Sistema Federato Interregionale di Autenticazione: MODELLO CONCETTUALE DI RIFERIMENTO

Versione 1.0.2

INDICE

1. Modifiche Documento ***4***

2. Introduzione ***5***

3. Domini ed entità interagenti ***7***

3.1. Domini **7**

3.1.1. Dominio di profilazione 7

3.1.2. Dominio fruitore 7

3.1.3. Dominio erogatore 7

3.1.4. Dominio certificatore 8

3.2. Autorità di certificazione o certificatori **8**

3.3. Altre entità coinvolte **9**

3.4. La gestione del profilo utente **10**

3.5. Servizi di base offerti dalle authority **12**

3.6. Considerazioni sulle interfacce offerte da un Service Provider **13**

4. Modelli di cooperazione ***15***

4.1. Modello 1 ..... **15**

4.1.1. Interazioni nel modello 1 17

4.2. Modello 2 ..... **19**

4.2.1. Interazioni nel modello 2 20

4.3. Modello 3 ..... **21**

4.3.1. Interazioni nel modello 3 22

4.4. Modello 4 ..... **23**

4.4.1. Interazioni nel modello 4 24

4.5. Valutazione dei modelli proposti **26**

4.6. Considerazioni sul caching delle asserzioni **27**

5. Modello di riferimento per l'autenticazione e autorizzazione nel sistema federato interregionale ***29***

5.1. Casi d'uso **29**

5.2. Scenario di riferimento **30**

5.3. Scenario in cooperazione applicativa **35**

5.3.1. Le entità interagenti nello scenario in cooperazione applicativa 39

5.3.2. Scenario generale d'interazione in cooperazione applicativa 42

6. Tecnologie di riferimento ***46***

6.1. SAML **46**

6.1.1. OpenSAML 48

6.1.2. Uso di SAML per il sistema di autorizzazione e autenticazione federata (INF-3) 49

6.2. XACML **50**

6.2.1. Implementazione Sun XACML 51

6.2.2. Uso di XACML per il sistema di autorizzazione e autenticazione federata (INF-3) 52

7. Acronimi ***53***

8. Bibliografia.....54

1. MODIFICHE DOCUMENTO

Descrizione Modifica	Edizione	Data
Prima revisione	0.1	25/05/2005
Aggiunta variante a modello 1	0.2	26/05/2005
Correzioni a diagrammi UML	0.3	27/05/2005
Ristrutturazione e organizzazione documento con 4 modelli e valutazione	0.4	9/6/2005
Revisione diagrammi UML	0.5	15/6/2005
Inserito Access Manager	0.6	23/6/2005
Revisione diagrammi UML	0.61	11/7/2005
Revisione introduzione		13/9/2005
Inserimento modello di riferimento con local proxy	0.7	18/10/2005
Aggiunto scenario di riferimento Iniziato scenario in cooperazione applicativa Prima stesura capitolo tecnologie	0.8	21/10/2005
Terminologia conformata a documentazione CNIPA SPCoop Modificato template documento Completato scenario in cooperazione applicativa Completata stesura capitolo tecnologie	0.9	26/10/2005
Revisione terminologia, correzioni ortografiche, correzione ai diagrammi	1.0	24/11/2005
Revisione impaginazione	1.0.1	14/12/2005
Revisione, correzioni e ulteriori precisazioni	1.0.2	16/03/2006

2. INTRODUZIONE

Obiettivo del presente documento è di definire e descrivere il modello logico di riferimento dell'infrastruttura interregionale di autenticazione e autorizzazione, specificando gli scenari per l'accesso ai servizi e per la fruizione degli stessi da parte delle varie tipologie di utenti interessati.

Lo scenario di riferimento è quello tipico di una rete regionale, ovvero una comunità a cui afferiscono uno o più domini in grado di offrire differenti tipologie di servizi ai propri utenti, e che possono dialogare con altri domini anche se appartenenti ad altre reti regionali.

Il modello proposto si basa sulla federazione tra community network che comunicano tra loro attraverso la rete Internet. L'obiettivo è assicurare la trasparenza del livello applicativo dei servizi offerti dai singoli domini rispetto alle specifiche modalità di interazione utilizzate all'interno delle singole comunità.

