Sistema Federato Interregionale di Autenticazione: SPECIFICA DELLE INTERFACCE APPLICATIVE ESTERNE

Versione 0.5

INDICE

1. MODIFICHE AL DOCUMENTO

Descrizione modifica	Edizione	Data
TOC + traccia contenuti	0.1	12/02/2007
Modifiche ai contenuti	0.2	23/02/2007
Modifiche ai contenuti	0.3	27/02/2007
Modifiche ai contenuti	0.4	01/03/2007
Modifiche ai contenuti	0.5	02/03/2007

2. INTRODUZIONE

Obiettivo del presente documento è la specifica delle interfacce applicative esterne – e del relativo modello dei dati – offerte dai componenti dell'architettura di riferimento del sistema federato interregionale di autenticazione, di competenza dell'intervento infrastrutturale ICAR INF-3. Tali componenti sono descritti nel documento di modellazione architetturale [1] e negli altri documenti ivi citati.

Il documento è organizzato come segue. La sez. 3 ricapitola brevemente i componenti dell'architettura di riferimento e gli scenari di interazione. La sez. 4 descrive in dettaglio le interfacce applicative esterne esposte dai componenti del sistema federato INF-3. La sez. **Errore. L'origine riferimento non è stata trovata.** espone le considerazioni conclusive.

3. ARCHITETTURA E SCENARI DI RIFERIMENTO

In vista della specifica di dettaglio delle interfacce applicative esterne, questa sezione presenta una sintesi dell'architettura generale del sistema federato di autenticazione INF-3; inoltre, riassume gli scenari di riferimento per le interazioni tra i diversi componenti architetturali.

Questi aspetti non vengono qui illustrati in dettaglio ma solo richiamati brevemente, in quanto già trattati nel documento di modellazione architetturale di riferimento (cfr. [1], sez. 4).

3.1. Architettura

Il diagramma di Figura 1 illustra ad alto livello l'architettura del sistema federato INF-3. In particolare vengono mostrate le entità coinvolte nell'erogazione dei servizi di autenticazione federata e le relative interfacce (solo quelle direttamente pertinenti al funzionamento del sistema federato).

N.B. I riquadri che circondano le entità rappresentate nel diagramma circoscrivono intuitivamente gli "ambiti di competenza" dei componenti rispetto alle responsabilità di modellazione e realizzazione assegnate all'interno del progetto ICAR, in particolare quelle di pertinenza di INF-3. Si sottolinea che questa suddivisione non vuole fornire indicazioni stringenti in merito al dispiegamento dei componenti rappresentati.

