# MODELLO DI GESTIONE FEDERATA DELLE IDENTITÀ DIGITALI (GFID)

*Versione 1.5.1*

DigitPA

# INDICE

# 1. PREFAZIONE

## 1.1. Autori

| | | |
|---|---|---|
| **Redatto da:** | Andrea Carmignani | RTI IBM-SI |
| **Verificato da:** | Nazzareno Ticconi | RTI IBM-SI |
| **Revisione a cura di:** | Stefano Fuligni | CNIPA |
| | Giovanni Olive | CNIPA |
| | Alessandro Vinciarelli | CNIPA |
| **Validato da:** | Francesco Tortorelli | CNIPA |
| **Approvato da:** | Commissione di coordinamento SPC | |

## 1.2. Modifiche Documento

| Descrizione Modifica | Edizione | Data |
|---|---|---|
| Emissione Prima Versione | 0.9 | 02/04/2008 |
| Adeguamento Format CNIPA | 1.0 | 18/07/2008 |
| Introduzione par. 4.1 SAML nel Cap 4 – Tecnologie e Standard di Riferimento | 1.1 | 06/08/2008 |
| Revisione interna | 1.2 | 04/09/2008 |
| Revisione specifiche SAML | 1.3 | 30/09/2008 |
| Adeguamento par. 10.4 Pubblica Amministrazione come IDP – Caratteristiche della Response | 1.4 | 03/12/2008 |
| Revisione impaginazione finale | 1.5 | 15/12/2008 |
| Adeguamento documentazione DigitPA | 1.5.1 | 26/07/2011 |

# 1.3. Riferimenti

| Codice | Titolo |
|---|---|
| | |

# 1.4. Acronimi e Definizioni

| Sigla | Descrizione |
|---|---|
| URI | Uniform Resource Identifier |
| WAYF | Where Are You From |
| GFID | Gestione Federata Identità Digitali |
| POC | Point of Contact |
| PA | Pubblica Amministrazione |
| SP | Service Provider |
| AARS | Attribute Authority Registry Service |
| ARS | Authority Registry Service |
| SPC | Sistema Pubblico di Connettività |
| SICA | Servizi di Interoperabilità, Cooperazione ed Accesso |
| CAD | Codice dell'Amministrazione Digitale |
| F-SSO | Federated Single Sign On |
| SAML | Security Assertion Markup Language |

# 2. OBIETTIVI E CONTESTO DI RIFERIMENTO

Il *Sistema Pubblico di Connettività e Cooperazione (SPC)* si colloca nel contesto definito dal Decreto legislativo n° 82 del 7 marzo 2005, pubblicato in G.U. del 16 maggio 2005, n. 112, recante il **"Codice dell'amministrazione digitale"** (C.A.D.) e successive modifiche ed integrazioni. Esso istituisce il SPC, definendone gli obiettivi, le funzionalità ed il modello di governance.

Il processo di regolamentazione normativa del SPC è proseguito nel tempo, arrivando alla pubblicazione del Decreto del Presidente del Consiglio dei Ministri n.1 del 1 aprile 2008, pubblicato in G.U. del 21 giugno 2008, n. 144, recante le **"Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettivita"**, previste dall'art. 71, comma 1-bis, del C.A.D, con il quale viene definito il quadro tecnico di riferimento per lo sviluppo dei servizi SPC e le regole per il funzionamento e l'adesione ai servizi SPC.

Parallelamente, come previsto dal modello condiviso di cooperazione applicativa per la P.A. italiana *SPCoop*, è stato avviato e portato a termine lo sviluppo dei *Servizi Infrastrutturali di interoperabilità, cooperazione ed accesso (SICA)* e del centro di gestione per l'erogazione di tali servizi (CG-SICA), infrastruttura condivisa a livello nazionale che abilita l'interoperabilità e la cooperazione applicativa fra le Amministrazioni pubbliche nonché l'accesso ai servizi applicativi da queste sviluppati e resi disponibili su SPC.

L'evoluzione dello scenario di riferimento e la disponibilità di servizi di infrastruttura per la cooperazione applicativa, hanno reso necessaria la definizione e pubblicazione di una serie di documenti che specificassero in dettaglio le modalità tecniche per l'interoperabilità e la cooperazione applicativa e l'utilizzo dei servizi SICA, come peraltro prevista dalle succitate regole tecniche.

Gli ultimi documenti tecnici relativi al SPCoop rilasciati alla fine del 2005, infatti, definivano un livello di condivisione che consentiva sia la stabilità del modello nel tempo rispetto al contesto organizzativo e tecnologico di riferimento, sia i necessari gradi di libertà per la sua implementazione; ciò a scapito del dettaglio tecnico necessario, invece, nel momento in cui si fa riferimento ad una specifica implementazione del modello ed a specifici servizi infrastrutturali.

I seguenti documenti sono stati redatti dal Raggruppamento Temporaneo di Imprese (IBM-Sistemi Informativi), incaricato dello sviluppo e dell'implementazione del Centro di Gestione dei servizi SICA, con la supervisione del CNIPA, ed hanno origine dalla documentazione sviluppata nel corso del progetto e nella fase di collaudo dei servizi stessi.

L'insieme di documenti prodotti specifica i modelli, le modalità, i dettagli tecnici di realizzazione, gestione ed utilizzo dei servizi SICA, le modalità di interfacciamento, le procedure qualificazione e gestione dei componenti infrastrutturali SPCoop, sulla base di quanto già previsto e definito nei documenti precedentemente condivisi e nel rispetto delle succitate regole tecniche.

| Titolo Documento |
|---|
| 1. Introduzione ai servizi SICA |
| 2. Specifiche di nomenclatura in SPCoop |
| 3. Specifiche di utilizzo del Servizio di Registro SICA |
| 4. Modalità di funzionamento del Client SICA |
| 5. Struttura dell'Accordo di Servizio e dell'Accordo di Cooperazione |
| 6. Descrizione delle specifiche di sicurezza negli Accordi di Servizio |
| 7. Aspetti di sicurezza applicativa nella cooperazione fra servizi |
| 8. Modalità di funzionamento del Catalogo Schemi e Ontologie |
| 9. Interfacce applicative tra Registro SICA generale e Registri SICA secondari |
| 10. Modalità di Qualificazione del Registro SICA secondario |
| 11. Modalità di Qualificazione della Porta di Dominio |
| 12. Schema d'interoperabilità IndicePA |
| 13. Guida ai servizi IndicePA |
| 14. Modello di Gestione Federata delle Identità Digitali (GFID) |
| 15. Modalità di accreditamento alla GFID |
| 16. Modello di funzionamento dell'Indice dei Soggetti |
| 17. Modello di funzionamento della Certification Authority |

## 2.1. Scopi del documento

Obiettivo del documento è la descrizione del modello di riferimento per la gestione delle identità digitali federate specificando entità, relazioni e scenari di autenticazione per accedere od erogare servizi in ambito federato all'interno dell'SPCoop.

Obiettivo del modello è definire differenti scenari e schemi di autenticazione nell'ambito della cooperazione applicativa e del SSO fra vari enti federati (F-SSO). Gli scenari descritti comprendono la cooperazione ottenuta tramite Web Services e tramite interazione Web Based. Il modello è aperto a differenti paradigmi di autenticazione (carte istituzionali CNS/CIE; identificativi e credenziali per soggetti non ancora dotati di carte istituzionali; ruoli associati alle persone), fornendo delle linee guida per l'identificazione e l'autenticazione di un utente SPCoop in ambito federato.

Il modello e gli schemi di autenticazione presentati nel documento, hanno l'obiettivo di bilanciare utilità, complessità e standard tecnologici, fattori fra loro differenti ed a volte antitetici ma tutti indispensabili per ottenere una soluzione che sia:

- basata sugli standard, il modello e la sua architettura devono basarsi sugli standard odierni ma devo essere in grado di accogliere le tecnologie emergenti una volta consolidate;
- capace di utilizzare prodotti commerciali dove possibile;
- scalabile;

- affidabile, l'architettura deve essere basata su best practices nazionali ed internazionali;
- con bassi impatti per l'utente finale;
- con bassi impatti a livello implementativo.

Il modello si basa sulla realizzazione di un framework cooperativo che integra policy (relazioni di "*trust*") ed infrastrutture tecnologiche fra le entità federate. Implementando il modello le Amministrazioni federate avranno accesso a molteplici nuove applicazioni tramite il riutilizzo delle credenziali e delle identità già utilizzate al loro interno, mantenendo inalterate le modalità con cui vengono gestite le identità dai singoli enti.

## 2.2. Note di lettura del documento

Nella definizione dei requisiti, delle specifiche e delle regole descritte nei documenti precedentemente indicati sono utilizzate le parole chiave DEVE, NON DEVE, OBBLIGATORIO, VIETATO, DOVREBBE, CONSIGLIATO, NON DOVREBBE, SCONSIGLIATO, POTREBBE, OPZIONALE che devono essere interpretate in conformità con [RFC2119]. In particolare:

- DEVE, OBBLIGATORIO significano che la definizione è un requisito assoluto, la specifica deve essere implementata, la consegna è inderogabile.
- DOVREBBE, CONSIGLIATO significano che in particolari circostanze possono esistere validi motivi per ignorare un requisito, non implementare una specifica, derogare alla consegna, ma che occorre esaminare e valutare con attenzione le implicazioni correlate alla scelta.
- PUÒ, OPZIONALE significano che un elemento della specifica è a implementazione facoltativa.
- NON DOVREBBE, SCONSIGLIATO significano che in particolari circostanze possono esistere validi di motivi per cui un elemento di specifica è accettabile o persino utile, ma, prima di implementarlo, le implicazioni correlate dovrebbero essere esaminate e valutate con attenzione.
- NON DEVE, VIETATO significano che c'e proibizione assoluta di implementazione di un determinato elemento di specifica.

## 2.3. Note sul Copyright

# 3. *APPROCCIO METODOLOGICO*

Lo scenario di riferimento alla base del modello è quello di un ente, più propriamente una Amministrazione Centrale od una Amministrazione locale, che offre ai propri utenti oltre ai suoi servizi specifici anche la possibilità di fruire di servizi offerti da altre Amministrazioni.

Il modello descritto trae ispirazione dagli standard ad oggi esistenti [SAML-Core, SAML-TechOv, WS-Security] oltre che dalle esperienze estere già in essere [E-auth_USGov], inoltre valorizza lo sforzo che le Regioni stanno compiendo nell'ambito del task INF-3 del del progetto ICAR nell'ambito della gestione federata delle identità digitali e della cooperazione applicativa.

L'approccio utilizzato parte inizialmente dalla definizione delle informazioni utilizzate nel modello per la gestione delle Identità digitali. A valle delle definizioni si introducono le entità logiche del modello assieme alle loro responsabilità.

Successivamente si descrivono gli scenari in ambito di interazione in modalità di cooperazione applicativa ed autenticazione federata degli utenti appartenenti ai soggetti cooperanti. Gli scenari descritti sono scenari generali, indipendenti dai possibili procedimenti amministrativi o dalle amministrazioni coinvolte. Le modalità di cooperazione che di volta in volta verranno individuate per portare a termine un determinato procedimento dovranno essere riportate ad uno degli scenari descritti nel modello.

# SEZIONE I – MODELLO CONCETTUALE GESTIONE FEDERATA IDENTITÀ DIGITALI

# 4. STANDARD E TECNOLOGIE DI RIFERIMENTO

## 4.1. SAML

Lo standard OASIS Security Assertion Markup Language (SAML) [SAML-TechOv] ha l'obiettivo di fornire una sintassi basata su XML e le relative regole di interpretazione per lo scambio di informazioni di sicurezza tra entità interagenti online. Tali informazioni sono costituite da asserzioni scambiate tra asserting party, (le entità che le emettono) e relying party (le entità che le richiedono e che possono farne uso per gli scopi di autenticazione e autorizzazione).

La specifica SAML, giunta alla versione 2.0, è organizzata in modo modulare, in particolare si basa sui alcuni "componenti" basilari (cfr. [SAML-TechOv]):

- **Asserzioni**: permettono di trasferire informazioni relative all'autenticazione e all'autorizzazione di utenti. La struttura delle asserzioni SAML è definita in [SAMLCore], sez. 2, e nei documenti correlati (in particolare la specifica per la descrizione del contesto di autenticazione 0).
- **Protocolli**: le asserzioni devono poter essere opportunamente scambiate tra le entità che interagiscono (per esempio un fornitore di servizi e un certificatore di identità). Per questo sono stati definiti opportuni protocolli per lo scambio di asserzioni, che avviene usualmente mediante un meccanismo di richiesta e risposta. I protocolli SAML sono definiti in, sez. 3.
- **Binding**: i protocolli stabiliscono la struttura delle informazioni che possono essere scambiate ma non determinano le specifiche modalità di trasporto. Per questo sono stati definiti opportuni binding che indicano come realizzare effettivamente in SAML lo scambio di informazioni di sicurezza attraverso determinati protocolli di trasporto (per esempio HTTP o SOAP). I binding SAML sono descritti in [SAML-Bindings].
- **Profili**: un profilo identifica una particolare combinazione di tipologie di asserzioni, protocolli e binding SAML atti a supportare un determinato caso d'uso ritenuto rilevante per l'interazione online tra entità. In [SAML-Profile], sez. 4, si trova la descrizione dei principali profili SAML che riguardano principalmente l'interazione con l'utente via browser web.

Inoltre, la specifica SAML prevede opportuni meccanismi di estendibilità (descritti in dettaglio caso per caso nei documenti citati) così come l'uso di metadati, cioè costrutti aventi una struttura standardizzata (cfr. Cap. 6) per la descrizione di alcune informazioni caratterizzanti le entità SAML a supporto delle interazioni tra loro.

# 5. MODELLO CONCETTUALE

Il contesto di riferimento del modello è il Sistema Pubblico di Connettività (SPC) ed in particolare il sistema pubblico di cooperazione (SPCoop). L'SPCoop è il sottosistema dell'SPC che comprende i sistemi di cooperazione applicativa e di interoperabilità e si basa sui seguenti principi:

- È un modello di cooperazione indipendente dai soggetti cooperanti in termini di asset informatici e tecnologici.
- Ogni soggetto cooperante mantiene la responsabilità dei propri servizi e dei dati da esso gestiti e custoditi.
- La cooperazione applicativa è regolata sulla base di accordi tra le parti.

Tali principi vengono tradotti in un architettura ed un modello organizzativo basato su elementi come:

- la cooperazione, che si basa su accordi servizio che descrivono l'accordo stipulato fra le parti riguardo l'erogazione/fruizione del servizio in questione.
- ogni amministrazione gestisce i flussi informativi appartenenti alla cooperazione applicativa tramite un unico "point of contact" indicato con il termine Porta di dominio dei Servizi Applicativi.

Risulta chiaro che per soddisfare tali necessità la cooperazione fra differenti Amministrazioni, o generici soggetti pubblici, deve essere supportata da una infrastruttura, non riconducibile a nessuna amministrazione specifica, in grado di supportare e facilitare la cooperazione fra amministrazioni. Tale componente è indicato con il termini SICA (Servizi di Interoperabilità, Cooperazione ed Accesso).

Il contesto di riferimento descritto trova nella gestione delle identità federate il modo più naturale per conciliare gli obiettivi di cooperazione fra differenti amministrazioni con la necessità di generare un basso impatto a livello implementativo ed infrastrutturale, così da mantenere gli investimenti operati sugli asset tecnologici da parte di ogni soggetto cooperante.

Il concetto di identità Federata è una delle evoluzioni più interessanti legate all'identity management, essa assimila ed estende alla cooperazione applicativa i concetti tipici del modello RBAC (Role Based Access Control), in cui i diritti di accesso ad una data risorsa sono basati sul ruolo posseduto dall'utente. Una gestione delle identità "*federata*" prevede in pratica la creazione di relazioni di fiducia tra realtà diverse per l'identificazione e l'autorizzazione degli utenti di una di esse ad accedere alle risorse governate da un'altra.

L'identità Federata è governata da un complesso di relazioni di trust appropriate che compongono un ambito fiduciario comune identificato in letteratura come "*Circle of Trust*". Il Circle Of Trust si basa su:

- l'accreditamento e la validazione all'interno del dominio federativo.
- enti che ricoprono il ruolo di certificatori/validatori delle identità.
- un insieme di accordi (policy) che comprendono un modello comune di cooperazione all'interno della federazione.
- la definizione di precise responsabilità nell'ambito della cooperazione.

Il principio è di creare un layer di astrazione che mascheri i sistemi, eventualmente già presenti, per la gestione delle identità. Attraverso esso aziende o amministrazioni diverse possano condividere le informazioni sulle identità e la sicurezza pur mantenendo inalterate le proprie soluzioni di gestione degli account utente e degli accessi applicativi (es:directory, metadirectory, infrastrutture a chiave pubblica, soluzioni di controllo accessi e SSO).

A livello macro all'interno della federazione l'utente che vuole fruire di un servizio applicativo deve in primo luogo autenticarsi presso il proprio dominio (dominio fruitore) presentando le sue credenziali. Il dominio fruitore, in caso di verifica positiva, emette un messaggio che garantisce l'identità dell'utente verificando i privilegi (ruolo) associati all'utente che sta chiedendo l'accesso.

Il dominio fruitore terminate le verifiche invia le informazioni al dominio erogatore del servizio applicativo dove vengono elaborate. Il compito del dominio erogatore è garantire che l'accesso dell'utente sia coerente con le procedure e le politiche locali.

Da una prima descrizione sommaria della federazione si può notare come accanto alla nozione di identità si accosta ora la nozione di ruolo come nuovo discriminante per richiedere o erogare un servizio.

Per garantire il livello di integrazione descritto serve necessariamente un sistema standard per passare le informazioni di sign-on ed eventualmente di autorizzazione fra i due domini federati. Il framework SAML nasce per indirizzare tali esigenze.

Come mostrato in figura 1 i macro scenari per un utente sono:

1. Utilizzo di un'applicazione all'interno del proprio dominio (evidenziato in giallo), è il tipico caso di un ente che ha il proprio sistema di gestione di Identity e Access Management. In questo caso non c'è cooperazione.
2. Nomadicità (evidenziato in grigio), l'utente richiede direttamente tramite il suo browser un'applicazione federata appartenente al dominio erogatore. Il richiedente viene diretto presso il proprio dominio per potersi autenticare e solo dopo può fruire dei servizi richiesti presso il dominio erogatore.
3. Utilizzo di un'applicazione federate tramite web services (evidenziato in nero), l'utente si è autenticato presso un'applicazione locale che coopera con una applicazione appartenente ad un'altra Amministrazione.

Nel caso 2 bisogna far interagire i domini federati tramite un bridge (indicato il figura come Federation Gateway) con l'obiettivo di :

- trasformare le informazioni da veicolare all'interno della federazione (l'identità ed i ruoli) in linguaggio SAML così da poter essere recepite dalla controparte e tradotte nel linguaggio interno adottato per controllare gli accessi alle applicazioni;
- disaccoppiare l'amministrazione dalla complessità della federazione, l'Amministrazione deve limitarsi ad interagire con il FG tramite pochi comandi SAML.

Nel caso 3 invece si utilizza la Porta di Dominio, che similmente al FG è il point of contact per i flussi informativi appartenenti alla cooperazione applicativa.

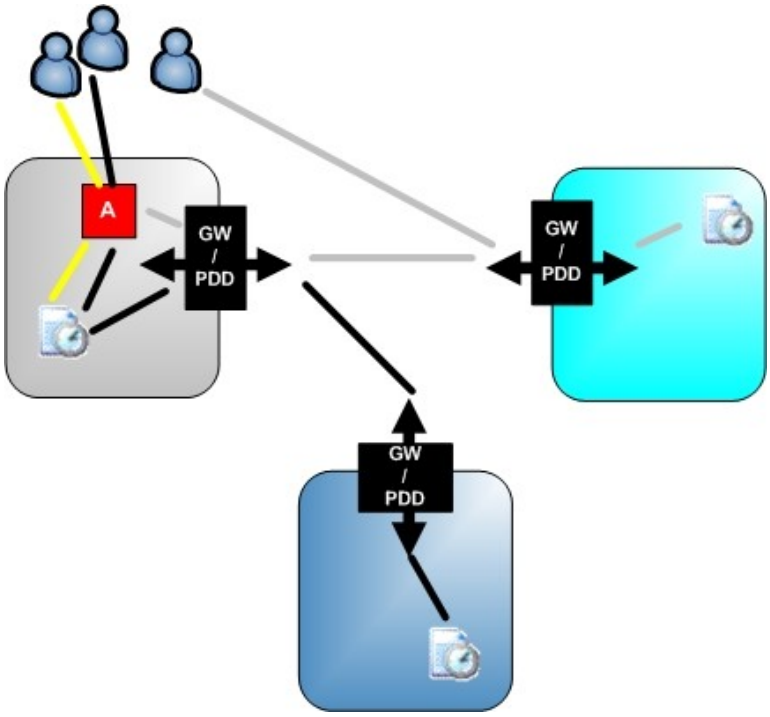



**Figura 1: Possibili Interazioni fra membri di una federazione**

Il modello, anche se inizialmente affronta la problematica ad un livello più astratto, prende sin da subito come riferimento il Framework SAML come metodo per comunicare le asserzioni di identificazione ed autorizzazione fra i domini federati.

## 5.1. Definizioni del modello

La gestione e la comunicazione di informazioni che confermino, in modo univoco, l'identità ed il ruolo ricoperto da un generico utente è alla base del modello per la gestione federata delle identità digitali. Il paragrafo introduce le principali definizioni ritenute di rilievo per il modello.

**Identità:** L'insieme delle caratteristiche essenziali ed uniche in grado di identificare un soggetto.[Abelson]

**Autenticazione:** il processo in cui si verifica la corrispondenza fra l'identità dichiarata e le credenziali fornite. La Carta d'identità elettronica [CIE] e la Carta nazionale dei servizi [CNS] sono l'unico strumento di autenticazione previsto dal Codice dell'Amministrazione Digitale (CAD) per l'accesso ai servizi web erogati dalle Pubbliche Amministrazioni. [DlgAmmDi].

**Attributo**: tutte le informazioni relative all'utente, la macchina o il servizio, necessarie a delinearne le caratteristiche all'interno di uno o più domini applicativi. Solitamente sono rappresentati da una coppia <nome attributo,valore attributo> .

**Profilo Utente:** lista di attributi associati ad un singolo utente. Descrivono caratteristiche come: gruppi; ruolo; professione; eventuale iscrizione ad un albo. Gli attributi possono far riferimento a domini fra loro disgiunti.

**Ruolo**: sottoinsieme di attributi del Profilo Utente che individuano il compito dell'utente all'interno dell'organizzazione. Esempi di ruolo sono: Ufficio XXX; Livello Dirigente.

**Profilo del Servizio**: Insieme di regole, relative ad un'applicazione, che ne definiscono le modalità di utilizzo da parte degli utenti. Queste regole possono essere espresse dall'insieme di risorse e degli attributi (*Ruolo*) che ne regolano l'accesso.

## 5.2. Definizione domini del modello

Concettualmente in una federazione si possono evidenziare differenti domini informatici. Ogni dominio è caratterizzato da una o più entità; ogni entità ha un ben determinato ruolo e chiare responsabilità.

Si definisce con il termine dominio informatico il sistema informativo di una amministrazione stabilendone il ruolo e la responsabilità all'interno del modello federato.

Tramite una descrizione di alto livello vengono identificati i domini che compongono il modello. Ogni sotto sezione approfondisce le caratteristiche dei singoli domini assieme alle entità che ne fanno parte.

I domini caratterizzanti il modello sono:

- Dominio fruitore del servizio.
- Dominio dei servizi erogabili da una Amministrazione.
- Dominio dei servizi infrastrutturali.

### 5.2.1. Dominio Fruitore del servizio

Il dominio fruitore indica il dominio da cui proviene la richiesta del servizio ed è composto dall'insieme dei soggetti che possono fruire dei servizi applicativi. Tali soggetti si possono dividere in:

- Entità persona (End User).
- Entità non persona (Applicazioni): tutte le entità catalogabili come applicazioni informatiche e che non ricadono nell'entità precedente.

### 5.2.2. Dominio dei servizi erogabili da una Amministrazione

Il dominio dei servizi erogabili da una Amministrazione descrive le entità logiche e quindi i possibili ruoli che una amministrazione può ricoprire. Ogni entità offre dei ben determinati servizi.

Nel dominio dei servizi erogabili da un'Amministrazione sono presenti tutte le entità in grado di verificare gli attributi o l'identità di un membro del dominio fruitore del servizio. Come attributi si intendono sia gli attributi atomici che aggregati, un esempio di attributo aggregato è il profilo. Le entità del dominio sono responsabili della creazione e gestione delle identità e dei ruoli oltre a fornire il servizio autenticazione alle entità del dominio fruitore.

Il dominio comprende:

- Service Provider, responsabile di fornire il servizio richiesto ad uno o più membri della federazione.
- Identity Provider, responsabile di mantenere e gestire le informazioni relative all'identità dell'End User.
- Attribute Authority, ente designato a validare tutti o parte degli attributi componenti il profilo di un generico utente.
- External Attribute Authority, sito non appartenente alla federazione che fornisce servizi di validazione per gli attributi esterni alla federazione (es: Ordini Professionali, Notariato, Comune di Residenza).
- Profile Authority, ente preposto alla memorizzazione e gestione dei profili utente. Si occupa di validare gli attributi presenti nel profilo interrogando le Attribute Authority di pertinenza.

### 5.2.3. Dominio dei servizi infrastrutturali

Le entità descritte interagiscono secondo delle regole di cooperazione e di gestione federata delle identità ben definite ed avvalendosi di servizi offerti a livello infrastrutturale. Il dominio dei servizi infrastrutturali comprende:

- authority registry: registro contenente tutti gli Identity Provider e le Profile Authority appartenenti alla federazione e che godono della fiducia di tutti i membri interni alla federazione;
- attribute authority registry: registro contenente la relazione fra ruolo(attributo) ed il suo certificatore, sia essa una Attribute Authority interna che esterna.

# 5.3. Entità astratte del modello

La sezione ha l'obiettivo di approfondire, per ogni dominio, la descrizione delle entità evidenziando le loro responsabilità e le relazioni esistenti.

Poiché si descrive un modello concettuale sin da ora si preferisce affiancare ad ogni entità il corrispettivo individuato nello standard SAML [SAML-Glos] così da permettere un graduale passaggio da un modello concettuale ad modello logico.

## *5.3.1. Entità del dominio Fruitore del servizio*

### 5.3.1.1. Entità Persona

L'entità persona, nel seguito indicate semplicemente come "*End User*", individua tutti gli utenti appartenenti ad una Amministrazione Centrale, una Amministrazione locale o semplicemente cittadini, che, tramite il sistema federato, accedono ai servizi offerti da altri enti differenti da quello di appartenenza. L'End User è in grado di fruire dei servizi esposti da un'Amministrazione un generico web browser.

### 5.3.1.2. Entità non Persona

L'entità non persona, nel seguito indicate genericamente "*Applicazione*" o "*Servizio di Front End*", descrive tutte le applicazioni software, siano essi applicativi di front-end, di back end o batch che, tramite il sistema federato, fruiscono di servizi offerti tramite cooperazione applicativa (es: tramite Web Services).

Lo standard SAML identifica entrambe le entità con il termine "*Principal*". Inoltre il web browser utilizzato dell'End User viene indicato con il termine User Agent (cfr.SAML-Glos).

## 5.3.2. Entità del dominio dei servizi erogati da una Amministrazione

### 5.3.2.1. Service provider

Identifica l'entità che a fronte di asserzioni autorizza o meno l'accesso ad un servizio erogato da un'Amministrazione verso le entità del dominio fruitore . Il Service Provider, nel seguito indicato anche come "*Servizio di Back End*" eroga il servizio a valle di asserzioni identificative e di ruolo provenienti da un membro del dominio certificatore. Il service provider è responsabile oltre che dell'erogazione del servizio anche della gestione delle autorizzazioni e dell'auditing.

**Federation Gateway**

Il Federation Gateway è una componente logico del Service Provider, è il singolo punto di contatto (P.O.C. Point of Contact) per tutte le richieste di accesso via web alle risorse offerte.

Disaccoppia i servizi di autorizzazione del Service Provider dalla complessità della federazione offrendo funzionalità di "Proxy SAML" o "SAML Gateway". In questo modo il Service Provider vede il sottosistema del Federation Gateway come l'unico IDP con cui interagire.

L' FG ha il compito di fornire all'End User la lista dei possibili enti certificatori tramite cui ottenere le certificazioni di identità e di ruolo necessarie per fruire dei servizi esposti dall'SP.

**Policy Enforcement Point**

Il componenente logico Policy Enforcerment Point si occupa di applicare le policy di autorizzazione, prima di concedere l'accesso ai singoli servizi esposti. Altre operazioni svolte sono: eventuale mapping degli attributi provenienti dall'esterno con gli attributi interni (Identity & Attribute mapping), auditing ed interfacciamento con le eventuali soluzioni di Identity & access management adottate internamente.

Lo standard SAML non identifica un'entità specifica per mansioni descritte a carico del federation gateway, si può comunque associare la generica entita SAML Authority, una entità capace di erogare o consumare asserzioni SAML utilizzata in modalità proxy (cfr.[SAML-Glos]).

L'entita Service Provider nella sua interezza è identificata nello standard SAML con il termini omonimo (cfr. [SAML-Glos])

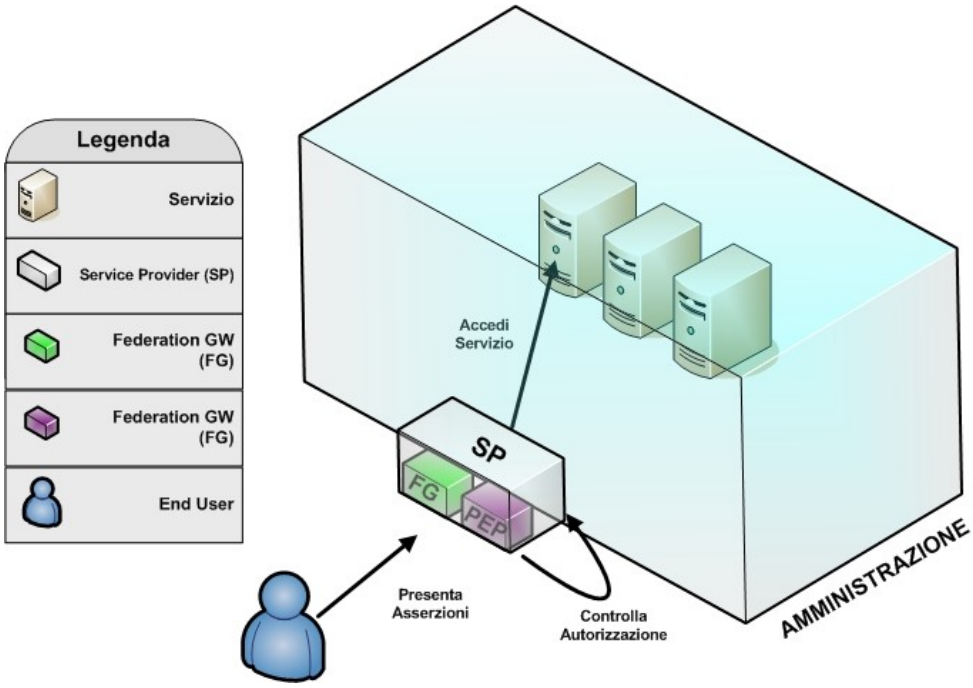



**Figura 2: Modalità di interazione fra l'end user ed servizi offerti dal Service Provider tramite il Federation Gateway**

## *5.3.3. Entità Validatrici*

All'interno del Dominio dei servizi erogati da una Pubblica Amministrazione sono comprese anche le entità responsabili di validare le informazioni inerenti i membri della federazione quali l'identità, il ruolo o altri specifici attributi. Sulle loro asserzioni di validità delle informazioni si basa l'accesso e l'autorizzazione ai Service Provider che erogano i servizi. Le entità validatrici si possono suddividere in 4 tipologie.

### 5.3.3.1. Identity Provider

Entità della federazione incaricata di gestire le informazioni relative all'identità dei membri della federazione. L'identity Provider fornisce il servizio di Autenticazione per l' Entità Persona o più genericamente al Dominio Fruitore del Servizio.

Nella categoria degli Identity Provider ricadono tutti i servizi di identity management presenti nella federazione. Un esempio concreto di Identity Provider può essere una Certification Authority, od un Directory su cui sono memorizzate le UID e password degli utenti. Gli identity Provider svolgono il ruolo di certificatori di Identità e quindi di "*garanti*" all'interno di un processo di autenticazione

### 5.3.3.2. Profile Authority

La Profile Authority è l'entità incaricata della gestione e manutenzione dei profili utente. La Profile Authority può essere interrogata anche remotamente. Possono esistere più Profile Authority.

Riprendendo la definizione presentata nel paragrafo 3.1, definiamo come profilo l'insieme delle informazioni inerenti una generica entità appartenente al dominio Fruitore del Servizio. All'interno del profilo ricadono informazioni concernenti l'anagrafica, quali nome, cognome e domicilio; le mansioni ricoperte a livello lavorativo come capo ufficio, direttore o dirigente; oppure qualifiche e peculiarità proprie dell'individuo come, ad esempio, l'iscrizione ad un albo.

Il profilo è composta da n-ple ad esempio così strutturate:

- Nome Attributo.
- Valore Attributo.
- Riferimento logico dell'Authority in grado di validare l'attributo.

