prima questa attestazione può essere prodotta da un sistema specifico, in back end ad un gestionale esistente, oppure con l'avvallo di un token individuale di firma quale una smartcard crittografica. Unico attributo indispensabile per l'identificazione e quindi contenuto all'interno del certificato d'identità è il codice identificativo univoco che possiamo individuare nel codice fiscale alias codice individuale.

Al Policy Manager compete la gestione e la verifica delle politiche di accesso. Questo sistema dovrà consentire la definizione delle politiche d'accesso relative allo specifico servizio da parte degli amministratori che ne hanno titolo (e responsabilità).

E' ancora onere del Policy Manager rilasciare, su richiesta dei sistemi che erogano i servizi, i risultati delle verifiche effettuate sulla base delle credenziali presentate dal richiedente, sottoforma di credenziali di autorizzazione. Queste credenziali svincoleranno il sistema d'erogazione da qualsiasi altra verifica.

Dove è possibile individuare una responsabilità specifica, di un Ente o un'Amministrazione sulla dichiarazione di un ruolo relativo ad un individuo o ad un altro Ente, sarebbe opportuno collocare

un sistema di gestione delle specifiche asserzioni (Assertion Server). L'Assertion Server rilascia, per gli attributi di cui ha responsabilità, un attestato che, sottoforma di documento elettronico, associa inequivocabilmente identità e attributo.Per rendere questa infrastruttura il meno invasiva possibile si ipotizza di integrare i sistemi di policy assertion e identity management al livello di porte di dominio.

3.5 Gestione del sistema

Come affermato precedentemente il server SAML estrae le informazioni di interesse da un repository xml. La gestione delle informazioni contenute nel repository è affidata ad un complesso di servizi apposito. Ovviamente tutta la sicurezza del sistema dipende da quanto sicuro è l'accesso a questi dati, in quanto essi possono venir modificati solo dal personale apposito.

I messaggi che viaggiano da e verso questi servizi sono tutti di tipo xml. Per garantirne la sicurezza questi messaggi vengono firmati dall'emittente, ed il servizio provvederà, una volta ricevuti, a verificare che la firma sia valida e che il certificato di firma appartenga all'operatore di competenza.

Per semplificare le varie funzioni è stata stabilita una gerarchia di ruoli all'interno del sistema.

All'interno dello stesso repository possono venire gestite più amministrazioni, ognuna delle quali ha i suoi utenti ed i suoi servizi.

La figura principale del sistema è l'*Authority Administrator* (AA), il quale ha il compito di gestire le amministrazioni che devono risiedere sul repository. Per creare un'amministrazione, l'AA deve creare un *Service Provider Administrator* (SPA), indicando a quale amministrazione esso appartiene. L'SPA a sua volta, come responsabile della sua amministrazione, deve creare uno o più *Service Provider Operator* (SPO), i quali si occupano della gestione degli utenti e dei servizi.

La gerarchia dei ruoli di amministrazione è quindi AA->SPA->SPO.

Ogni operatore avrà a disposizione dei servizi non visibili agli altri, in quanto le funzioni sono specializzate per il singolo ruolo.

Per quanto riguarda la gestione dei servizi e dei ruoli da parte degli SPO, essi avranno a disposizione una lista di entry tra le quali scegliere.

Di seguito sono riportati i servizi reagivi ad ogni ruolo:

i. Authority Administrator

gestione Service Provider Administrator:

- addSPA: servizio che permette l'inserimento di un SPA. Nell'inserimento va indicato il certificato dell'SPA creato (certificato col quale l'SPA firmerà le sue richieste) e l'amministrazione dell'SPA.
- getSPA: servizio che permette la ricerca di un SPA.
- delSPA: servizio che permette la cancellazione di un SPA.
- setSPA: servizio che permette la modifica si un SPA.

ii. Service Provider Administrator

gestione Service Provider Operator:

- addSPO: servizio che permette l'inserimento di un SPO. Nell'inserimento va indicato il certificato dell'SPO creato (certificato col quale l'SPO firmerà le sue richieste). Inoltre viene anche indicata la lista dei ruoli e dei servizi sui quali l'SPO può operare.
- getSPO: servizio che permette la ricerca di un SPO.
- delSPO: servizio che permette la cancellazione di un SPO.
- setSPO: servizio che permette la modifica si un SPO.

iii. Service Provider Operator

gestione Servizi:

- addService: servizio che permette la creazione di un Servizio, con i relativi ruoli che ne permettono l'accesso. Ovviamente tale Servizio deve comparire nella lista di competenza del SPO.
- getService: servizio che permette la ricerca di un Servizio.
- delService: servizio che permette la cancellazione di un Servizio.
- setService: servizio che permette la modifica di un Servizio.

gestione Utenti:

- addUser: servizio che permette l'inserimento di un utente nell'amministrazione. Vengono anche specificati (se ci sono) i ruoli dell'utente.
- getUser: servizio che permette la ricerca di un utente.
- delUser: servizio che permette la cancellazione di un utente.
- setUser: servizio che permette la modifica di un utente.

gestione Autorizzazioni Individuali:

- addAuthorization: servizio che permette l'inserimento di una autorizzazione individuale. Nella autorizzazione vanno indicati il servizio ed il codice individuale dell'utente.
- getAuthorization: servizio che permette la ricerca di una autorizzazione.
- delAuthorization: servizio che permette la cancellazione di una autorizzazione.
- setAuthorization: servizio che permette la modifica di una autorizzazione.