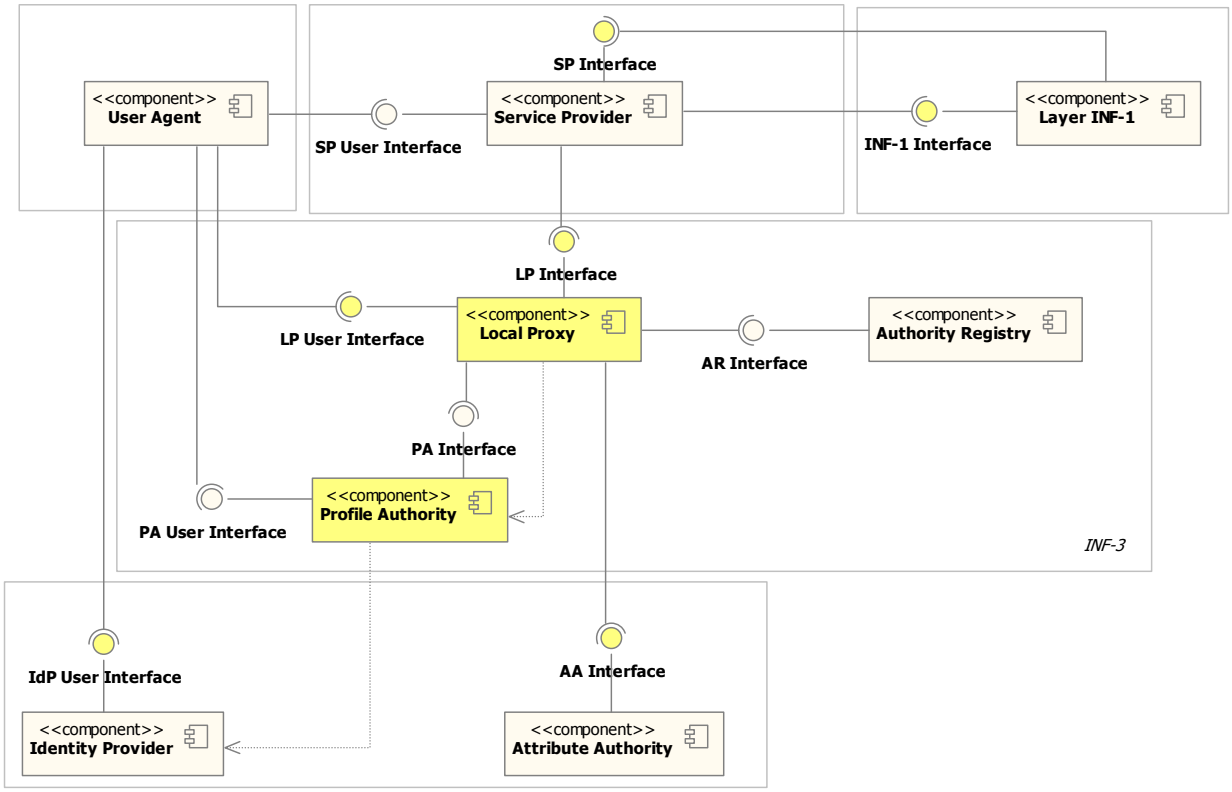

Figura 1. Vista architetturale d'insieme del sistema federato di autenticazione

Si fornisce qui di seguito una sintetica descrizione di ciascun componente e delle interfacce offerte. Maggiori dettagli relativi ad alcuni componenti saranno illustrati nel seguito, in particolare per quel che riguarda le interfacce offerte (e attese) coinvolte nelle interazioni con le altre entità che si interfacciano con il sistema federato INF-3 (cfr. sez. 3.1.1).

Lo **User Agent** è un client web (per esempio un web browser) usato dall'utente per accedere ai servizi offerti dai Service Provider. Allo User Agent si richiede di supportare i protocolli HTTP e HTTPS con scambio mutuo di certificati tra client e server.

Il **Service Provider** è il fornitore dei servizi applicativi. Il componente espone due interfacce:

- `SP User Interface`: permette agli utenti l'accesso via web tramite User Agent ai servizi offerti;
- `SP Interface`: permette l'interazione con altri Service Provider in modalità di cooperazione applicativa.

Il **Local Proxy** è il componente che, dal punto di vista del Service Provider, si comporta da proxy verso il sistema di autenticazione federato INF-3. Il componente espone due interfacce:

- `LP User Interface`: l'interfaccia utente per l'interazione con l'utente tramite User Agent (utilizzabile per esempio nel caso di un servizio "WAYF", con cui il Local Proxy può chiedere all'utente di indicare la sua Profile Authority di riferimento);
- `LP Interface`: l'interfaccia applicativa per l'interazione con altri componenti architetturali, per esempio il Service Provider.

Si notino le dipendenze d'uso esistenti tra il Local Proxy e la Profile Authority, e tra quest'ultima e l'Identity Provider, che verranno chiarite nel seguito.

L'**Authority Registry** è il componente che permette di recuperare le coordinate di accesso e altre informazioni relative alle authority. Il componente espone un'interfaccia:

- `AR Interface`: l'interfaccia applicativa che supporta le operazioni di interrogazione del registro.

L'**Identity Provider** è il componente responsabile della certificazione dell'identità degli utenti. Esso espone un'interfaccia:

- `IdP User Interface`: l'interfaccia web destinata all'immissione delle credenziali di autenticazione da parte dell'utente.

La **Profile Authority** è il componente che svolge il ruolo di repository dei profili utente e che si occupa di interagire con l'Identity Provider ai fini dell'autenticazione dell'utente. Il componente espone due interfacce:

- `PA Interface`: l'interfaccia applicativa che supporta le operazioni di interrogazione dei profili utente.
- `PA User Interface`: l'interfaccia web per l'interazione con l'utente (creazione e gestione dei profili utente, scelta dell'Identity Provider, selezione del profilo, ecc.).

In casi particolari questo componente può agire da Attribute Authority.

La **Attribute Authority** è il componente in grado di certificare gli attributi presenti in un profilo utente. Il componente espone un'interfaccia:

- `AA Interface`: l'interfaccia applicativa che supporta le operazioni di interrogazione ai fini della validazione degli attributi utente.

Infine, il **layer INF-1** permette l'interazione applicativa inter-dominio offrendo ai componenti del sistema INF-3 (in particolare ai Service Provider) un'opportuna interfaccia:

- `INF-1 Interface`: l'interfaccia applicativa offerta ai Service Provider per la fruizione di altri servizi in cooperazione applicativa.

3.1.1. Identificazione delle interfacce applicative esterne

Nel seguito del documento verranno dettagliate soltanto le interfacce coinvolte nelle interazioni tra i componenti del sistema federato INF-3 e le entità esterne a esso. Tali interfacce si possono identificare sulla base del diagramma di Figura 1 (con particolare riferimento a quelle che "intersecano" il riquadro "INF-3") e di considerazioni legate agli scenari di riferimento (cfr. sez. 3.2) e agli standard tecnologici adottati (anzitutto SAML 2.0).