I servizi definiti da ciascun dominio facente capo a una specifica comunità possono essere resi disponibili agli altri domini della comunità, così come ai domini appartenenti a comunità diverse, attraverso una interfaccia di dominio. L'interfaccia di dominio costituisce concettualmente il punto di ingresso per l'accesso alle risorse applicative offerte dal dominio. Essa si può ulteriormente specializzare in portale e porta di dominio: il primo gestisce l'interazione tra tali servizi e gli utenti umani (per esempio i cittadini), mentre la seconda rappresenta il punto di accesso utilizzato dalle applicazioni software che vogliono accedere ai servizi esposti dal dominio. Inoltre, la porta di dominio rappresenta per i servizi definiti internamente a un dominio il punto di accesso verso gli altri domini.

In corrispondenza di tali due modalità di accesso ad un servizio, è possibile evidenziare come, in generale, le interazioni tra i vari attori in gioco (utenti e servizi di altri domini) si articolano su due livelli. Il primo per mettere in comunicazione il browser dell'utente con il front-end del servizio e il secondo che lega il front-end con uno o più back-end. La prima interazione avviene, come è usuale, tra un browser (detto anche User Agent, nel seguito) e un web server. La seconda, in un'ottica di cooperazione applicativa, tra porte di dominio di enti diversi che partecipano alla realizzazione del servizio che l'utente ha richiesto di poter fruire. Questo documento ha lo scopo di illustrare le modalità con cui, in entrambe le fasi, l'identità dei soggetti interagenti viene accertata e sono effettuate tutte le opportune verifiche di autorizzazione.

Nel seguito si fornirà una descrizione delle entità presenti nel modello proposto, illustrandone le funzionalità. Nella seconda parte saranno presentati alcuni scenari di funzionamento in cui le entità introdotte assumono un ben preciso ruolo e interagiscono l'una con l'altra. La terminologia impiegata nel presente documento si conforma a quella del Modello di Funzionamento Organizzativo del Sistema Pubblico di Cooperazione (SPCoop) definito dal CNIPA nell'ambito del SPC. Inoltre, vengono dettagliati alcuni concetti illustrati nel cap. 5 del documento sull'organizzazione del Sistema Federato Interregionale di Autenticazione [4].

Il linguaggio di descrizione adottato nel documento è UML, facendo in prevalenza ricorso ai diagrammi dei casi d'uso, ai diagrammi delle classi e ai diagrammi di collaborazione. Per quel che riguarda in particolare i diagrammi delle classi, si fa notare che le dipendenze tra le entità (rappresentate da linee tratteggiate) esprimono una relazione "debole" o d'uso, per esempio l'invocazione di una funzionalità

offerta da un componente, mentre le associazioni (rappresentate da linee a tratto continuo) indicano l'esistenza di un legame "stabile" o strutturale tra le entità.

3. DOMINI ED ENTITÀ INTERAGENTI

In questo capitolo sono presentati i concetti base che compongono il modello per la gestione federata delle identità e delle politiche di autorizzazione. Tale modello si compone di due concetti principali che sono i domini informatici (chiamati semplicemente "domini" nel seguito) e le entità o soggetti certificatori (chiamati anche authority). Oltre ad essi saranno citati altri elementi che svolgono un ruolo attivo nel processo di fruizione di un servizio.

3.1. Domini

Nei modelli architetturali che caratterizzano l'organizzazione dei sistemi informativi della Pubblica Amministrazione è stato da tempo introdotto, ed è comunemente adottato, il concetto di dominio informatico. Il dominio rappresenta il sistema informativo di una amministrazione in senso lato ed in particolare definisce il **perimetro di sicurezza informatica** di responsabilità di una amministrazione. Nell'interazione descritta nel seguito si farà riferimento a quattro tipi di domini distinti:

- dominio di profilazione (D_{PROF} o D_PROF)
- dominio fruitore (D_F o DF)
- dominio erogatore (D_E o DE)
- dominio certificatore (D_{CERT} o D_CERT)

3.1.1. Dominio di profilazione

Un dominio viene detto *di profilazione* per un dato utente quando in esso è stata eseguita la procedura di riconoscimento iniziale, durante la quale a quell'utente sono state richieste alcune informazioni che da quel momento in poi sono state memorizzate in una struttura dati chiamata "profilo utente". Tale struttura viene gestita da una specifica entità detta Profile Authority, illustrata nel seguito.

3.1.2. Dominio fruitore

Un dominio si dice *fruitore* relativamente ad un'interazione di accesso ad un servizio, quando in essa ha origine la richiesta di tale servizio. Per gli scopi di questa trattazione, il dominio fruitore viene a coincidere di fatto con lo stesso utente richiedente, nella figura del suo User Agent (UA), come un comune browser web.