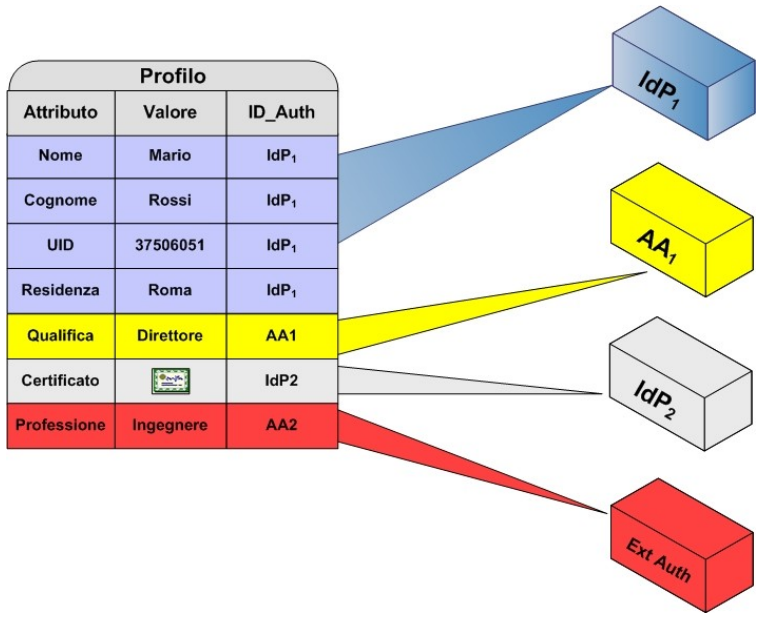



**Figura 3: Esempio di un possibile profilo gestito dalla Profile Authority. Si noti come le varie informazioni possono essere certificate differenti Authority**

La profile Authority oltre al compito di gestire i profili ha un ruolo attivo nel processo di F-SSO. La PA è incaricata di gestire l'autenticazione dell'End User presso uno degli IdP federati e di preparare il portafoglio di asserzioni a valle della scelta del profilo da parte dell'End User. Le asserzioni presenti nel portafoglio saranno poi consumate per accedere ai servizi erogati da una Amministrazione

#### 5.3.3.3. Attribute authority

Entità designata a certificare tutti o parte degli attributi componenti il profilo di un generico utente. Il ruolo di Attribute Authority può essere svolto anche da entità esterne alla federazione (vedi definizione successiva). Un esempio di attributo può essere il titolo di studio, l'iscrizione ad un albo, il ruolo locale ad un'amministrazione, la residenza. Ogni Attribute Authority è responsabile per la certificazione di un determinato attributo o sottoinsieme di attributi. L'attribute authority può svolgere l'attività di certificatore di ruolo. Un'attribute Authority appartenente alla federazione viene anche indicata con il termine Internal Attribute Authority per differenziarla delle External Attribute Authority descritte nel paragrafo successivo.

#### 5.3.3.4. External Attribute Authority

Le Authority esterne sono siti non federati (es: non appartenenti all'SPCoop). Forniscono servizi applicativi limitati e ben definiti come, ad esempio, la certificazione di uno o più attributi di cui sono responsabili e che non sono locali alla federazione.

Lo standard SAML indica l'identity provider e l'attribute authority con il termine omonimo (cfr.[SAML-Glos]). L'External Attribute Authority è riconducibile ad un'attribute authority esterna alla federazione. Differentemente la Profile Authority si può identificare con il termine generico di SAML Authority (cfr. [SAML-Glos]).

### *5.3.4. Servizi infrastrutturali*

La federazione si basa sul concetto di Trust, ossia che le asserzioni prodotte da un'authority e scambiate con altre entità dei domini sono affidabili. L'authority è il garante di tali informazioni.

E' importante quindi l'esistenza di un ente "*super-partes*" che abbia un rapporto di trust con tutte le entità della federazione, in grado di asserire quali sono le authority "*credibili*", ossia parte della federazione, e che possono certificare determinati attributi.

Il servizi infrastrutturali hanno lo scopo di soddisfare la necessità di un garante mettendo a disposizione della Federazione servizi mirati a fornire le informazioni sulle authority "*trustate*" all'interno della Federazione.

#### 5.3.4.1. Authority Registry (AR)

Entità riconosciuta a livello di federazione che permette di rintracciare in modo univoco i riferimenti agli Identity Provider e le Profile Authority appartenenti alla Federazione. L'Authority Registry per ogni Authority, sia essa un IdP o PA, contiene la descrizione, l'URI associata oltre ad eventuali informazioni aggiuntive. Sulle informazioni contenute all'interno dell'AR si basano le entità che erogano servizi per verificare l'identità degli End User o per ridirigere questi ultimi verso la Profile Authority di competenza.

### 5.3.4.2. Attribute Authority Registry (AAR)

Registro contenente la relazione fra ruolo interno od esterno alla federazione e URI del suo certificatore (Attribute Authority di competenza). Le informazioni contenute all'interno dell'AAR permettono ai servizi di verificare gli attributi e completare cosi il portafoglio di asserzioni necessario per ottenere un generico servizio applicativo.

### 5.3.4.3. Authority Registry Service (ARS)

Il Servizio nasce per soddisfare l'esigenza di fornire ai membri della federazione la lista completa di tutti gli IdP o le Profile Auhority federate assieme alle loro URI. Il servizio si basa sulle informazioni presenti all'interno dell'Authority Registry.

### 5.3.4.4. Attribute Authority Registry Service (AARS)

Il servizio fornisce la lista completa delle attribute authority, sia "internal" che "external" alla federazione, assieme alle loro URI. Il servizio si basa sulle informazioni presenti all'interno dell'Attribute Authority Registry.

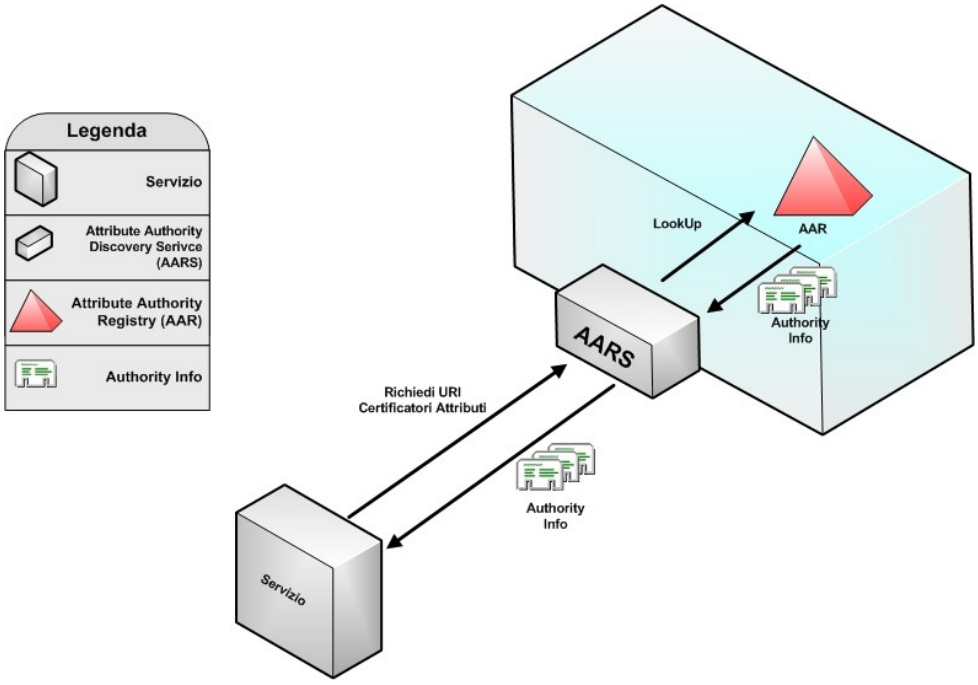


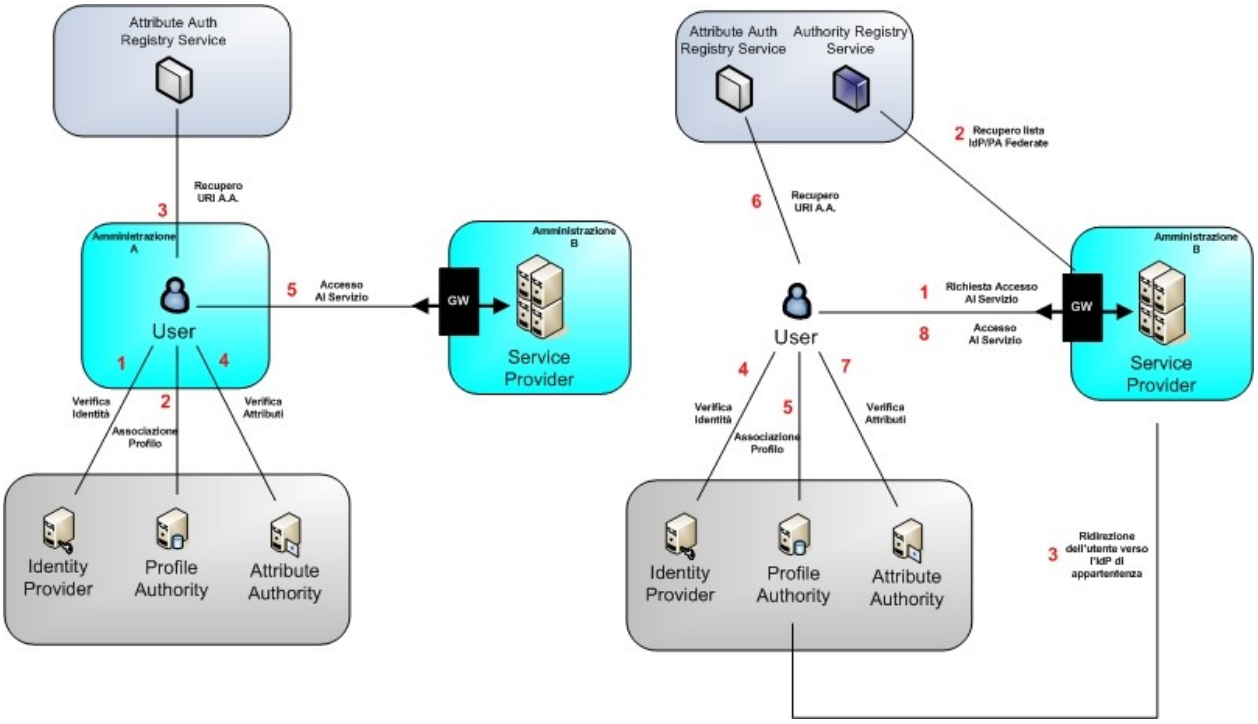

**Figura 4: Modalità di interazione fra il generico servizio e l'Attribute Authority Registry Service**

# 5.3.5. Modalità di interazione fra i servizi federati

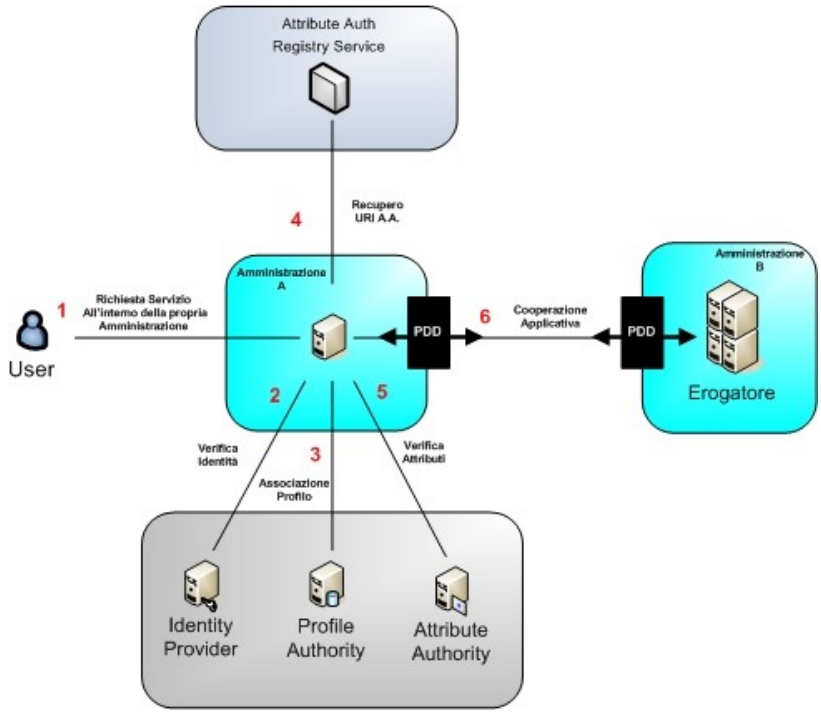
Esistono due modalità principali di accesso ai servizi erogati da un'Amministrazione. La prima tramite il web browser verso il SAML Gateway (nel modello il Federatoin Gateway sottosistema dell'SP); la seconda invece tramite le Porte di Dominio nel caso di cooperazione applicativa fra l'applicazione denominata di front end e l'applicazione che eroga il servizio denominata di back end.

Nel caso di interazione tramite web browser, l'entità "End User" interagisce con i membri del dominio Certificatori, principalmente con l'Identity Provider e la Profile Authority. L'Authority Registry Service viene utilizzato principalmente qualora l'utente si presenti direttamente senza essere stato precedentemente autenticato dal proprio IDP di competenza.

Nel caso di cooperazione applicativa tramite web services l'entità coinvolta del dominio Fruitore del Servizio è l'entità non persona "*Applicazione*". Tale entità interagisce con le authority presenti nel dominio dei certificatori per verificare gli attributi di chi richiede il servizio cooperativo e ad esempio non presenti nel portafoglio di asserzioni presentato. Qualora ci siano degli attributi da verificare contatta l'Attribute Authority Service per reperire il riferimento dell'authority da contattare.




**5a)** **5b)**




**5c)**

**Figura 5: I domini, le entità e le relazioni all'interno del modello di Gestione Federata delle Identità Digitali. Utilizzo di una applicazione federata via web (5a), nomadicità (5b) ed utilizzo di un'applicazione federata tramite cooperazione applicativa**

## 5.4. Scenari di cooperazione

Come accennato le interazioni fra i vari attori (utenti e servizi) si articolano su due livelli. Il primo livello d'interazione avviene tramite User Agent, il generico Web Browser, il secondo, in un'ottica di cooperazione applicativa, tramite web services.

Si introducono gli scenari volti a permettere la cooperazione applicativa, illustrando le modalità con cui l'identità dei richiedenti il servizio viene accertata e come sono effettuate le verifiche di autorizzazione opportune.

Gli scenari sono divisi nelle seguenti categorie:

- Collaborazione applicativa fra Pubbliche Amministrazioni, indica gli scenari riferiti alla cooperazione fra le applicazioni erogate dalle Pubbliche Amministrazione. Più in generale si riferisce a quegli scenari in cui un'applicazione ha la necessità di accedere a dei servizi offerti da una applicazione appartenente ad un dominio differente dal proprio.

- Autenticazione Federata per gli End User o F-SSO, contempla gli scenari che coinvolgono direttamente gli End User.

Ogni scenario individuato è caratterizzato da:

- Obiettivo dello scenario.
- Descrizione.
- Identificazione delle entità coinvolte per ogni modello, e loro responsabilità.
- Descrizione delle modalità di interazione fra le entità tramite una descrizione di alto livello delle interfacce e statement SAML associati.

### *5.4.1. Il profilo utente e la cooperazione*

Per agevolare la comprensione degli scenari si approfondisce la descrizione del profilo utente e di come è articolata la sua costruzione. Il profilo utente svolge un ruolo basilare per la corretta autorizzazione all'atto dell'erogazione del servizio da parte del service provider.

Il profilo è una lista di attributi associati all'utente assieme agli identificativi dei corrispondenti enti validatori. Il ruolo primario della Profile Auhority è gestire e fornire tali profili su richiesta; la certificazioni degli attributi invece rimane a carico delle Attribute Authority.

Per gestire il profilo la Profile Authority mette a disposizione delle funzioni per la creazione del profilo associato ad un utente assieme alle funzioni necessarie per impostare i valori degli attributi e le authority competenti per la successiva validazione.

Nel documento e negli scenari esposti si assume che:

- Possono esistere più Profile Authority all'interno della federazione.
- Un utente può afferire a più Profile Authority.
- Un utente può avere più profili, non necessariamente sulla stessa PA, o se necessario può avere viste multiple.

L'associazione fra l'utente ed il profilo avviene solitamente al momento della richiesta di un servizio. All'interno del processo di identificazione e di verifica del ruolo necessario per accedere il servizio si evidenziano dei passi fondamentali:

1. l'utente deve selezionare una PA fra quelle disponibili all'interno della federazione.
2. presso la PA selezionata l'utente deve scegliere l'IdP su cui vuole autenticarsi prima di recuperare il profilo o la vista che vuole utilizzare.
3. a valle dell'autenticazione presso l'IdP l'utente può selezionare il profilo desiderato presso la PA;
4. la PA interroga le Attribute Authority presenti nel profilo selezionato per preparare il portafoglio delle asserzioni.
5. completato il portafoglio di asserzioni l'utente si può richiedere un servizio.

6. l'autorizzazione avviene tramite la verifica degli attributi del profilo rispetto alle policy di autorizzazione locali al servizio.

### 5.4.2. Collaborazione applicativa fra Pubbliche Amministrazioni

Lo scenario tipico di collaborazione fra Pubbliche Amministrazioni è la cooperazione applicativa fra una entità "*Applicazione*" appartenente al dominio Fruitori del Servizio denominata "*Servizio di front end*" ed una entità "*Service Provider*" del dominio *Erogatore del Servizio* identificato come "*servizio di back end*".

La figura sottostante riprende i macro scenari introdotti inizialmente, evidenziando in rosso lo scenario a cui si fa riferimento:

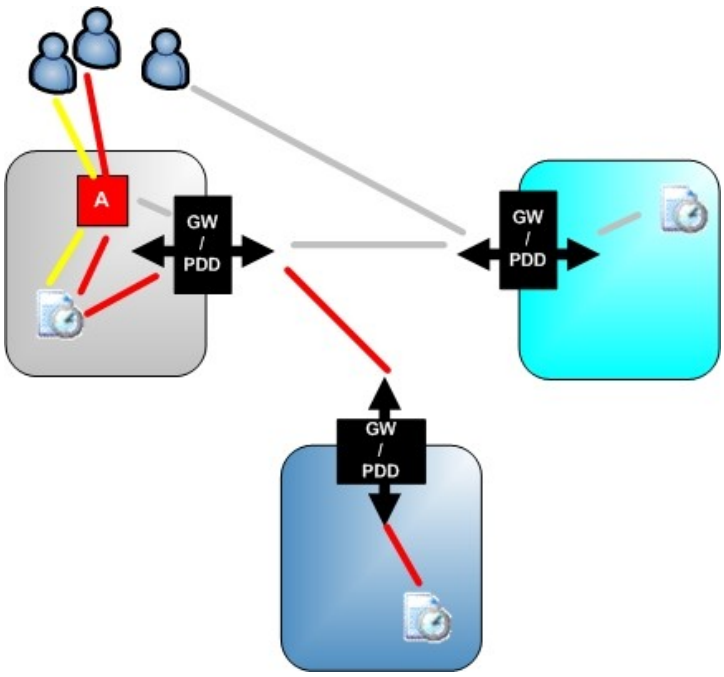



**Figura 6: Macro entità coinvolte nella Collaborazione fra Pubbliche Amministrazioni**

#### 5.4.2.1. Scenario 1: cooperazione applicativa di base tramite web services

Si presume che l'utente sia già autenticato presso il servizio di front end ed autorizzato tramite gli attributi presenti nel profilo utente. Il servizio di front end per soddisfare la richiesta dell'utente ha bisogno di un servizio offerto in ambito cooperativo dal servizio di back end.

Il servizio di front end recupera dal portafoglio delle asserzioni tutte le asserzioni necessarie a richiedere il servizio. Recuperate tali informazioni inoltra la richiesta al servizio di back end tramite web services. Il servizio di back end ricevute le asserzioni può verifica l'autorizzazione (Policy Enforcement) ed eroga il servizio.

La tipologia di informazioni che il servizio di front end deve reperire sono descritte all'interno della parte specifica dell'accordo di servizio.

L'accordo di Servizio definisce le prestazioni del servizio e le modalità di erogazione/fruizione, del servizio, le interfacce di scambio dei messaggi tra erogatore e fruitore, i requisiti di qualità di servizio dell'erogazione/fruizione, ed i requisiti di sicurezza dell'erogazione/fruizione. Inoltre mantiene un riferimento all'ontologia/schema concettuale che definisce la semantica dell'informazione veicolata dal servizio [SPCoop-AS].

In questo scenario non vengono utilizzati i servizi infrastrutturali a supporto della federazione

Le entità coinvolte sono:

- Servizio di Front End.
- Servizio di Back End.

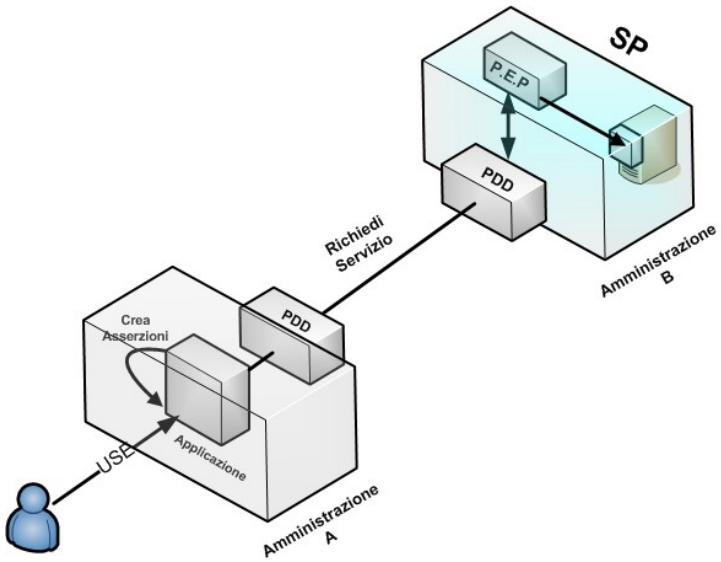



**Figura 7: Cooperazione Applicativa di Base. Entità coinvolte nello scenario e loro interazioni**

La figura mostra come il servizio di front end debba reperire tutte le informazioni descritte all'interno della parte specifica di sicurezza dell'accordo di servizio necessarie per contattare il servizio di back end. Il servizio di back end deve limitarsi alla verifica del portafoglio di attributi per autorizzare o meno la fruizione del servizio.

Il diagramma di flusso successivo descrive le interazioni fra le entità e delinea ad alto livello le interfacce necessarie all'implementazione dello scenario. Nel diagramma non vengono prese in considerazione le porte di dominio:

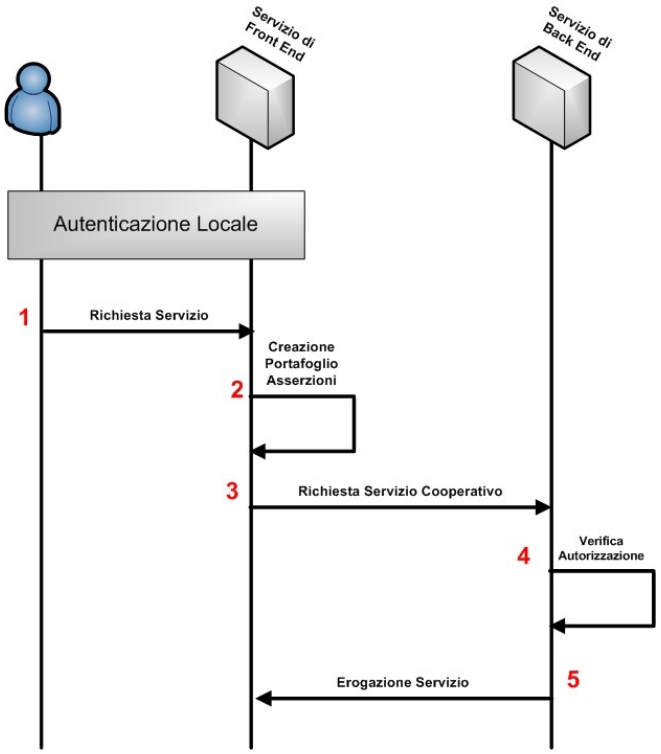



**Figura 8:Cooperazione Applicativa di base. Diagramma di Flusso**

| Passo | Descrizione |
|---|---|
| 1 | L'end user richiede un servizio all'applicazione locale. |
| 2 | L'applicazione di front end per soddisfare la richiesta dell'utente ha bisogno di un servizio offerto in ambito cooperativo dall'applicazione di back end. Prepara il portafoglio di asserzioni. |
| 3 | Il servizio di front end richiede il servizio tramite web services al Service Provider. |
| 4 | L'SP ricevuta la richiesta verifica il portafoglio di asserzioni per permettere l'eventuale accesso al servizio. |
| 5 | In caso affermativo eroga il servizio. |

**Scheda riepilogativa:**

| | |
|---|---|
| **ID Scenario** | **Scenario 1 – WS-basic** |
| **Obiettivo** | Cooperazione applicativa fra una entità "*applicazione*" appartenente al dominio "Fruitori del Servizio" denominato servizio di front end ed una entità "*'applicazione*" del dominio "Erogatore del Servizio" identificato come servizio di back end. |
| **Descrizione** | Il servizio di front end per soddisfare la richiesta dell'utente ha bisogno di cooperare con il servizio di back end. Il servizio di front end raccoglie tutte le asserzioni necessarie, completato il portafoglio di asserzioni inoltra la richiesta al servizio di back end tramite web services. |
| **Entità Coinvolte** | Servizio di Front End; Servizio di Back End. |
| **Pre Requisiti** | L'utente è già autenticato presso il servizio di front end. Ha già interagito con l'identity provider per l'identificazione e con la profile authority per l'autorizzazione. |
| **Macro interfacce** | Servizio di Front End<br>• *<List SAMLAttributeStmnt> User_portfolio* Creazione_Portafoglio Asserzioni (*<List> Attributi, <ID> ID_User*): dato un utente ID_User ed una lista di attributi restituisce il portafoglio di attributi necessari a richiedere il servizio.<br><br>Servizio di Back End<br>• Richiesta_Servizio(<ID_serv> *ID_Servizio, <List> Param, < List SAMLAttributeStmnt> User_portfolio, <ID> ID_User*): a fronte di una richiesta pervenuta dal servizio ID_Servizio contenente l'Id_User dell'utente ed il suo portafoglio di asserzioni associato User_porfolio, l'applicazioni di back end eroga il servizio a valle dei controlli autorizzativi. |

**Table 1: Scheda Riepilogativa dello scenario di cooperazione applicativa base**

### 5.4.2.2. Scenario 2: cooperazione applicativa tramite web services con verifica di attributi presso il Servizio Front End

Similmente allo scenario precedente anche in questo caso si descrive la cooperazione applicativa fra un "*Servizio di front end*" ed un "*Servizio di back end*". La differenza è che in questo scenario si prevede la necessità di interpellare una o più Attribute Authority (Internal/External) per certificare degli attributi non presenti nel portafoglio delle asserzioni presentato dall'utente ma necessari per richiedere il servizio.

Si presume che l'utente sia già autenticato presso il servizio di front end e che quest'ultimo abbia già ricevuto il portafoglio delle asserzioni associato al profilo selezionato dall'end user.

Il servizio di front end per soddisfare la richiesta dell'utente ha bisogno interagire in ambito cooperativo con il servizio di back end.

Il servizio di front end preleva dal portafoglio delle asserzioni quelle necessarie per richiedere il servizio di back and. Prima di richiedere il servizio verifica se c'è la necessità di attributi aggiuntivi non presenti nel portafoglio delle asserzioni.

Per verificare gli attributi aggiuntivi contatta l' Attribute Authority Registry Service (AARS) in modo da reperire le URI delle Attribute Authority presso cui validare gli attributi aggiuntivi. Completato il set delle asserzioni necessarie invia la richiesta al servizio di back end tramite web services. Il servizio di back end ricevuto il portafoglio delle asserzioni può verificare l'autorizzazione (Policy Enforcement) ed erogare il servizio.

Le entità coinvolte sono:

- Servizio di Front End.
- Attribute Authority (Internal/External).
- Servizio di Back End.
- Servizio di AARS e AAR.

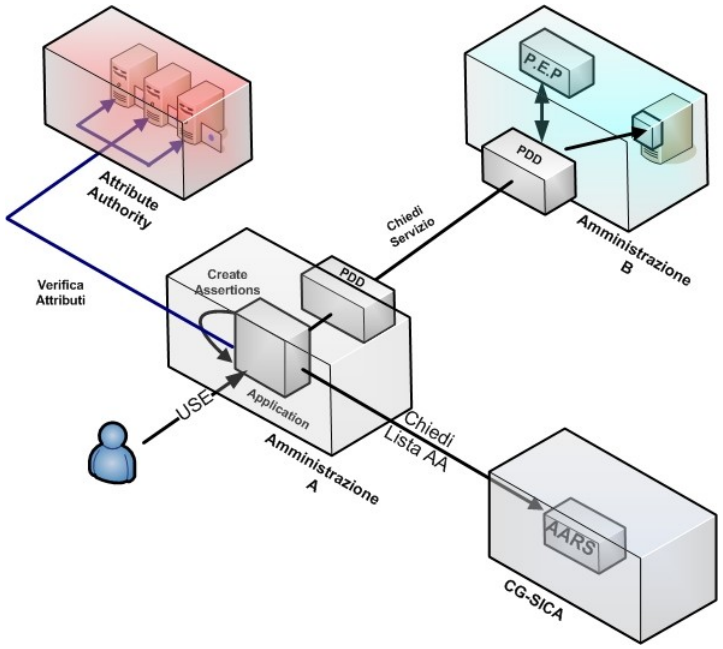



**Figura 9: Cooperazione Applicativa: Il servizio di front end certifica gli attributi esterni.**

**Entità coinvolte e loro interazioni**

Il diagramma di flusso descrive le interazioni fra le entità e ne delinea ad alto livello le interfacce:

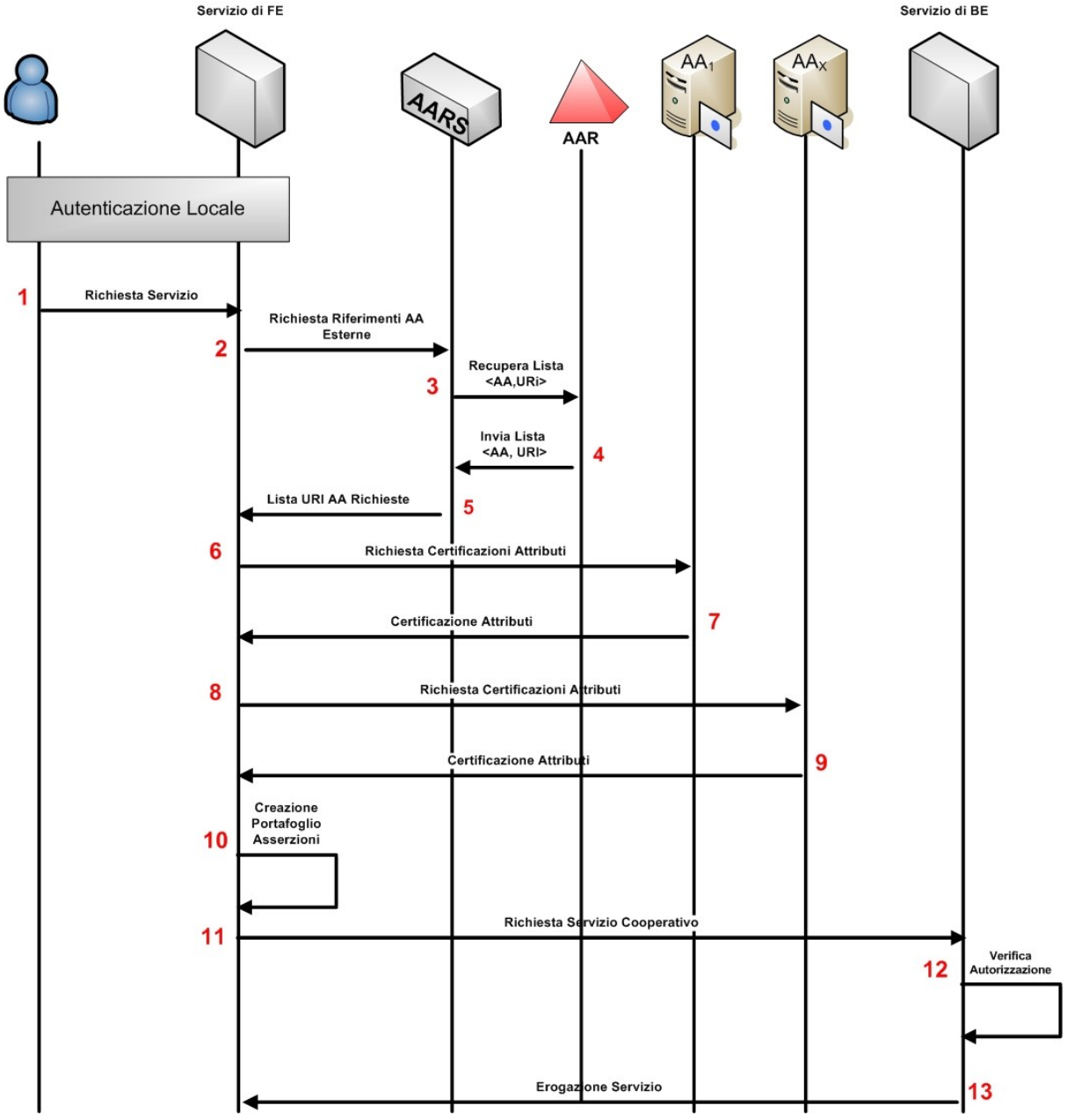



**Figura 10: Cooperazione Applicativa: Il servizio di Front End certifica gli attributi esterni.Diagramma di Flusso**

| Passo | Descrizione |
|---|---|
| 1 | L'end user richiede un servizio all'applicazione locale (servizio di front end). |
| 2 | Il servizio di front end per soddisfare la richiesta dell'utente ha bisogno di interagire in ambito cooperativo con il servizio di back end. Per completare il portafoglio delle asserzioni deve validare degli attributi aggiuntivi presso delle Attribute Authority. Contatta l'Attribute Authority Registry Service per ricevere le URI. (SAML Query). |
| 3 | L'AARS ricevuta la richiesta interroga l'Attribute Authority Registry per recuperare la lista delle tuple (AA, URI). |
| 4 | L'AAR fornisce all'AARS la lista delle AA con le URI associate. |
| 5 | L'AARS invia la lista delle AA assieme alle URI al servizio di FE (SAML Response). |
| 6 | Il servizio di front end richiede le asserzioni di attributo alle authority competenti contattando le URI ricevute dall'AARS (SAML Attribute Query). |
| 7 | L'attribute authority emette le asserzioni di attributo (SAML Response). |
| 8 | Si ripete il passo 4 con un'altra authority presente nella lista. |
| 9 | Si ripete il passo 5. |
| 10 | Il servizio di front end, collezionate le asserzioni di attributo, prepara il portafoglio delle asserzioni. |
| 11 | Il servizio di front end richiede il servizio tramite web services al servizio di BE. |
| 12 | Il servizio di BE ricevuta la richiesta verifica il portafoglio delle asserzioni per autorizzare l'eventuale accesso al servizio. |
| 13 | In caso affermativo eroga il servizio. |

**Scheda riepilogativa:**

| ID Scenario | Scenario 2 – WS-ExT_AA |
|---|---|
| **Obiettivo** | Cooperazione applicativa fra una entità "*applicazione*" appartenente al dominio "Fruitori del Servizio" denominato servizio di front end ed una entità "*applicazione*" del dominio Erogatore del Servizio identificato come servizio di back end.<br>Prevede la necessità di interpellare una o più Attribute Authority esterne per certificare degli attributi non presenti nel profilo utente. |
| **Descrizione** | Il servizio di front end raccoglie tutte le asserzioni necessarie per richiamare il servizio di back end. Per completare il portafoglio di asserzioni necessita la validazione di ulteriori attributi,<br>Per reperire l'URI della Authority da interpellare si avvale del servizio di Attribute Authority Registry Service (AARS). |

| | |
|---|---|
| | Completato il portafoglio delle asserzioni richiede la cooperazione del servizio di back end tramite web services. |
| **Entità Coinvolte** | Servizio di Front End; Attribute Authority (External o Internal); Servizio di Front End; Attribute Authority Registry Service, Attribute Authority Registry. |
| **Pre Requisiti** | L'utente è già autenticato presso l'applicazione. L'applicazione ha già interagito localmente con l'identity provider per l'identificazione e con la profile authority per l'autorizzazione. |
| **Macro interfacce** | Servizio di FE:<br>• <SAMLQuery_Element> SAMLQuery CreateQuery (<QueryType> Type), genera la richiesta della lista degli IdP, PA o AA federati verso i servizi di registry infrastrutturali. Se Type è "PA" il registry service interrogato è l'ARS altrimenti se Type assume il valore "AA" il registry service interrogato è l'AARS;<br>• *<List SAMLAttributeStmnt> User_portfolio* Creazione_Portafoglio Asserzioni (*<List> Attributi,* <ID> *ID_User*): dato un utente ID_User ed una lista di attributi restituisce il portafoglio di attributi necessari a richiedere il servizio;<br>• <SAML AttrQuery_Element> AttrQuery CreateAttrQuery (<String> Attribute, <String> Id_User, <URI> Authority): la funzione dato l'utente Id_User, l'attributo Attribute e l'URI dell'authority di competenza da vericare fornisce l'elemento SAML AttributeQuery istanziato opportunamente;<br><br>Attribute Authority:<br>• *<AttrQueryResponse > Result* Richiedi_certificazione_Attributo(< SAML AttrQuery_Element> AttrQuery): ricevuto un elemento SAML Attribute Query e restituisce la verifica tramite una Attribute Response istanziata opportunamente;<br><br>Servizio di BE<br>• Richiesta_Servizio(<ID_serv> *ID_Servizio,<List String> Param, < List SAMLAttributeStmnt > User_Portfolio,* <ID> *ID_User*): a fronte di una richiesta pervenuta dal servizio ID_Servizio contenente l'Id_User dell'utente ed il suo portafoglio di asserzioni associato User_porfolio, il Service provider eroga il servizio a valle dei controllo autorizzativi;<br><br>AARS:<br><SAMLQueryResponse> Response Send_AttrAuth_list( |

| | |
|---|---|
| | <SAMLQuery_Element> SAMLQuery), fornisce la lista della Attribute Authority assieme alle URI associate tramite una SAML Response istanziata opportunamente; |

**Table 2: Scheda Riepilogativa dello scenario di cooperazione applicativa tramite web services con certificazione di attributi esterni alla federazione**

Contestualizzando lo scenario descritto all'interno del framework SAML possiamo asserire che:

- per trasferire le richieste ai servizi infrastrutturali o alle Attribute Authority si utilizza il SOAP Binding che definisce come i messaggi SAML possono essere trasportati all'interno del protocollo SOAP.
- Per le richieste ai servizi infrastrutturali come l'AARS ed alle Attribute Authority si utilizzano le asserzioni di attributo veicolate tramite i costrutti <AttributeQuery> e <Response>.