In particolare, le interfacce che verranno descritte in dettaglio nel presente documento sono le seguenti:

- `LP User Interface`
- `LP Interface`
- `IdP User Interface`
- `AA Interface`

Saranno inoltre fornite indicazioni in merito all'interazione applicativa tra Service Provider (interfacce `SP Interface` e `INF-1 Interface`) per quanto riguarda le modalità con cui vengono veicolate le asserzioni.

N.B. Per via del maggiore livello di dettaglio richiesto dalla descrizione, nel seguito del documento alcune caratteristiche delle interfacce applicative (per esempio le convenzioni di nomenclatura) potranno variare leggermente rispetto a quelle più generiche presenti nei diagrammi visti finora.

3.2. Scenari di riferimento

Al fine di illustrare come i componenti architetturali interagiscano effettivamente tra loro, nell'ambito del sistema federato di autenticazione sono stati considerati due scenari di riferimento (cfr. [1], sez. 4.4):

- l'accesso a un Service Provider da parte di un utente mediante uno User Agent (web browser),
- l'accesso da parte di un Service Provider a un altro Service Provider appartenente a un dominio remoto a seguito di una richiesta inoltrata da un utente mediante il proprio User Agent.

I due scenari evidenziano i ruoli delle diverse entità coinvolte nelle interazioni e gli specifici meccanismi di autenticazione e autorizzazione di volta in volta utilizzati. Le interazioni sono dettagliate in termini di operazioni svolte e di messaggi scambiati (e relativi protocolli).

Per i dettagli sugli scenari di riferimento si rimanda al documento citato. Nel seguito del documento, nell'ambito della descrizione delle interfacce esterne (cfr. sez. 4) verranno ripresi e ulteriormente precisati alcuni aspetti dei due scenari.

4. INTERFACCE APPLICATIVE ESTERNE

Questa sezione entra nel dettaglio delle interfacce applicative esterne dei componenti architetturali del sistema federato INF-3 e dell'uso che si intende fare delle tecnologie di riferimento, in particolare lo standard SAML, riprendendo ed estendendo quanto già scritto nel documento di modellazione architetturale (cfr. [1], sez. 4.2).

N.B. Per via del maggiore livello di dettaglio richiesto dalla descrizione, alcune caratteristiche delle interfacce applicative (per esempio le convenzioni di nomenclatura) possono variare leggermente rispetto a quelle più generiche presenti nei diagrammi visti finora.

La sezione è organizzata come segue:

- la sez. 4.1 descrive in dettaglio le interazioni tra il Local Proxy e il Service Provider;
- la sez. 4.2 illustra le modalità di interfacciamento con gli Identity Provider e le Attribute Authority;
- la sez. 4.3 riporta alcune ipotesi di interazione con il layer INF-1;
- la sez. 4.4 fornisce alcune informazioni generali sull'uso che si intende fare dei costrutti SAML.

4.1. Interazioni tra Service Provider e Local Proxy

La Figura 2 illustra le interfacce offerte dal componente Local Proxy.

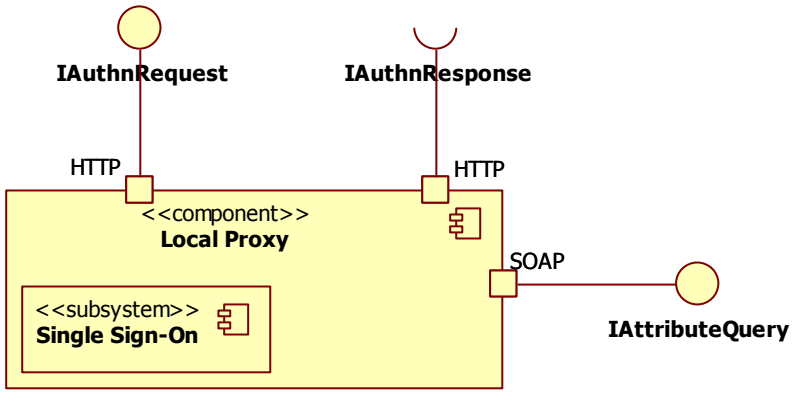

Figura 2. Interfacce del componente Local Proxy

Secondo quanto previsto dagli scenari di riferimento, il Local Proxy viene interrogato dal Service Provider nei seguenti casi:

- richiesta di autenticazione dell'utente,

- richiesta di attributi dell'utente.

4.1.1. Richiesta di autenticazione

Gli scenari di interazione a fini di autenticazione si basano su alcuni profili standard SAML, in particolare si considerano qui i profili "Service Provider initiated", in cui cioè il meccanismo di autenticazione è innescato dalla richiesta inoltrata dall'utente al Service Provider, il quale a sua volta si rivolge opportunamente all'autorità di certificazione d'identità in modalità "pull".

Il profilo SAML a cui si fa riferimento è il "SP-Initiated SSO" (cfr. [6], sez. 4.1), in particolare nelle sue due versioni: "Redirect/POST binding" e "POST/POST binding". Nel caso in esame il Service Provider svolge il ruolo omonimo previsto dal profilo, mentre il Local Proxy svolge il ruolo di "Identity Provider".