3.1.3. Dominio erogatore

Un dominio viene detto *erogatore* relativamente ad un'interazione di accesso ad un servizio, quando in esso è presente il fornitore del servizio richiesto. In tale dominio, come sarà illustrato nel seguito, potranno essere presenti ulteriori entità, come quella incaricata di verificare che il richiedente possieda tutti i requisiti necessari per l'accesso al servizio indicato, eventualmente ottenendoli da terze parti

fidate. Questo dominio di fatto coincide con quello che è chiamato DSA (dominio dei servizi applicativi), secondo la terminologia CNIPA.

3.1.4. Dominio certificatore

Un dominio viene detto *certificatore* relativamente ad un'interazione di accesso ad un servizio, quando in esso sono presenti uno o più soggetti certificatori, nel seguito detti anche authority, in grado di asserire la validità di uno o più attributi contenuti nel profilo gestito dalla Profile Authority del dominio di profilazione dell'utente. Per questo motivo il profilo, oltre a contenere i dati veri e propri relativi all'utente, dovrebbe memorizzare dei riferimenti a tutte le authority coinvolte, che fanno capo ad uno o più domini certificatori.

I suddetti domini informatici, nel momento in cui interagiscono per svolgere attività di cooperazione tese all'erogazione di servizi, diventano parte di un **Dominio di Cooperazione**, definito dalla nomenclatura CNIPA, nell'ambito del Sistema Pubblico di Cooperazione. Tale dominio organizzativo concorre a formare una comunità di domini informatici e dispone di un'entità di riferimento, detta **Responsabile del Dominio di Cooperazione** (RDC), come illustrato nel documento [4].

3.2. Autorità di certificazione o certificatori

All'interno dei domini elencati nella sezione precedente, operano un certo numero di entità, che espongono servizi atti a certificare alcune informazioni contenute nel profilo degli utenti. Tali entità sono chiamate *authority* e hanno la caratteristica di godere della fiducia di altre entità presenti nei vari domini coinvolti. Questo significa che le "descrizioni" prodotte da un'authority, relativamente alla validità o invalidità delle informazioni nei profili utente sono considerate vere per definizione, da parte di tutti coloro che si fidano di tale authority. Si possono distinguere almeno tre tipologie di authority:

- **certification authority**: sono le authority abilitate a certificare l'identità di un utente, nel processo di autenticazione. Un utente viene dotato di un certo numero di credenziali, da parte di ciascuna certification authority a cui fa capo. In questo modo, diverse certification authority possono certificare diversi tipi di credenziali, come ad esempio credenziali costituite da nome utente e password, oppure da codice fiscale e PIN. Un utente potrebbe avere un profilo contenente credenziali certificate da più di una certification authority. Nel seguito il termine certification authority sarà spesso abbreviato con l'acronimo CA.
- **attribute authority**: sono le authority abilitate a certificare alcuni degli attributi contenuti nel profilo di un utente, ed utilizzati nel processo di autorizzazione. Un utente in generale è dotato di un certo numero di attributi che, insieme alle credenziali, concorrono a formare il suo profilo. Esempi di attributi sono la residenza, la professione, il titolo di studio e l'iscrizione ad un albo e sono in generale certificate da authority presenti in domini diversi. Si pensi al caso di un utente del dominio (di profilazione) del Comune di Milano, che svolge anche il ruolo di rappresentante legale di una società appartenente al dominio del Comune di Roma: l'attribute authority competente per

certificare questa qualifica farà parte del dominio, remoto, di Roma. Nel seguito il termine attribute authority sarà spesso abbreviato con l'acronimo AA.

- **profile authority**: sono le entità incaricate della gestione dell'archivio dei profili utente presenti nei domini di profilazione. Ad esse è demandato il compito di rispondere alle richieste di attributo formulate dal dominio erogatore, per la verifica dell'identità e/o del livello di autorizzazione. La Profile Authority, di seguito abbreviata con l'acronimo PA, fa parte del dominio di profilazione dell'utente di cui gestisce il profilo e può essere interrogata remotamente da parte di domini diversi, come il dominio erogatore.