Tutti questi servizi sono messi a disposizione attraverso un'interfaccia utente che permette la scelta dell'operazione desiderata a seconda dell'operatore.

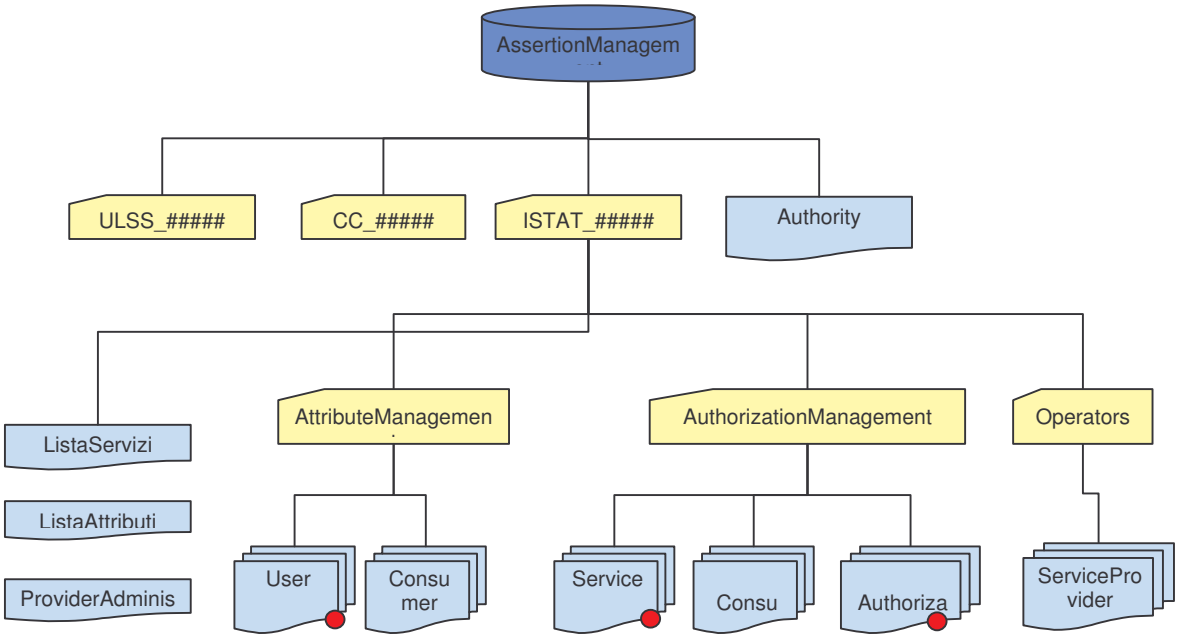
3.6 Trattamenti della porta di dominio

Si è precedentemente accennato ai trattamenti che devono essere attivati sulle porte di dominio per poter utilizzare il server SAML.

Il primo trattamento si chiama **interrogaAttributoSaml**, e viene attivato sulla porta di dominio delegata. Tramite questo trattamento la porta richiede al server SAML indicato nei parametri del trattamento i valori dell'attributo (il cui nome è specificato sempre nei parametri) dell'utente richiedente. Una volta ottenuta la risposta, se esistono attributi per l'utente viene preparato il messaggio WSS da inviare alla porta applicativa insieme alla richiesta del servizio.

La porta applicativa riceverà la richiesta del servizio, estrarrà le varie asserzioni del WSS precedentemente elencate e provvederà a chiamare il trattamento **interrogaAutorizzazioneSaml**, il quale chiederà al server SAML indicato nei suoi parametri se l'asserzione di attributo contentuta nella richiesta permette all'utente in questione di accedere al servizio. In caso affermativo verrà attivato il servizio richiesto, altrimenti verrà respinta tale richiesta.

3.7 Struttura del repository



Il repository xml è stato strutturato fisicamente su un solo livello, cioè tutti i documenti xml inseriti sono figli della stessa radice *AssertionManagement*. La struttura viene quindi data a livello logico, in base a degli attributi specificati per ogni entry.

Avremo l'attributo ***root*** che indicherà a quale amministrazione appartiene l'entry, e l'attributo ***path*** che indicherà invece sotto quale ramo logico verrà inserito il documento all'interno dell'amministrazione.

Esterno ad ogni amministrazione (e quindi con attributo ***root*** di valore '\') c'è l'AA.

Internamente ad ogni amministrazione invece (e quindi con l'attributo ***root*** valorizzato col nome dell'amministrazione) sono previsti i seguenti valori dell'attributo ***path:***

- '/' : ovvero la directory radice. In questo ramo vanno inseriti la *ListaServizi* e la *ListaRuoli* (i due xml contenenti la lista completa dei ruoli e dei servizi disponibili) e l'SPA dell'amministrazione.
- 'AttributeManagement': il ramo contenente la lista degli utenti.
- 'AuthorizationManagemnt': il ramo contenente i servizi e le autorizzazioni individuali.
- 'Operators': il ramo contiene la lista degli SPO per questa amministrazione.