Secondo il profilo "SP-Initiated SSO" la richiesta di autenticazione SAML (`<AuthnRequest>`) può essere inoltrata dal Service Provider al Local Proxy usando il binding HTTP Redirect o il binding HTTP POST. La relativa risposta SAML (`<Response>`) può invece essere inviata dal Local Proxy al Service Provider solo tramite il binding HTTP POST. (Non si considerano in questa sede i binding HTTP Artifact.)

La richiesta di autenticazione nel caso del binding HTTP Redirect ha le seguenti caratteristiche:

- il Service Provider invia allo User Agent (il browser dell'utente) una risposta HTTP Redirect avente status 302 o 303;
- il Location Header della risposta HTTP contiene l'URI di destinazione del componente Single Sign-On esposto dall'Identity Provider (interfaccia IAuthnRequest);
- la risposta HTTP contiene un costrutto SAML `<AuthnRequest>` codificato come una URL query variable di nome "SAMLRequest";
- la query string è codificata con encoding DEFLATE.

Il browser dell'utente quindi processa la risposta HTTP Redirect e indirizza una richiesta HTTP GET del componente Single Sign-On dell'Identity Provider (interfaccia IAuthnRequest) mantenendo il query parameter "SAML Request".

Analogamente, la richiesta di autenticazione nel caso del binding HTTP POST ha le seguenti caratteristiche:

- il Service Provider invia allo User Agent (il browser dell'utente) una risposta HTTP con status 200 contenente una form HTML;
- la form HTML contiene un costrutto SAML `<AuthnRequest>` codificato come valore di un hidden form control di nome "SAMLRequest";
- per comodità, la form HTML può essere corredata di uno script che la renda autopostante.

Il browser dell'utente processa quindi la risposta e invia una richiesta HTTP POST e verso il componente Single Sign-On dell'Identity Provider (interfaccia IAuthnRequest).

In entrambi i casi, le caratteristiche che deve avere la `<AuthnRequest>` sono le seguenti:

- deve essere presente l'attributo `ID` univoco (cfr. sez. 4.4);
- deve essere presente l'elemento `<Issuer>` a indicare l'entità emittente (il Service Provider);
- può non essere presente l'elemento `<Subject>` (per esempio nel caso in cui esso non sia ancora noto al Service Provider);
- l'elemento `<NameIDPolicy>` e il relativo attributo `AllowCreate` devono segnalare all'Identity Provider tramite il Local Proxy che non è ammesso che l'identificativo dell'utente venga creato contestualmente alla fase di autenticazione (in altre parole, si richiede che il subject sia già registrato presso il certificatore d'identità);
- l'attributo `ForceAuthn` deve valere "false" (cioè si richiede che il Local Proxy non autentichi direttamente l'utente);
- l'attributo `ProxyCount` dell'elemento `<Scoping>` deve correttamente indicare il numero di redirezioni permesse verso i certificatori di identità: nel caso in esame deve valere almeno "2";
- l'elemento `<IDPList>` dell'elemento `<Scoping>`, se presente, può contenere la lista delle entità che il Service Provider considera fidate ai fini dell'elaborazione della richiesta di autenticazione, cioè almeno il Local Proxy;
- l'elemento `<RequesterID>` dell'elemento `<Scoping>`, nel caso delle interazioni a valle di quella tra Service Provider e Local Proxy, deve indicare le entità che hanno emesso originariamente la richiesta di autenticazione e quelle che in seguito l'hanno propagata (cfr. [7], sez. 3.4.1.2 e 3.4.1.5 per le questioni legate al proxying);
- l'elemento `<Conditions>` può indicare i limiti di validità attesi dell'asserzione ricevuta in risposta;
- può essere presente l'elemento `<RequestedAuthnContext>` a indicare il contesto di autenticazione atteso (per esempio la "forza" delle credenziali richieste);
- deve essere presente l'elemento `<Signature>` apposto dal Service Provider.

Conclusa la fase di autenticazione, il Local Proxy costruisce una SAML `<Response>` firmata da inviare al Service Provider, e in particolare al sottosistema Assertion Consumer. La `<Response>` viene inserita in una form HTML come hidden form control di nome "SAMLResponse". Il componente Single-Sign On del Local Proxy invia la form HTML al browser dell'utente in una risposta HTTP (anche in questo caso, è possibile rendere la form autopostante mediante un opportuno script).

Il browser dell'utente processa quindi la risposta HTTP e invia una richiesta HTTP POST verso il servizio Assertion Consumer del Service Provider contenente la SAML `<Response>` firmata.