Le caratteristiche principali dei costrutti citati si possono così riassumere:

- <Attribute Query >
  - <ID> univoco;
  - <Issuer> contiene l'ID dell'applicazione che fa la richiesta;
  - <Subject> contiene l'id dell'utente soggetto della verifica;
  - <Attribute> contiene l'attributo di cui si vuole conoscere il valore;

  deve essere firmata dall'Applicazione Richiedente.
- <Response>
  - <ID> univoco;
  - <InResponseTo> contiene l'ID associato alla Attribute Query a cui sta rispondendo;
  - <Issuer> contiene l'ID dell'Attribute Authority che emette la Response;
  - <Subject> contiene l'id dell'utente soggetto della verifica;
  - <Assertion> contiene la risposta alla richiesta di verifica (<AttributeStatement>);

  ogni <Assertion> deve essere firmata dall'AA.

  Il trasporto delle richieste avviene tramite SOAP Binding. L'applicazione una volta collezionate tutte le asserzioni aggiuntive dalle varie Attribute Authority arricchisce il portafoglio delle asserzioni. Il portafoglio delle asserzioni è composto da varie <Assertion> firmate dalle AA competenti.

### 5.4.2.3. Scenario 3: cooperazione applicativa tramite web services con certificazione degli attributi da parte del Service Provider

Ci possono essere delle occasioni in cui i dati trattati sono di una riservatezza tale per cui chi offre il servizio di back end preferisce verificare personalmente alcuni attributi anziché affidarsi completamente a quanto presente nel portafoglio delle asserzioni.

Un simile approccio, per quanto singolare in un'ottica di federazione e quindi di trust fra le parti, viene per completezza trattato dal modello.

Il nuovo scenario è una variante dello scenario precedente in cui chi si preoccupa di interagire con il servizio AARS e le Attribute Authority(Internal/External) non è il servizio di Front End ma bensì quello di Back End.

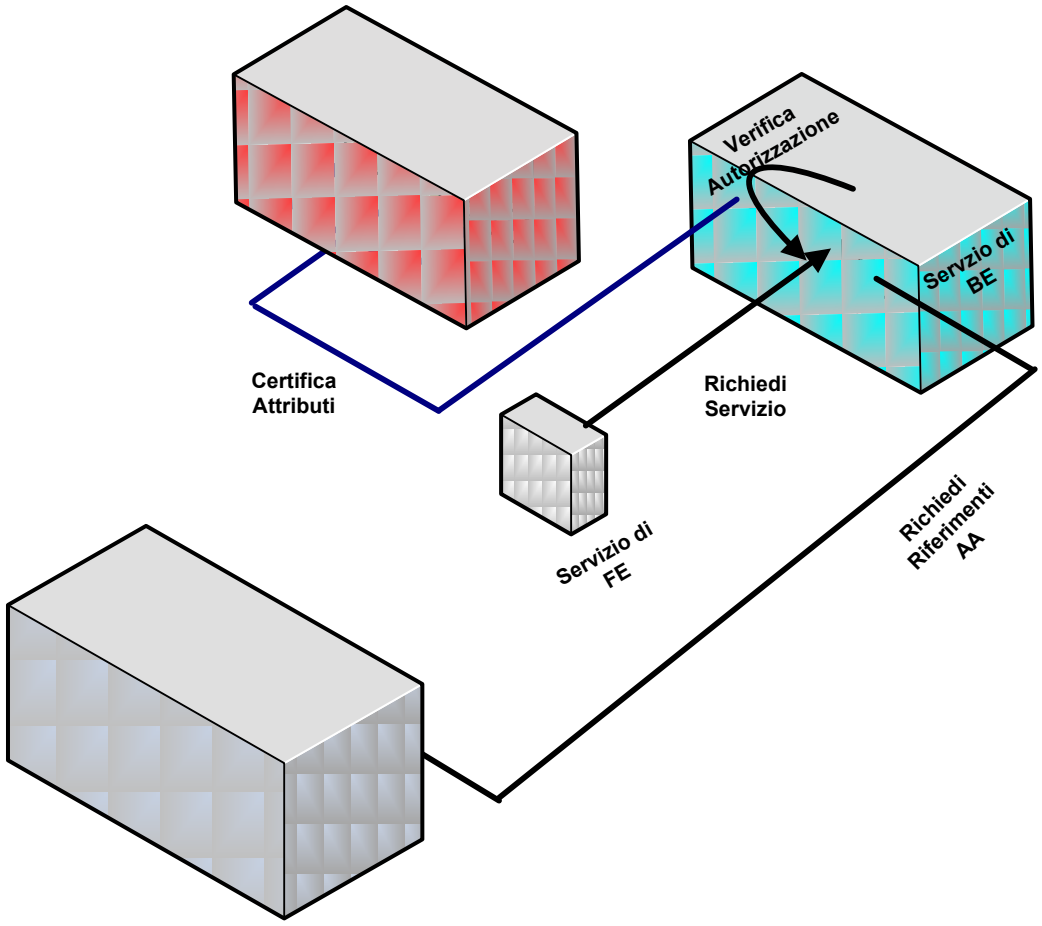



**Figura 11:Cooperazione Applicativa: Il servizio di back end verifica gli attributi.**

Entità coinvolte

- Servizio di Front End.
- Attribute Authority (Internal/External).
- Servizio di Back End.
- Servizio di AARS e AAR.

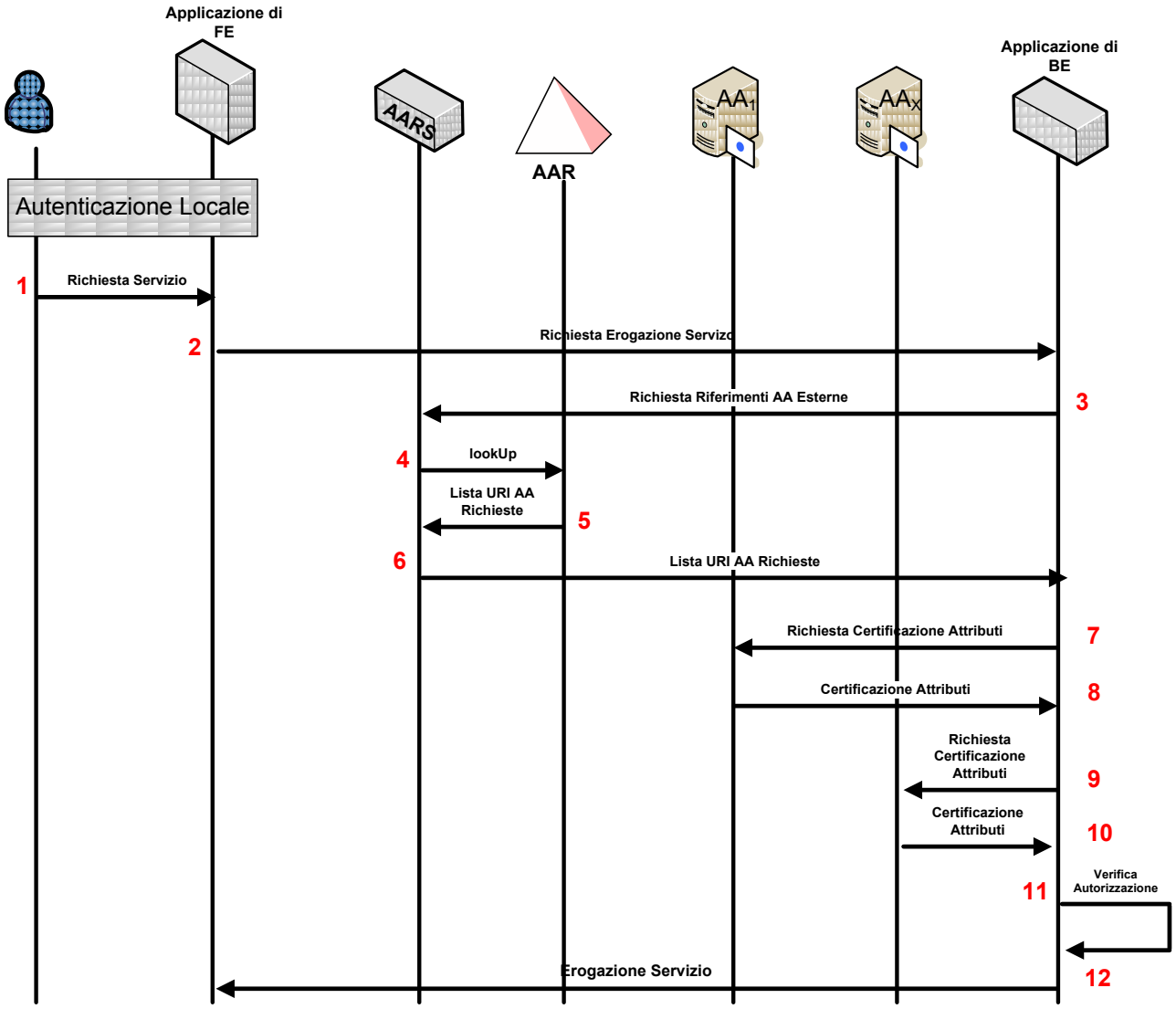



**Figura 12:Cooperazione Applicativa: Il service Provider certificazione gli attributi esterni alla federazione.Diagramma di Flusso**

| Passo | Descrizione |
|---|---|
| 1 | L'end user richiede un servizio all'applicazione locale. |

| | |
|---|---|
| 2 | L'applicazione di front end per soddisfare la richiesta dell'utente ha bisogno di un servizio offerto in ambito cooperativo dall'applicazione di back end. Contatta quindi il servizio di back end per richiedere il servizio. |
| 3 | Il servizio di back end prima erogare il servizio verifica che ci siano le autorizzazioni necessarie verificando le informazioni pervenute assieme alla richiesta e verificando ulteriori attributi necessari per accedere al servizio. Per completare la verifica deve richiedere la collaborazione della Attribute Authority. Contatta l'AARS per ricevere le loro URI. (SAML Query). |
| 4 | L'AARS ricevuta la richiesta interroga l'Attribute Authority Registry (AAR). |
| 5 | L'AAR restituisce per ogni attributo l'Authority e l'URI associata. |
| 6 | L'AARS invia la lista delle AA assieme alle URI al di Back End (SAML Response). |
| 7 | Il servizio di back end richiede le asserzioni di attributo alle authority competenti contattando le URI ricevute dall'AARS. (SAML AttributeQuery). |
| 8 | L'attribute authority emette le asserzioni di attributo. (SAML Response). |
| 9 | Si ripete il passo 7 con un'altra authority presente nella lista. |
| 10 | Si ripete il passo 8. |
| 11 | L'applicazioni di BE verifica le asserzioni ricevute dalle AA per autorizzare l'eventuale accesso al servizio. |
| 12 | In caso affermativo eroga il servizio. |

In questo caso, come mostrato dal diagramma di flusso, il Service Provider deve essere in grado di contattare le Attribute Authority per la verifica e la certificazione degli attributi utente.

L'interfaccia del servizio di front end descritta nella scheda riepilogativa si arricchisce del seguente metodo:

- Richiesta_Servizio_Auth(<ID_Serv> *ID_Servizio,<List String> Param, <List String> Attributi, <ID String> ID_User*): richiede il servizio identificato da "*ID_Servizio*", per conto dell'utente "*ID_User*". *Opzionalmente* gli attributi da verificare per autorizzare o meno il servizio sono contenuti all'interno della lista *"Attributi"*,

divenendo cosi composta da due metodi:

- Richiesta_Servizio (<ID_Serv> *ID_Servizio,<List String> Param, <List String> Attributi, <ID> ID_User*).
- Richiesta_Servizio_Auth (<ID_Serv> *ID_Servizio, <List String> Param, < SAMLAttributeStmnt > User_Portfolio, <ID> ID_User*).

Di seguito la scheda riepilogativa:

| **ID Scenario** | **Scenario 2 – WS-ExT_AA** |
|---|---|

| | |
|---|---|
| **Obiettivo** | Cooperazione applicativa fra una entità "application" appartenente al dominio "Fruitori del Servizio" denominata servizio di front end ed una entità "'application" del dominio "Erogatore del Servizio" identificata come servizio di back end.<br><br>Prevede la necessità di interpellare una o più Attribute Authority esterne per certificare degli attributi necessari per autorizzare l'erogazione del servizio.<br><br>Il controllo degli attributi viene svolto direttamente dal servizio di back end. |
| **Descrizione** | Ricevuta la richiesta dal servizio di front end il servizio di back end verifica ulteriori asserzioni necessarie ad erogare il servizio.<br><br>Per reperire l'URI delle Authority da interpellare si avvale del servizio di Attribute Authority Registry Service (AARS).<br><br>Completata la verifica e solo in caso di esito positivo il servizio di BE eroga il servizio. |
| **Entità Coinvolte** | Applicazione; Attribute Authority (Internal/External); Service Provider, Servizio di AADS, Attribute Authority Registry. |
| **Pre Requisiti** | L'utente è già autenticato presso l'applicazione. L'applicazione ha già interagito localmente con l'identity provider per l'identificazione e con la profile authority per l'autorizzazione. |
| **Macro interfacce** | Applicazione:<br>• *<List SAMLAttributeStmnt> User_portfolio* Creazione_Portafoglio Asserzioni (*<List> Attributi, <ID> ID_User*): dato un utente ID_User ed una lista di attributi restituisce il portafoglio di attributi necessari a richiedere il servizio;<br><br>Attribute Authority:<br>• *<AttrQueryResponse > Result* Richiedi_certificazione_Attributo(< SAML AttrQuery_Element> AttrQuery): ricevuto un elemento SAML Attribute Query e restituisce la verifica tramite una Attribute Response istanziata opportunamente;<br><br>Servizio di BE<br>• Richiesta_Servizio_Auth (<ID>*ID_Servizio, <List String> Param, <List String> Attributi, <ID> ID_User*): a fronte di una richiesta pervenuta dal servizio ID_Servizio contenente l'Id_User dell'utente ed lista di asserzioni da verificare, il Service provider certifica gli attributi presso le authority esterne ed eroga il servizio a valle dei controllo autorizzativi;<br>• <SAMLQuery_Element> SAMLQuery CreateQuery (<QueryType> Type), genera la richiesta della lista degli IdP, PA o |

| | |
|---|---|
| | AA federati verso i servizi di registry infrastrutturali. Se Type è "PA" il registry service interrogato è l'ARS altrimenti se Type assume il valore "AA" il registry service interrogato è l'AARS;<br><br>AARS:<br>• <SAMLQueryResponse> Response Send_AttrAuth_list( <SAMLQuery_Element> SAMLQuery), fornisce la lista della Attribute Authority assieme alle URI associate tramite una SAML Response istanziata opportunamente; |

### 5.4.3. Autenticazione Federata End User

Il paragrafo copre gli aspetti legati all'identificazione e l'autenticazione di un utente che fruisce di applicazioni federate tramite WEB. Differentemente dagli scenari presentati in precedenza, l'utente interagisce con l'Amministrazione che eroga il servizio tramite il proprio Browser.

L'Amministrazione che eroga il servizio interagisce con l'End User tramite un Federation Gateway che ha in carico la gestione dell'autenticazione dell'utente nella federazione, così da disaccoppiare l'Amministrazione stessa ed i suoi servizi dalla complessità intrinseca della federazione.

La figura sottostante riprende i macro scenari introdotti inizialmente, evidenziando in rosso lo scenario a cui si fa riferimento. Lo scenario introdotto è il caso di nomadicità dell'utente scenario classico del SSO Federato.

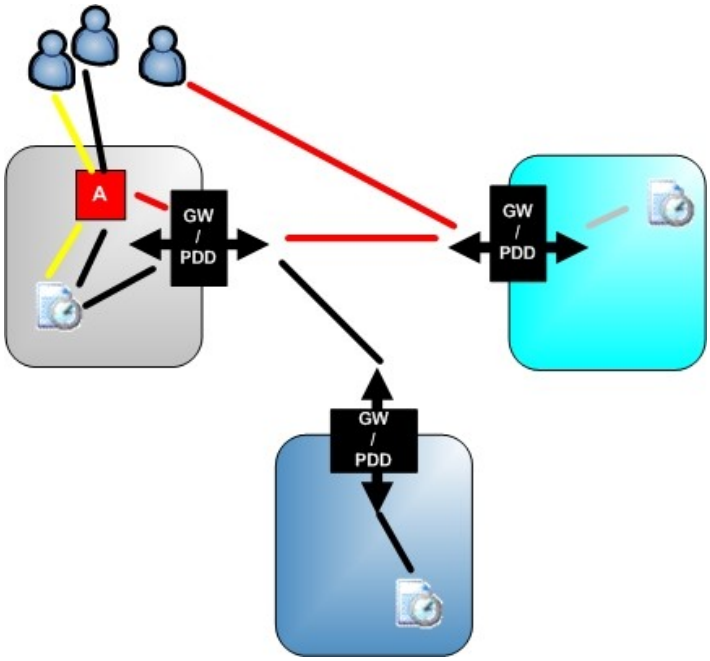



**Figura 13:Macro entità coinvolte nella autenticazione Federata degli End User**

#### 5.4.3.1. Scenario 4: Autenticazione Federata End User (F-SSO)

Lo scenario descrive la successione di eventi che avvengono quando un End User inizia il processo di autenticazione a valle della richiesta di un servizio presso una Amministrazione appartenente alla federazione, caso tipico di nomadicità dell'utente.

Al momento in cui l'end user si presenta presso il Federation Gateway del fornitore del servizio, quest'ultimo non ha alcuna informazione relativa alla sua identità, in quanto l'End User non appartiene all'Amministrazione che eroga il servizio. Per autorizzare l'End User l'ente erogante il servizio ha bisogno di un'asserzione identificativa da uno degli IdP appartenenti alla federazione oltre alle asserzioni necessarie per autorizzare l'accesso al servizio richiesto.

Per permettere il processo di Autenticazione dell'End User il Federation Gateway visualizza tutte le Profile Authority registrate all'interno della federazione. La lista viene costruita in base alle informazioni presenti all'interno dell'Authority Registry e fornite tramite l'Authority Registry Service. Il FG ridireziona l'End User verso la Profile Authority selezionata per iniziare il processo di autenticazione e la scelta del profilo idoneo a fruire il servizio.

Presso la PA l'End User deve selezionare l'IdP su cui intende eseguire il processo di autenticazione. Anche in questo caso la PA presenta una lista contenente tutti gli IdP membri della federazione. La lista viene costruita in base agli IdP presenti all'interno dell'Authority Registry e forniti tramite l'Authority Registry Service.

Terminato il processo di autenticazione l'End User può selezionare il profilo che intende utilizzare. La PA, ricevuto il profilo selezionato, prepara il portafoglio delle asserzioni.

Per preparare il portafoglio delle asserzioni la PA deve richiedere la verifica degli attributi componenti il profilo presso le authority competenti. La lista della authority interne ed esterne alla federazione viene fornita dall'Attribute Authority Registry Service.

Completato il set di asserzioni la PA ridirige l'End User verso il FG che ha originato inizialmente la richiesta di autenticazione per l'End User. Ricevute le asserzioni necessarie il FG può completare il processo di autorizzazione e permettere l'accesso al servizio inizialmente richiesto.

Le entità coinvolte sono:

- End User.
- Federation Gateway.
- Identity Provider.
- Profile Authority.
- Attribute Authority Registry Service.
- Authority Registry Service.

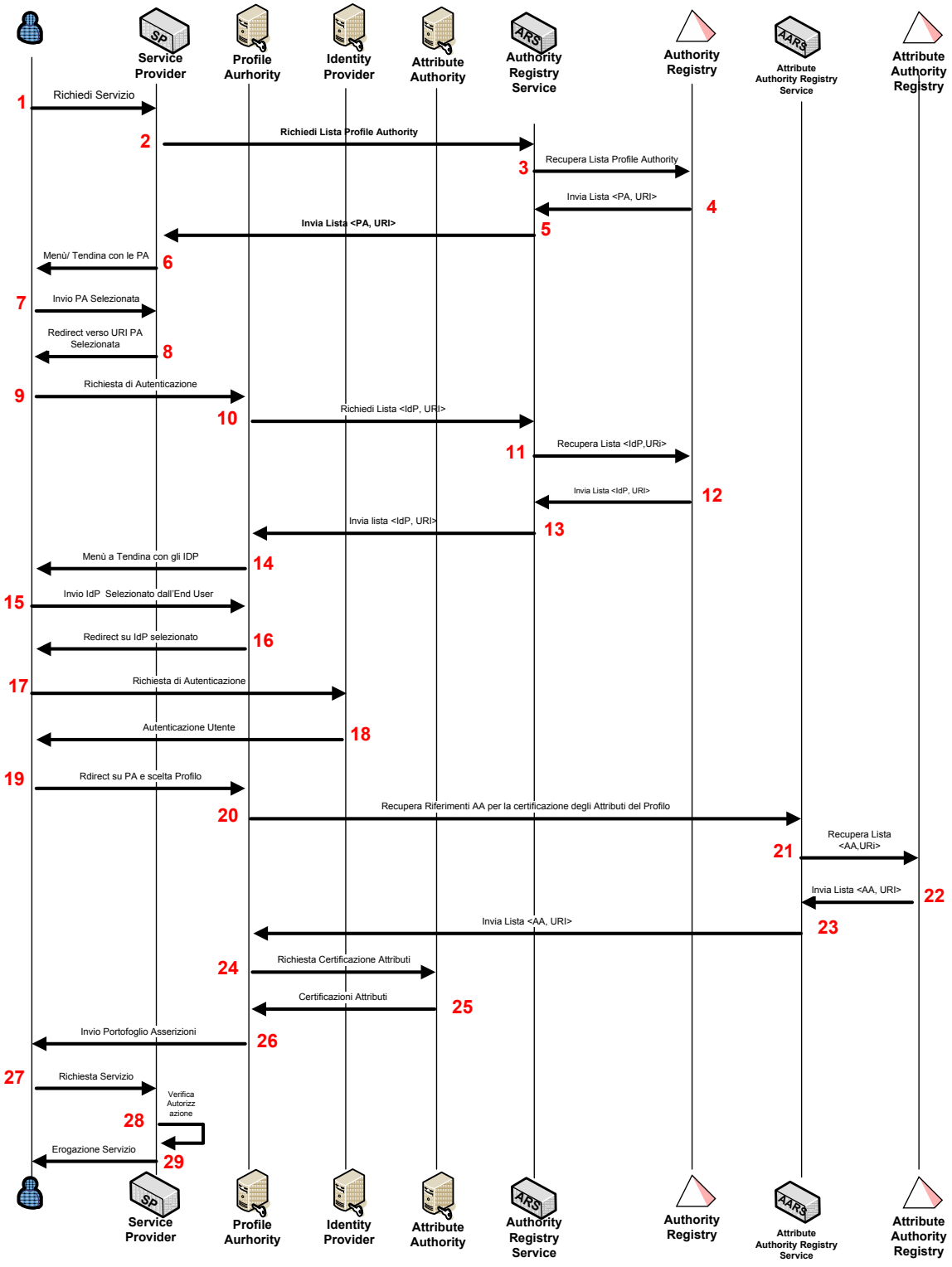



**Figura 14: Autenticazione Federata End User. Diagramma di Flusso**

| Passo | Descrizione |
|---|---|
| 1 | L'end user tramite il proprio Web browser (UA) contatta il Service Provider per richiedere il servizio. La richiesta viene presa in carico dal sottosistema del Federation Gateway. |
| 2 | L'SP (tramite l'FG) richiede all'ARS la lista delle PA appartenenti alla federazione (SAML Query). |
| 3 | L'ARS interroga l'Authority Registry per recuperare la lista delle tuple (PA, URI). |
| 4 | L'AR fornisce all'ARS la lista delle PA con le URI associate . |
| 5 | L'ARS invia la lista delle PA assieme alle URI al FG (SAML Response). |
| 6 | L' SP (tramite l'FG) mostra all'End User la lista delle PA richiedendo di scegliere la PA contenente il profilo necessario a fruire il servizio richiesto. |
| 7 | L'End User tramite l'UA sceglie la PA. |
| 8 | L'SP (tramite l'FG) ridirige l'UA dell'End User verso la PA selezionata attraverso una richiesta di autenticazione (SAML AuthnRequest). |
| 9 | L'UA inoltra la richiesta alla PA. |
| 10 | La PA contattata dall'utente interroga l'ARS per reperire la lista degli IdP federati da mostrare all'End User. |
| 11 | L'ARS ricevuta la richiesta interroga l'Authority Registry per recuperare la lista delle tuple (IdP, URI). |
| 12 | L'AR fornisce all'ARS la lista degli IdP con le URI associate. |
| 13 | L'ARS invia la lista delle IdP assieme alle URI alla PA richiedente (SAML Response). |
| 14 | La PA richiede all'End User di selezionare il proprio IdP dalla lista degli IdP federati. |
| 15 | L'End User selezione l'IdP tramite il suo UA. |
| 16 | La PA ridirige l'UA dell'End User verso IdP selezionato con una richiesta di autenticazione (SAML AuthnRequest). |
| 17 | L'UA inoltra la richiesta di autenticazione all'IdP. |
| 18 | L'IdP autentica l'End User sulla base delle credenziali fornite e restituisce una asserzioni di autenticazione (SAML Response ). |
| 19 | Lo UA inoltra alla PA l'asserzione ricevuta dall'IdP. |
| 20 | La PA dopo aver verificato l'asserzione pervenuta dall'IdP permette la selezione del profilo. Una volta ricevuto il profilo inizia il processo di costruzione del portafoglio delle asserzioni. Contatta l'AARS per ricevere la lista delle Attribute Authority. |
| 21 | L'AARS ricevuta la richiesta interroga l'Attribute Authority Registry per recuperare la lista delle tuple (AA, URI) (SAML Query). |
| 22 | L'AAR fornisce all'AARS la lista delle AA con le URI associate. |

| | |
|---|---|
| 23 | L'ARS invia la lista delle AA assieme alle URI alla PA richiedente (SAML Response). |
| 24 | La PA basandosi sulla lista (AA,URI) può interrogare le Attribute Auhtority per validare gli attributi presenti nel profilo (SAML AttributeQuery). |
| 25 | L'Attribute Authority contattata per la verifica degli attributi di sua competenza invia il responso della validazione (SAML Response). |
| 26 | Completato il processo di validazione degli attributi presenti nel profilo la Profile Authority fornisce il portafoglio delle asserzioni tramite una Response. |
| 27 | L'utente si presenta nuovamente al Federation Gateway per fruire del servizio inizialmente richiesto. Il sottosistema Federation Gateway inoltra la response all'SP |
| 28 | L'SP (tramite il sottosistema PEP) verifica le asserzioni presentate ed esegue il processo di autorizzazione. |
| 29 | L'SP permette l'accesso al servizio. |

**Scheda riepilogativa:**

| ID Scenario | Scenario – WeBAuth-FSSO |
|---|---|
| **Obiettivo** | Processo di autenticazione per un utente Nomade. |
| **Descrizione** | Per autorizzare l'End User il'FG dell'ente erogante il servizio ha bisogno di un'asserzione identificativa da uno degli IdP appartenenti alla federazione oltre alle asserzioni necessarie per autorizzare l'accesso al servizio richiesto.<br><br>Per permettere il processo di Autenticazione dell'End User il Service Provider visualizza tutte le profile authority registrate all'interno della federazione tramite l'ausilio dell'Authority Registry Service. L'SP ridireziona l'End User verso la Profile Authority selezionata dove inizia il processo di autenticazione e la scelta del profilo idoneo al servizio richiesto. Presso la PA l'End User seleziona l'IdP su cui intende eseguire il processo di autenticazione. Anche in questo caso viene presentata all'End User una lista contente tutti gli IdP membri della Federazione. La lista viene costruita tramite il servizio dell'Authority Registry Service e le informazioni presenti nell'Authority Registry.<br><br>Conclusa l'autenticazione e la scelta del profilo la PA si occupa di preparare il portafoglio delle asserzioni in base alle informazioni presenti nel profilo stesso.<br><br>Per preparare il portafoglio delle asserzioni richiede la verifica degli attributi componenti il profilo alle authority competenti. La lista della AA interne ed esterne alla federazione viene fornita dall'Attribute Authority Registry Service a partire dalle Informazioni presenti nell'Attribute Authority Registry.<br><br>Completato il set di asserzioni la PA ridirige l'End User verso l'SP che ha originato inizialmente la richiesta di autenticazione per l'End User. Ricevute le asserzioni l'SP può completare il processo di autorizzazione e permettere l'accesso al servizio inizialmente richiesto. |

| | |
|---|---|
| **Entità Coinvolte** | End User; Service Provider; Identity Provider; Authority Registry Service, Identity Provider, Profile Authority, Attribute Authority Registry Service, Attribute Authority. |
| **Pre Requisiti** | Esiste:<br>• un IdP federato in grado di autenticare l'utente,<br>• una PA con un profilo associato all'utente. |
| **Macro interfacce** | SP:<br>• Void WebUserInterface (Void), l'interfaccia permette agli utenti web l'accesso ai servizi tramite Web Browser;<br>• <SAMLQuery_Element> SAMLQuery CreateQuery (<QueryType> Type), genera la richiesta della lista degli IdP, PA o AA federati verso i servizi di registry infrastrutturali. Se Type è "PA" il registry service interrogato è l'ARS altrimenti se Type è assume il valore "AA" il registry service interrogato è l'AARS;<br>• <SAML AuthnRequest_Element> AuthRqst sendAuthRqst (<String> PA): la funzione data la PA scelto dall'utente fornisce l'elemento SAML AuthnRequest istanziato opportunamente;<br><br>Profile Authority<br>• <SAMLQuery_Element> SAMLQuery CreateQuery (<QueryType> Type), genera la richiesta della lista degli IdP, PA o AA federati verso i servizi di registry infrastrutturali. Se Type è "PA" il registry service interrogato è l'ARS altrimenti se Type è assume il valore "AA" il registry service interrogato è l'AARS;<br>• <Profile_Element Profile> Get_Profile(ID ID_User, String Profile), riceve in input l'ID dell'utente associato al profilo richiesto. Opzionalmente si possono richiedere delle viste.<br>• <SAML AttrQuery_Element> AttrQuery CreateAttrQuery (<String> Attribute, <String> Id_User, <URI> Authority): la funzione dato l'utente Id_User, l'attributo Attribute e l'URI dell'authority di competenza, fornisce l'elemento SAML AttributeQuery istanziato opportunamente;<br><br>Attribute Authority:<br>• <*AttrQueryResponse* > *Results* Richiedi_certificazione_Attributo(< SAML AttrQuery_Element> AttrQuery): ricevuto un elemento SAML Attribute Query restituisce la verifica tramite una Attribute Response istanziata opportunamente;<br><br>ARS: |

| | |
|---|---|
| | • <SAMLQueryResponse> Response Send_Auth_list( <SAMLQuery_Element> SAMLQuery), fornisce la lista della Authority (Idp o PA) assieme alle URI associate tramite una SAML Response istanziata opportunamente;<br><br>AARS:<br>• <SAMLQueryResponse> Response Send_AttrAuth_list( <SAMLQuery_Element> SAMLQuery), fornisce la lista della Attribute Authority assieme alle URI associate tramite una SAML Response istanziata opportunamente;<br><br>IDP:<br>• <SAML Response_Element> Response SendAuthResponse (<SAML AuthnRequest_Element> AuthRqst): L'Idp riceve una asserzione SAML di tipo AuthnRequest con cui inizia il processo di autenticazione dell'utente. A valle delle verifiche emette una asserzione SAML Reponse. |

Contestualizzando lo scenario descritto all'interno del framework SAML possiamo asserire che:

- il meccanismo utilizzato per trasferire le Asserzioni SAML fra IDP e PA è l'HTTP POST Binding che definisce come le informazioni SAML possono essere trasportate all'interno di una form HTML;
- il meccanismo utilizzato per trasferire le richieste di autenticazione SAML (AuthnRequest) dall'SP alla PA e dalla PA all'IdP è l'HTTP Redirect Binding;
- per trasferire le richieste ai servizi infrastrutturali o alle Attribute Authority si utilizza il SOAP Binding che definisce come i messaggi SAML possono essere trasportati all'interno del protocollo SOAP.
- Il profilo di autenticazione SAML a cui si fa riferimento è il Web Browser SSO nello specifico lo scenario utilizza la metodologia di autenticazione "SP initiated" in cui un Service provider ridireziona l'utente su un Identity Provider per l'autenticazione . L'IdP produce un'asserzione rappresentante l'avvenuta autenticazione dell'utente e ridireziona nuovamente l'utente verso il service provider;
- per l'autenticazione si utilizzano le asserzioni di identità veicolate tramite i costrutti <AuthnRequest> e <Response>.
- Per le richieste ai servizi infrastrutturali ed alle Attribute Authority si utilizzano le asserzioni di attributo veicolate tramite i costrutti <AttributeQuery> e <Response>.