Come detto sopra, sia le CA che le AA fanno logicamente parte dei domini certificatori. Casi particolari sono quelli in cui una CA o una AA o entrambe fanno parte anche di uno degli altri domini (fruitore o erogatore), perché gli stessi svolgono anche funzioni di certificazione. In tali casi, infatti, domini concettualmente diversi possono coincidere fisicamente, per le funzioni svolte in essi dalle entità presenti. Ad esempio, dominio fruitore e dominio di profilazione coincidono quando un utente sta operando nello stesso dominio ove si è registrato (ad esempio nel suo comune, o altro ente di appartenenza). Il formato delle certificazioni prodotte dai tipi di authority presentati si conforma alle specifiche prodotte in seno al consorzio OASIS[1], relativamente al linguaggio SAML [1]. Tale notazione è nata allo scopo di formalizzare uno standard utile per trasmettere questo genere di informazioni sotto forma di documenti chiamati "asserzioni" e presenta tutti gli elementi necessari per certificare i diversi attributi del profilo di un utente.

Le asserzioni prodotte da un'authority e scambiate con altre entità dei domini descritti possono essere considerate affidabili, proprio in quanto provenienti da un'authority (e quindi in qualche modo firmate da tale entità) invece che da un soggetto qualunque. A loro volta, tuttavia, le varie authority dovranno comprovare la propria abilitazione a firmare asserzioni relativamente agli attributi che intendono certificare. Se così non fosse, infatti, qualunque authority potrebbe certificare qualunque tipo di attributo di qualunque utente. Per evitare questo, si fa ricorso ad un garante, esterno a tutti i domini e considerato fidato da tutte le authority di tutti i domini. Insieme agli attributi certificati da un'authority, all'interno dell'asserzione prodotta verranno inseriti anche tutti i nomi degli attributi certificabili da tale authority, e tale informazione sarà firmata dal garante.

3.3. Altre entità coinvolte

Oltre alle authority, nel modello di interazione sono presenti i fornitori di servizi, ai quali gli utenti accedono. Ogni servizio è caratterizzato, tra le altre cose, da un insieme di informazioni (un "profilo") tra le quali si trovano i requisiti necessari perché un utente autenticato possa usufruire del servizio stesso. Un generico fornitore di servizio sarà indicato con il termine Service Provider e spesso abbreviato con l'acronimo SP. Si noti che un fornitore di servizi funge da entry-point per tutte le richieste di accesso alle risorse e aggiunge la logica necessaria alla verifica del contesto di sicurezza e

[1] OASIS website: http://www.oasis-open.org

all'attivazione delle fasi di autenticazione e autorizzazione. A ogni servizio, pertanto, non si può accedere direttamente ma in maniera schermata da questo strato di filtraggio che provvede ad effettuare tutti i controlli di accesso necessari. Il SP farà poi riferimento ad entità esterne per l'attuazione dei processi di autenticazione e autorizzazione.

Due di tali entità supplementari sono un Access Manager (AM), con il compito di accedere alle varie authority (o di mettere in contatto l'utente con esse) per ottenere una certificazione relativamente agli attributi oggetto di verifica. La seconda entità è il Gestore delle Politiche di Autorizzazione (GPA), in carico di verificare che gli attributi certificati e ottenuti dall'AM, rispondano ai requisiti imposti dal fornitore del servizio, per consentire o negare l'accesso al servizio richiesto. In generale tali due componenti fanno capo al dominio erogatore, come sarà illustrato nel seguito del documento.

La Figura 1 riassume quanto descritto sopra, illustrando i vari tipi di domini citati, e le entità in essi presenti, con le relazioni mutue tra esse. Si noti che nel dominio erogatore possono esistere in generale diversi SP, i quali possono avvalersi anche di un unico AM e GPA per attivare le procedure di autenticazione e autorizzazione. È ovviamente possibile il caso in cui esistano più AM e GPA distinti, associati a SP diversi. Analogamente, all'interno del dominio certificatore sono in generale presenti più CA e più AA.