Le caratteristiche che deve avere la `<Response>` inviata dal Local Proxy al Service Provider in risposta alla richiesta di autenticazione sono le seguenti:

- deve essere presente l'attributo `ID` univoco (cfr. sez. 4.4);

- deve essere presente l'attributo `InResponseTo`, il cui valore deve fare riferimento all'`ID` della richiesta a cui si risponde;
- deve essere presente l'elemento `<Issuer>` a indicare l'entità emittente, cioè il Local Proxy;
- deve essere presente l'elemento `<Subject>` che identifica l'utente autenticato;
- deve essere presente un elemento `<Assertion>` di avvenuta autenticazione contenente un elemento `<AuthnStatement>`;
- nella `<Assertion>` di autenticazione, nell'elemento `<Conditions>` devono essere presenti i vincoli di validità dell'asserzione (per esempio `NotBefore`, `NotOnOrAfter`, `OneTimeUse`, `ProxyRestrictions`);
- nella `<Assertion>` di autenticazione, nell'elemento `<AuthnContext>` deve essere presente la descrizione del contesto di autenticazione effettivo;
- ciascuna `<Assertion>` deve recare la `<Signature>` dell'authority emittente;
- deve essere presente l'elemento `<Signature>` apposto dal Local Proxy.

In tutte le risposte fornite da authority di certificazione deve essere inoltre presente l'asserzione di abilitazione.

Per quel che riguarda la rappresentazione della "forza" delle credenziali di autenticazione, si fa riferimento alla struttura del costrutto `<AuthnContext>` come descritto nella specifica SAML.

4.1.2. Richiesta di attributi

Nel caso della richiesta di attributi, l'interazione tra Service Provider e Local Proxy avviene attraverso l'interfaccia applicativa `IAttributeQuery` esposta dal Local Proxy.

Gli scenari di interazione per la richiesta di attributi da parte del Service Provider si basano sul "SAML SOAP binding" previsto dalla specifica (cfr. [10], sez. 3.2). Questo binding prevede che i costrutti SAML di richiesta e risposta siano inclusi nel body dei messaggi SOAP scambiati (al massimo una richiesta o una risposta per messaggio).

Il binding prescrive inoltre l'uso di "SOAP over HTTP", che prevede l'uso di un header SOAPAction come parte di una richiesta SOAP HTTP (cfr. [10], sez. 3.2.3).

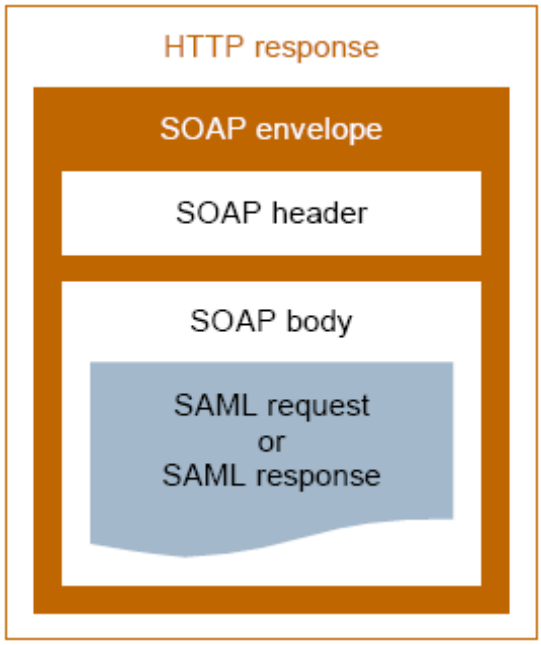

Figura 3. Costrutti SAML trasportati con binding SOAP over HTTP (cfr. [6], sez. 3.3.4)

```
 1: <?xml version="1.0" encoding="UTF-8"?>
 2: <env:Envelope
 3:   xmlns:env="http://www.w3.org/2003/05/soap/envelope/">
 4:   <env:Body>
 5:     <samlp:AuthnRequest
 6:       xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 7:       xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
 8:       Version="2.0"
 9:       ID="f0485a7ce95939c093e3de7b2e2984c0"
10:       IssueInstant="2005-01-31T12:00:00Z"
11:       Destination="https://www.AirlineInc.com/IdP/" >
12:       AssertionConsumerServiceIndex="1"
13:       AttributeConsumingServiceIndex="0" >
14:       <saml:Issuer>http://www.CarRentalInc.com</saml:Issuer>
15:       <samlp:RequestedAuthnContext>
16:         <saml:AuthnContextClassRef>
17:           urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
18:         </saml:AuthnContextClassRef>
19:       <samlp:NameIDPolicy
20:          Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
21:       </samlp:NameIDPolicy>
22:     </samlp:AuthnRequest>
23:   </env:Body>
24: </env:Envelope>
```

Figura 4. Esempio di SAML Authentication Request in una SOAP Envelope (cfr. [6], sez. 3.3.4)

```
 1: <?xml version="1.0" encoding="UTF-8"?>
 2: <env:Envelope  xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
 3:   <env:Body>
 4:     <samlp:Response
 5:       xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 6:       xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
 7:       Version="2.0"
 8:       ID="i92f8b5230dc04d73e93095719d191915fdc67d5e"
 9:       IssueInstant="2005-11-10T06:47:42.000Z"
10:       InResponseTo="f0485a7ce95939c093e3de7b2e2984c0">
11:       <saml:Issuer>http://www.AirlineInc.com</saml:Issuer>
12:       <samlp:Status>
13:         <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
14:       </samlp:Status>
15:                   ...SAML assertion...
16:     </samlp:Response>
17:   </env:Body>
18: </env:Envelope>
```