Le caratteristiche principali dei costrutti citati si possono così riassumere:

- <AuthnRequest>:
  - < ID> univoco;

- <Issuer> contiene l'ID del SP che emette la richiesta;
- <Protocol Binding> se presente deve essere urn:oasis:names:tc:SAML:2.0bindings:HTTP-POST;
- <Subject> contiene l'id dell'utente soggetto della richiesta dell'authenticazione. Tale elemento è opzionale in quanto l'SP potrebbe non avere l'informazione all'atto della verifica;
- <Force Auth> contiene il valore "false" nelle ridirezioni fra FG e PA mentre deve essere impostato a "true" nella ridirezione fra PA e IdP in modo che la verifica dell'identità del soggetto è fatta dall'IdP senza ulteriori ridirezioni;
- deve essere firmata dall'SP richiedente;

è trasportata attraverso l'HTTP Redirect-Binding su SSL.

- <Response>
  - < ID> univoco;
  - <Version> deve esse "2.0";
  - <Issuer> contiene l'ID del IdP che emette la <Response>;
  - <InResponseTo> contiene l'ID associato alla AuthnRequest a cui sta rispondendo;
  - <Subject> contiene l'ID dell'utente autenticato;
  - <Assertion> contiene la risposta alla richiesta di autenticazione (<AuthnStatement>). L'<Assertion> deve contenere nell'elemento <Conditions> i vincoli associati alla validità dell'asserzioni di autenticazione. Lo <AuthnStatement> deve contenere al suo interno:
    - <AuthInstant> che identifica l'stante in cui è avvenuta l'autenticazione;
    - <AuthContext> che descrive il contesto di autenticazione;
  - l'<Assertion> deve essere firmata dall'IDP

La response deve essere comunicata tramite l'http Post binding e su canale SSL.

- <Attribute Query >
  - <ID> univoco;
  - <Issuer> contiene l'ID dell'applicazione che fa la richiesta;
  - <Subject> contiene l'id dell'utente soggetto della verifica;
  - <Attribute> contiene l'attributo di cui si vuole conoscere il valore

deve essere firmata dalla Profile Authority Richiedente.

- <Response>
  - <ID> univoco;
  - <InResponseTo> contiene l'ID associato alla Attribute Query a cui sta rispondendo;
  - <Issuer> contiene l'ID dell'Attribute Authority che emette la Response;
  - <Subject> contiene l'id dell'utente soggetto della verifica;
  - <Assertion> contiene la risposta alla richiesta di verifica (<AttributeStatement>)

ogni <Assertion> deve essere firmata dall'AA.

Il trasporto delle richieste avviene tramite SOAP Binding.

La Profile Authority una volta collezionate tutte le asserzioni provenienti dalle Attribute Authority crea il portafoglio delle asserzioni. Il portafoglio delle asserzioni è composto da varie <Assertion> firmate dalle AA competenti ed è inviato tramite una Response al Federation Gateway.

# 6. L'UTILIZZO DEI METADATI COME MEZZO PER LA PROPAGAZIONE DELLE INFORMAZIONI DEGLI ATTORI DEL MODELLO

Nel contesto della specifica SAML 2.0 è prevista la possibilità di descrivere informazioni dette metadati (cfr.[SAML-Metadata]) da associare alle diverse entità interagenti. I metadati descrivono le peculiarità dell'entità e sono necessari per abilitare scenari di interazione complessi.

Un classico esempio sono le modalità con cui recuperare l'elenco delle chiavi pubbliche da utilizzare per verificare la firma digitale (cfr. [XML-Sign]) presente nelle richieste ricevute da una certa entità, oppure i servizi da essa offerti in termini di indirizzo URL e tipo di binding supportato ecc.

La specifica definisce degli schemi XML precostituiti che determinano la struttura dei descrittori dei metadati delle entità presenti nell'abito federativo. In particolare, esistono tre tipologie di descrittori corrispondenti ai ruoli che una entità può ricoprire in ambito SAML: Service Provider, Identity Provider e Attribute Authority. A partire da questi template è possibile derivare la struttura dei metadati per tutte le entità descritte nel modello.

Prima di una qualsiasi interazione appare chiaro quindi che le entità che necessitino di interagire devono avere a disposizione i metadati della controparte.

La specifica SAML 2.0 richiede di disporre di un sistema per la pubblicazione e lo scambio dei metadati ma non entra nel merito di come esso debba essere dispiegato, lasciando libertà di implementazione. La specifica infatti ipotizza soltanto che l'indirizzo del servizio di pubblicazione dei metadati di una certa entità possa essere noto a priori oppure pubblicato in un DNS (cfr.[SAML-Metadata], sez. 4). Nel modello un servizio simile al servizio di DNS viene svolto dai servizi di registry ARS e AARS.

Ciascuna entità del modello che ha necessità di pubblicare e rendere accessibili da remoto i propri metadati espone una interfaccia *IMetadataRetrieve*: Tale interfaccia è costituita da un servizio HTTPS, il cui indirizzo è well-known o è rintracciabile tramite i servizi di registry ARS/AARS.

Tramite i servizi di registry è possibile ottenere il documento XML (content type "application/samlmetadata+xml") con i relativi metadati che descrivono l'entità (cfr.[SAML-Metadata], sez. 4.1).

Di seguito vengono elencati i principali elementi dei metadati atti a descrivere le entità del modello.

Tutte le entità sono descritte mediante un elemento **<EntityDescriptor>** avente le seguenti caratteristiche:

- **entityID**: attributo che indica l'identificativo univoco (un URI) dell'entità;
- **cacheDuration**: attributo che indica la durata (in millisecondi) della cache di un file di metadati; un documento di metadati letto e memorizzato localmente ha validità fino alla scedenza di tale periodo di tempo; successivamente è necessario richiedere nuovamente il file alla relativa entità.

Inoltre, nei metadati di ogni entità è necessario inserire un elemento descrittore dell'entità stessa, all'interno del quale si possono specificare alcuni valori aggiuntivi.

Di seguito si introducono le caretteristiche salienti dei metadati associati alle varie entità rimandando all'Appendice C per degli esempi di metadati.

**Service Provider:**

Nel caso del Service Provider l'elemento specifico che descrive l'entità è denominato **<SPSSODescriptor>,** al cui interno si possono specificare tra gli altri i seguenti valori:

- **AuthnRequestsSigned**: attributo con valore booleano che indica se le richieste di autenticazione prodotte dal Service Provider sono firmate;
- **WantAssertionsSigned:** attributo con valore booleano che esprime il requisito che le asserzioni ricevute in risposta siano firmate;
- **protocolSupportEnumeration**: attributo che enumera gli URI indicanti i protocolli supportati dall'entità (poiché si tratta di un'entità SAML 2.0, deve indicare almeno il valore del relativo protocollo: "urn:oasis:names:tc:SAML:2.0:protocol");
- **<KeyDescriptor>:** elemento che contiene l'elenco dei certificati e delle corrispondenti chiavi pubbliche dell'entità, utili per la verifica della firma dei messaggi prodotti da tale entità nelle sue interazioni con le altre (cfr.[SAML-Metadata], sez. 2.4.1.1);
- **<NameIDFormat>:** elemento che indica i formati di NameID supportati (NameID è l'elemento utilizzato nelle richieste e risposte SAML per identificare il subject cui si riferisce un'asserzione): può adottare il formato di un indirizzo e-mail, di un entity identifier SAML o altri formati ancora, oppure rimanere non specificato ("urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified") (cfr.[SAML-Core], sez. 8.3).
- **<AssertionConsumerService>:** uno o più elementi che specificano l'indirizzo del servizio AssertionConsumer (attributo **`Location`**) ed il binding (attributo **`Binding`**, valorizzato a "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST") utilizzato per inviare a tale servizio risposte SAML contenenti asserzioni;

- **<AttributeConsumingService>:** zero o più elementi che specificano i servizi esposti da un Service Provider. Oltre all'indice posizionale (attributo `index`) per ogni servizio viene definito il nome (o i nomi) (elemento **<ServiceName>)** e l'elenco degli attributi che il servizio richiede (elementi **<RequestedAttribute>)** (cfr.[SAML-Metadata], sez. 2.4.4.1).

**Identity Provider**

Nel caso dell'Identity Provider l'elemento specifico che descrive l'entità è denominato **<IDPSSODescriptor**>, al cui interno si possono specificare tra gli altri i seguenti valori:

- **protocolSupportEnumeration:** (Vedi Service Provider);
- **<KeyDescriptor>:** (Vedi Service Provider);
- **<NameIDFormat>:** (Vedi Service Provider);
- **WantAuthnRequestSigned**: attributo con valore booleano che esprime il requisito che le richieste di autenticazione ricevute siano firmate;
- **<SingleSignOnService**>: uno o più elementi (analogamente all'AssertionConsumerService del Service Provider) che specificano l'indirizzo del Single Sign-On Service (attributo **Location**) e il binding (attributo **Binding**, che può valere "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-REDIRECT" oppure "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST") utilizzato per comunicare mediante costrutti SAML con tale servizio.

**Attribute Authority**

Nel caso della Attribute Authority l'elemento specifico che descrive l'entità è denominato **<AttributeAuthorityDescriptor>,** al cui interno si possono specificare tra gli altri i seguenti valori:

- **protocolSupportEnumeration:** (Vedi Service Provider);
- **<KeyDescriptor>:** (Vedi Service Provider);
- **<NameIDFormat>:** (Vedi Service Provider);
- **<AttributeService>:** uno o più elementi (analoghi a quelli appena illustrati nel caso del Service Provider e dell'Identity Provider) che specificano l'indirizzo dell'AttributeService (attributo **Location**) ed il binding utilizzato per comunicare con tale servizio (attributo **Binding**). A differenza dei servizi illustrati precedentemente, in questo caso il binding utilizzato è SOAP (indicato dal valore "urn:oasis:names:tc:SAML:2.0:bindings:SOAP").

**Authority Registry**

Lo stesso elemento **<AttributeAuthorityDescriptor>** è utilizzato per descrivere l'**Authority Registry**, in quanto tale entità nel modello svolge il ruolo di una particolare Attribute Authority e ha pertanto un funzionamento analogo.

Nel caso generale in cui un'entità svolga più di un ruolo (per esempio come la **Profile Authority** che svolge quello di Service Provider e Identity Provider allo stesso tempo) il suo file di metadati dovrà contenere i descrittori di tutte le entità "impersonate".

Per maggiori dettagli sulla sintassi e il contenuto dei metadati che descrivono un'entità si rimanda alla specifica [SAML-Metadata] e ai documenti correlati.

### *6.1.1. Scenario di interazione*

Come accennato nei paragrafi precedenti ci possono essere vari modalità con cui recuperare i metadati del partner con cui si deve interagire.

Il meccanismo di scambio dei metadati può essere utilizzato prima e dopo ogni interazione tra due entità. In particolare, prima dell'invio di una richiesta o di una risposta SAML, il mittente richiede all'entità destinataria (tramite l'interfaccia IMetadataRetrieve da essa esposta) il relativo file dei metadati, al fine di conoscere la modalità di invio e l'indirizzo a cui spedire il messaggio. Ricevuto la richiesta, per poter rispondere anche l'entità destinataria richiede all'entità mittente il file dei metadati al fine di conoscere la lista dei certificati dalla quale estrarre le relative chiavi pubbliche, necessarie alla verifica della firma del messaggio. Il recupero dei metadati avviene tramite HTTPS Get.

Ai fini prestazionali utilizzando opportuni meccanismi di caching, tale richieste possono essere soddisfatte recuperando le copia-cache locali dei documenti richiesti se presente.

L'indirizzo del servizio da invocare per il recupero dei metadati di una data entità può essere reperito tramite i Servizi di Registry in modo **statico** o in modo **dinamico**. Si introducono due tipologie di recupero in modo che il modello possa accettare anche entità che non hanno ad oggi la capacità di recuperare a run time i metadati.

I passi da intraprendere per reperire l'indirizzo del servizio da invocare per il recupero dei metadati di una entità sono invarianti rispetto al metodo prescelto. Nel caso statico vengono intrapresi manualmente, nel caso dinamico vengono svolti automaticamente delle entità richiedenti interrogando le Authority Registry.

Similmente una volta conosciuto l'indirizzo per il recupero dei metadati tale recupero può avvenire in modalità statica o dinamica secondo le capacità del servizio. Nel caso della modalità statica ad esempio i metadati potranno essere prelevati dall'indirizzo individuato, tramite il browser, salvati in locale ed importati manualmente nel servizio.

Una modalità per gestire il meccanismo di instaurazione e convalida della fiducia reciproca (cioè il "trust") tra entità, relativamente al contenuto dei metadati scambiati, consiste nel richiedere che tutti i file dei metadati di ciascuna entità siano firmati digitalmente da una terza parte fidata (il cosiddetto "garante" della federazione).

Tale modalità non è l'unica praticabile ma offre vantaggi rispetto ad altri approcci, per esempio in scalabilità rispetto all'instaurazione di un trust "locale" tra ciascuna coppia di entità.

### 6.1.2. Struttura dei metadati

La struttura prevista dallo standard SAML per i metadati è descritta in [SAML-Metadata]. I metadati di esempio sono firmati (come detto in precedenza, si può trattare della firma apposta dal garante della federazione ai fini dell'instaurazione del "trust" reciproco), inoltre, si fa notare come in generale l'elemento `<KeyDescriptor>` contenga, al suo interno, non un unico certificato bensì una catena di certificati relativi all'entità descritta (un certificato "foglia" con la chiave pubblica utilizzabile per la verifica delle firme prodotte e i suoi relativi certificati "padre").

In Appendice sono riportati esempi di file XML contenenti i metadati di alcune delle entità citate nel modello.

# SEZIONE II - APPLICAZIONE DEL MODELLO AL CONTESTO DELLA PUBBLICA AMMINISTRAZIONE

Nel modello descritto una Pubblica Amministrazione, può ricoprire il ruolo di più entità contemporaneamente. Infatti essa può ricoprire sia il ruolo di erogatrice dei servizi sia il ruolo di Identity Provider, mettendo a disposizione i propri servizi agli utenti federati e nello stesso tempo permettendo ai suoi utenti di fruire di applicazioni esterne. Diversamente può decidere di essere solamente Identity Provider e Profile Authority per i propri utenti.

La granuralità delle entità permette ad una Pubblica Amministrazione di decidere il grado di coinvolgimento all'interno della Federazione implementando una o più entità. Un ente può scegliere un coinvolgimento come Authority dove si impegna a certificare degli attributi ben determinati, oppure decidere di implementare contemporaneamente i ruoli di Identity Provider, Attribute Authority e Profile Authority.

Una Pubblica Amministrazione che voglia cooperare in ambito federato deve mettere a disposizione i propri servizi tramite due tipologie di interfacce: il Federation Gateway/SP e la porta di dominio. Il Federation Gateway/SP è il punto d'accesso ai servizi tramite Web F-SSO, la porta di dominio costituisce invece l'unico punto di ingresso per le applicazioni esterne per la cooperazione applicativa.

## 7. ENTITÀ LOGICHE DELLA PUBBLICA AMMINISTRAZIONE E RELAZIONE CON LE ENTITÀ CONCETTUALE

E' possibile associare le entità concettuali descritte nel capitolo precedente a delle entità fisiche proprie del ecosistema SPCoop.

**Autorità Locale di Dominio(ALD):** svolge le funzioni di Identity Provider per soggetti che non utilizzano certificati X.509 emessi da CA accreditate presso la Bridge CA SPCoop. Fornisce identità autenticate secondo policy locali (distinguendo tra autenticazione con valore legale e non e tra autenticazione forte e debole). L'ALD può svolgere funzioni di Attribute Authority relativamente a ruoli lavorativi degli End User (ad es. responsabile d'ufficio, responsabile di un determinato procedimento amministrativo o privato. La ALD può svolgere inoltre la funzioni Profile Authority. L'ALD è conforme allo standard SAML.

L'ALD accorpa le entità "Identity Provider", "Profile Authority" ed "Attribute Authority".

**Centro Gestione Servizi di Interoperabilità, Cooperazione ed Accesso (CG-SICA):** ospita i servizi abilitanti alla cooperazione applicativa in ambito SPCoop (servizi infrastrutturali) come:

- **Servizio SICA generale**, gestisce il ciclo di vita degli accordi di servizio;
- **Servizio indice dei soggetti,**offre l'accesso in tempo reale agli elenchi on-line relativi al personale delle amministrazioni partecipanti all'SPCoop;
- Servizi a supporto per la qualificazione della porta di dominio e dei registri SICA secondari.

Assieme ai servizi menzionati il CG-SICA ospita anche i servizio di Gestione Federata delle Identità Digitali (GFID).

**Il servizio GFID** svolge il ruolo di entità "*super partes*" offrendo all'interno della federazione i due sottoservizi di:

- **AARS per la verifica di attributi esterni alla federazione,** fornisce la lista delle Attribute Authority (Interne/esterne) assieme alle URI associate. Il servizio comprende le entità del modello di *Attribute Authority Registry* e *Attribute Authority Registry Services*
- **ARS per Applicazioni SPCoop e Utenti Federati,** fornisce ai membri della federazione, la lista completa di tutti gli IdP o le Profile Authority appartenenti alla Federazione assieme alle loro URI. Il servizio comprende le entità del modello di *Authority* Registry e *Authority Registry Service*
- **Profile Authority**

Tramite questi sottoservizi il GFID implementa i servizi infrastrutturali introdotti nel modello fornendo le ALD e le PA di riferimento su cui autenticare il richiedente del servizio oltre ad i riferimenti dei certificatori di attributo interni ed esterni all'SPCoop.

## 7.1. Ruoli della Pubblica Amministrazione nella Federazione: Architettura ed Interfacce

La figura mostra delle possibili modalità tramite cui un'Amministrazione può partecipare al network federativo:

- Amministrazione ricopre solamente il ruolo di Identity Provider (Amministrazione A).
- Amministrazione ricopre solamente il ruolo di erogatore di servizi (Amministrazione B).
- Amministrazione ricopre sia il ruolo di SP che quello di IDP (Amministrazione C).
- Ente esterno che ricopre il ruolo di External Authority.

Nella figura sono presenti anche i servizi infrastrutturali tramite il CG-SICA.

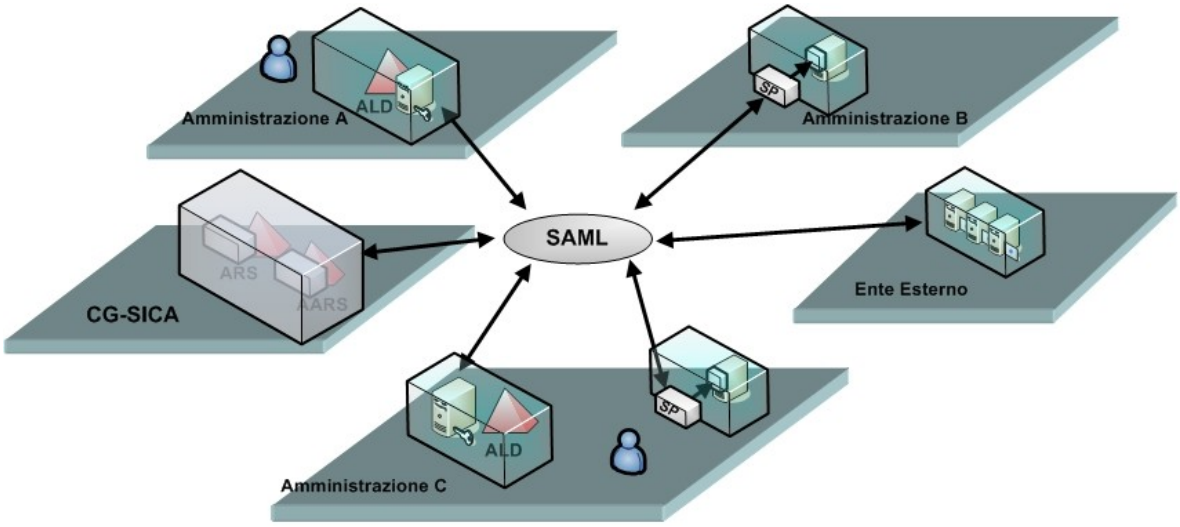



**Figura 15: Esempio di entità ed interazioni fra le entità del modello in ambito SPCoop**

La figura evidenzia come tutte le entità, siano esse ALD, Attribute Authority, o servizi infrastrutturali devono comunque essere conformi al framework SAML.

E' cura di ogni singola amministrazione decidere quale tipologia di protocollo, prodotto o paradigma di autenticazione utilizzare al suo interno. Questo significa che l'amministrazione che vuole offrire i propri servizi all'esterno del proprio ambito organizzativo deve utilizzare un componente che traduca le informazioni provenienti da un generico IdP sottoforma di asserzioni SAML in informazioni compatibili con le applicazioni interne al dominio e con il sistema di controllo accessi già in uso.

Similmente l'ALD può autenticare l'end user nel modo a lui più congeniale ma le informazioni di autenticazione utili alla richiesta di un servizio applicativo in ambito federato dovranno essere inviate sempre sottoforma di asserzione di identità SAML.

Riassumendo possiamo suddividere le varie entità esposte nel modello in tre aree fondamentali:

- Entità localizzate all'interno di un'Amministrazione che eroga servizi.
- Entità localizzate all'interno di un'Amministrazione che ha federato i propri utenti per fruire dei servizi messi a disposizione da altre Amministrazioni.
- Entità localizzate all'interno del CG-SICA.
- Entità esterne alla Federazione.

La tabella suddivide le entità secondo questa tassonomia e per ognuna di esse riassume le modalità di interazione fondamentali.

E' importante sottolineare che una Amministrazione che decide di federare i propri utenti non deve necessariamente implementare tutte le entità presenti al punto 3 della tabella. Ad esempio può decidere di implementare il servizio di Identity provider avvalendosi dei servizi di Profile Authority erogati da

una terza parte(es: CG-SICA). Per gli attributi di propria competenza dovrà esercitare il ruolo anche di Attribute Authority.

| 1 - Amministrazione Erogante i Servizi | | |
|---|---|---|
| **Entità** | **Ruolo** | **Interfaccia** |
| **Service Provider** | Disaccoppia l'amministrazione che offre i servizi dalla complessità della federazione stessa. Il Service Provider è composto dal Federation Gateway che svolge il ruoli di punto di contatto (P.O.C. Point of Contact) per tutte le richieste di accesso alle risorse offerte dall'Amministrazione e il Policy Enforcement Point per l'applicazione dello policy di autorizzazione prima dell'accesso ai servizi. | Accesso utente Web<br>SAML AuthnRequest<br>SAML AttributeQuery<br>SAML Response<br>Web Service per Cooperazione Applicativa |
| **2 - Amministrazione con Utenti Federati** | | |
| **Entità** | **Ruolo** | **Interfaccia** |
| **Attribute Authority** | Verifica tutti o parte degli attributi componenti il profilo di un generico utente. | SAML Attribute Query<br>SAML Response |
| **Profile Authority** | Gestisce il profilo utente e prepara il portafoglio delle asserzioni. | Accesso utente Web<br>SAML AuthnRequest<br>SAML Attribute Query<br>SAML Response |
| **Identity Provider** | Fornisce il servizio di Autenticazione per l' End User. | Accesso utente Web<br>SAML AuthnRequest<br>SAML Response |
| **3 - Servizi Infrastrutturali CG-SICA** | | |
| **Entità** | **Ruolo** | **Interfaccia** |
| **Authority Registry Service** | Fornisce la lista completa di tutti gli IdP o le Profile Auhority appartenenti alla Federazione assieme alle loro URI. | SAML Attribute Query<br>SAML Response |
| **Attribute Authority Registry Service** | Fornisce la lista delle Attribute Authority (Interne/esterne) assieme alle URI associate. | SAML Attribute Query<br>SAML Response |
| **Profile Authority** | Gestisce il profilo utente e prepara il portafoglio delle asserzioni. | Accesso utente Web<br>SAML AuthnRequest<br>SAML Attribute Query |

| | | |
|---|---|---|
| | | SAML Response |
| **Attribute Authority Registry Service** | Fornisce la lista delle Attribute Authority (Interne/esterne) assieme alle URI associate. | SAML Attribute Query<br>SAML Response |
| Entità Esterna alla Federazione | | |
| **Entità** | **Ruolo** | **Interfaccia** |
| **Attribute Authority** | Verifica tutti o parte degli attributi componenti il profilo di un generico utente. | SAML Attribute Query<br>SAML Response |

L'architettura riportata in tabella è dettagliata in figura,

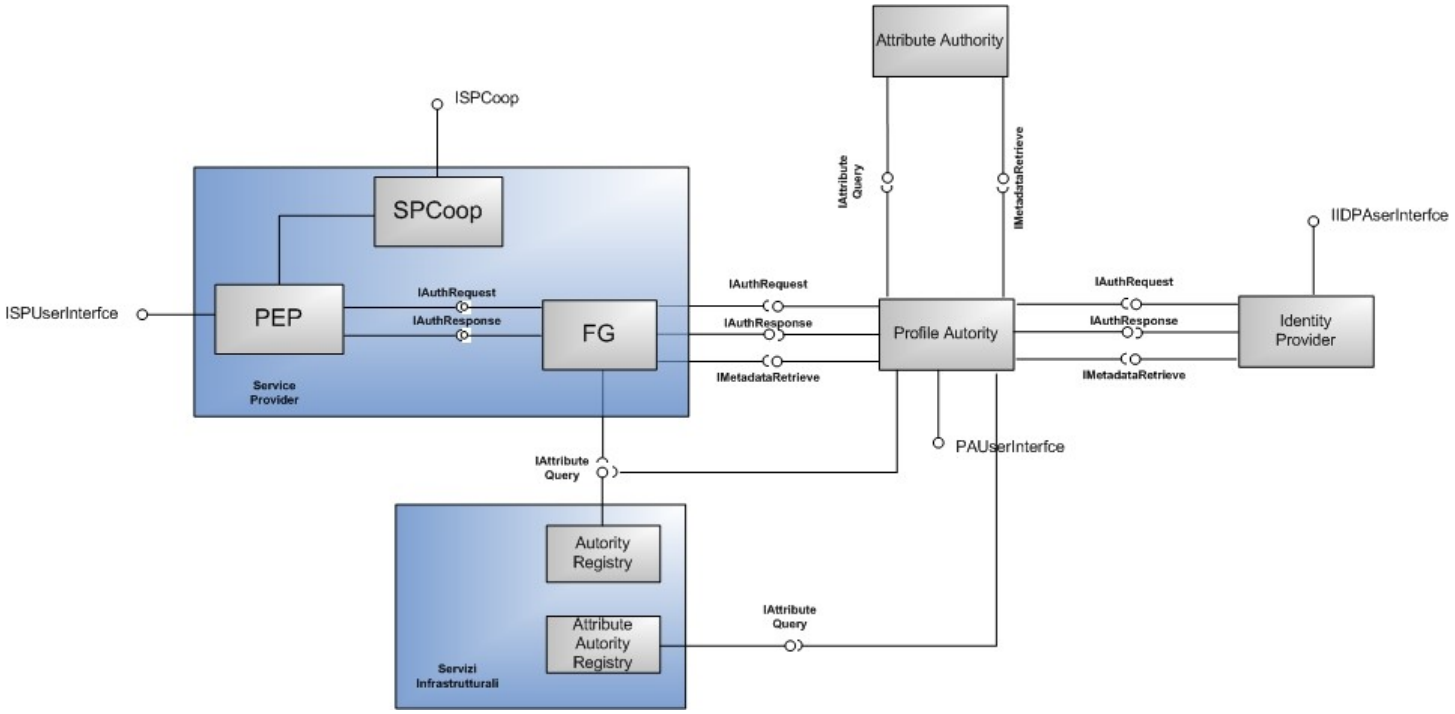



**Figura 16: Architettura del modello di gestione federate delle identità digitali**

Il **Service Provider** come fornitore di servizi applicativi espone le seguenti interfacce:

- **ISPUserInterface :** permette agli utenti l'accesso via web tramite User Agent alle risorse e ai servizi offerti;
- **IAuthnRequest** e **IAuthnResponse**: permettono l'inoltro e la ricezione di richieste e risposte di autenticazione SAML;

- **IMetadataRetrieve**: permette il reperimento dei metadati SAML;
- **ISPCoop**: permette l'interazione in modalità di cooperazione applicativa fra due Amministrazioni;

L'**Identity Provider** come responsabile della certificazione dell'identità degli utenti espone le seguenti interfacce:

- **IIDPUserInterface:** permette agli utenti l'interazione via web con il componente tramite User Agent in fase di challenge di autenticazione;
- **IAuthnRequest** e **IAuthnResponse**: permettono l'inoltro e la ricezione di richieste e risposte di autenticazione SAML;
- **IMetadataRetrieve**: permette il reperimento dei metadati SAML da parte delle entità richiedenti.

La **Profile Authority** come repository dei profili utente si occupa di interagire con l'Identity Provider ai fini dell'autenticazione dell'utente e con le attribute authority per verificare gli attributi componenti il profilo. Espone le seguenti interfacce:

- **IPAUserInterface:** permette agli utenti l'interazione via web con il componente tramite User Agent (per esempio in fase di scelta o creazione profilo);
- **IAttributeQuery**: interfaccia applicativa che supporta le operazioni di interrogazione del profilo utente mediante richieste di attributo SAML. Viene utilizzata anche per interrogare le authority del GC-SICA;
- **IMetadataRetrieve**: permette il reperimento dei metadati SAML.
- **IAuthnRequest** e **IAuthnResponse**: permettono l'inoltro e la ricezione di richieste e risposte di autenticazione SAML;

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

- **IAttributeQuery**: interfaccia applicativa che supporta le operazioni di richiesta di attributo SAML;
- **IMetadataRetrieve**: permette il reperimento dei metadati SAML SAML da parte delle entità richiedenti.

L'**Authority Registry** è il componente che implementa i servizi ARS e AARS e che permette di recuperare le coordinate di accesso e altre informazioni relative alle authority del modello (Identity Provider, Profile Authority, Attribute Authority). Il componente espone le seguenti interfacce:

- **IAttributeQuery**: interfaccia applicativa che supporta le operazioni di interrogazione del registro mediante richieste di attributo SAML;
- **IMetadataRetrieve**: permette il reperimento dei metadati SAML.

Componenti diversi possono esporre le medesime interfacce (pur potendo sussistere differenze negli specifici messaggi scambiati a seconda dei casi tra i diversi componenti).

Per questo motivo, nel seguito del documento si userà la denominazione di **Relying Party** (cfr.[SAML-Glos]) per indicare un generico componente che interagisce mediante richieste SAML con una certa entità del modello (per esempio al fine di ottenere il rilascio di asserzioni). Analogamente, si userà la denominazione di **Asserting Party** (cfr. [SAML-Glos]) qualora occorra indicare genericamente un componente in grado di rispondere a richieste SAML e di emettere asserzioni.

# 8. SERVIZI INFRASTRUTTURALI

## 8.1. Registry ARS e AARS

I servizi di registry hanno il compito di fornire l'elenco delle authority appartenenti alla federazione. Anche se logicamente i servizi sono due, a livello implementativo ha senso unirli in un unico servizio che svolga le funzionalità di entrambi.

Il Servizio viene contattato ogni qualvolta si ha bisogno di ottenere:

- l'elenco delle Profile Authority;
- l'elenco degli Identity Provider;
- l'elenco delle Attribute Authority;
- ottenere informazioni relative a una singola authority della federazione.

In tutti questi casi l'interazione consiste nell'inoltro da parte di un generico Relying Party (ad esempio il sottosistema FG del Service Provider o la Profile Authority) di una richiesta di attributi opportunamente formattata e nella ricezione della relativa risposta.

La figura sottostante evidenzia l'interfaccia dei servizi di registry ARS e AARS. Tali servizi, trattati separatamente nel modello, vengono offerti da una unica applicazione. L'applicativo deputato ad offrire in modo congiunto i servizi di ARS e AARS viene indicato nel seguito come Authority Registry

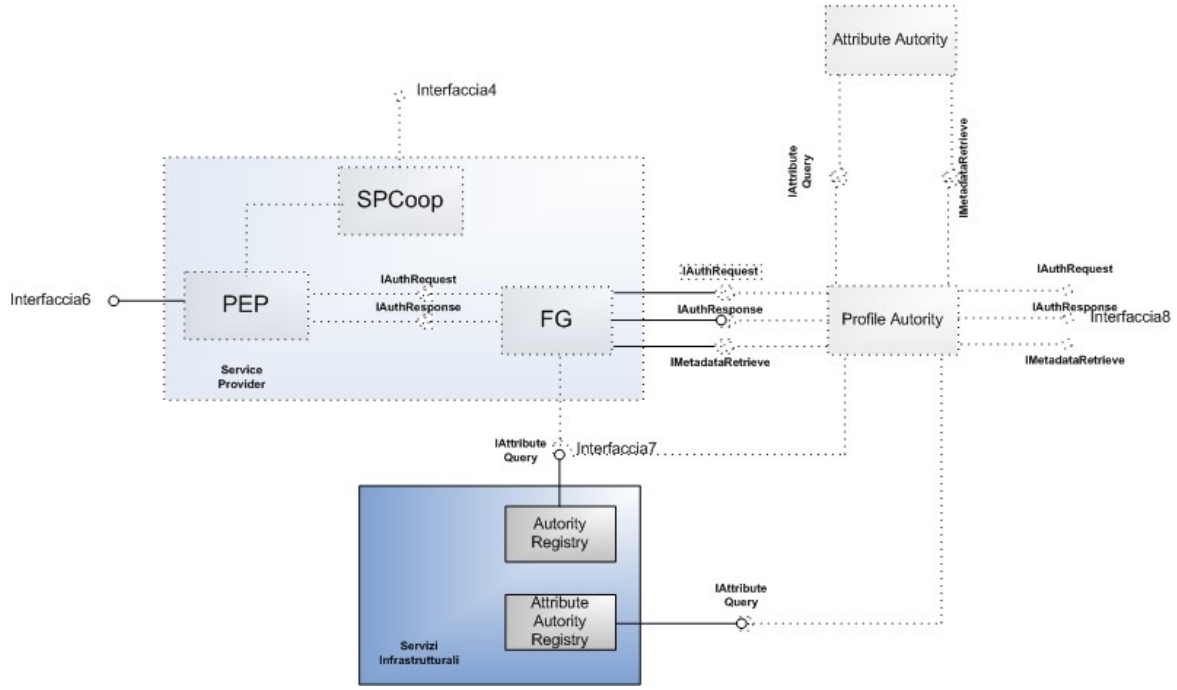



**Figura 17: Architettura dei Registry Service**

Il componente Authority Registry si può assimilare ad una particolare Attribute Authority. In questo caso gli scenari di interazione si basano sul formato delle asserzioni, sui protocolli (cfr. [SAML-Core]) e sui binding ("SAML SOAP binding") previsti dalla specifica (cfr. [SAML-Bindings], sez. 3.2).