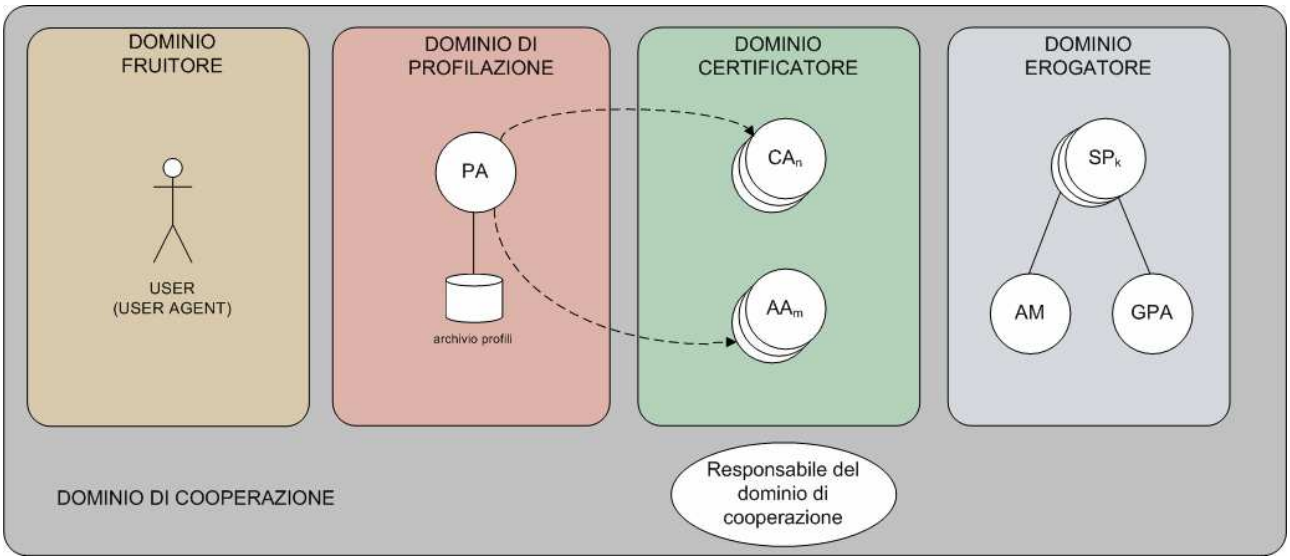

Figura 1: I domini e le entità contenute

3.4. La gestione del profilo utente

Le PA presenti nei domini di profilazione dei vari utenti memorizzano le informazioni ad essi relative in un registro atto a contenere nomi di attributi, loro valori e dei puntatori alle varie AA competenti a certificare la validità degli stessi, presenti nei vari domini certificatori. Nel caso generale PA e AA possono appartenere a domini diversi, ovvero dominio di profilazione e domini certificatori possono essere distinti. In alcuni dei modelli di interazione presentati nel seguito, si vedrà come una generica PA possa essere presente anche nei domini erogatori e certificatori, in modo da funzionare come un proxy

delle CA e AA alle quali i profili utente rimandano. Come già accennato infatti, tali profili saranno costituiti da un insieme di attributi dichiarati dall'utente, ma la cui veridicità può essere accertata soltanto consultando l'authority competente, che rilascerà un'opportuna certificazione, sotto forma di asserzione di attributo firmata digitalmente. L'atto della consultazione di una authority può avvenire o direttamente da parte di entità del dominio erogatore, nel processo di verifica dell'identità oppure può essere mediata da un'ulteriore PA, presente nello stesso dominio certificatore, insieme all'authority stessa. In questo modo ciascuna PA di un dominio svolgerebbe anche il ruolo di entry-point, nei confronti di domini esterni, per le interrogazioni che riguardano le certificazioni di attributi di competenza di authority locali, che verrebbero così ad essere mascherate. Qualora una PA svolgesse anche il ruolo di mediatore o proxy nei confronti delle PA di altri domini, le si attribuirebbe automaticamente un ruolo attivo nel processo di gestione federata delle identità e autorizzazioni. Tale ruolo è invece molto ridimensionato nel caso in cui essa si limitasse alla sola gestione del profilo, ovvero alle operazioni di accesso e memorizzazione.

È bene notare che una PA, in quanto aggregatore di asserzioni di attributo o semplice gestore di un insieme di puntatori alle authority certificatrici degli attributi del profilo utente, non necessariamente deve a sua volta certificare l'aggregato di asserzioni, ma semplicemente fornirlo su richiesta, in quanto le certificazioni sono fornite dalle CA e AA a cui il profilo fa riferimento.

Nella Figura 2 viene illustrato un esempio di struttura per le informazioni memorizzate nel registro di una PA, in cui si fa riferimento anche agli attributi di autenticazione, di presenti presso la relativa CA.