Figura 5. Esempio di SAML Response in una SOAP Envelope (cfr. [6], sez. 3.3.4)

I costrutti SAML a cui si fa riferimento sono la `<AttributeQuery>` e la relativa `<Response>`. Tali costrutti servono al Service Provider per interrogare il Local Proxy al fine di certificare il valore assunto da determinati attributi del profilo utente.

Le caratteristiche che deve avere in questo caso la `<AttributeQuery>` sono le seguenti:

- deve essere presente l'attributo `ID` univoco (cfr. sez. 4.4);
- deve essere presente l'elemento `<Issuer>` a indicare l'entità emittente (il Service Provider);
- deve essere presente l'elemento `<Subject>` a indicare l'utente a cui si riferisce la richiesta di attributi;
- devono essere presenti uno o più elementi `<Attribute>`, il cui `Name` indica l'attributo di cui si vuole conoscere il valore;
- in ciascun elemento `<Attribute>` possono essere presenti elementi `<AttributeValue>` per richiedere la verifica che l'attributo abbia i valori specificati;
- deve essere presente l'elemento `<Signature>` apposto dal Service Provider.

Le caratteristiche che deve avere la `<Response>` di risposta a una richiesta di attributi sono le seguenti:

- deve essere presente l'attributo `ID` univoco (cfr. sez. 4.4);
- deve essere presente l'attributo `InResponseTo`, il cui valore deve fare riferimento all'`ID` della richiesta a cui si risponde;
- deve essere presente l'elemento `<Issuer>` ad indicare l'entità emittente (il Local Proxy);
- deve essere presente l'elemento `<Subject>` a indicare l'utente;
- devono essere presenti una o più `<Assertion>` contenenti `<AttributeStatement>`;
- ciascuna `<Assertion>` deve avere i rispettivi elementi `<Issuer>` e `<Subject>`;
- ciascuna `<Assertion>` deve essere firmata dall'authority emittente;

- ciascuna `<Assertion>` deve contenere un elemento `<Conditions>` che ne determini i vincoli di validità;
- ciascun `<AttributeStatement>` deve contenere gli `<Attribute>` (e i relativi `<AttributeValue>`) relativi agli attributi richiesti;
- deve essere presente l'elemento `<Signature>` apposto dall'entità emittente.

La `<Response>` complessiva emessa dal Local Proxy e destinata al Service Provider è firmata dal Local Proxy stesso e può contenere più `<Assertion>` emesse e firmate da Attribute Authority diverse, ovvero il Portafoglio delle Asserzioni. Il Portafoglio delle Asserzioni rappresenta infatti l'insieme delle asserzioni SAML ricevute a seguito di una richiesta effettuata dal Service Provider a fini autorizzativi.

4.2. Interazioni con Identity Provider e Attribute Authority

L'interazione tra Profile Authority e Identity Provider avviene con modalità analoghe a quelle già descritte nel caso dell'interazione tra Service Provider e Local Proxy a fini di autenticazione (cfr. sez. 4.1.1). Si fa quindi ricorso al costrutto `<AuthnRequest>` e al relativo costrutto `<Response>` di risposta. In accordo con quanto definito dal profilo "SP-Initiated SSO", in questo caso il ruolo di Service Provider viene svolto dalla Profile Authority.

Rispetto all'interazione tra Service Provider e Local Proxy, cambiano leggermente le caratteristiche che deve avere la `<AuthnRequest>` in questo scenario:

- deve essere presente l'attributo `ID` univoco (cfr. sez. 4.4);
- deve essere presente l'elemento `<Issuer>` a indicare l'entità emittente (la Profile Authority);
- può non essere presente l'elemento `<Subject>` (per esempio nel caso in cui esso non sia ancora noto);
- l'elemento `<NameIDPolicy>` e il relativo attributo `AllowCreate` devono segnalare all'Identity Provider che non è ammesso che l'identificativo dell'utente venga creato contestualmente alla fase di autenticazione (in altre parole, si richiede che il subject sia già registrato presso il certificatore d'identità);
- l'attributo `ForceAuthn` deve valere "true" per prevenire ulteriori redirezioni (cioè si richiede che sia proprio quell'Identity Provider ad autenticare direttamente l'utente);
- l'attributo `ProxyCount` dell'elemento `<Scoping>` deve correttamente indicare il numero di redirezioni permesse verso i certificatori di identità: nel caso in esame deve valere "0";
- l'elemento `<IDPList>` dell'elemento `<Scoping>`, se presente, può contenere la lista delle entità che l'entità emittente considera fidate ai fini dell'elaborazione della richiesta di autenticazione, cioè l'Identity Provider;

- l'elemento `<Conditions>` può indicare i limiti di validità attesi dell'asserzione ricevuta in risposta;
- può essere presente l'elemento `<RequestedAuthnContext>` a indicare il contesto di autenticazione atteso (per esempio la "forza" delle credenziali richieste);
- deve essere presente l'elemento `<Signature>` apposto dalla Profile Authority.