Le interfacce che caratterizzano il Servizio sono:

- **IAttributeQuery:** interfaccia applicativa che supporta le operazioni di interrogazione del registro mediante richieste di attributo SAML;
- **IMetadataRetrieve**: permette il reperimento dei metadati SAML.

### *8.1.1. Scenario di interazione F-SSO*

Lo scenario di interazione descrive l'inoltro di una opportuna richiesta da parte di un Relying Party (es: Federation Gateway, Profile Authority) al componente Authority Registry e la ricezione della relativa risposta. L'interazione con il componente Authority Registry avviene attraverso l'interfaccia applicativa **`IAttributeQuery`**.

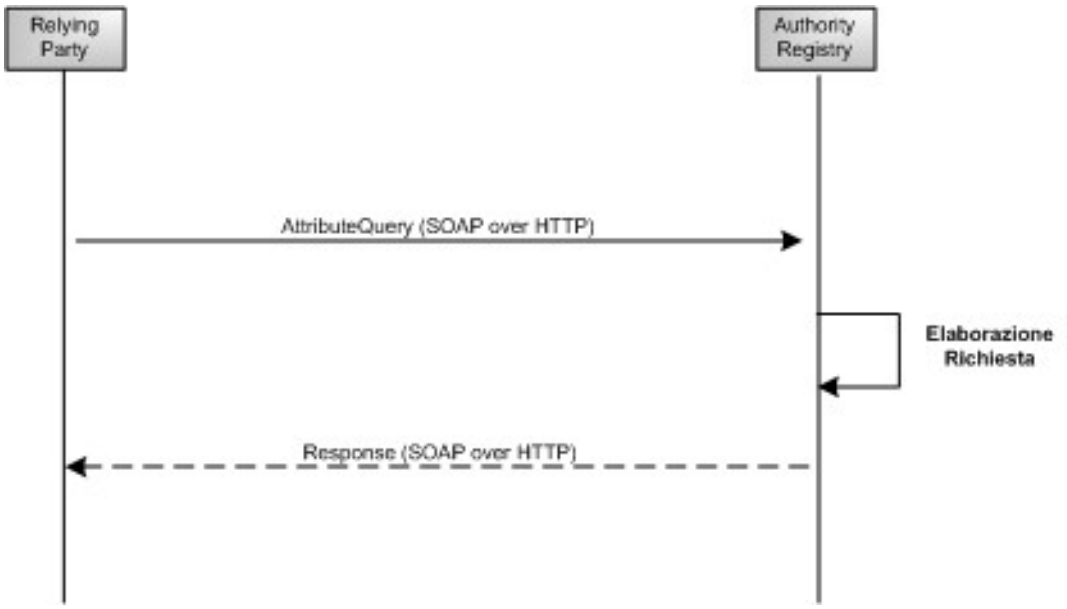



**Figura 18: Generica richiesta ad una Authority Registry e relativa risposta**

| Passo | Descrizione | Interfaccia | SAML | Binding |
|---|---|---|---|---|
| 1 | Il Relying Party invia all'Authority Registry una richiesta di attributi | IAttributeQuery | <AttributeQuery> | SOAP Over HTTP |

| | | | | |
|---|---|---|---|---|
| | opportunamente formattata. Ciò avviene utilizzando l'elemento <AttributeQuery> della specifica SAML e interagendo mediante "SAML SOAP binding" | | | |
| 2 | L'Authority Registry elabora la richiesta ricevuta | - | - | - |
| 3 | L'Authority Registry risponde alla richiesta del Relying Party con una <Response> SAML contenente l'asserzione contenente a sua volta statement di attributo opportunamente formattati e interagendo mediante "SAML SOAP binding | IAttributeQuery | <Response> | SOAP Over HTTP |

### *8.1.2. Struttura dei messaggi*

Nel caso del "discovery" di Identity Provider, Profile Authority e Attribute Authority della federazione, la query indirizzata all'Authority Registry è priva di statement di attributo e contiene un subject "speciale", che può essere rispettivamente "IDP_LIST" o "PA_LIST" o "AA_LIST". Questa scelta è determinata dall'esigenza di sopperire nel caso in esame all'assenza di un subject "reale" da poter utilizzare ai fini del discovery, e dall'obbligatorietà dell'elemento <Subject> nella AttributeQuery SAML.

A fronte di una query contenente uno dei subject "speciali" appena descritti, l'Authority Registry risponde con una <Response> SAML contenente un solo attributo che ha tanti valori quante sono le authority del tipo specificato presenti nel suo database interno. Ciascun valore è strutturato in un file XML il cui schema è rappresentato in Figura 19

Tale file contiene informazioni quali l'entityID (lo stesso valore presente nei metadati dell'entità), la descrizione, il tipo, l'URL del servizio di richiesta metadati e il dominio di appartenenza dell'authority descritta.

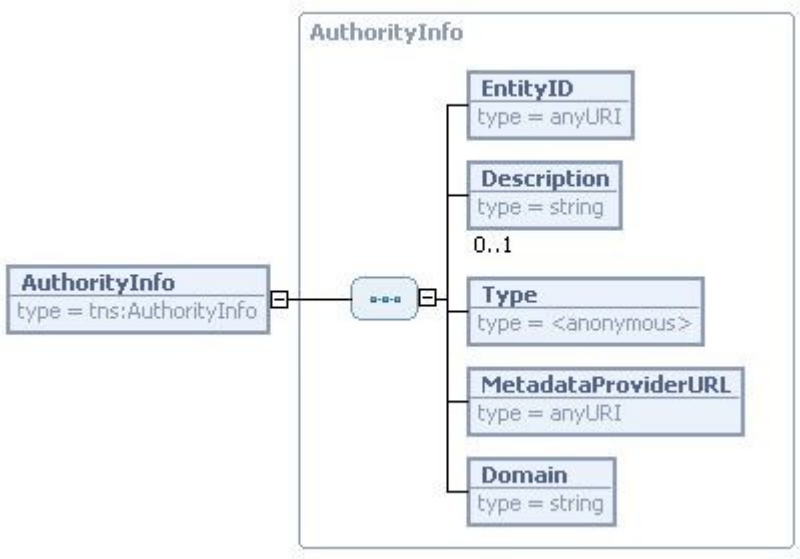



**Figura 19:Rappresentazione grafica dello schema XML contenente le informazioni su una generica authority**

```
    <?xml version="1.0" encoding="UTF-8"?>
    <schema xmlns="http://www.w3.org/2001/XMLSchema"
            targetNamespace="http://www.cnipa.gov.it/ar/b001"
            xmlns:tns="http://www.cnipa.gov.it/ar/b001"
            elementFormDefault="qualified">
        <element name="AuthorityInfo" type="tns:AuthorityInfo"></element>
        <complexType name="AuthorityInfo">
           <sequence>
                 <element name="EntityID" type="anyURI" maxOccurs="1"
                       minOccurs="1">
                 </element>
                 <element name="Description" type="string" maxOccurs="1"
                       minOccurs="0">
                 </element>
                 <element name="Type" type="string" maxOccurs="1"
minOccurs="1">
                 </element>
                 <element name="MetadataProviderURL" type="anyURI"
```

```
                        maxOccurs="1" minOccurs="1">
                    </element>
                    <element name="Domain" type="string" maxOccurs="1"
minOccurs="1">
                    </element>
                </sequence>
            </complexType>
        </schema>
```

Il file XML sottostante basato sullo schema illustrato contiene informazioni quali l'entityID (coincide con l'analogo valore presente nei metadati dell'entità), la descrizione (opzionale), il tipo ("Profile Authority", "Identity Provider" ecc.), l'URL del servizio di reperimento metadati e il dominio di appartenenza dell'authority descritta. Segue un esempio del file XML che descrive una Profile Authority.

```
    <?xml version="1.0" encoding="UTF-8"?>
    <AuthorityInfo xmlns="http://www.cnipa.gov.it/ar/b001">
      <EntityID>https://pa.cnipa.gov.it:3443/pa</EntityID>
      <Description>Profile Authority 1</Description>
      <Type>Profile Authority</Type>
      <MetadataProviderURL>https://pa.cnipa.gov.it:3443/pa/MetadataPublisherSerl
vet</MetadataProviderURL>
      <Domain>domain1</Domain>
    </AuthorityInfo>
```

### *8.1.3. Binding SOAP over HTTP per l'inoltro di richieste da parte di un Relaying Party (PA, SP)*

L'interazione con i servizi infrastrutturali consiste nell'inoltro di una richiesta di attributi e nella ricezione della relativa risposta. I costrutti SAML a cui si fa riferimento sono la <AttributeQuery> e la relativa <Response>. Gli scenari di interazione per la richiesta di attributi si basano sul "SAML SOAP binding" previsto dalla specifica (cfr. [SAML-Core], 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).

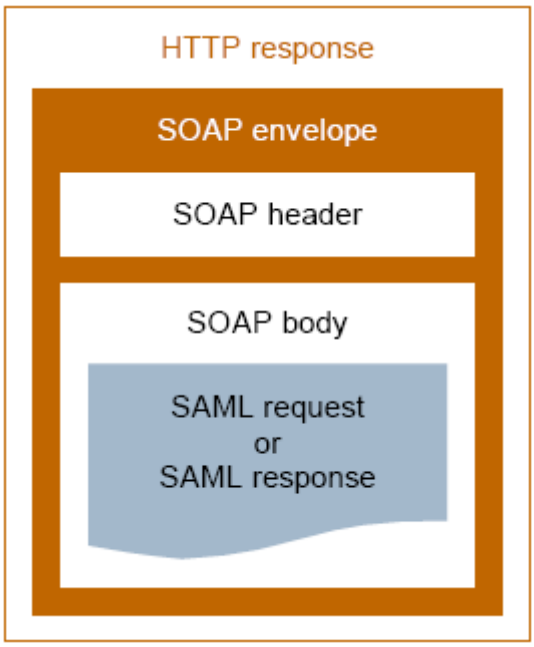



**Figura 20. Costrutti SAML trasportati con binding SOAP over HTTP (cfr. SAMLCore, sez. 3.3.4)**

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. [SAML-Core], sez. 3.2.3).

### *8.1.4. Caratteristiche dell'AttributeQuery per richiesta elenco Authority*

Coerentemente con quanto previsto dalla specifica SAML (cfr.[SAML-Core]), le caratteristiche che deve avere la `<AttributeQuery>` nel caso di discovery di authority della federazione sono le seguenti:

- deve essere presente l'attributo `ID` univoco, per esempio basato su un Universally Unique Identifier (UUID) (cfr. 0) o su una combinazione *origine* + *timestamp*;
- deve essere presente l'attributo `Version`, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata;
- deve essere presente l'attributo `IssueInstant` a indicare l'istante di emissione della richiesta, in formato UTC;
- deve essere presente l'attributo `Destination`, a indicare l'indirizzo (URI reference) a cui è stata inviata la richiesta, cioè l'Attribute Service dell'Authority Registry;

- deve essere presente l'elemento `<Issuer>` a indicare l'entityID dell'entità emittente, cioè il Relying Party;
- deve essere presente l'elemento `<Subject>` (il cui elemento `<NameID>` può assumere uno dei formati specifici previsti dalla specifica SAML per gli identificativi, cfr. 0, sez. 8.3, tra cui il formato "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" qualora non riconducibile a uno degli altri formati) a indicare il tipo di authority a cui si riferisce il discovery, e in particolare può valere (salvo introduzione di altre tipologie di authority, come osservato in precedenza):
  - "PA_LIST" se si vuole ottenere l'elenco delle Profile Authority della federazione,
  - "IDP_LIST" se si vuole ottenere l'elenco degli Identity Provider della federazione, oppure
  - "AA_LIST" se si vuole ottenere l'elenco delle Attribute Authority della federazione;
- deve essere presente l'elemento `<Signature>` apposto dall'entità emittente.

Per maggiori dettagli sulla struttura standard di una richiesta di attributo SAML, si rimanda alla già citata specifica [SAML-Core] e ai documenti correlati.

Un esempio AttributeQuery da una Relying Party verso i servizi di registry è mostrato in Appendice B.

### 8.1.5. Caratteristiche della Response per risposta elenco Authority

Coerentemente con quanto previsto dalla specifica SAML (cfr. [SAML-Core]), l'elenco delle Authority restituite avviene tramite Response. Le caratteristiche che deve avere la `<Response>` di risposta a una richiesta di discovery di authority sono le seguenti:

- deve essere presente l'attributo `ID` univoco, per esempio basato su un Universally Unique Identifier (UUID) (cfr. 0) o su una combinazione *origine* + *timestamp*;
- deve essere presente l'attributo `Version`, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata);
- deve essere presente l'attributo `IssueInstant` a indicare l'istante di emissione della risposta, in formato UTC;
- deve essere presente l'attributo `InResponseTo`, il cui valore deve fare riferimento all'`ID` della richiesta a cui si risponde;
- deve essere presente l'attributo `Destination`, a indicare l'indirizzo (URI reference) a cui è inviata la richiesta, cioè l'Attribute Service del Relying Party;

- deve essere presente l'elemento <Status> a indicare l'esito (sotto-elemento <StatusCode>) della richiesta a cui si risponde;
- deve essere presente l'elemento <Issuer> a indicare l'entityID dell'entità emittente, cioè l'Authority Registry stesso;
- deve essere presente un elemento <Assertion> contenente un elemento <AttributeStatement>;
- l'elemento <Assertion> deve avere gli attributi Version, ID e IssueInstant opportunamente valorizzati (vedi quanto detto sopra circa gli attributi dell'elemento <Response>);
- l'elemento <Assertion> deve contenere gli elementi <Issuer> (l'Authority Registry stesso) e <Subject> (es: "PA_LIST" o "IDP_LIST");
- l'elemento <Assertion> deve essere firmato dall'authority emittente (l'Authority Registry stesso);
- l'elemento <Assertion> deve contenere un elemento <Conditions> che ne determini i vincoli di validità temporale;
- l'elemento <AttributeStatement> contenuto nell'elemento <Assertion> deve contenere un solo elemento <Attribute> con attributo Name e contenente i relativi elementi <AttributeValue>, tanti quante sono le authority, presenti nel database interno, del tipo specificato nella richiesta a cui si sta rispondendo;
- ciascun elemento <AttributeValue> deve adottare il formato XML strutturato descritto in precedenza e può essere codificato in formato Base64;
- deve essere presente l'elemento <Signature> apposto dall'entità emittente.

Per maggiori dettagli sulla struttura standard di una risposta a una richiesta di attributo SAML, si rimanda alla già citata specifica [SAML-Core] ed ai documenti correlati.

Un esempio Response dall'Authority Registry verso una relying party è mostrato in Appendice B.

### 8.1.6. Caratteristiche dell'AttributeQuery per richiesta singola Authority

Nel caso della richiesta di informazioni relative a una specifica authority della federazione, le caratteristiche che deve avere la <AttributeQuery> sono le seguenti:

- deve essere presente l'attributo `ID` univoco, per esempio basato su un Universally Unique Identifier (UUID) (cfr. 0) o su una combinazione *origine* + *timestamp*;
- deve essere presente l'attributo `Version`, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata;
- deve essere presente l'attributo `IssueInstant` a indicare l'istante di emissione della richiesta, in formato UTC;
- deve essere presente l'attributo `Destination`, a indicare l'indirizzo (URI reference) a cui è inviata la richiesta, cioè l'AttributeService della Attribute Authority;
- deve essere presente l'elemento `<Issuer>` a indicare l'entityID dell'entità emittente, cioè il Relying Party;
- deve essere presente l'elemento `<Subject>` a indicare l'entityID dell'authority a cui si riferisce la richiesta di informazioni, contenente l'elemento `<NameID>` e i relativi attributi `Format` e `NameQualifier`;
- deve essere presente l'elemento `<Signature>` apposto dall'entità emittente.

Per maggiori dettagli sulla struttura standard di una richiesta di attributo SAML, si rimanda alla già citata specifica [SAML-Core] e ai documenti correlati.

### 8.1.7. Caratteristiche della Response per risposta singola Authority

Le caratteristiche che deve avere la `<Response>` di risposta a una richiesta di informazioni su una singola authority sono le seguenti:

- deve essere presente l'attributo `ID` univoco, per esempio basato su un Universally Unique Identifier (UUID) (cfr.[UUID]) o su una combinazione *origine* + *timestamp*;
- deve essere presente l'attributo `Version`, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata;
- deve essere presente l'attributo `IssueInstant` a indicare l'istante di emissione della risposta, in formato UTC;
- deve essere presente l'attributo `InResponseTo`, il cui valore deve fare riferimento all'`ID` della richiesta a cui si risponde;
- deve essere presente l'attributo `Destination`, a indicare l'indirizzo (URI reference) a cui è inviata la richiesta, cioè l'AttributeService del Relying Party;

- deve essere presente l'elemento `<Status>` a indicare l'esito (sotto-elemento `<StatusCode>`) della richiesta a cui si risponde;
- deve essere presente l'elemento `<Issuer>` a indicare l'entityID dell'entità emittente, cioè l'Authority Registry stesso;
- deve essere presente un elemento `<Assertion>` contenente un elemento `<AttributeStatement>`;
- l'elemento `<Assertion>` deve avere gli attributi `Version`, `ID` e `IssueInstant` opportunamente valorizzati (vedi quanto detto sopra circa gli attributi dell'elemento `<Response>`);
- l'elemento `<Assertion>` deve contenere gli elementi `<Issuer>` (l'Authority Registry stesso) e `<Subject>` (l'entityID dell'authority di cui si forniscono le informazioni);
- l'elemento `<Assertion>` deve essere firmato dall'authority emittente;
- l'elemento `<Assertion>` deve contenere un elemento `<Conditions>` che ne determina i vincoli di validità temporale;
- l'elemento `<AttributeStatement>` contenuto nell'elemento `<Assertion>` deve contenere gli elementi `<Attribute>` (con attributo `Name` e i relativi elementi `<AttributeValue>`) corrispondenti agli attributi che descrivono l'entità ("Type", "Domain", "Description", "EntityID", "MetadataProviderURL");
- deve essere presente l'elemento `<Signature>` apposto dall'entità emittente.

Per maggiori dettagli sulla struttura standard di una risposta a una richiesta di attributo SAML, si rimanda alla già citata specifica SAML-Core e ai documenti correlati.

## 8.2. Profile Authority

La profile Authority ha il compito di gestire il profilo dell' End User occupandosi di prepare il portafoglio di asserzioni sia di identità che di attributo.

All'arrivo dell' End User, a valle di una redirect del Service Provider, la Profile Auhority deve:

1. Contattare i servizi di registry per recuperare i metadati degli IDP disponibili per l'autenticazione dell'End User;
2. Recuperare i metadati degli IdP presenti nella lista;
3. Ridirezionare l'End User verso L'IdP scelto;
4. Ricevere la Response dall'IdP con l'asserzione di Autenticazione;
5. Mostrare i profili associati all'End User;

6. A valle della selezione del profilo, contattare i servizi di Registry per recuperare la lista dei metadati inerenti le Attribute Authority appartenenti alla federazione;
7. Recuperare i metadati delle Attribute Authority presenti nella lista fornita dai servizi di registry;
8. Per ogni attributo presente nel profilo richiedere un'asserzione di attributo tramite una SAML Attribute Query;
9. A valle della ricezione delle response dalle Attribute Authority interpellate, costruisce una response da inviare al Service Provider. La response contiene una Asserzione con all'interno gli Statement di autenticazione e di attributo;

Il recupero dei metadati (punti 2, 3, 6,7) possono essere saltati qualora tali dati siano già presenti nella cache ed ancora validi.

Nella figura sottostante vengono riportate le interfacce della Profile Authority.

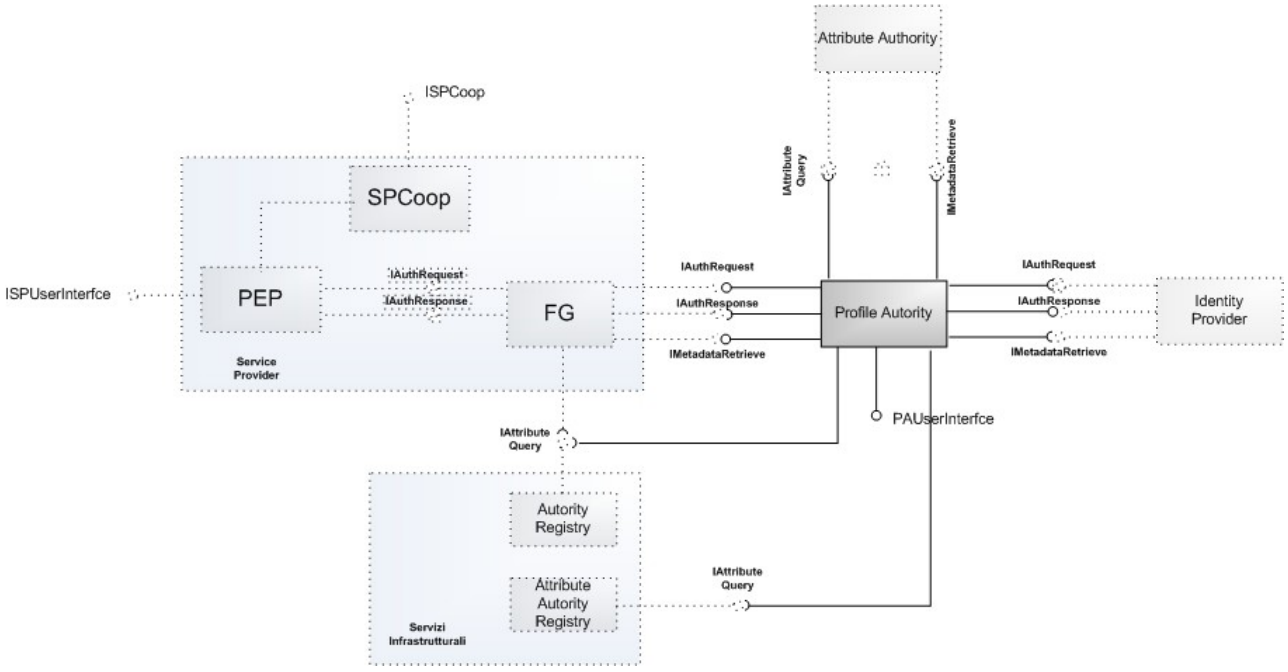



**Figura 21: Architettura della Profile Authority**

Il componente espone le seguenti interfacce:

- **IPAUserInterface :** permette agli utenti l'interazione via web con il componente tramite User Agent (per esempio in fase di scelta o creazione del profilo);
- **IAttributeQuery**: interfaccia applicativa che supporta le operazioni di interrogazione del profilo utente mediante richieste di attributo SAML. Viene utilizzata anche per interrogare le authority del GC-SICA;
- **IMetadataRetrieve**: permette il reperimento dei metadati SAML.
- **IAuthnRequest** e **IAuthnResponse**: permettono l'inoltro e la ricezione di richieste e risposte di autenticazione SAML;

### *8.2.1. Scenario di interazione F-SSO*

Lo scenario di interazione descrive l'inoltro di una opportuna richiesta da parte di un Relying Party (es: il sottosistema Federation Gateway del Service Provider) al componente Profile Auhtority e la relativa risposta. L'inoltro avviene tramite una redirect del browser dell'End User. L'interazione con il componente Authority Registry avviene attraverso l'interfaccia applicativa **`IAttributeQuery`**, l'interazione invece con il Service Provider e l'identity provider avviene tramite le interfacce **`IAuthnRequest`** e **`IAuthnResponse`**.

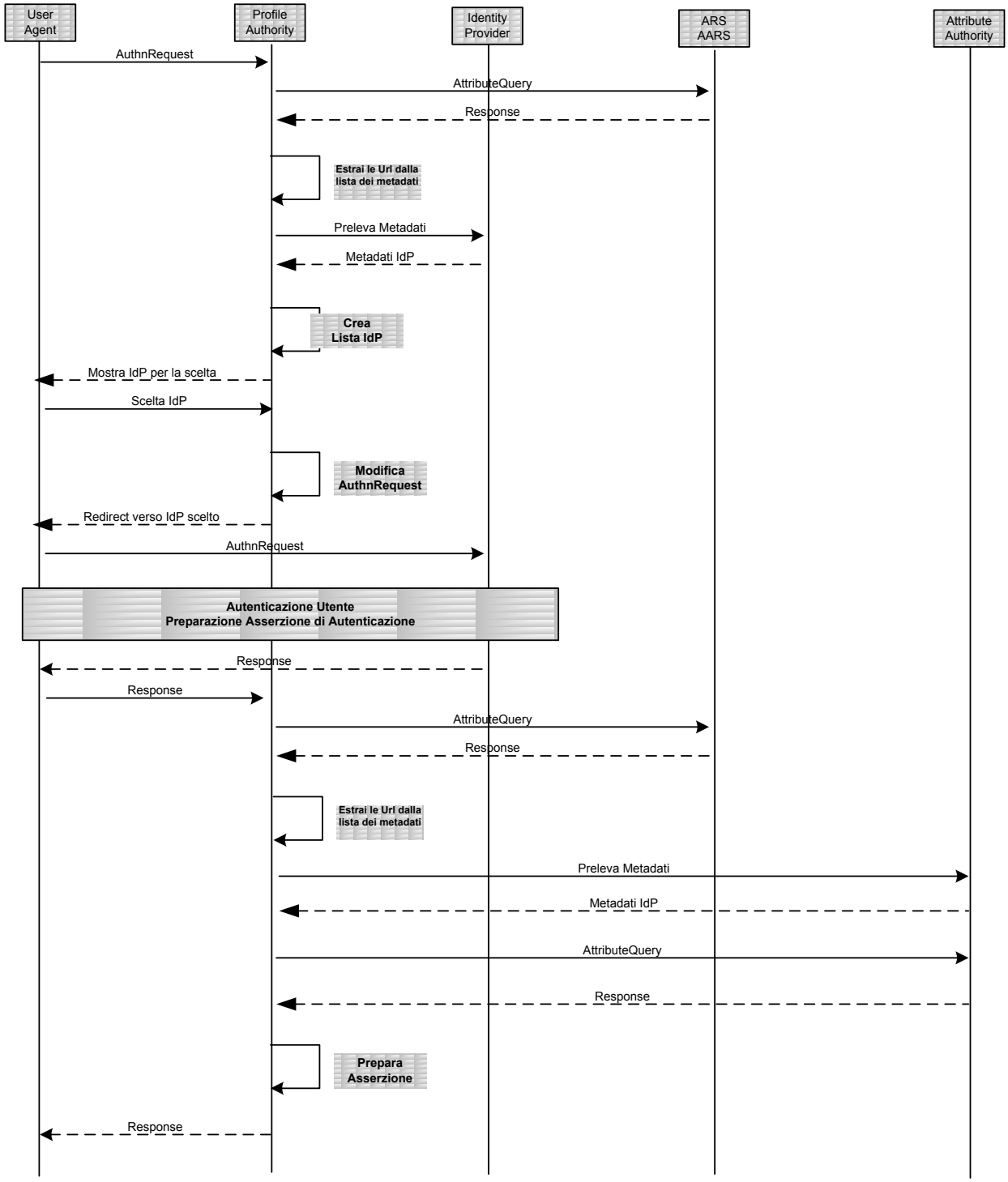



**Figura 22: Flusso di una richiesta di autenticazione gestita tramite la Profile Authority**

| Passo | Descrizione | Interfaccia | SAML | Binding |
|---|---|---|---|---|
| 1 | L'end user tramite il proprio Web browser (UA) contatta la Profile | IAuthRequest | <AuthnRequest> | HTTP Redirect |

| | | | | |
|---|---|---|---|---|
| | Authority per richiedere l'autenticazione. | | | HTTP POST |
| 3 | La PA contatta i servizi di registry (l'ARS) per prelevare la lista degli IDP inviando all'Authority Registry una richiesta di attributi opportunamente formattata. | IAttributeQuery | <AttributeQuery> | SOAP over HTTP |
| 4 | L'Authority Registry risponde alla richiesta del Relying Party con una <Response> SAML contenente l'asserzione contenente a sua volta uno o più statement di attributo opportunamente formattati. | IAttributeResponse | <AttributeResponse> | SOAP over HTTP |
| 5 | La PA estrae le URI degli IdP. | - | - | - |
| 6 | Per ogni IDP presente nella lista la PA contatta l'URI ricevuta per scaricare i metadati dell'IDP. | IMetadataRetrieve | | HTTPS GET |
| 7 | L'IDP fornisce i metadati. | IMetadataRetrieve | - | HTTPS |
| 8,9 | Dopo aver reperito tutte le informazioni sugli IDP disponibili fornisce una tendina con la scelta degli IDP e la mostra all'utente. | IUserInterface | - | HTTP |
| 10 | L'utente sceglie l'IDP su cui vuole autenticarsi. | IUserInterface | - | HTTP |
| 11 | La PA modifica la <AuthnRequest> in modo che appaia all'IdP a cui dovrà essere rimandata come se fosse stata emessa dalla PA e non dallo SP | - | - | - |
| 12 | La PA invia la <AuthnRequest> modificata all'IdP selezionato. | IAuthnRequest | <AuthnRequest> | HTTP Redirect<br>HTTP POST |
| 13 | L'IdP riceve la richiesta ed autentica l'utente. | - | - | - |
| 14 | L' IDP restituisce allo User Agent la <Response> SAML contenente l'asserzione che a sua volta contiene lo statement di autenticazione dell'utente più eventuali statement di attributo. | - | <Response> | HTTP POST |
| 15 | Lo user agent inoltra la binding HTTP-POST. | IAuthnResponse | <Response> | HTTP POST |
| 16 | La PA contatta i servizi di Registry (l'AARS) per prelevare la lista delle AA inviando all'Authority Registry una richiesta di attributi opportunamente formattata. | IAttributeQuery | <AttributeQuery> | SOAP over HTTP |
| 17 | L'Authority Registry risponde alla richiesta del Relying Party con una <Response> SAML contenente | IAttributeQuery | <AttributeResponse> | SOAP over HTTP |

| | | | | |
|---|---|---|---|---|
| | l'asserzione. L'asserzione può a sua volta contenere uno o più statement di attributo opportunamente formattati. | | | |
| 18 | La PA estrae le URI delle AA | - | - | - |
| 19 | Per ogni AA presente nella lista la PA contatta l'URI ricevuta per scaricare i metadati della AA | IMetadataRetrieve | | HTTPS GET |
| 20 | L'AA fornisce i metadati | IMetadataRetrieve | - | HTTPS |
| 21 | La Profile Authority Per ogni attributo presente nel profilo richiede la verifica all'authority competente. Per fare ciò invia a tutte la AA all'Attribute Authority una richiesta di attributi. | IAttributeQuery | <AttributeQuery> | SOAP Over HTTP |
| 22 | L'Authority Registry elabora la richiesta ricevuta rispondendo alla richiesta di attributi del Relying Party tramite una <Response> SAML contenente una asserzione. L'asserzione può contenere a sua volta più statement di attributo | IAttributeQuery | <Response> | SOAP Over HTTP |
| 23 | La PA prepara una response con all'interno una Asserzioni contenente sia lo statement di autenticazione sia quello di attributo. La response è costruita in modo che l'issuer sia la PA . | - | - | - |
| 24 | L'FG invia la response allo UA, La <Response> viene inserita in una form HTML inviata al browser dell'utente in una risposta HTTP | IAuthnResponse | Response | HTTP-POST |

### 8.2.2. Binding per l'inoltro di richieste da parte di un Relying party (SP/FG)

Il binding utilizzato per l'inoltro delle richieste verso una Profile Authority è il binding HTTP Redirect oppure l'HTTP POST. Per ulteriori dettagli si rimanda al capitolo "Binding per l'inoltro di richieste verso un Asserting Party ( IDP,PA)"

### 8.2.3. Binding per l'inoltro di richieste verso una asserting party (AA, IDP)

Similmente al paragrafo precedente il binding utilizzato per l'inoltro delle richieste verso un è il binding HTTP Redirect oppure l'HTTP POST. Per ulteriori dettagli si rimanda al capitolo "Binding per l'inoltro di richieste verso un Asserting Party ( IDP,PA)"

Diversamente binding utilizzato per l'inoltro delle richieste verso una Attribute Authority è il binding SOAP over http. Per ulteriori dettagli si rimanda al capitolo "Binding SOAP over HTTP per l'inoltro di richieste da parte di un Relaying Party (PA, SP)"

### *8.2.4. Caratteristiche della AuthnRequest e Response*

Le caratteristiche dell'AuthnRequest sono simili a quanto presentato nel paragrafo "Caratteristiche della AuthnRequest" relativo alla Service Provider a cui si rimanda.

Similmente per la Response le caratteristiche sono quelle presentate nel paragrafo "Caratteristiche della Response" inerente l' IDP e a cui si rimanda.

### *8.2.5. Caratteristiche della AttributeQuery e Response*

Le caratteristiche delle AttributeQuery e Response sono simili a quanto descritto nell'ambito dell'Attribute Authority nei paragrafi "Caratteristiche dell' AttributeQuery" e "Pubblica Amministrazione come Profile Authority".

# 9. PUBBLICA AMMINISTRAZIONE COME EROGATORE DI SERVIZI

## 9.1. Servizi Web tramite F-SSO

Un'Amministrazione che ricopre il ruolo di erogatore di servizi ricopre il ruolo di Service Provider e nello specifico a fronte di un tentativo di accesso federato deve:

1. essere in grado di ricevere la richiesta alla risorsa protetta ed avviare il processo di autenticazione;
2. interagire con l'authority registry per prelevare i metadati sulle profile authority della federazione;
3. proporre la lista delle Profile Authority presso cui l'utente può reperire le informazioni necessarie per accedere al servizio richiesto;
4. inoltrare la richiesta di autenticazione verso la PA scelta dall'utente;
5. ricevere I dati necessari all'accesso veicolati tramite SAML Response;
6. applicare le politiche di accesso locale (Policy enforcement);
7. erogare il servizio.