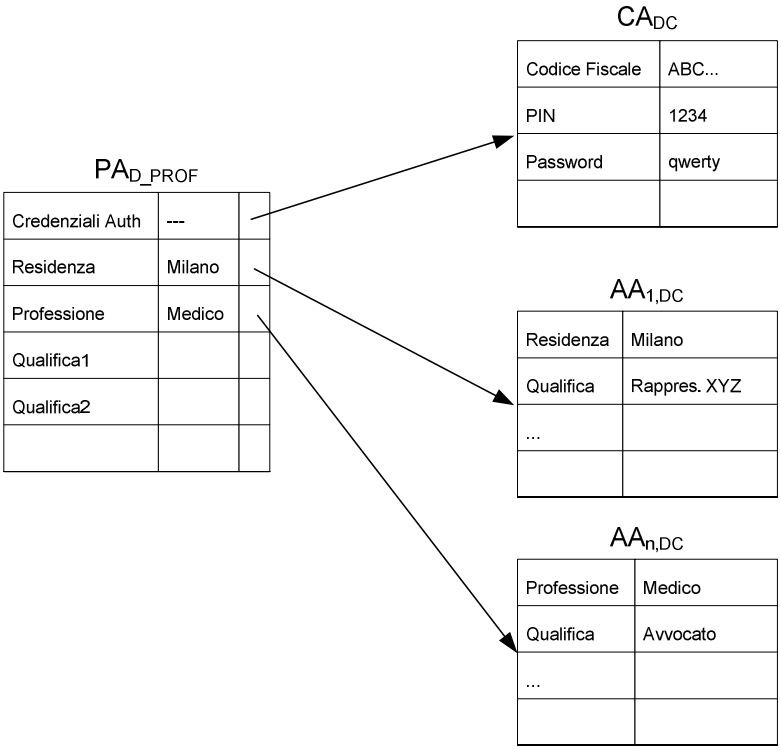

Figura 2: Informazioni memorizzate da una Profile Authority

3.5. Servizi di base offerti dalle authority

Nelle sezioni precedenti si è illustrato come SP e authority costituiscano i mattoni elementari, distribuiti nei vari domini informatici, alla base del processo di autenticazione e autorizzazione nel sistema federato. In Figura 3 sono descritte le interfacce offerte dalle authority descritte sopra, mediante le quali è possibile accedere ai servizi di certificazione e di consultazione del profilo utente. In particolare, si vede come le varie CA, AA e PA presentano sia funzionalità comuni che specifiche di ognuna di esse.