Le caratteristiche che deve avere la `<Response>` inviata dall'Identity Provider alla Profile Authority in risposta alla richiesta di autenticazione appena descritta sono le seguenti:

- deve essere presente l'attributo `ID` univoco (cfr. sez. 4.4);
- deve essere presente l'attributo `InResponseTo`, il cui valore deve fare riferimento all'`ID` della richiesta a cui si risponde;
- deve essere presente l'elemento `<Issuer>` a indicare l'entità emittente, cioè l'Identity Provider;
- deve essere presente l'elemento `<Subject>` che identifica l'utente autenticato;
- deve essere presente un elemento `<Assertion>` di avvenuta autenticazione contenente un elemento `<AuthnStatement>`;
- nella `<Assertion>` di autenticazione, nell'elemento `<Conditions>` devono essere presenti i vincoli di validità dell'asserzione (per esempio `NotBefore`, `NotOnOrAfter`, `OneTimeUse`, `ProxyRestrictions`);
- nella `<Assertion>` di autenticazione, nell'elemento `<AuthnContext>` deve essere presente la descrizione del contesto di autenticazione effettivo;
- ciascuna `<Assertion>` deve recare la `<Signature>` dell'authority emittente;
- deve essere presente l'elemento `<Signature>` apposto dall'Identity Provider.

In tutte le risposte fornite da authority di certificazione deve essere inoltre presente l'asserzione di abilitazione.

Per quel che riguarda la rappresentazione della "forza" delle credenziali di autenticazione, si fa riferimento alla struttura del costrutto `<AuthnContext>` come descritto nella specifica SAML.

L'interazione tra Local Proxy e le Attribute Authority avviene con modalità analoghe a quelle già descritte nel caso dell'interazione tra Service Provider e Local Proxy a fini di raccolta degli attributi utente (cfr. sez. 4.1.2). L'interazione tra Local Proxy e una Attribute Authority avviene attraverso l'interfaccia applicativa `AA Interface` esposta dalla Attribute Authority.

Le caratteristiche che deve avere in questo caso la `<AttributeQuery>` sono le seguenti:

- deve essere presente l'attributo `ID` univoco (cfr. sez. 4.4);
- deve essere presente l'elemento `<Issuer>` a indicare l'entità emittente (il Local Proxy);

- deve essere presente l'elemento `<Subject>` a indicare l'utente a cui si riferisce la richiesta di attributi;
- devono essere presenti uno o più elementi `<Attribute>`, il cui `Name` indica l'attributo di cui si vuole conoscere il valore;
- in ciascun elemento `<Attribute>` possono essere presenti elementi `<AttributeValue>` per richiedere la verifica che l'attributo abbia i valori specificati;
- deve essere presente l'elemento `<Signature>` apposto dal Local Proxy.

Le caratteristiche che deve avere la `<Response>` di risposta a una richiesta di attributi sono le seguenti:

- deve essere presente l'attributo `ID` univoco (cfr. sez. 4.4);
- deve essere presente l'attributo `InResponseTo`, il cui valore deve fare riferimento all'`ID` della richiesta a cui si risponde;
- deve essere presente l'elemento `<Issuer>` ad indicare l'entità emittente (la Attribute Authority);
- deve essere presente l'elemento `<Subject>` a indicare l'utente;
- devono essere presenti una o più `<Assertion>` contenenti `<AttributeStatement>`;
- ciascuna `<Assertion>` deve avere i rispettivi elementi `<Issuer>` e `<Subject>`;
- ciascuna `<Assertion>` deve essere firmata dall'authority emittente;
- ciascuna `<Assertion>` deve contenere un elemento `<Conditions>` che ne determini i vincoli di validità;
- ciascun `<AttributeStatement>` deve contenere gli `<Attribute>` (e i relativi `<AttributeValue>`) relativi agli attributi richiesti;

deve essere presente l'elemento `<Signature>` apposto dall'entità emittente.