Nella figura sottostante si riportano le interfacce del Service Provider:

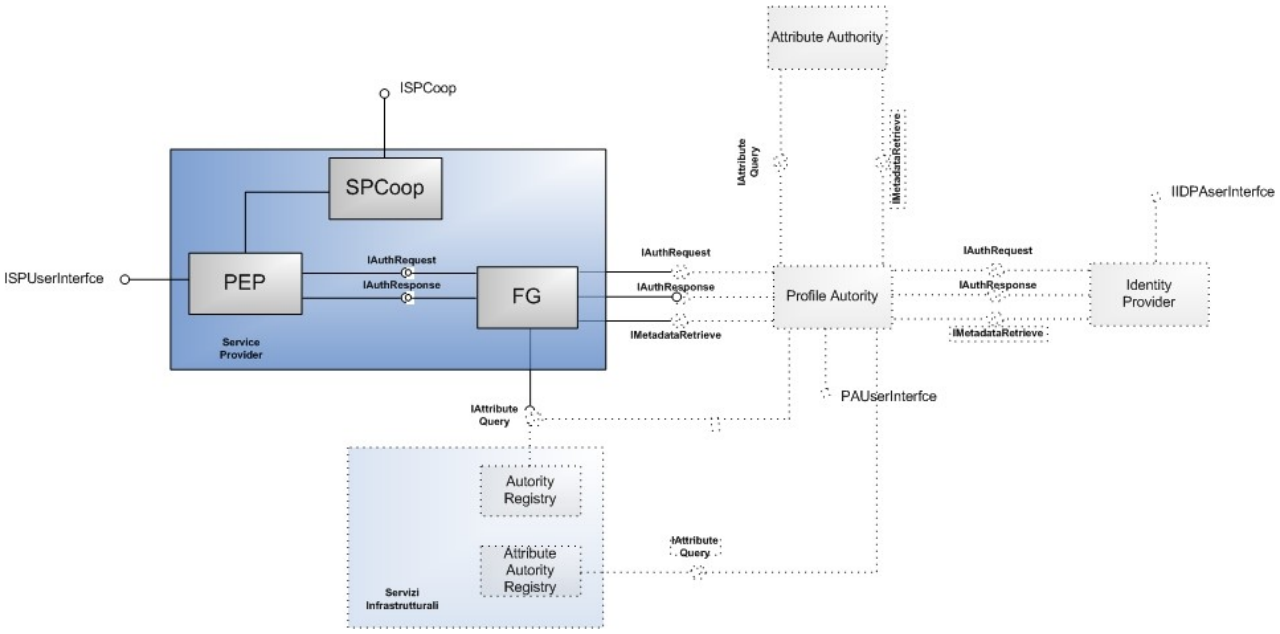



**Figura 23: Architettura Del Service Provider**

Le interfacce che caratterizzano l'SP sono:

- **ISPUserInterface :** permette agli utenti l'accesso via web tramite User Agent alle risorse e ai servizi offerti;
- **IAuthnRequest** e **IAuthnResponse**: permettono l'inoltro e la ricezione di richieste e risposte di autenticazione SAML;
- **IMetadataRetrieve**: permette il reperimento dei metadati SAML;
- **ISPCoop**: permette l'interazione in modalità di cooperazione applicativa fra due Amministrazioni;

Le attività e le interfacce descritte sono suddivise fra due sottosistemi logici il Policy Enforcerment Point (PEP) ed il Federation Gateway (FG).

L'amministrazione può decidere di implementare le funzionalità a carico dei due sottosistemi in due modalità:

## 9.2. Scenario Interazione Dinamica

Il PEP ha il FG come unico IDP a cui fare riferimento. Il FG maschera la complessità della federazione. In questo caso il PEP deve conoscere solamente i metadati del FG. Il diagramma di flusso relativamente alla gestione di una richiesta di accesso al servizio è quello disegnato in figura:

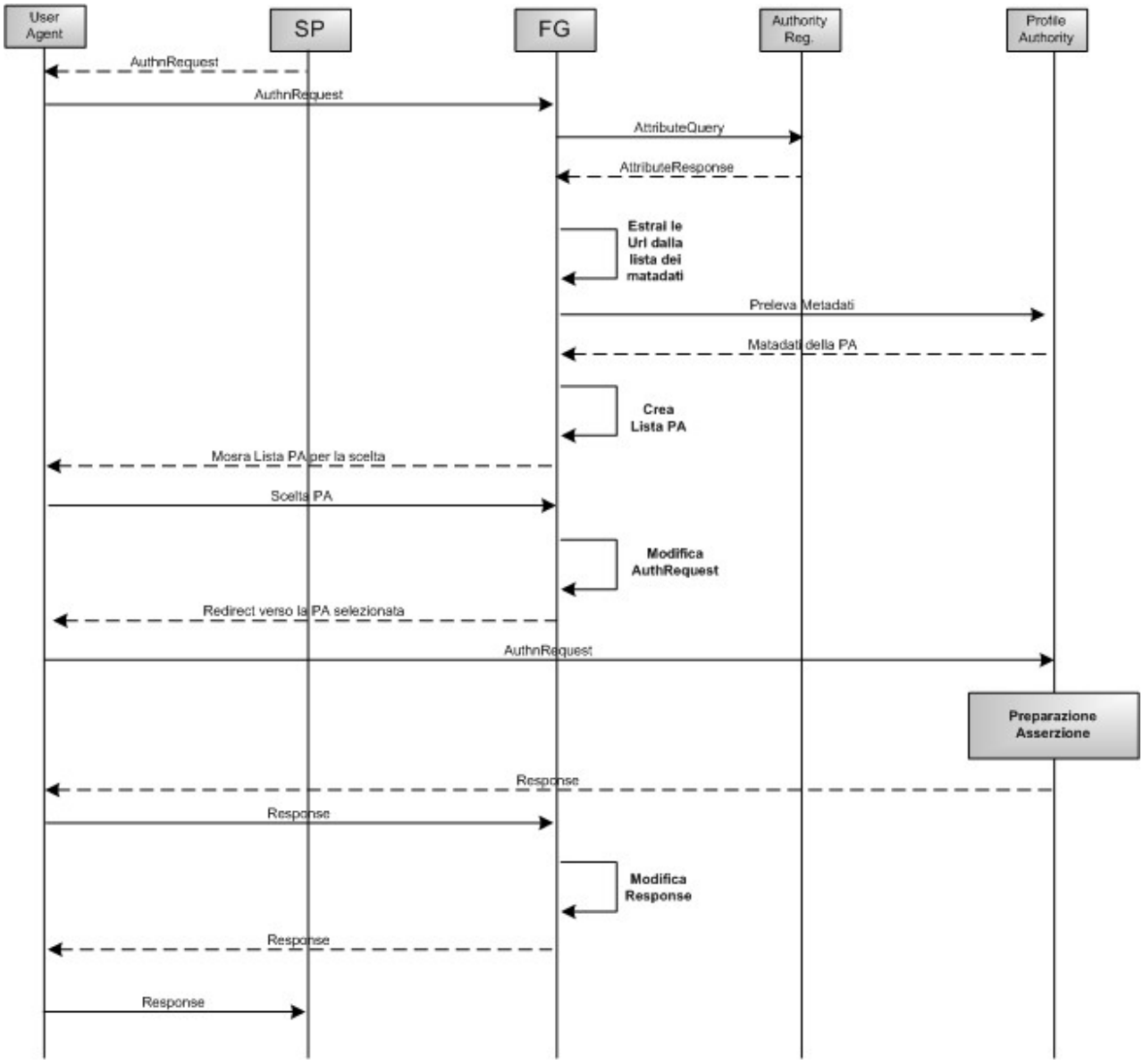



**Figura 24: Flusso di una richiesta di Autenticazione generate da un Service Provider**

| Passo | Descrizione | Interfaccia | SAML | Binding |
|---|---|---|---|---|
| 1 | L'end user tramite il proprio Web browser (UA) contatta il Service Provider per richiedere il servizio. Il SP invia allo User Agent una richiesta di autenticazione (per esempio a seguito di una richiesta di risorsa effettuata dall'utente) da far pervenire al sottosistema FG come se fosse l'IdP a cui richiedere l'autenticazione. | IAuthRequest | <AuthnRequest> | HTTP REDIRECT<br>HTTP POST |
| 2 | Lo User Agent inoltra la richiesta di autenticazione contattando il FG con modalità simile al passo 1. | - | <AuthnRequest> | HTTP REDIRECT<br>HTTP POST |
| 3 | Il FG contatta l'ARS per prelevare la lista delle PA inviando all'Authority Registry una richiesta di attributi opportunamente formattata. | IAttributeQuery | <AttributeQuery> | SOAP OVER HTTP |
| 4 | L'Authority Registry risponde alla richiesta del Relying Party con una <Response> SAML contenente l'asserzione contenente a sua volta statement di attributo opportunamente formattati. | IAttributeQuery | <AttributeResponse> | SOAP over HTTP |
| 5 | L'FG estrae le URI delle PA. | - | - | - |
| 6 | Per ogni PA presente nella lista l'FG contatta l'URI ricevuta per scaricare i metadati della PA. | IMetadataRetrieve | | HTTPS GET |
| 7 | La PA fornisce i metadati. | IMetadataRetrieve | - | HTTPS |
| 8,9 | Dopo aver reperito tutte le informazioni sulle PA disponibili fornisce una tendina con la scelta delle PA el la mostra all'utente. | IUserInterface | - | HTTP |
| 10 | L'utente sceglie la PA. | IUserInterface | - | HTTP |
| 11 | Il FG modifica la <AuthnRequest> in modo che appaia all'IdP a cui dovrà essere rimandata come se fosse stata emessa dal FG e non dall' SP. | - | - | - |
| 12 | Il FG invia la <AuthnRequest> modificata alla PA selezionata. | IAuthnRequest | <AuthnRequest> | HTTP-REDIRECT<br>HTTP POST |
| 13 | La PA riceve la richiesta e prepara il portafoglio delle asserzioni. | - | - | - |
| 14 | La PA restituisce allo User Agent la <Response> SAML contenente l'asserzione che a sua volta contiene lo statement di autenticazione dell'utente destinato più eventuali statement di attributo. La response viene inviata tramite binding HTTP-POST. | - | >Response> | HTTP-POST |

| | | | | |
|---|---|---|---|---|
| 15 | Lo user agent inoltra la <Response> al FG tramite binding HTTP-POST. | IAuthnResponse | <Response> | HTTP-POST |
| 16 | Il FG modifica la SAML Response per farla sembrare generata da lui in funzione di IdP. In particolare, viene sostituito l'Issuer presente nella response con il valore dell'entityID del FG e l'indirizzo (URL) del servizio AssertionConsumerService con quello del corrispondente servizio residente sul SP. | - | - | - |
| 17 | L'FG invia la response allo UA. La <Response> viene inserita in una form HTML inviata al browser dell'utente in una risposta HTTP. | IAuthnResponse | <Response> | HTTP-POST |
| 18 | Il browser dell'utente elabora la risposta HTTP e invia una richiesta HTTP-POST contenente la <Response> firmata verso. | - | <Response> | HTTP-POST |
| 19 | Lo SP riceve la <Response>. | IAuthnResponse | <Response> | HTTP-POST |

## 9.3. *Scenario interazione statica*

La soluzione statica sostituisce il FG implementando le sue funzionalità con dei processi e delle procedure operative manuali off-line, le interfacce deputate alla richiesta delle PA federate ed al reperimento dei metadati. In questo caso la sottoentità PEP del SP è composta dal solo sottosistema omonimo:

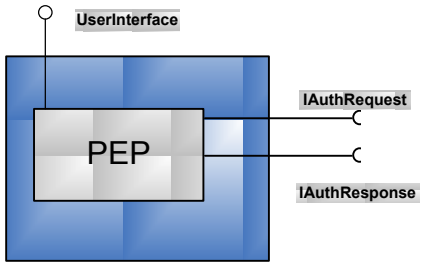



**Figura 25: Architettura SP nello scenario statico**

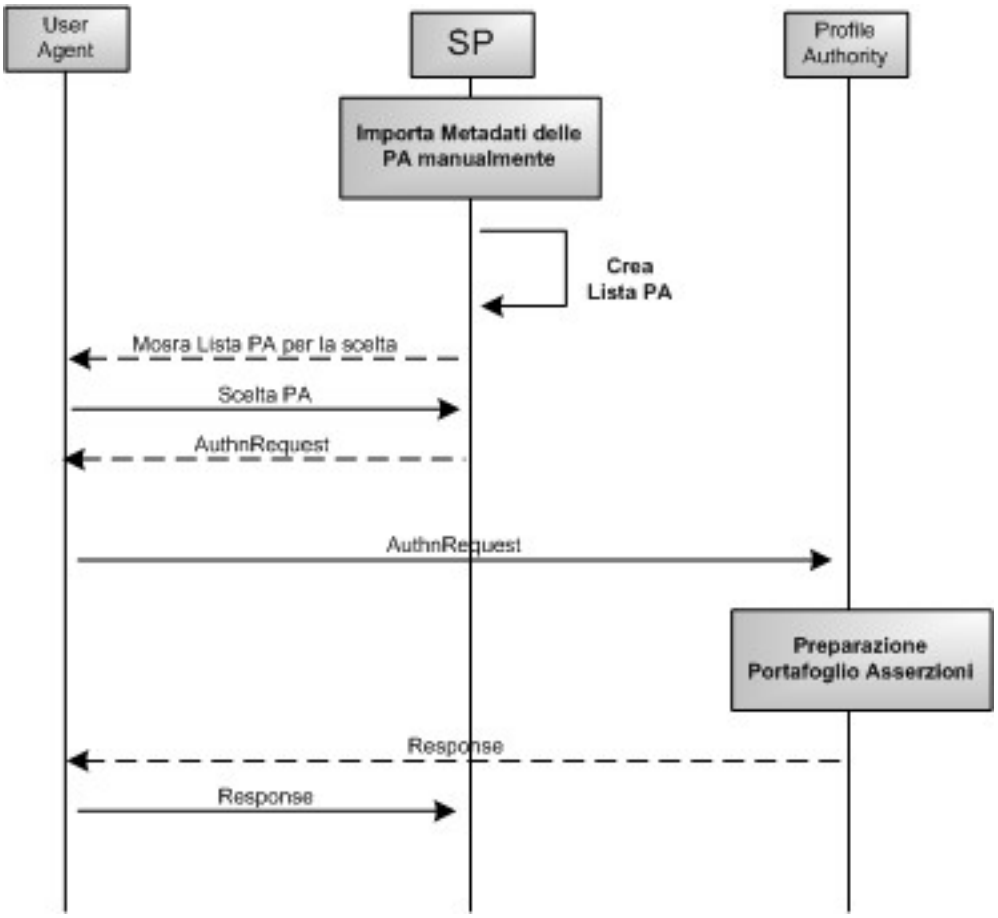



**Figura 26: Flusso di una richiesta di Autenticazione generata da un Service Provider in modalità statica**

| Passo | Descrizione | Interfaccia | SAML | Binding |
|---|---|---|---|---|
| 1 | Vengono importati manualmente tutti i metadati delle PA accreditate nella federazione. La sorgente delle informazioni è il CG-SICA. | - | - | - |
| 2,3 | Il SP crea la lista delle PA da mostrare all'End User. | IUserInterface | - | HTTP |
| 4 | L'utente scegli la PA. | IUserInterface | - | HTTP |
| 5 | Il SP invia la <AuthnRequest> alla PA selezionata. | IAuthnRequest | AuthnRequest | HTTP Redirect<br>HTTP POST |
| 6 | La PA riceve la richiesta e prepara il portafoglio delle asserzioni. | - | - | - |
| 7 | La PA restituisce allo User Agent la <Response> SAML contenente l'asserzione che a sua volta contiene lo statement di | - | Response | http POST |

| | | | | |
|---|---|---|---|---|
| | autenticazione dell'utente più eventuali statement di attributo. | | | |
| 8 | Il browser dell'utente elabora la risposta HTTP e invia una richiesta HTTP-POST contenente la <Response> firmata verso il SP. | - | Response | http-POST |
| 9 | L'SP riceve la <Response>. | IAuthnResponse | Response | http-POST |

Precondizioni per l'utilizzo dello scenario statico è che:

1. Vengano prelevate dal CG-SICA la lista delle Profile authority federate.
2. Per ogni PA presente nella lista si contatta l'URI associata prelevando (in modo autonomo) i metadati della PA.
3. I metadati prelevati dall'URI vengano importati all'interno del componente concettuale SP. Viene così costruita la lista delle PA che saranno mostrate all'utente.
4. A seguito di comunicazione di aggiornamento della lista da parte del SICA (secondo modalità da definire) la lista della PA dovrà essere aggiornata aggiungendo i metadati delle nuove entità o cancellando i metadati delle PA eventualmente deprecate.

Una amministrazione che vuole erogare servizi e per implementare il ruolo di SP ha due alternative:

1. scenario dinamico, l'Amministrazione si può avvalere del software di un vendor più un elemento ad hoc che implementi le funzionalità del FG. Questo elemento può essere implementato direttamente in base alle specifiche delle interfacce fornite anche avvalendosi di reference implementation disponibili;
2. scenario statico, l'Amministrazione può utilizzare soluzioni di mercato unitamente a dei delle procedure operative manuale che consentano la gestione delle funzionalità svolte dal sottosistema FG.

### *9.3.1. Binding per l'inoltro di richieste verso un Asserting Party ( IDP,PA)*

#### 9.3.1.1. Binding http redirect

La richiesta di autenticazione nel caso del binding HTTP Redirect viene veicolata con le seguenti modalità:

- come risposta alla richiesta di accesso dell'End User ad un servizio o risorsa, il Service Provider invia allo User Agent un messaggio HTTP di redirezione, cioè avente uno status code con valore 302 ("Found") o 303 ("See Other");

- il Location Header del messaggio HTTP contiene l'URI di destinazione del servizio di Single Sign-On esposto dal sottosistema FG in caso di scenario dinamico o dall'Identity Provider in caso di scenario statico. L'interfaccia è sempre la IAuthnRequest);
- il messaggio HTTP trasporta i seguenti parametri (tutti URL-encoded):
    1. "SAMLRequest": un costrutto SAML `<AuthnRequest>` codificato in formato Base64 e compresso con algoritmo DEFLATE. Come da specifica, il messaggio SAML non contiene la firma in formato XML Digital Signature esteso (come avviene in generale nel caso di binding HTTP POST). Ciò a causa delle dimensioni eccessive che esso raggiungerebbe per essere veicolato in una query string. La specifica indica come modalità alternativa quella di specificare con parametri aggiuntivi l'algoritmo utilizzato per firmare e la stringa con la codifica Base64 URL-encoded dei byte del messaggio SAML;
    2. "RelayState": identifica la risorsa (servizio) originariamente richiesta dall'utente e a cui trasferire il controllo alla fine del processo di autenticazione;
    3. "SigAlg": identifica l'algoritmo usato per la firma che può essere DSAwithSHA1 oppure RSAwithSHA1; il valore esteso di questo parametro è contestualizzato da un namespace appartenente allo standard XML Digital Signature. Come indicato al punto 1, tuttavia, la firma prodotta non fa uso della struttura XML definita in tale standard;
    4. "Signature": contiene la firma digitale della query string, così come prodotta prima di aggiungere questo parametro, utilizzando l'algoritmo indicato al parametro precedente.

Il browser dell'utente elabora quindi tale messaggio HTTP Redirect indirizzando una richiesta HTTP con metodo GET al servizio di Single Sign-On dell'Identity Provider (interfaccia IAuthnRequest) sotto forma di URL con tutti i sopraindicati parametri contenuti nella query string.

Un esempio di tale URL è il seguente, nel quale sono evidenziati in grassetto i parametri citati (i valori di alcuni parametri sono stati ridotti per brevità, inoltre il valore del parametro "RelyState" è stato reso non immediatamente intellegibile, come suggerito dalla specifica, sostituendo la stringa in chiaro con l'Id della richiesta: il Relying Party tiene traccia della corrispondenza):

```
    https://idp.cnipa.gov.it:6443/idp/SSOServiceProxy?
SAMLRequest=nVPLbtswELz3KwTeZb0M2SYsBa6NoAbSRrGUHnqjqFVDQCJVLuU4f19KlhEDbVygR5
K7O7Mzw%2FXdqW2cI2gUSiYkmPnEAclVJeTPhDwX9%2B6S3KWf1sjapqOb3rzIA%2FzqAY2zQQRtbNtW
Se

    […]

    ZwPAU88aUQvQ%2F8oe8S68piBDNabB5s3AyThb1XZMCxxEhhPj5qLZddW2sZIcoP4fBW%2BWccq
H0fZ6iNir0tUQGeCWZaGZxE5pM4n8Nz7p%2Be2D3S6L51x1NljO%2BCO2qh8zO%2Bji%2FfnN098%3D&
RelayState=s29f6c7d6bbf9e62968d27309e2e4beb6133663a2e&SigAlg=http%3A%2F%2Fwww
.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=LtNj%2BbMc8j%2FhglWzHPMmo0E
SQzBaWlmQbZxas%2B%2FIfNO4F%2F7WNoMKDZ4VVYeBtCEQKWp12pU7vPB5WVVMRMrGB8ZRAdHmmPp0h
J9opO3NdafRc04Z%2BbfnkSuQCN9NcGV%2BajT
```

```
[…]
ra169jhaGRReRQ9KkgSB3aTpQGaffAYUPVo2XZiWy6f9Z7zsmV%2FFoT8dg%3D%3D
```

**Figura 27: Esempio di SAML AuthnRequest veicolata tramite HTTP POST**

#### 9.3.1.2. Binding http POST

La richiesta di autenticazione nel caso del binding HTTP POST viene trasferita con le seguenti modalità:

- come risposta alla richiesta di accesso dell'utente ad un servizio o risorsa, il SP invia allo User Agent (il browser dell'utente) un messaggio HTTP con status code avente valore 200 ("OK");
- il messaggio HTTP contiene una form HTML all'interno della quale è trasportato un costrutto SAML `<AuthnRequest>` codificato come valore di un hidden form control di nome "SAMLRequest". Rispetto al binding HTTP Redirect, l'utilizzo di una form HTML permette di superare i limiti di dimensione della query string. Pertanto, l'intero messaggio SAML in formato XML può essere firmato in accordo alla specifica XML Digital Signature. Il risultato a valle della firma è quindi codificato in formato Base64;
- la form HTML contiene un secondo hidden form control di nome "RelayState" che contiene il corrispondente valore del Relay State, cioè della risorsa originariamente richiesta dall'utente e alla quale dovrà essere trasferito il controllo al termine della fase di autenticazione;
- la form HTML è corredata da uno script che la rende auto-postante all'indirizzo indicato nell'attributo "action".

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

Un esempio di form HTML per trasferire in HTTP POST la richiesta di autenticazione è descritto in figura 28. Osservando attentamente il codice riportato in figura si può notare il valore del parametro "SAMLRequest" (ridotto per brevità); il valore del parametro RelyState reso non immediatamente intellegibile (cfr. sez. precedente); l'elemento `<input type="submit" value="Go"/>`, che ha lo scopo di visualizzare all'interno del web browser il pulsante di invio della form utilizzabile dall'utente, non strettamente necessario in quanto la form è resa auto-postante.

```
<html>
  <body onload="javascript:document.forms[0].submit()">
```

```
        <form method="post"
action="https://lp.cnipa.gov.it:6443/lp/SSOServiceProxy">
            <input type="hidden" name="RelayState"
                           value="s2645f48777bd62ec83eddc62c066da5cb987c1eb3">
            <input type="hidden" name="SAMLRequest"
value="PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPHNhbWxwOkF1dGhuUmVxd
WVzdCBBc3NlcnRpb25Db25zdW1lclNlcnZpY2VVUkw9Imh0dHA6Ly9zcC5pY2FyLml0OjgwODAvaWNhc
[…]
N0ZWRUcmFuc3BvcnQ8L3NhbWw6QXV0aG5Db250ZXh0Q2xhc3NSZWY+PC9zYW1scDpSZXF1ZXN0ZWRBdX
RobkNvbnRleHQ+PHNhbWxwOlNjb3BpbmcgUHJveHlDb3VudD0iMiIgeG1sbnM6c2FtbHA9InVybjpvYX
NpczpuYW1lczp0YzpTQU1MOjIuMDpwcm90b2NvbCIvPjwvc2FtbHA6QXV0aG5SZXF1ZXN0Pg==">
            <input type="submit" value="Go"/>
        </form>
  </body>
</html>
```

**Figura 28: Esempio di SAML AuthnRequest veicolata tramite HTTP POST**

## 9.3.2. Caratteristiche della AuthnRequest

L'authnrequest che deve essere inviata al FG o all'IDP tramite i binding esposti in precedenza deve confermare le seguenti caratteristiche:

- deve essere presente l'attributo `ID` univoco, per esempio basato su un Universally Unique Identifier (UUID) o su una combinazione *origine* + *timestamp*.(Esempio ID = Assertion-uuidae7136e4-0118-18d8-999d-cff934ae63db);
- deve essere presente l'attributo `Version`, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata;
- deve essere presente l'attributo `IssueInstant` a indicare l'istante di emissione della richiesta, in formato UTC (esempio: "2008-03-13T18:04:15.531Z");
- deve essere presente l'attributo `ProtocolBinding`, una URI reference che identifica il binding da utilizzare per inoltrare il messaggio di risposta (`<Response>`): deve valere "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST";
- deve essere presente l'attributo `Destination`, a indicare l'indirizzo (URI reference) a cui è inviata la richiesta, ad esempio il servizio SSO Service del Federation Gateway o dell'Identity Provider;
- deve essere presente l'attributo `IsPassive` con valore "false", poiché non si vuole prevenire l'interazione esplicita tra certificatore di identità e utente;

- deve essere presente l'attributo `AssertionConsumerServiceURL` ad indicare l'URL a cui inviare il messaggio di risposta alla richiesta di autenticazione (in questo caso l'indirizzo del servizio AssertionConsumingService del Service Provider);
- deve essere presente l'elemento `<Issuer>` a indicare l'entityID del Relying Party emittente (N.B. la specifica SAML considera opzionale questo elemento; tuttavia esso è necessario ai fini del reperimento dei metadati o per la verifica della firma da parte dell'entità destinataria);
- può non essere presente l'elemento `<Subject>` (per esempio nel caso in cui esso non sia ancora noto al Relying Party);
- l'elemento `<NameIDPolicy>` avente il relativo attributo `AllowCreate` valorizzato a "false" segnala 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). All'interno dell'elemento `<NameIDPolicy>` deve essere presente l'attributo `Format` valorizzato con l'URI "urn:oasis:names:tc:SAML:2.0:nameid-format:transient";
- opzionalmente può essere presente l'attributo `ProxyCount` dell'elemento `<Scoping>`. In caso sia presente deve correttamente indicare il numero di redirezioni ammesse verso altri certificatori di identità; per esempio, deve valere "0" se si vuole impedire che l'Identity Provider contattato propaghi a sua volta la richiesta di autenticazione. Negli scenari in esame ad esempio se presente deve valere 2 nel caso della interazione con il FG e la PA (scenario dinamico) o valere 1 nel caso di interazione fra diretta con la PA (scenario statico);
- opzionalmente può essere presente l'attributo `AttributeConsumingServiceIndex`. Se presente deve essere posto pari all'indice posizionale della struttura AttributeConsumingService presente nei metadati del Relying Party (avente il ruolo di Service Provider) ed atta a descrivere i requisiti in termini di attributi necessari per accedere al servizio richiesto dall'utente (offerto dal Relying Party stesso se svolge il ruolo di Service Provider, o da un'entità a monte di esso qualora il Relying Party stia semplicemente propagando la richiesta di autenticazione);
- opzionalmente può essere presente l'elemento `<IDPList>` dell'elemento `<Scoping>`. Se presente, contiene la lista delle entità (rappresentate da elementi `<IDPEntry>` nei quali è specificato il rispettivo entityID nell'attributo `ProviderID`) che il Relying Party considera fidate ai fini dell'elaborazione della richiesta di autenticazione;
- opzionalmente possono essere presenti zero o più elementi `<RequesterID>` dell'elemento `<Scoping>`. Se presente deve indicare l'URL del servizio di reperimento metadati di ciascuna delle entità che hanno emesso originariamente la richiesta di autenticazione e di quelle che in seguito la hanno propagata, possibilmente mantenendo un ordine che indichi la sequenza di

propagazione (per esempio, il primo elemento <RequesterID> dell'elemento <Scoping> è relativo all'ultima entità che ha propagato la richiesta);