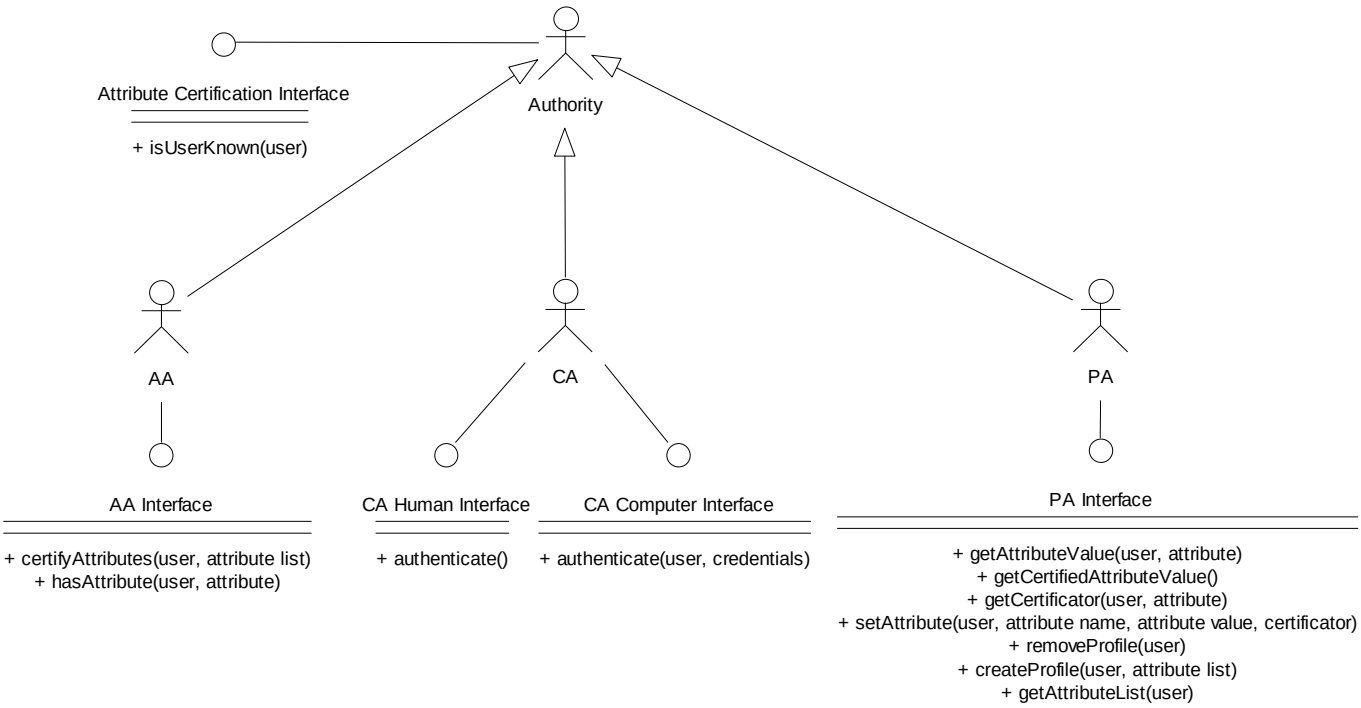

Figura 3: Interfacce per l'accesso alle authority

Tutti i tipi di authority espongono la funzionalità per conoscere se un dato utente è noto, ovvero il cui profilo è gestito da tale authority (funzione *isUserKnown*).

Ogni AA offre le seguenti funzionalità, relative alle certificazioni di attributo:

- *certifyAttributes* – usata per ottenere un'asserzione di attributo in formato SAML che sancisce la validità degli attributi specificati
- *hasAttribute* – usata per verificare che un dato attributo di un dato utente sia noto all'authority

Ogni CA può essere contattata o direttamente da un utente, ad esempio tramite interfaccia web, oppure in modo automatico da parte di applicazioni informatiche. Contestualmente si possono definire le due interfacce relative a tali modalità. Le funzioni sono in entrambi i casi quelle di autenticazione (*authenticate*): mentre nel caso dell'interazione con un utente via web l'operazione richiede come passo intermedio che l'utente specifichi le proprie credenziali, prima di restituire la corrispondente asserzione

di autenticazione, nel caso di interazione applicativa tali credenziali e l'identificativo dell'utente da autenticare devono essere forniti nella stessa chiamata di funzione, non potendo realizzare l'interazione precedente.

Infine, ogni PA offre le funzionalità relative alla gestione dei profili di cui è responsabile, ovvero l'inserimento di nuovi profili, la rimozione di profili esistenti, e la manipolazione degli attributi associati ad un profilo:

- *getAttributeList* – usata per ottenere l'elenco degli attributi presenti nel profilo di un certo utente
- *getAttributeValue* – usata per ottenere il valore di un attributo del profilo utente
- *getCertifiedAttributeValue* – usata per ottenere il valore di un attributo dopo aver contattato la relativa authority in grado di certificarlo, accedendo al puntatore presente nel profilo utente
- *getCertificator* – usata per ottenere il puntatore (indirizzo, entry-point) all'authority competente per la certificazione di un dato attributo di un dato utente
- *setAttribute* – usata per impostare il valore di un attributo del profilo di un certo utente o per crearlo ex-novo se non è presente. È necessario specificare anche il puntatore (o entry-point) dell'authority che può certificare tale attributo.
- *createProfile* – usata per inizializzare un nuovo profilo utente da zero, utilizzando la lista di attributi fornita
- *removeProfile* – usata per rimuovere il profilo di un utente specificato

Si osserva il fatto che ciascuna authority potrebbe, nel caso generale, restringere l'accesso alle proprie funzionalità, ad un numero ridotto di soggetti. Ad esempio, le varie authority potrebbero consentire l'accesso unicamente ad altre authority nel circle of trust (CoT) con un garante (o super-authority) esterno, oppure consentire l'accesso anche ad altre entità come i SP, previa autenticazione, per esempio mediante certificati digitali firmati da un garante.