4.3. Interazioni con il layer INF-1

Dal punto di vista dell'architettura INF-3, il layer INF-1 mette a disposizione le funzionalità di inoltro delle richieste applicative nei casi di interazione inter-dominio in cooperazione applicativa. A questo riguardo si possono fare delle ipotesi in merito all'interfaccia attesa esposta dallo strato INF-3. Ci si aspetta che il componente offra almeno un'interfaccia:

- `INF-1 Interface`: a questa interfaccia applicativa si rivolgeranno i componenti architetturali (anzitutto i Service Provider) quando devono fruire di servizi appartenenti a domini differenti. Il requisito principale è che il layer INF-1 esponga opportuni metodi per inoltrare in modo trasparente e sicuro a un generico Service Provider appartenente a un altro dominio un'invocazione applicativa corredata di tutte le asserzioni SAML necessarie alla fruizione del servizio remoto. A titolo d'esempio si fa l'ipotesi che il layer INF-1 esponga

un'interfaccia Web service e che sia in grado di trasportare intatti gli header del messaggio SOAP contenenti i costrutti SAML che costituiscono il portafoglio delle asserzioni destinato al Service Provider del dominio remoto.

Dualmente a quanto appena detto, ci si aspetta che il componente utilizzi la seguente interfaccia esposta dal Service Provider:

- `SP Interface`: per poter inoltrare al servizio destinatario le richieste di servizio in cooperazione applicativa, a sua volta il layer INF-1 contatterà i Service Provider dei domini remoti tramite l'apposita interfaccia.

4.4. Altre considerazioni sull'uso di SAML

Si descrivono di seguito ulteriori vincoli che il sistema federato di autenticazione INF-3 impone sull'utilizzo dello standard SAML.

Per quel che riguarda gli elementi dei costrutti SAML:

- `ID` (attributo di diversi costrutti SAML): deve essere univoco, per esempio basato su un Universally Unique Identifier (UUID) (cfr. [15]) o su una combinazione *origine* + *timestamp*.
- `Version` (attributo di diversi costrutti SAML): deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata in ICAR.
- `<Issuer>` (elemento di diversi costrutti SAML): nell'ambito del modello INF-3 questo elemento deve obbligatoriamente essere presente e indica l'entità che ha emesso il messaggio SAML.
- `<RequestedAuthnContext>` (elemento di `<AuthnRequest>`): questo elemento può essere sfruttato nel caso in cui si voglia sempre avere la possibilità di specificare la forza delle credenziali richieste da un Service Provider a un Identity Provider.
- `<Conditions>` (elemento di `<Assertion>`): la presenza di questo elemento può essere resa obbligatoria e in particolare deve contenere gli attributi `NotBefore` e `NotOnOrAfter` che indicano opportunamente l'intervallo di validità dell'asserzione. Inoltre:
  - `<OneTimeUse>`: l'uso di questo elemento può influenzare eventuali politiche di caching adottate all'interno del modello architetturale del sistema federato di autenticazione;
- `<ProxyRestriction>`: anche in questo caso, l'uso di questo elemento può influenzare eventuali meccanismi di propagazione di asserzioni all'interno del modello architetturale del sistema federato di autenticazione.

5. BIBLIOGRAFIA

[1] ICAR-INF3, Sistema Federato Interregionale di Autenticazione: Modello architetturale di riferimento, versione 1.1, 2007.

[2] CNIPA, Sistema pubblico di cooperazione: Quadro Tecnico d'Insieme, versione 1.0, 14 ottobre 2005.
http://www.cnipa.gov.it/site/_files/SPCoop-QuadroInsieme_v1.0_20051014.pdf

[3] CNIPA, Sistema pubblico di cooperazione: Servizi di Sicurezza, versione 1.0, 14 ottobre 2005.
http://www.cnipa.gov.it/site/_files/SPCoop-ServiziSicurezza_v1.0_20051014.pdf

[4] CNIPA, Sistema pubblico di cooperazione: Servizi di Registro, versione 1.0, 14 ottobre 2005.
http://www.cnipa.gov.it/site/_files/SPCoop-ServiziRegistro_v1.0_20051014.pdf

[5] CNIPA, Sistema pubblico di cooperazione: Accordo di Servizio, versione 1.0, 14 ottobre 2005.
http://www.cnipa.gov.it/site/_files/SPCoop-AccordoServizio_v1.0_20051014.pdf

[6] OASIS Security Services (SAML) TC, Security Assertion Markup Language (SAML) V2.0 Technical Overview, Working Draft 10, 9 ottobre 2005.
http://www.oasis-open.org/committees/download.php/14361/sstc-saml-tech-overview-2.0-draft-10.pdf

[7] OASIS Security Services (SAML) TC, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005.
http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[8] OASIS Security Services (SAML) TC, Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005.
http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

[9] OASIS Security Services (SAML) TC, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005.
http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[10] OASIS Security Services (SAML) TC, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005.
http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

[11] OASIS Security Services (SAML) TC, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005.
http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[12]OASIS Security Services (SAML) TC, Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005.
http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf

[13]OASIS Web Services Security (WSS) TC, Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)
http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[14]OASIS Web Services Security (WSS) TC, Web Services Security: SAML Token Profile 1.1, OASIS Standard, 1 febbraio 2006.
http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf

[15]A Universally Unique IDentifier (UUID) URN Namespace (IETF RFC 4122), luglio 2005.
http://www.ietf.org/rfc/rfc4122.txt