- l'elemento <Conditions> se presente deve indicare i limiti di validità attesi dell'asserzione ricevuta in risposta, per esempio specificando gli attributi NotBefore e NotOnOrAfter opportunamente valorizzati in formato UTC;
- può essere presente l'elemento <RequestedAuthnContext> (cfr. [SAMLCore], sez. 3.3.2.2.1) ad indicare il contesto di autenticazione atteso, ossia la "robustezza" delle credenziali richieste (autenticazione mediante username e password, mediante smartcard ecc.). Il contesto di autenticazione è descritto mediante il riferimento a "classi" definite dalla specifica SAML (cfr.[SAMLAuthContext] sez. 3), eventualmente estendibili, dette "authentication context class": ciascuna di queste classi, referenziate dagli elementi <AuthnContextClassRef>, indica in ordine di preferenza il contesto di autenticazione (atteso o effettivo) secondo alcune dimensioni di riferimento, quali per esempio i meccanismi di autenticazione con cui l'Identity Provider può identificare l'utente. L'elemento <RequestedAuthnContext> prevede un attributo Comparison con il quale indicare il metodo per stabilire il rispetto del vincolo sul contesto di abilitazione: i valori ammessi per questo attributo sono "exact", "minimum", "better", "maximum" (nel presente documento si adotta sempre il valore "exact", che richiede l'esatta corrispondenza con uno dei contesti descritti). Nel caso dell'elemento <RequestedAuthnContext>, questa informazione si riflette sulle tipologie di meccanismi utilizzabili dall'Identity Provider ai fini dell'autenticazione dell'utente. Segue un esempio di <RequestedAuthnContext> che fa riferimento a una "authentication context class" di tipo "password" (autenticazione mediante password attraverso una sessione HTTP non protetta, cfr. [SAMLAuthContext], sez. 3.4.8) o in subordine a una di tipo "public key X.509" (cfr. [SAMLAuthContext], sez. 3.4.11):

```
<samlp:RequestedAuthnContext Comparison="exact">
      <saml:AuthnContextClassRef>
            urn:oasis:names:tc:SAML:2.0:ac:classes:Password
      </saml:AuthnContextClassRef>
      <saml:AuthnContextClassRef>
            urn:oasis:names:tc:SAML:2.0:ac:classes:X509
      </saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

- nel caso del binding HTTP POST, deve essere presente l'elemento <Signature> apposto dal Relying Party.

Per maggiori dettagli sulla struttura standard di una risposta a una richiesta di autenticazione SAML, si rimanda alla già citata specifica [SAMLCore].

Un esempio Authnrequest dal SP verso una Assertion Party è mostrato in Appendice B.

### 9.3.3. Caratteristiche della Response

Per i dettagli della Response che deve essere interpretata dal SP si faccia riferimento alla Response emessa dall'IDP.

### 9.3.4. Binding per l'inoltro di richieste verso i servizi infrastrutturali

Si faccia riferimento al paragrafo Binding SOAP over HTTP per l'inoltro di richieste da parte di un Relaying Party (PA, SP) relative ai servizi di Authority Registry.

### 9.3.5. Caratteristiche richiesta verso un Authority Registry

Si faccia riferimento ai paragrafi relativi alle tipologie di richieste verso gli Authoriy Registry presenti nel capitolo omonimo.

## 9.4. Cooperazione Applicativa tramite Web Services

In ambito di cooperazione applicativa le modalità per il trasferimento delle informazioni di sicurezza in termini di asserzioni di ruolo e di identità avvengano tramite SOAP over HTTP.

L'interazione fra il dominio fruitore ed il dominio erogatore all'interno dell'SPCoop è regolata dalle specifiche di sicurezza declinate all'interno dell'accordo si servizio dell'applicazione di back end. Le modalità in cui queste informazioni di identità e di ruolo sono veicolate fra le porte di dominio sono dettagliate all'interno del documento di Specifiche di Sicurezza in ambito di Cooperazione Applicativa SPCoop.

# 10. PUBBLICA AMMINISTRAZIONE COME IDP

Un'Amministrazione responsabile della certificazione degli utenti ricopre il ruolo di Identity Provider. Nello specifico a fronte di una richiesta di autenticazione accesso federato deve:

1. essere in grado di ricevere ed interpretare la richiesta di autenticazione pervenuta da una delle Profile Authority accreditate;
2. autenticare l'utente;
3. costruire la risposta inerente la richiesta di autenticazione pervenuta ed inoltrarla alla Profile Authority;

## 10.1. Scenario di Interazione F-SSO

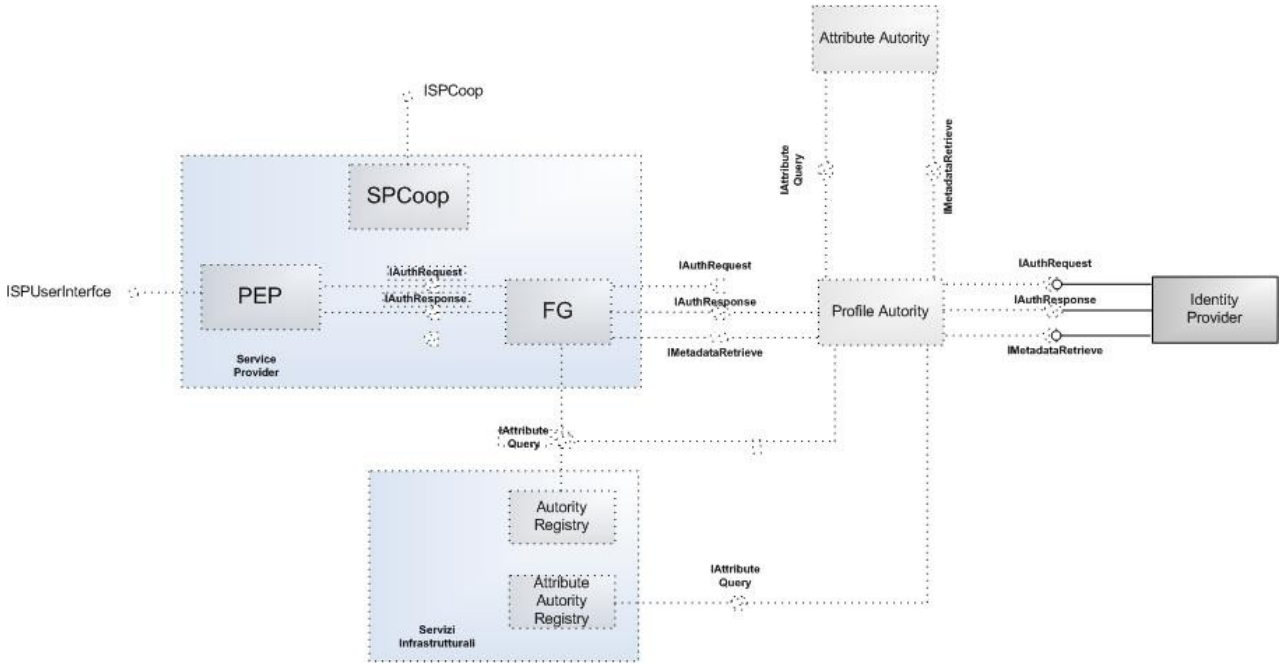



**Figura 29: Architettura dell'Identity Provider**

Le interfacce che caratterizzano l'Identity provider sono:

- **IIDPUserInterface :** permette agli utenti l'interazione via web con il componente tramite User Agent in fase di challenge di autenticazione;

- **IAuthnRequest** e **IAuthnResponse**: permettono l'inoltro e la ricezione di richieste e risposte di autenticazione SAML;
- **IMetadataRetrieve**: permette il reperimento dei metadati SAML da parte delle entità richiedenti.

L'interazione con l'Identity Provider consiste nell'inoltro da parte di una Relying Party (nel nostro casi la Profile Authority) di una richiesta di autenticazione e nella ricezione della relativa risposta. Gli scenari di interazione a fini dell'autenticazione si basano sui profili standard previsti dalla specifica SAML 2.0. Nel modello si prendono in considerazione i profili di tipo "Service Provider initiated", in cui cioè il meccanismo di autenticazione è innescato dalla richiesta inoltrata dall'utente (tramite il suo User Agent) ad un Service Provider, il quale a sua volta si rivolge opportunamente all'autorità di certificazione d'identità in modalità "pull".

Come accennato nei capitoli precedenti il profilo SAML a cui si fa riferimento in particolare è il "Web Browser SSO" (cfr. [SAML-TechOv]sez. 4.1) nelle sue due versioni "SP-Initiated": "Redirect/POST binding" e "POST/POST binding". Secondo tale profilo la richiesta di autenticazione SAML (basata sul costrutto <AuthnRequest>) può essere inoltrata da un Relying Party (per esempio una Profile Authority) all'Identity Provider usando il binding HTTP Redirect o il binding HTTP POST. La relativa risposta SAML (basata sul costrutto <Response>) può invece essere inviata dall'Identity Provider al Relying Party solo tramite il binding HTTP POST. Il modello non prende in considerazione il binding HTTP Artifact.

### *10.1.1. Scenario di interazione*

Lo scenario di interazione descrive l'inoltro di una richiesta di autenticazione da parte di una Profile Authority (Relying Party) al componente Identity Provider e la ricezione della relativa risposta. L'interazione con il componente Identity Provider avviene attraverso le interfacce *IAuthnRequest* e *IAuthnResponse*. Richiesta e risposta SAML transitano attraverso lo User Agent dell'utente.

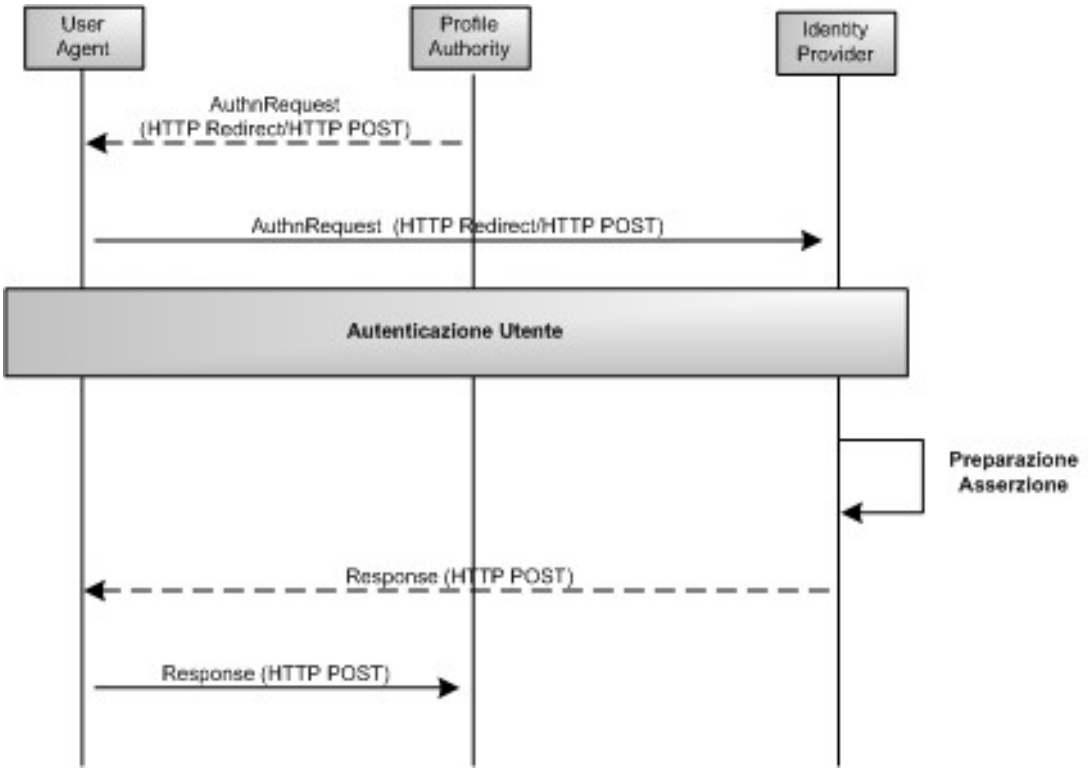



**Figura 30: Richiesta di Autenticazione presso un Identity Provider e relative risposta**

| Passo | Descrizione | Interfaccia | SAML | Binding |
|---|---|---|---|---|
| 1 | La Profile Authority invia allo User Agent una richiesta di autenticazione (per esempio a seguito della selezione dell' IDP da parte dell'utente) da far pervenire all'Identity Provider. | IAuthnRequest | AuthnRequest | HTTP Redirect<br>HTTP POST |
| 2 | Lo User Agent inoltra la richiesta di autenticazione contattando L'Identity Provider secondo la modalità adottata al passo 1. | - | AuthnRequest | HTTP Redirect<br>HTTP POST |
| 3 | L'Identity Provider esamina la richiesta ricevuta e se necessario esegue una challenge di autenticazione con l'utente. | - | - | HTTP |
| 4 | L'Identity Provider a valle dell'autenticazione prepara l'asserzione contenente lo statement di autenticazione dell'utente destinato al Relying Party (più eventuali statement di | - | - | - |

| | | | | |
|---|---|---|---|---|
| | attributo emessi dall'Identity Provider stesso). | | | |
| 5 | L'Identity Provider restituisce allo User Agent la <Response> SAML contenente l'asserzione preparata al punto precedente. | - | Response | HTTP POST |
| 6 | Lo User Agent inoltra alla Profile Authority la <Response> SAML emessa dall'Identity Provider. | IAuthnResponse | Response | HTTP POST |

## 10.2. Binding per l'inoltro di richieste da parte di un Relaying Party (PA, SP)

Conclusa la fase di autenticazione, l'Identity Provider costruisce una <Response> firmata diretta al Relying Party, e in particolare al relativo servizio AssertionConsumerService. La <Response> viene inserita in una form HTML come campo nascosto di nome "SAMLResponse. L'IDP invia la form HTML al browser dell'utente in una risposta HTTP

Il browser dell'utente elabora quindi la risposta HTTP e invia una richiesta HTTP POST contenente la <Response> firmata verso il servizio AssertionConsumerService del Relying Party.

Un esempio di tale form è il seguente (anche in questo caso, il valore del parametro "SAMLResponse" è stato ridotto per brevità).

```
<html>
   <body onload="javascript:document.forms[0].submit()">
        <form method="post"
action="http://rp.cnipa.gov.it:8080/cniparp/AssertionConsumerService">
            <input type="hidden" name="SAMLResponse"
value="PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPHNhbWxwOlJlc3BvbnNlIERlc3RpbmF0aW9uPSJodHRwOi8vc3AuaWNhci5pdDo4MDgwL2ljYXItc3AvQXNzZXJ0aW9uQ29uc3VtZXJTZXJ2aWNlIiBJRD0iczJhNTdmN2RhYTUyMTc2NWZmOTQ2ODM0ZmY2NjIzNTA3ZTcwNGI1MDQ3IiBJblJlc3BvbnNlVG89InMyOGQ5MWEyNmJkNGQ2MGY0N2E0OTkxMzMwMGZhZjc2MzFiZjMxNDBlOSIgSXNzdWVJbnN0YW50PSIyMDA4LTAzLTA0VDIyOjEzOjQ4LjUwMFoiIFZlcnNpb249IjIuMCIgeG1sbnM6c2Ftbl[…]
2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmFjOmNsYXNzZXM6UGFzc3dvcmRQcm90ZWN0ZWRUcmFuc3BvcnQ8L3NhbWw6QXV0aG5Db250ZXh0Q2xhc3NSZWY+PC9zYW1sOkF1dGhuQ29udGV4dD48L3NhbWxwOkF1dGhuUmVxdWVzdD4=">
            <input type="hidden" name="RelayState"
value="s28d91a26bd4d60f47a49913300faf7631bf3140e9">
            <input type="submit" value="Go"/>
        </form>
    </body>
</html>
```

**Figura 31: Esempio di Response veicolata tramite HTTP POST**

## 10.3. Caratteristiche dell'AuthnRequest

Per i dettagli della AuthnRequest che deve essere interpretata dall'IdP si faccia riferimento alla AuthnRequest emessa dal SP.

## 10.4. Caratteristiche della Response

Le caratteristiche che deve avere la `<Response>` inviata dall'Identity Provider al Relying Party in risposta alla richiesta di autenticazione sono le seguenti:

- deve essere presente l'attributo `ID` univoco, per esempio basato su un Universally Unique Identifier (UUID) (cfr. UUID) o su una combinazione *origine* + *timestamp*;
- deve essere presente l'attributo `Version`, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata;
- deve essere presente l'attributo `IssueInstant` a indicare l'istante di emissione della risposta, in formato UTC;
- deve essere presente l'attributo `InResponseTo`, il cui valore deve fare riferimento all'`ID` della richiesta a cui si risponde;
- deve essere presente l'attributo `Destination`, a indicare l'indirizzo (URI reference) a cui è inviata la risposta, cioè l'AssertionConsumerService del Relying Party;
- deve essere presente l'elemento `<Status>` a indicare l'esito (sotto-elemento `<StatusCode>`) della richiesta a cui si risponde;
- deve essere presente l'elemento `<Issuer>` a indicare l'entityID dell'entità emittente, cioè l'Identity Provider stesso;
- deve essere presente un elemento `<Assertion>` ad attestare l'avvenuta autenticazione, contenente un elemento `<AuthnStatement>`;
- nella `<Assertion>` di autenticazione deve essere presente l'elemento `<Subject>` a indicare il soggetto che si è autenticato;
- nell'elemento `<Subject>` deve essere presente l'elemento `<NameID>` atto a qualificare meglio il subject dell'asserzione: in particolare deve essere presente l'attributo `Format` avente valore "urn:oasis:names:tc:SAML:2.0:nameid-format:transient" (cfr. SAMLCore, sez. 8.3), e l'attributo `NameQualifier` che qualifica il dominio a cui afferisce tale valore (per esempio un URI riconducibile all'Identity Provider stesso);

- nell'elemento <Subject> dell'asserzione di autenticazione deve essere presente almeno un elemento <SubjectConfirmation> con attributo Method avente valore "urn:oasis:names:tc:SAML:2.0:cm:bearer";
- nella <Assertion> di autenticazione deve essere presente l'elemento <Issuer> a indicare l'entityID dell'authority emittente, cioè l'Identity Provider stesso;
- nella <Assertion> di autenticazione, nell'elemento <Conditions> devono essere presenti almeno i vincoli di validità temporale dell'asserzione (per esempio NotBefore, NotOnOrAfter);
- nella <Assertion> di autenticazione, nell'elemento <AuthnContext> deve essere presente la descrizione del contesto di autenticazione effettivo;
- all'interno dell'asserzione possono essere presenti zero o più elementi <AttributeStatement>, relativi ad asserzioni di attributo che l'Identity Provider può rilasciare contestualmente alla risposta di autenticazione.

  In particolare se la Response è nei confronti di una Profile Authority e se l'IDP vuole offrire all'utente la possibilità di fruire dei servizi offerti dalla PA deve necessariamente inviare all'interno della <AttributeStatement> un elemento <Attribute> contenente il codice fiscale dell'utente autenticato.

  Tramite il codice fiscale la Profile Authority è in grado identificare univocamente l'utente e fornire i profili ad esso associati. L'elemento <Attribute> deve essere identificato tramite l'attributo <Name> pari a "CodiceFiscale".

  Di seguito si riporta un esempio di attribute statement con all'interno l'attributo relativo al codice fiscale utente.

```
<saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml:Attribute Name="CodiceFiscale"  xmlns:saml="urn....">
      <saml:AttributeValue xmlns:xs=..xsi:type="xs:string">
            CRMNDR72A21HSOIP
       </saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

- nella <Assertion> di autenticazione può essere presente l'elemento <Advice>, contenente altri elementi <Assertion>: questo meccanismo è utilizzabile nei casi in cui gli statement emessi dall'Identity Provider si basino su altre asserzioni SAML, ottenute per esempio da altre authority, delle quali è necessario fornire evidenza in forma originale unitamente alla risposta alla richiesta di autenticazione;
- deve essere presente l'elemento <Signature> apposto dall'Identity Provider.

Per maggiori dettagli sulla struttura standard di una risposta a una richiesta di autenticazione SAML, si rimanda alla già citata specifica [SAMLCore].

Un esempio Response dall'IDP verso una relying party è mostrato in Appendice A.

# 11. PUBBLICA AMMINISTRAZIONE COME ATTRIBUTE AUTHORITY

Un'Amministrazione che decide di ricoprire il ruolo di Attribute Authority si deve mettersi in condizione di poter certificare un determinato set di attributi presenti in un profilo utente. Nello specifico a fronte di una richiesta di uno o più attributi relativi ad un soggetto:

1. essere in grado di ricevere ed interpretare la richiesta di attributo pervenuta da una delle Profile Authority accreditate;
2. elaborare la richiesta;
3. costruire la risposta inerente la richiesta pervenuta ed inoltrarla alla Profile Authority;

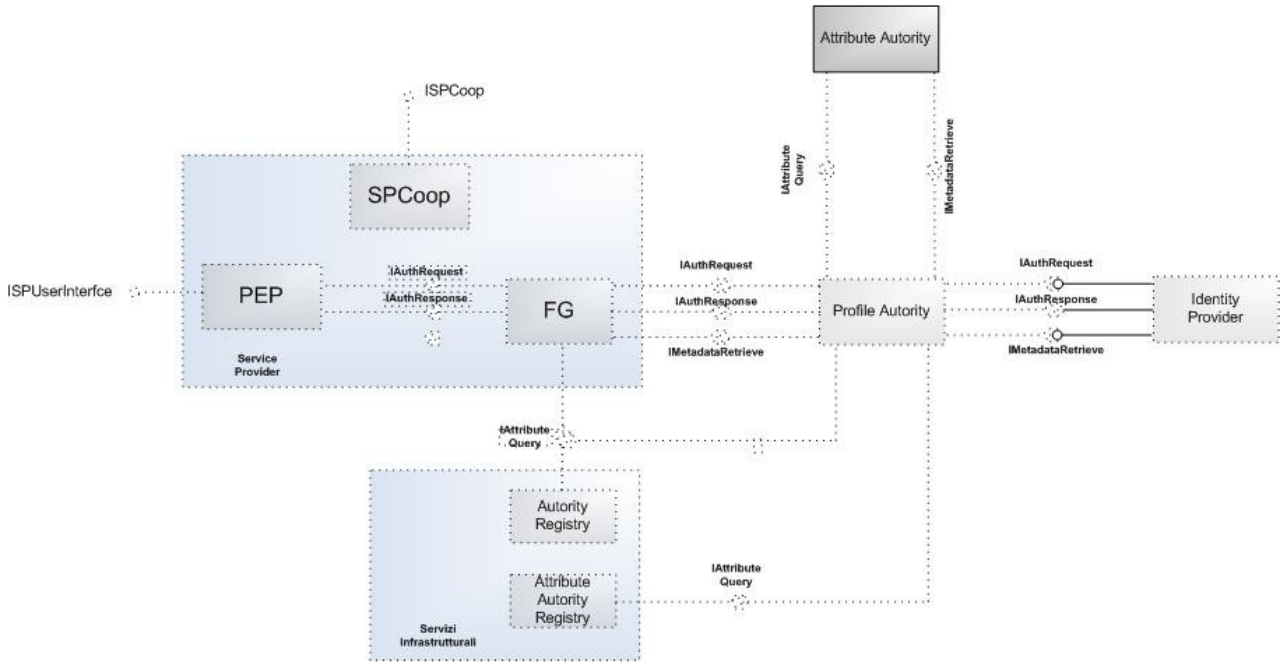



**Figura 32: Architettura dell'Attribute authority**

Il componente espone le seguenti interfacce:

- **`IAttributeQuery`**: interfaccia applicativa che supporta le operazioni di richiesta di attributo SAML;
- **`IMetadataPublisher`**: permette il reperimento dei metadati SAML da parte delle entità richiedenti.

## 11.1. Scenario di interazione

Lo scenario di interazione descrive l'inoltro di una richiesta di attributi da parte di un Relying Party al componente Attribute Authority e la ricezione della relativa risposta. L'interazione con il componente Attribute Authority avviene attraverso l'interfaccia applicativa `IAttributeQuery`.

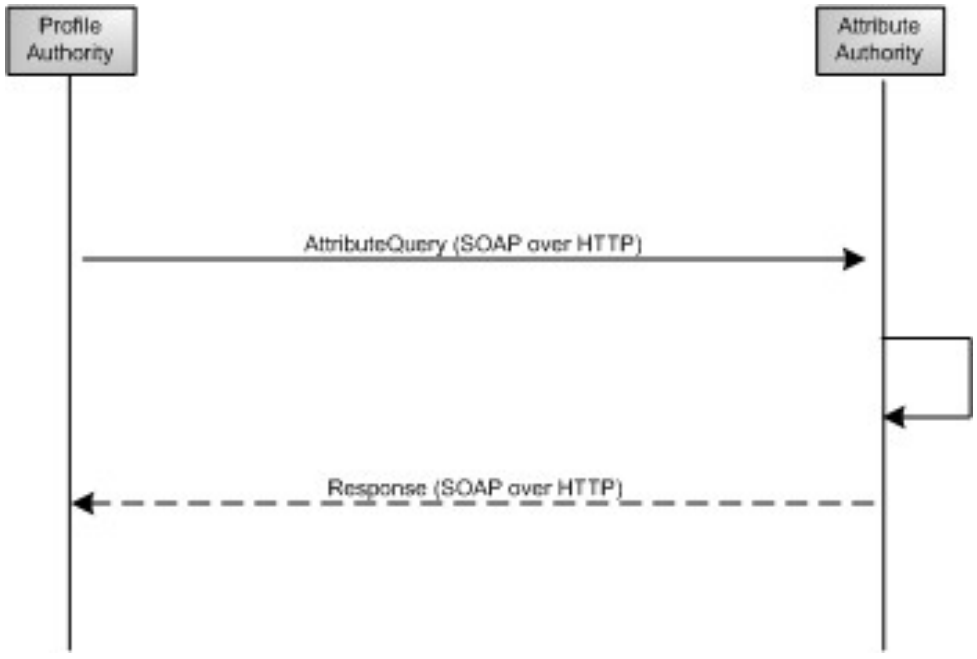



**Figura 33: Richiesta di Attributi presso un'Attribute Authority e relativa risposta**

| Passo | Descrizione | Interfaccia | SAML | Binding |
|---|---|---|---|---|
| 1 | La Profile Authority invia all'Attribute | IAttributeQuery | <AttributeQuery> | SOAP |

| | | | | |
|---|---|---|---|---|
| | Authority una richiesta di attributi. Ciò avviene utilizzando il costrutto <AttributeQuery> della specifica SAML e interagendo mediante "SAML SOAP binding". | | | Over HTTP |
| 2 | L'Authority Registry elabora la richiesta ricevuta. | - | - | - |
| 3 | La Attribute Authority risponde alla richiesta di attributi del Relying Party con una <Response> SAML contenente l'asserzione contenente a sua volta gli statement di attributo e interagendo mediante "SAML SOAP binding". | IAttributeQuery | <Response> | SOAP Over HTTP |

## 11.2. Binding per l'inoltro di richieste verso l'Attribute Authority

Il binding utilizzato per l'inoltro delle richieste verso una Attribute Authority è il binding SOAP over http. Per ulteriori dettagli si rimanda al capitolo "Binding SOAP over HTTP per l'inoltro di richieste da parte di un Relaying Party (PA, SP)".

## 11.3. Caratteristiche dell' AttributeQuery

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

- deve essere presente l'attributo `ID` univoco, per esempio basato su un Universally Unique Identifier (UUID) (cfr.UUID) o su una combinazione *origine* + *timestamp*;
- deve essere presente l'attributo `Version`, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata;
- deve essere presente l'attributo `IssueInstant` a indicare l'istante di emissione della richiesta, in formato UTC;
- deve essere presente l'attributo `Destination`, a indicare l'indirizzo (URI reference) a cui è inviata la richiesta, cioè l'AttributeService della Attribute Authority;
- deve essere presente l'elemento `<Issuer>` a indicare l'entityID dell'entità emittente (il Relying Party); qualora fosse necessario specificare insieme alla richiesta di attributi altre informazioni (per esempio il servizio richiesto in origine dall'utente al Service Provider), data la mancanza di opportune strutture all'interno della `<AttributeQuery>` e volendo evitare di estendere la

specifica, il valore dell'elemento `<Issuer>` può essere ottenuto concatenando al valore dell'issuer vero e proprio tali informazioni in formato stringa separate dal carattere "#";

- deve essere presente l'elemento `<Subject>` a indicare il soggetto a cui si riferisce la richiesta di attributi, contenente l'elemento `<NameID>` e i relativi attributi `Format` e `NameQualifier` (cfr. quanto detto nelle sezioni precedenti a proposito della risposta a una richiesta di autenticazione);
- possono essere presenti uno o più elementi `<Attribute>`, il cui attributo `Name` indica lo specifico attributo di cui si vuole conoscere il valore (come da specifica, se non è presente alcun elemento `<Attribute>` ciò significa che la richiesta del Relying Party riguarda tutti gli attributi relativi al subject specificato, cfr. [SAMLCore], sez. 3.3.2.3);
- in ciascun elemento `<Attribute>` possono essere presenti uno o più elementi `<AttributeValue>` per richiedere la verifica che l'attributo abbia i valori specificati;
- deve essere presente l'elemento `<Signature>` apposto dall'entità emittente.

Per maggiori dettagli sulla struttura standard di una richiesta di attributo SAML, si rimanda alla già citata specifica [SAMLCore] e ai documenti correlati.

Di seguito viene riportato un esempio di richiesta di attributi (sono stati omessi per brevità i valori della firma e dei certificati codificati in formato Base64).

## 11.4. Caratteristiche della Response

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

- deve essere presente l'attributo `ID` univoco, per esempio basato su un Universally Unique Identifier (UUID) (cfr. UUID) o su una combinazione *origine* + *timestamp*;
- deve essere presente l'attributo `Version`, che deve valere sempre "2.0", coerentemente con la versione della specifica SAML adottata;
- deve essere presente l'attributo `IssueInstant` a indicare l'istante di emissione della risposta, in formato UTC;
- deve essere presente l'attributo `InResponseTo`, il cui valore deve fare riferimento all'`ID` della richiesta a cui si risponde;
- deve essere presente l'attributo `Destination`, a indicare l'indirizzo (URI reference) a cui è inviata la richiesta, cioè l'AttributeService del Relying Party;

- deve essere presente l'elemento `<Status>` a indicare l'esito (sotto-elemento `<StatusCode>`) della richiesta a cui si risponde;
- deve essere presente l'elemento `<Issuer>` a indicare l'entityID dell'entità emittente, cioè la Attribute Authority stessa;
- devono essere presenti uno o più elementi `<Assertion>` contenenti elementi `<AttributeStatement>`;
- ciascun elemento `<Assertion>` deve avere i rispettivi rispettivi attributi `ID`, `Version` e `IssueInstant` con l'usuale significato già riportato in precedenza, oltre agli elementi `<Issuer>` e `<Subject>`;
- in particolare, l'elemento `<Subject>` deve contenere l'elemento `<NameID>` e i relativi attributi `Format` e `NameQualifier` (cfr. quanto detto nella sezioni precedenti a proposito della risposta a una richiesta di autenticazione);
- ciascun elemento `<Assertion>` deve essere firmato dall'authority emittente;
- ciascun elemento `<Assertion>` deve contenere un elemento `<Conditions>` che ne determina i vincoli di validità temporale;
- ciascun elemento `<AttributeStatement>` deve contenere gli elementi `<Attribute>` (con attributo `Name` e i relativi elementi `<AttributeValue>`) corrispondenti agli attributi richiesti, eventualmente codificati in formato Base64 per permettere la trasmissione di valori strutturati;
- in ciascun elemento `<Assertion>` può eventualmente essere presente l'elemento `<Advice>`, contenente altri elementi `<Assertion>` di cui è necessario fornire evidenza in forma originale in sede di risposta alla richiesta di attributo;
- deve essere presente l'elemento `<Signature>` apposto dall'entità emittente.

Per maggiori dettagli sulla struttura standard di una risposta a una richiesta di attributo SAML, si rimanda alla già citata specifica [SAML-Core] e ai documenti correlati.

Un esempio di risposta a una richiesta di attributi è mostrato in Appendice A.

# 12. PUBBLICA AMMINISTRAZIONE COME PROFILE AUTHORITY

Si rimanda alla descrizione della Profile Auhority presentata al capitolo 7 inerente i servizi infrastrutturali, nello specifico al paragrafo 7.2 "Profile Authority".

# 13. SCENARIO DI INTERAZIONE CON LA CA DEL CG-SICA COME ALD

Lo scenario di Interazione con la CA del CG-SICA quando svolge il ruolo di ALD (nello specifico di IDP) non si differenzia da quanto detto relativamente all'interazione con un generico IdP.

I binding sono l'HTTP Redirect e HTTP POST come descritti in precedenza.

L'Authentication Request che si deve inoltrare alla CA ha le stesse caratteristiche della AuthnRequest descritta nel pragrafo "8.3.2 Caratteristiche della Authentication Request".

La richiesta si differenzia per l'elemento `<RequestedAuthnContext>`. Tale elemento opzionale indica il contesto di autenticazione che deve essere valorizzato in modo che venga richiesta l'autenticazione dell'utente tramite certificato. In questo caso il sub-elemento `<AuthnContextClassRef>` se presente deve essere pari a "`urn:oasis:names:tc:SAML:2.0:ac:classes:X509`", così come mostrato in figura.

```
<samlp:RequestedAuthnContext Comparison="exact">
      <saml:AuthnContextClassRef>
            urn:oasis:names:tc:SAML:2.0:ac:classes:X509
      </saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

# 14. BIBLIOGRAFIA


| | |
|---|---|
| [E-Auth_USGov] | Technical Approach for the Authentication service Component V2.0 |
| [h-inf3-conc] | Sistema Federato Interregionale di Autenticazione: Modello Concettuale di Riferimento V 1.0.2 |
| [SAML-Glos] | Glossary for the OASIS Security Assertion MarkUp Language V2.0 |
| [SPCoop-AS] | Sistema Pubblico di Cooperazione: ACCORDO DI SERVIZIO V 1.0 |
| [SPCoop_exe] | Sistema Pubblico di cooperazione: Executive Summary v 2.1 |
| [Abelson] | H.Abelson, L.Lessig, "Digital Identity in Cyberspace", MIT |
| [RBAC] | R. Sandhu, D. Ferraiolo, R. Kuhn, "The NIST Model for Role Based Access Control: Towards a Unified Standard," Proceedings, 5th ACM Workshop on Role Based Access Control |
| [NIST-RBAC] | Role Based Access Control Implementation Standard - NIST |
| [DlgAmmDi] | Decreto legislativo 5 marzo 2005, n. 82 Codice dell'Amministrazione Digitale |
| [CNIPA-SPCDef] | Sistema Pubblico di Cooperazione: TERMINI E DEFINIZIONI |
| [SAML-TechOv] | OASIS Security Services (SAML) TC, Security Assertion Markup Language (SAML) V2.0 Technical Overview, Draft 15, 5 marzo 2008. |

| | |
|---|---|
| [SAML-Core] | OASIS Security Services (SAML) TC, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005 |
| [WS-Security] | Web Services Security (WS-Security) specification |
| [SAML-Metadata] | OASIS Security Services (SAML) TC, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005 |
| [SAML-Bindings] | OASIS Security Services (SAML) TC, Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005 |
| [SAML-Profile] | OASIS Security Services (SAML) TC, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005. |
| [SAML-AuthContext] | OASIS Security Services (SAML) TC, Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 marzo 2005. |
| [UUID] | A Universally Unique IDentifier (UUID) URN Namespace (IETF RFC 4122), luglio 2005. http://www.ietf.org/rfc/rfc4122.txt |
| [XMLData] | W3C, XML Schema Part 2: Datatypes, W3C Recommendation, 2 maggio 2001. |
| [XMLSig] | W3C, XML Schema Part 2: Datatypes, W3C Recommendation, 2 maggio 2001. |

# APPENDICE A: STRUTTURA DEI MESSAGGI - ESEMPI

## AttributeQuery verso un'Authority Registry (elenco Authority)

Si riporta un esempio di richiesta di discovery di authority, in particolare di Profile Authority (sono stati omessi per brevità i valori della firma e dei certificati codificati in formato Base64). L'esempio mostra una richiesta di attributo firmata, il cui subject speciale assume il valore "PA_LIST".

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AttributeQuery xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://ar.cnipa.gov.it:4443/ar/AttributeQueryHandlerServlet"
ID="s2727910b89abe781c00981403811802c55545e158" IssueInstant="2008-03-11T16:15:45.100Z" Version="2.0">
<saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://rp.cnipa.gov.it:6443/rp</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
```

```
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Reference URI="#s2727910b89abe781c00981403811802c55545e158"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds
saml samlp"/>
                    </ds:Transform>
     </ds:Transforms>
     <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">NERf/qWiM+/pn5oLgXcvJuLezcA=</ds:DigestValue>
     </ds:Reference>
     </ds:SignedInfo>
     <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     [FIRMA]
     </ds:SignatureValue>
           <ds:KeyInfo>
              <ds:X509Data>
                 <ds:X509Certificate>
```

```
                    [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
                  <ds:X509Certificate>
                    [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
                  <ds:X509Certificate>
                    [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
               </ds:X509Data>
            </ds:KeyInfo>
         </ds:Signature>
         <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
NameQualifier="https://ar.cnipa.gov.it/ar">PA_LIST</saml:NameID>
         </saml:Subject>
      </samlp:AttributeQuery>
```

I casi di interrogazione dell'Authority Registry per ottenere l'elenco di altri tipi di authority della federazione (Identity Provider o Attribute Authority) sono del tutto analoghi all'esempio di richiesta mostrato nell'esempio precedente.

# Response emessa da un'Authority Registry (elenco Authority)

Si riporta un esempio di risposta ad una richiesta di discovery di authority (in questo caso di Profile Authority) della federazione (sono stati omessi per brevità i valori dei certificati codificati in formato Base64). L'esempio mostra una risposta firmata ad una richiesta di attributo: la risposta conferma il subject speciale indicato nella richiesta ("PA_LIST") e contiene un elemento `<AttributeStatement>` contenente a sua volta un attributo "AuthorityList" che assume tanti valori quante sono le entità di tipo Profile Authority di cui è a conoscenza l'Authority Registry. Ciascun valore rappresenta il descrittore in formato XML dell'entità, adotta la struttura illustrata in sez. 7.1.2 ed è codificato in formato Base64 (evidenziate in giallo).

```
    <?xml version="1.0" encoding="UTF-8"?>
    <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://rp.cnipa.gov.it:6443/rp" ID="s2faa6630ca8d2ae99c76c24a7357050168c6611fe"
InResponseTo="s2727910b89abe781c00981403811802c55545e158" IssueInstant="2008-03-11T16:15:46.550Z"
Version="2.0">
       <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://ar.cnipa.gov.it:4443/ar</saml:Issuer>
       <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:Reference URI="#s2faa6630ca8d2ae99c76c24a7357050168c6611fe"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
```

```
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds
saml samlp xs xsi"/>
                    </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">Vg51EO5st0iPlumfVo/WsbuN5OU=</ds:DigestValue>
    </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    [FIRMA]
    </ds:SignatureValue>
          <ds:KeyInfo>
             <ds:X509Data>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
                <ds:X509Certificate>
```

```
                    [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
               </ds:X509Data>
            </ds:KeyInfo>
         </ds:Signature>
         <samlp:Status>
            <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
         </samlp:Status>
         <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="s27663dd73edfdcc2b3596a6fd2ef551d0b49f377d" IssueInstant="2008-03-11T16:15:46.550Z" Version="2.0">
            <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://ar.cnipa.gov.it:4443/ar</saml:Issuer>
            <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Reference URI="#s27663dd73edfdcc2b3596a6fd2ef551d0b49f377d"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

```
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="ds saml xs"/>
                    </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">JDgQ/QPVpf1rzpAG9690b5W3Fi0=</ds:DigestValue>
    </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    [FIRMA]
    </ds:SignatureValue>
          <ds:KeyInfo>
             <ds:X509Data>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
```

```
            </ds:X509Data>
         </ds:KeyInfo>
         </ds:Signature>
         <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
NameQualifier="https://ar.cnipa.gov.it/ar">PA_LIST</saml:NameID>
         </saml:Subject>
         <saml:Conditions NotBefore="2008-03-11T16:15:46.550Z" NotOnOrAfter="2008-09-07T16:15:46.550Z"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
         <saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:Attribute Name="AuthorityList">
               <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4NCjxBdXRob3JpdHlJbmZvIHht
   […]
   aXQ6MzQ0My9pY2FyLXBhL01ldGFkYXRhUHVibGlzaGVyU2VydmxldDwvTWV0YWRhdGFQcm92aWRl
   clVSTD4NCgk8RG9tYWluPmRvbWFpbjE8L0RvbWFpbj4NCjwvQXV0aG9yaXR5SW5mbz4=</saml:AttributeValue>
               <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4NCjxBdXRob3JpdHlJbmZvIHht
   […]
   aXQ6MzQ0My9pY2FyLXBhL01ldGFkYXRhUHVibGlzaGVyU2VydmxldDwvTWV0YWRhdGFQcm92aWRl
   clVSTD4NCgk8RG9tYWluPmRvbWFpbjI8L0RvbWFpbj4NCjwvQXV0aG9yaXR5SW5mbz4=</saml:AttributeValue>
               </saml:Attribute>
```

```
        </saml:AttributeStatement>
      </saml:Assertion>
    </samlp:Response>
```

Ecco infine alcuni possibili valori di attributo restituiti in una risposta, una volta decodificati:

```
<AuthorityInfo xmlns="http://www.cnipa.gov.it/ar/b001">
 <EntityID>https://pa.cnipa.gov.it:3443/pa</EntityID>
 <Description>Profile Authority 1</Description>
 <Type>Profile Authority</Type>
 <MetadataProviderURL>https://pa.cnipa.gov.it:3443/pa/MetadataPublisherServlet</MetadataProviderURL>
 <Domain>domain1</Domain>
</AuthorityInfo>

<AuthorityInfo xmlns="http://www.cnipa.gov.it/ar/b001">
 <EntityID>https://pa.cnipa.gov.it:3443/pa</EntityID>
 <Description>Profile Authority 2</Description>
 <Type>Profile Authority</Type>
 <MetadataProviderURL>https://pa.cnipa.gov.it:3443/pa/MetadataPublisherServlet</MetadataProviderURL>
 <Domain>domain2</Domain>
</AuthorityInfo>
```

I casi di risposta all'interrogazione dell'Authority Registry per ottenere l'elenco di altri tipi di authority della federazione (Identity Provider o Attribute Authority) sono del tutto analoghi all'esempio di risposta mostrato.

# AttributeQuery verso un'Authority Registry (singola Authority)

Si riporta un esempio di richiesta di informazioni relative ad una singola authority (sono stati omessi per brevità i valori della firma e dei certificati codificati in formato Base64). L'esempio riguarda una richiesta relativa all'Attribute Authority il cui entityID è "https://aa3.cnipa.gov.it:3443/aa".

```
     <?xml version="1.0" encoding="UTF-8"?>
     <samlp:AttributeQuery xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://ar.cnipa.gov.it:4443/ar/AttributeQueryHandlerServlet"
ID="s20f06ab70beeadab093bc7fa77d095bcdb7a2508b" IssueInstant="2008-03-11T16:30:29.711Z" Version="2.0">
               <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://rp.cnipa.gov.it:6443/rp</saml:Issuer>
               <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
```

```
    <ds:Reference URI="#s20f06ab70beeadab093bc7fa77d095bcdb7a2508b"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="ds saml samlp"/>
                        </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
    </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    [FIRMA]
    </ds:SignatureValue>
    <ds:KeyInfo>
            <ds:X509Data>
               <ds:X509Certificate>
                [CERTIFICATO CODIFICATO IN BASE64]
               </ds:X509Certificate>
```

```
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
            </ds:Signature>
            <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
               <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
NameQualifier="https://ar.cnipa.gov.it/ar">https://aa3.cnipa.gov.it:3443/aa</saml:NameID>
            </saml:Subject>
    </samlp:AttributeQuery>
```

# Response emessa da un'Authority Registry (singola Authority)

Si riporta un esempio di risposta ad una richiesta di attributi (sono stati omessi per brevità i valori delle firme e dei certificati codificati in formato Base64). L'esempio illustra una risposta relativa ai valori degli attributi che descrivono l'Attribute Authority il cui entityID è "https://aa3.cnipa.gov.it:3443/aa".

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://rp.cnipa.gov.it:3443/rp" ID="s2eead4ff755c52c4200aca7bd8e9ff0cb1c4f6679"
InResponseTo="s20f06ab70beeadab093bc7fa77d095bcdb7a2508b" IssueInstant="2008-03-11T16:30:31.068Z"
Version="2.0">
<saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://ar.cnipa.gov.it:4443/ar</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
<ds:Reference URI="#s2eead4ff755c52c4200aca7bd8e9ff0cb1c4f6679"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="ds saml samlp xs xsi"/>
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
```

```
<ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
[FIRMA]
</ds:SignatureValue>
<ds:KeyInfo>
                <ds:X509Data>
                   <ds:X509Certificate>
                    [CERTIFICATO CODIFICATO IN BASE64]
                   </ds:X509Certificate>
                   <ds:X509Certificate>
                    [CERTIFICATO CODIFICATO IN BASE64]
                   </ds:X509Certificate>
                   <ds:X509Certificate>
                    [CERTIFICATO CODIFICATO IN BASE64]
                   </ds:X509Certificate>
                </ds:X509Data>
             </ds:KeyInfo>
          </ds:Signature>
          <samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
             <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
```

```
            </samlp:Status>
            <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="s28dca503bf85e4743829fdecf56e324349cbefe8e" IssueInstant="2008-03-11T16:30:31.068Z" Version="2.0">
              <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://ar.cnipa.gov.it:4443/ar</saml:Issuer>
              <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:Reference URI="#s28dca503bf85e4743829fdecf56e324349cbefe8e"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="ds saml xs"/>
                    </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
```

```
    </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    [FIRMA]
    </ds:SignatureValue>
    <ds:KeyInfo>
                    <ds:X509Data>
                    <ds:X509Certificate>
                     [CERTIFICATO CODIFICATO IN BASE64]
                    </ds:X509Certificate>
                    <ds:X509Certificate>
                     [CERTIFICATO CODIFICATO IN BASE64]
                    </ds:X509Certificate>
                    <ds:X509Certificate>
                     [CERTIFICATO CODIFICATO IN BASE64]
                    </ds:X509Certificate>
                    </ds:X509Data>
                 </ds:KeyInfo>
              </ds:Signature>
              <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                 <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
NameQualifier="https://ar.cnipa.gov.it/ar">https://rp.cnipa.gov.it:6443/rp</saml:NameID>
              </saml:Subject>
```

```
                <saml:Conditions NotBefore="2008-03-11T16:30:31.068Z" NotOnOrAfter="2008-09-07T16:30:31.068Z"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
                <saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                   <saml:Attribute Name="Type">
                      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Attribute
Authority</saml:AttributeValue>
                   </saml:Attribute>
                   <saml:Attribute Name="Domain">
                      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">domain3</saml:AttributeValue>
                   </saml:Attribute>
                   <saml:Attribute Name="Description">
                      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Attribute Authority
3</saml:AttributeValue>
                   </saml:Attribute>
                   <saml:Attribute Name="EntityID">
                      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">https://aa3.cnipa.gov.it:3443/aa</saml:AttributeValue>
                   </saml:Attribute>
                   <saml:Attribute Name="MetadataProviderURL">
                      <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">https://aa3.cnipa.gov.it:3443/aa/MetadataPublisherServlet</saml:AttributeValue>
```

```
                    </saml:Attribute>
                </saml:AttributeStatement>
            </saml:Assertion>
    </samlp:Response>
```

# AuthnRequest verso un IDP

Si riporta un esempio di richiesta di autenticazione, valida sia nel caso di binding HTTP POST che di binding HTTP Redirect (sono stati omessi per brevità i valori della firma e dei certificati codificati in formato Base64). L'esempio illustra una richiesta di autenticazione firmata in cui il Relying Party chiede che il contesto di autenticazione dell'utente coincida (`Comparison="exact"`) con uno quelli enumerati: "Password", "PasswordProtectedTransport" (autenticazione mediante password attraverso una sessione protetta), "SoftwarePKI" (autenticazione mediante un certificato X.509) o "Smartcard" (cfr. [SAMLAuthContext], sez. 3.4).

```
    <?xml version="1.0" encoding="UTF-8"?>
    <samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://rp.cnipa.gov.it:3443/rp/AssertionConsumerService"
AttributeConsumingServiceIndex="1" Destination="https://idp.cnipa.gov.it:9443/idp/SSOService"
ForceAuthn="false" ID="s271a3a6f1592559c0f7958ed2bb54b0cb66263bdc" IsPassive="false" IssueInstant="2008-03-
11T18:04:15.531Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0">
       <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://rp.cnipa.gov.it:3443/rp</saml:Issuer>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

```
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Reference URI="#s271a3a6f1592559c0f7958ed2bb54b0cb66263bdc"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds
saml samlp"/>
                    </ds:Transform>
     </ds:Transforms>
     <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
     </ds:Reference>
     </ds:SignedInfo>
     <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     [FIRMA]
     </ds:SignatureValue>
     <ds:KeyInfo>
              <ds:X509Data>
```

```
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
             </ds:X509Data>
          </ds:KeyInfo>
       </ds:Signature>
       <samlp:NameIDPolicy AllowCreate="false" />
       <samlp:RequestedAuthnContext Comparison="exact">
          <saml:AuthnContextClassRef
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnC
ontextClassRef>
          <saml:AuthnContextClassRef
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTran
sport</saml:AuthnContextClassRef>
          <saml:AuthnContextClassRef
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI</saml:Aut
hnContextClassRef>
```

```
            <saml:AuthnContextClassRef
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard</saml:Authn
ContextClassRef>
        </samlp:RequestedAuthnContext>
        <samlp:Scoping ProxyCount="0">
            <samlp:RequesterID>https://rp.cnipa.gov.it:3443/rp</samlp:RequesterID>
        </samlp:Scoping>
    </samlp:AuthnRequest>
```

# Response emessa da un IDP

Si riporta un esempio di risposta ad una richiesta di autenticazione (sono stati omessi per brevità i valori delle firme e dei certificati codificati in formato Base64). L'esempio illustra una risposta firmata di autenticazione andata a buon fine (elemento `<Status>` con `StatusCode` "urn:oasis:names:tc:SAML:2.0:status:Success") in cui l'Identity Provider comunica che l'utente si è autenticato con modalità "PasswordProtectedTransport" (è questo il contesto di autenticazione effettivo). Nell'asserzione di autenticazione, anch'essa firmata, sono indicati anche i rispettivi limiti di validità temporale. L'IDP, inoltre, invia un <AttributeStatement> relativa ad asserzioni di attributo che l'Identity Provider può rilasciare contestualmente alla risposta di autenticazione

```
    <?xml version="1.0" encoding="UTF-8"?>
    <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://rp.cnipa.gov.it:3443/rp/AssertionConsumerService"
ID="s2ac7aaa73903777311080cb716dede7e6c405e0d0" InResponseTo="s271a3a6f1592559c0f7958ed2bb54b0cb66263bdc"
IssueInstant="2008-03-11T18:30:55.640Z" Version="2.0">
```

```
        <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://idp.cnipa.gov.it:9443/idp</saml:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Reference URI="#s2ac7aaa73903777311080cb716dede7e6c405e0d0"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds
saml samlp"/>
                    </ds:Transform>
     </ds:Transforms>
     <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
     </ds:Reference>
     </ds:SignedInfo>
     <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

```
     [FIRMA]
     </ds:SignatureValue>
           <ds:KeyInfo>
              <ds:X509Data>
                 <ds:X509Certificate>
                  [CERTIFICATO CODIFICATO IN BASE64]
                 </ds:X509Certificate>
                 <ds:X509Certificate>
                  [CERTIFICATO CODIFICATO IN BASE64]
                 </ds:X509Certificate>
                 <ds:X509Certificate>
                  [CERTIFICATO CODIFICATO IN BASE64]
                 </ds:X509Certificate>
              </ds:X509Data>
           </ds:KeyInfo>
        </ds:Signature>
        <samlp:Status>
           <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </samlp:Status>
        <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="s29b7d3cd258e50b3e5e52c49075178ea55d3e2a09" IssueInstant="2008-03-11T18:30:55.640Z" Version="2.0">
           <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://idp.cnipa.gov.it:9443/idp</saml:Issuer>
```

```
          <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Reference URI="#s29b7d3cd258e50b3e5e52c49075178ea55d3e2a09"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                          <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="ds saml"/>
                       </ds:Transform>
     </ds:Transforms>
     <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
     </ds:Reference>
     </ds:SignedInfo>
     <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     [FIRMA]
     </ds:SignatureValue>
```

```
            <ds:KeyInfo>
               <ds:X509Data>
                  <ds:X509Certificate>
                   [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
                  <ds:X509Certificate>
                   [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
                  <ds:X509Certificate>
                   [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
               </ds:X509Data>
               </ds:KeyInfo>
            </ds:Signature>
            <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
               <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:transient"
NameQualifier="https://idp.cnipa.gov.it/idp">xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">_4789ef0a007214
9739147728fafcefd4</saml:NameID>
               <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                  <saml:SubjectConfirmationData InResponseTo="s2f746bd8767dfe1ead32731c2a761f71a49f5a4cc"
NotBefore="2008-03-11T18:30:55.640Z" NotOnOrAfter="2008-03-11T18:35:55.640Z"
Recipient="https://rp.cnipa.gov.it:3443/rp/AssertionConsumerService"/>
               </saml:SubjectConfirmation>
```

```
            </saml:Subject>
            <saml:Conditions NotBefore="2008-03-11T18:30:55.640Z" NotOnOrAfter="2008-03-11T18:35:55.640Z"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
            <saml:AuthnStatement AuthnInstant="2008-03-11T18:30:55.640Z"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
               <saml:AuthnContext>

<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContext
ClassRef>
               </saml:AuthnContext>
            </saml:AuthnStatement>
            <saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                <saml:Attribute Name="CognomeUtente" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                  <saml:AttributeValue xmlns:xs=http://www.w3.org/2001/XMLSchema
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance xsi:type="xs:string">Carmuti</saml:AttributeValue>
               </saml:Attribute>
               <saml:Attribute Name="EmailUtente"xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                  <saml: AttributeValue xmlns:xs=http://www.w3.org/2001/XMLSchema
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance xsi:type="xs:string">Carmuti@mail.it</saml:AttributeValue>
               </saml:Attribute>
               <saml:Attribute Name="CodiceFiscale"xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
                  <saml: AttributeValue xmlns:xs=http://www.w3.org/2001/XMLSchema
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance xsi:type="xs:string">CRMNDR72A21K501S</saml:AttributeValue>
```

```
            </saml:Attribute>
          </saml:AttributeStatement>
       </saml:Assertion>
    </samlp:Response>
```

# AttributeQuery verso una Attribute Authority

Si riporta un esempio di richiesta di attributi (sono stati omessi per brevità i valori della firma e dei certificati codificati in formato Base64). L'esempio illustra come la richiesta si riferisca ad un soggetto ben preciso (l'elemento <Subject> ha come valore il codice fiscale della persona) e riguardi specificamente gli attributi "lastname", "birthplace" e "firstname".

```
    <?xml version="1.0" encoding="UTF-8"?>
    <samlp:AttributeQuery xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://aa.cnipa.gov.it:5443/aa/AttributeQueryHandlerServlet"
ID="s207e487be6a26e83e348110abf399756c19c7e462" IssueInstant="2008-03-11T21:33:44.250Z" Version="2.0">
       <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://rp.cnipa.gov.it:3443/rp</saml:Issuer>
       <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
```

```
     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Reference URI="#s207e487be6a26e83e348110abf399756c19c7e462"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds
saml samlp"/>
                    </ds:Transform>
     </ds:Transforms>
     <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
     <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
     </ds:Reference>
     </ds:SignedInfo>
     <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     [FIRMA]
     </ds:SignatureValue>
           <ds:KeyInfo>
              <ds:X509Data>
                 <ds:X509Certificate>
```

```
                    [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
                  <ds:X509Certificate>
                    [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
                  <ds:X509Certificate>
                    [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
               </ds:X509Data>
            </ds:KeyInfo>
         </ds:Signature>
         <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
            <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
NameQualifier="https://rp.cnipa.gov.it/rp">CGNNMO50A01F205J</saml:NameID>
         </saml:Subject>
         <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="lastname"/>
         <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="birthplace"/>
         <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="firstname"/>
      </samlp:AttributeQuery>
```

# Response emessa da una Attribute Authority

Si riporta un esempio di risposta a una richiesta di attributi (sono stati omessi per brevità i valori delle firme e dei certificati codificati in formato Base64). L'esempio illustra una risposta relativa ai valori degli attributi specificati ("lastname", "birthplace" e "firstname") dell'utente indicato (elemento <Subject>).

```
    <?xml version="1.0" encoding="UTF-8"?>
    <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://rp.cnipa.gov.it:3443/rp" ID="s2e3b65bc518f37ef666554aaa3c1c51ae1a1d9abc"
InResponseTo="s207e487be6a26e83e348110abf399756c19c7e462" IssueInstant="2008-03-11T21:34:14.515Z"
Version="2.0">
       <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://aa.cnipa.gov.it:5443/aa</saml:Issuer>
       <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:Reference URI="#s2e3b65bc518f37ef666554aaa3c1c51ae1a1d9abc"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

```
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="ds
saml samlp xs xsi"/>
                    </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
    </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    [FIRMA]
    </ds:SignatureValue>
          <ds:KeyInfo>
             <ds:X509Data>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
```

```
            </ds:X509Data>
         </ds:KeyInfo>
      </ds:Signature>
      <samlp:Status>
         <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </samlp:Status>
      <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="s2bd64563525823db91c2cf9f724b52a579d7fc4a3" IssueInstant="2008-03-11T21:34:14.515Z" Version="2.0">
         <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://aa.cnipa.gov.it:5443/aa</saml:Issuer>
         <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:Reference URI="#s2bd64563525823db91c2cf9f724b52a579d7fc4a3"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="ds saml xs"/>
```

```
                    </ds:Transform>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
    <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
    </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    [FIRMA]
    </ds:SignatureValue>
          <ds:KeyInfo>
             <ds:X509Data>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
                <ds:X509Certificate>
                 [CERTIFICATO CODIFICATO IN BASE64]
                </ds:X509Certificate>
             </ds:X509Data>
          </ds:KeyInfo>
```

```
            </ds:Signature>
            <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
               <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
NameQualifier="https://aa.cnipa.gov.it/aa">CGNNMO50A01F205J</saml:NameID>
            </saml:Subject>
            <saml:Conditions NotBefore="2008-03-11T21:34:14.515Z" NotOnOrAfter="2008-09-07T21:34:14.515Z"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"/>
            <saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
               <saml:Attribute Name="lastname">
                  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Cognome</saml:AttributeValue>
               </saml:Attribute>
               <saml:Attribute Name="birthplace">
                  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Roma</saml:AttributeValue>
               </saml:Attribute>
               <saml:Attribute Name="firstname">
                  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Nome</saml:AttributeValue>
               </saml:Attribute>
            </saml:AttributeStatement>
         </saml:Assertion>
      </samlp:Response>
```

# APPENDICE B: METADATI - ESEMPI

## Metadati Service Provider

L'esempio che segue si riferisce ai metadati firmati di un Service Provider. In aggiunta a quanto vale in generale, come detto in precedenza, in questo caso le principali informazioni veicolate sono:

- attributo `AuthnRequestsSigned`: il valore "true" indica che il Service Provider emette richieste di autenticazione firmate;
- elemento `<AssertionConsumerService>`: il servizio (in termini di URL e relativo binding "HTTP POST") a cui contattare il Service Provider per l'invio di risposte SAML;
- elementi `<AttributeConsumingService>`: descrivono i quattro servizi esposti dal Service provider, in termini di indice posizionale, nome e attributi richiesti per l'accesso (per esempio, nel caso del servizio "Servizio 1" gli attributi il cui valore è necessario fornire sono "firstname", "lastname" e "birthdate").

Nell'elemento `<EntityDescriptor>` è presente l'attributo opzionale `cacheDuration`, che indica la durata massima di permanenza in cache ammessa per questo file di metadati (cioè per ciascuna delle informazioni in esso contenute) da parte di un generico client. La durata è espressa nel formato previsto dalla specifica XML Schema (cfr. [XMLData], sez. 3.2.6) nel caso specifico, "P30DT0H0M0.000S" indica una durata pari a 30 giorni.

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="http://sp.cnipa.gov.it/sp" cacheDuration="P30DT0H0M0.000S">
 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
            <ds:Reference URI="" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                              <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="ds md saml" />
                        </ds:Transform>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
                  <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
            </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[FIRMA]</ds:SignatureValue>
```

```
            <ds:KeyInfo>
                  <ds:X509Data>
                        <ds:X509Certificate>
                         [CERTIFICATO CODIFICATO IN BASE64]
                        </ds:X509Certificate>
                        <ds:X509Certificate>
                         [CERTIFICATO CODIFICATO IN BASE64]
                        </ds:X509Certificate>
                        <ds:X509Certificate>
                         [CERTIFICATO CODIFICATO IN BASE64]
                        </ds:X509Certificate>
                  </ds:X509Data>
            </ds:KeyInfo>
      </ds:Signature>
      <md:SPSSODescriptor AuthnRequestsSigned="true"
            protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <md:KeyDescriptor use="signing">
                  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:X509Data>
                              <ds:X509Certificate>
                               [CERTIFICATO CODIFICATO IN BASE64]
                              </ds:X509Certificate>
```

```
                        <ds:X509Certificate>
                         [CERTIFICATO CODIFICATO IN BASE64]
                        </ds:X509Certificate>
                        <ds:X509Certificate>
                         [CERTIFICATO CODIFICATO IN BASE64]
                        </ds:X509Certificate>
                  </ds:X509Data>
            </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:NameIDFormat>
            urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
      </md:NameIDFormat>
      <md:AssertionConsumerService index="1"
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="http://sp.cnipa.gov.it:8080/sp/AssertionConsumerService" />
      <md:AttributeConsumingService index="1">
            <md:ServiceName xml:lang="it">Servizio 1</md:ServiceName>
            <md:RequestedAttribute
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                  Name="firstname"
                  FriendlyName="First name">
            </md:RequestedAttribute>
```

```
            <md:RequestedAttribute
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                  Name="lastname"
                  FriendlyName="Last name">
            </md:RequestedAttribute>
            <md:RequestedAttribute
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                  Name="birthdate"
                  FriendlyName="Birthdate">
            </md:RequestedAttribute>
      </md:AttributeConsumingService>
      <md:AttributeConsumingService index="2">
            <md:ServiceName xml:lang="it">Servizio 2</md:ServiceName>
            <md:RequestedAttribute
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                  Name="lastname"
                  FriendlyName="Last name">
            </md:RequestedAttribute>
            <md:RequestedAttribute
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                  Name="birthplace"
                  FriendlyName="Birthplace">
```

```
            </md:RequestedAttribute>
            <md:RequestedAttribute
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                  Name="work"
                  FriendlyName="Work">
            </md:RequestedAttribute>
      </md:AttributeConsumingService>
      <md:AttributeConsumingService index="3">
            <md:ServiceName xml:lang="it">Servizio 3</md:ServiceName>
            <md:RequestedAttribute
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                  Name="lastname"
                  FriendlyName="Last name">
            </md:RequestedAttribute>
            <md:RequestedAttribute
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                  Name="nationality"
                  FriendlyName="Nationality">
            </md:RequestedAttribute>
            <md:RequestedAttribute
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                  Name="mobile"
```

```
                    FriendlyName="Mobile phone number">
                </md:RequestedAttribute>
            </md:AttributeConsumingService>
            <md:AttributeConsumingService index="4">
                <md:ServiceName xml:lang="it">Servizio 4</md:ServiceName>
                <md:RequestedAttribute
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                    Name="gender"
                    FriendlyName="Gender">
                </md:RequestedAttribute>
                <md:RequestedAttribute
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                    Name="work"
                    FriendlyName="Work">
                </md:RequestedAttribute>
                <md:RequestedAttribute
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
                    Name="address"
                    FriendlyName="Address">
                </md:RequestedAttribute>
            </md:AttributeConsumingService>
        </md:SPSSODescriptor>
```

```
    </md:EntityDescriptor>
```

# Metadati Identity Provider

L'esempio che segue si riferisce ai metadati firmati di un Identity Provider. In aggiunta a quanto vale in generale, come detto in precedenza, in questo caso le principali informazioni veicolate sono:

- attributo `WantAuthnRequestsSigned`: il valore "true" indica che le richieste inoltrate all'Identity Provider dovranno essere firmate;
- elementi `<SingleSignOnService>`: i servizi (in termini di URL e relativi binding, "HTTP POST" e "HTTP Redirect") a cui è possibile contattare l'Identity Provider per l'invio di richieste di autenticazione SAML.

Anche in questo esempio è presente l'attributo `cacheDuration` (cfr. Metadati Service Provider).

```
    <?xml version="1.0" encoding="UTF-8"?>
    <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
     entityID="https://idp.cnipa.gov.it/idp" cacheDuration="P30DT0H0M0.000S">
     <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
           <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                 <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
```

```
                  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
                  <ds:Reference URI="" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
                              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                    <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="ds md saml" />
                              </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
                        <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
                  </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[FIRMA]</ds:SignatureValue>
            <ds:KeyInfo>
                  <ds:X509Data>
                        <ds:X509Certificate>
                         [CERTIFICATO CODIFICATO IN BASE64]
                        </ds:X509Certificate>
                        <ds:X509Certificate>
```

```
                    [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
                  <ds:X509Certificate>
                    [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
            </ds:X509Data>
      </ds:KeyInfo>
</ds:Signature>
<md:IDPSSODescriptor WantAuthnRequestsSigned="true"
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <ds:X509Data>
                        <ds:X509Certificate>
                          [CERTIFICATO CODIFICATO IN BASE64]
                        </ds:X509Certificate>
                        <ds:X509Certificate>
                          [CERTIFICATO CODIFICATO IN BASE64]
                        </ds:X509Certificate>
                        <ds:X509Certificate>
                          [CERTIFICATO CODIFICATO IN BASE64]
                        </ds:X509Certificate>
```

```
                        </ds:X509Data>
                    </ds:KeyInfo>
                </md:KeyDescriptor>
                <md:NameIDFormat>
                    urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
                </md:NameIDFormat>
                <md:SingleSignOnService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Location="https://idp.cnipa.gov.it:9443/idp/SSOService" />
                <md:SingleSignOnService
                    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-REDIRECT"
                    Location="https://idp.cnipa.gov.it:9443/idp/SSOService" />
            </md:IDPSSODescriptor>
        </md:EntityDescriptor>
```

# Metadati Attribute Authority

L'esempio che segue si riferisce ai metadati firmati di una Attribute Authority. In aggiunta a quanto vale in generale, come detto in precedenza, in questo caso le principali informazioni veicolate sono:

- elemento <AttributeService>: il servizio (in termini di URL e relativo binding "SOAP") a cui contattare la Attribute Authority per l'invio di richieste di attributo SAML;

- elemento <AttributeProfile>: enumerazione dei profili di rappresentazione di attributi supportati dall'entità (cfr.[SAML-Profile], sez. 8); nel caso specifico solo "basic" (cfr. [SAML-Profile], sez. 8.1).
- elementi <Attribute>: gli attributi (nome e "friendly name") certificati dall'authority: "job", "role", "dept", "salary".

Anche in questo esempio è presente l'attributo cacheDuration (cfr. sez. Metadati Service Provider).

```
    <?xml version="1.0" encoding="UTF-8"?>
    <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
     entityID="https://aa.cnipa.gov.it/aa"    cacheDuration="P30DT0H0M0.000S">
     <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
               <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
               <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
               <ds:Reference URI="" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                    <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                         <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
                         <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                              <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="ds md saml" />
                         </ds:Transform>
```

```
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
                        <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
                  </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[FIRMA]</ds:SignatureValue>
            <ds:KeyInfo>
                  <ds:X509Data>
                        <ds:X509Certificate>
                         [CERTIFICATO CODIFICATO IN BASE64]
                        </ds:X509Certificate>
                        <ds:X509Certificate>
                         [CERTIFICATO CODIFICATO IN BASE64]
                        </ds:X509Certificate>
                        <ds:X509Certificate>
                         [CERTIFICATO CODIFICATO IN BASE64]
                        </ds:X509Certificate>
                  </ds:X509Data>
            </ds:KeyInfo>
      </ds:Signature>
      <md:AttributeAuthorityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
            protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
```

```
<md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509Data>
                  <ds:X509Certificate>
                   [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
                  <ds:X509Certificate>
                   [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
                  <ds:X509Certificate>
                   [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
            </ds:X509Data>
      </ds:KeyInfo>
</md:KeyDescriptor>
<md:AttributeService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="https://aa.cnipa.gov.it:5443/aa/AttributeQueryHandlerServlet"/>
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
<md:AttributeProfile>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</md:AttributeProfile>
<saml:Attribute FriendlyName="Professione" Name="job" />
<saml:Attribute FriendlyName="Ruolo" Name="role" />
```

```
            <saml:Attribute FriendlyName="Dipartimento" Name="dept" />
            <saml:Attribute FriendlyName="Stipendio" Name="salary" />
      </md:AttributeAuthorityDescriptor>
    </md:EntityDescriptor>
```

# Metadati Authority Registry

L'esempio che segue si riferisce ai metadati di un Authority Registry. In aggiunta a quanto vale in generale, come detto in precedenza, in questo caso le principali informazioni veicolate sono:

- elemento `<AttributeService>`: il servizio (in termini di URL e relativo binding "SOAP") a cui contattare l'Authority Registry per l'invio di richieste di attributo SAML;
- elemento `<AttributeProfile>`: enumerazione dei profili di rappresentazione di attributi supportati dall'entità (cfr. .[SAML-Profile], sez. 8); nel caso specifico solo "basic" (cfr. .[SAML-Profile], sez. 8.1);
- elementi `<Attribute>`: gli attributi (nome e "friendly name") certificati dall'authority: "AuthorityList", "Domain", "MetadataProviderURL", "EntityID", "Description", "Type" (per il significato di questi attributi si veda la sez.[Registry ARS e AARS]).

Anche in questo esempio è presente l'attributo `cacheDuration` (cfr. sez.Metadati ServiceProvider).

```
    <?xml version="1.0" encoding="UTF-8"?>
    <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
     entityID="https://ar.cnipa.gov.it/ar"
```

```
      cacheDuration="P30DT0H0M0.000S">
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
                  <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
                  <ds:Reference URI="" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                              <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
                              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                    <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
PrefixList="ds md saml" />
                              </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
                        <ds:DigestValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[DIGEST]</ds:DigestValue>
                  </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">[FIRMA]</ds:SignatureValue>
            <ds:KeyInfo>
```

```
            <ds:X509Data>
      <ds:X509Certificate>[CERTIFICATO CODIFICATO IN BASE64]</ds:X509Certificate>
      <ds:X509Certificate>[CERTIFICATO CODIFICATO IN BASE64]</ds:X509Certificate>
      <ds:X509Certificate>[CERTIFICATO CODIFICATO IN BASE64]</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </ds:Signature>
      <md:AttributeAuthorityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
         protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
         <md:KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
               <ds:X509Data>
                  <ds:X509Certificate>
                   [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
                  <ds:X509Certificate>
                   [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
                  <ds:X509Certificate>
                   [CERTIFICATO CODIFICATO IN BASE64]
                  </ds:X509Certificate>
               </ds:X509Data>
```

```
                </ds:KeyInfo>
            </md:KeyDescriptor>
            <md:AttributeService
                Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
                Location="https://ar.cnipa.gov.it:4443/ar/AttributeQueryHandlerServlet"/>
            <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
            <md:AttributeProfile>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</md:AttributeProfile>
            <saml:Attribute FriendlyName="Elenco authority" Name="AuthorityList" />
            <saml:Attribute FriendlyName="Dominio" Name="Domain" />
            <saml:Attribute FriendlyName="Metadata Provider URL" Name="MetadataProviderURL" />
            <saml:Attribute FriendlyName="ID authority" Name="EntityID" />
            <saml:Attribute FriendlyName="Descrizione" Name="Description" />
            <saml:Attribute FriendlyName="Tipo" Name="Type" />
     </md:AttributeAuthorityDescriptor>
    </md:EntityDescriptor>
```

# APPENDICE C: DISPIEGAMENTO E INTEROPERABILITÀ

La seconda Sezione del documento ha evidenziato quali sono i servizi infrastrutturali erogati dal CG-SICA e quali sono i servizi di cui una Amministrazione deve dotarsi per poter divenire membro della federazione.

Si è visto come tali servizi siano differenti secondo il ruolo che l'Amministrazione intende ricoprire. Se intende erogare uno o più servizi ad utenti appartenenti ad altre Amministrazioni è necessario che l'Amministrazione adotti un software che possa svolgere il compito assegnato al Service Provider ed in particolare i servizi svolti dai suoi sottosistemi :

- Federation Gateway il tramite tra la federazione e le risorse messe a disposizione dall'Amministrazione.
- Policy Enforcement Point il punto dove vengono applicate le policy di accesso prima di consentire l'erogazione del servizio.

Non ci sono ad oggi restrizioni su come il Federation Gateway debba essere implementato, può essere un prodotto commerciale od un prodotto implementato direttamente dall'Amministrazione. L'unica precondizione è la capacità di essere compatibile con le operazioni SAML e la sintassi definita per la cooperazione all'interno del modello in modo da garantire l'interoperabilità.

Oltre al Federation Gateway l'Amministrazione deve essere in grado di trasformare dal "linguaggio interno" verso la sintassi SAML e viceversa le informazioni verso/e provenienti da il Federation Gateway. Questa operazione nel modello è fatta direttamente dal Service Provider o dalla singola applicazione.

Se l'Amministrazione intende ricoprire il ruolo di Identity Provider all'interno della federazione deve dotarsi di una soluzione capace di propagare l'identità dei propri utenti all'esterno del proprio dominio interagendo secondo lo scenario di F-SSO descritto in precedenza e tramite le interfacce SAML descritte per l'IdP.

Una Amministrazione che voglia abilitare i propri utenti ai servizi federati deve anche fornire il riferimento di una Profile Authority dove reperire i profili a loro associati.

E' importante sottolineare che la Profile Authority non deve essere necessariamente all'interno o a carico dell'Amministrazione. Gli utenti che un'Amministrazione intende federare devono avere un profilo associato e localizzato in una qualsiasi PA registrata all'interno dell'Authority Registry.(es: la profile authority del CG-SICA).

In riferimento all'Attribute Authority, una Amministrazione deve comunque fornire un garante per gli attributi di ruolo di sua responsabilità e presenti nel profilo dei propri utenti (es:responsabile di ufficio, responsabile di un dato procedimento amministrativo). L'AA designata deve essere presente all'interno dell'Attribute Authority Registry.

Le Amministrazioni che intendono federare i propri utenti possono avvalersi di software commerciale o diversamente decidere di utilizzare prodotti custom, anche in questo caso devono garantire l'interoperabilità con l'infrastruttura del servizio GFID. Alternativamente possono utilizzare l'Autorità Locale di Dominio che nasce con lo scopo di fornire un servizio capace di svolgere simultaneamente i ruoli di IDP, Profile Authority e Attribute Authority o solo un suo sottoinsieme secondo le necessità specifiche dell'Amministrazione.