3.6. Considerazioni sulle interfacce offerte da un Service Provider

Per quanto riguarda le interfacce esposte da un generico SP, esse saranno molto semplici, al limite costituite da un unico metodo "service". Tuttavia è necessario operare la distinzione tra interfaccia esposta per utenti e interfaccia a disposizione per sistemi automatici, per le ragioni indicate nella sezione 2, relativamente all'articolazione di una generica interazione per l'accesso ad un servizio, nelle due fasi di fruizione del front-end e di aggregazione dei risultati mediante interazione tra front-end e back-end. L'interfaccia per utenti umani, infatti, si riferisce al caso in cui il SP rappresenta il front-end di un servizio complesso ed è contattato dall'utente ad esempio tramite un browser web (User Agent). La seconda interfaccia invece è utilizzata nel secondo livello di interazione, quando il front-end deve

contattare uno o più sistemi di back-end, per richiedere parti del servizio complessivo ed ottenere le relative risposte. In questo secondo caso, può ad esempio avvenire mediante i concetti di *porta di dominio*, ovvero di *porta delegata* e *porta applicativa*, ovvero mediante scambio di messaggi SOAP [2] opportunamente strutturati (buste di e-government [3]), secondo il paradigma RPC (remote procedure call).

4. MODELLI DI COOPERAZIONE

In questa sezione vengono proposti alcuni modelli di interazione tra le entità illustrate in precedenza in cui esse assumono di volta in volta ruoli leggermente diversi con vari livelli di complessità. Si precisa che tutti i seguenti modelli affrontano esplicitamente il caso dell'interazione tra utente e front-end del servizio.

4.1. Modello 1

Nel modello 1 è previsto che ciascun dominio sia dotato di una o più CA e AA. In questo modo ogni dominio è anche certificatore relativamente ad attributi di profili utente di propria competenza. Se un dominio è poi anche erogatore di un servizio, questo comporta il fatto che la verifica dell'identificazione e/o autorizzazione passi anzitutto per le authority del dominio stesso, le quali contattano le rispettive controparti in altri domini. Inoltre, in questo modello le PA svolgono un ruolo attivo di intermediazione, oltre che di gestione del profilo. In questo modello ciascuna CA mantiene un registro nel quale sono elencati i puntatori a tutte le CA degli altri domini. Ciò vale anche per le PA, che mantengono un analogo registro elencante tutte le PA degli altri domini. In questo modo si realizza un circle of trust a due livelli ed è consentita la comunicazione diretta tra CA e PA di un dominio con le rispettive controparti in altri domini.

La Figura 4 mostra un esempio di registry delle CA di tre domini, in ognuno dei quali sono riportate le informazioni sugli entry point delle CA degli altri. L'analogo avviene, come detto, per la PA (nei modelli 1 e 2).

CA registry Dominio A

Dominio A	CA,Dominio A
Dominio B	CA, Dominio B
Dominio C	CA, Dominio C
...	...

CA registry Dominio B

Dominio B	CA,Dominio B
Dominio A	CA, Dominio A
Dominio C	CA, Dominio C
...	...

CA registry Dominio C

Dominio C	CA,Dominio C
Dominio A	CA, Dominio A
Dominio B	CA, Dominio B
...	...

Figura 4: Registry delle CA

In particolare, nel dominio di profilazione sono presenti una o più CA che possano autenticare l'utente richiedente, e la PA che ne gestisce il profilo. Nel dominio erogatore, invece, oltre alla CA e PA locali (rispettivamente CA_DE e PA_DE), sono presenti anche il fornitore del servizio (SP_DE), l'access manager (AM_DE) ed il gestore delle politiche di autorizzazione (GPA_DE). Il fornitore del servizio ha conoscenza di tutti gli altri elementi del suo dominio ed è quindi in grado di contattarli. Tra questi due domini, DE e D_PROF, si può vedere come la CA sia in grado di comunicare con la propria controparte nell'altro dominio, grazie alle relazioni di federazione presenti. Inoltre, ogni PA di un dominio costituisce l'entry point per le operazioni di verifica degli attributi di un utente. Questo è alla

base della comunicazione esistente tra il gestore delle politiche di autorizzazione del dominio erogatore e la PA del dominio fruitore.

In Figura 5 è illustrato il modello 1, indicando per ciascun dominio le relazioni tra le entità elementari in esso contenute e quelle che lo legano ad entità di altri domini. In figura, ciò che è indicato con D_CERT vuole rappresentare un generico dominio certificatore esterno sia a D_PROF che a DE. In esso è presente anzitutto una PA locale (PA_{D_CERT}) responsabile di contattare le varie AA ($AA_{i,DC}$) di propria competenza, secondo quanto scritto nella parte di profilo utente in esse memorizzato. La comunicazione con un D_CERT avviene ad opera della PA del dominio fruitore.

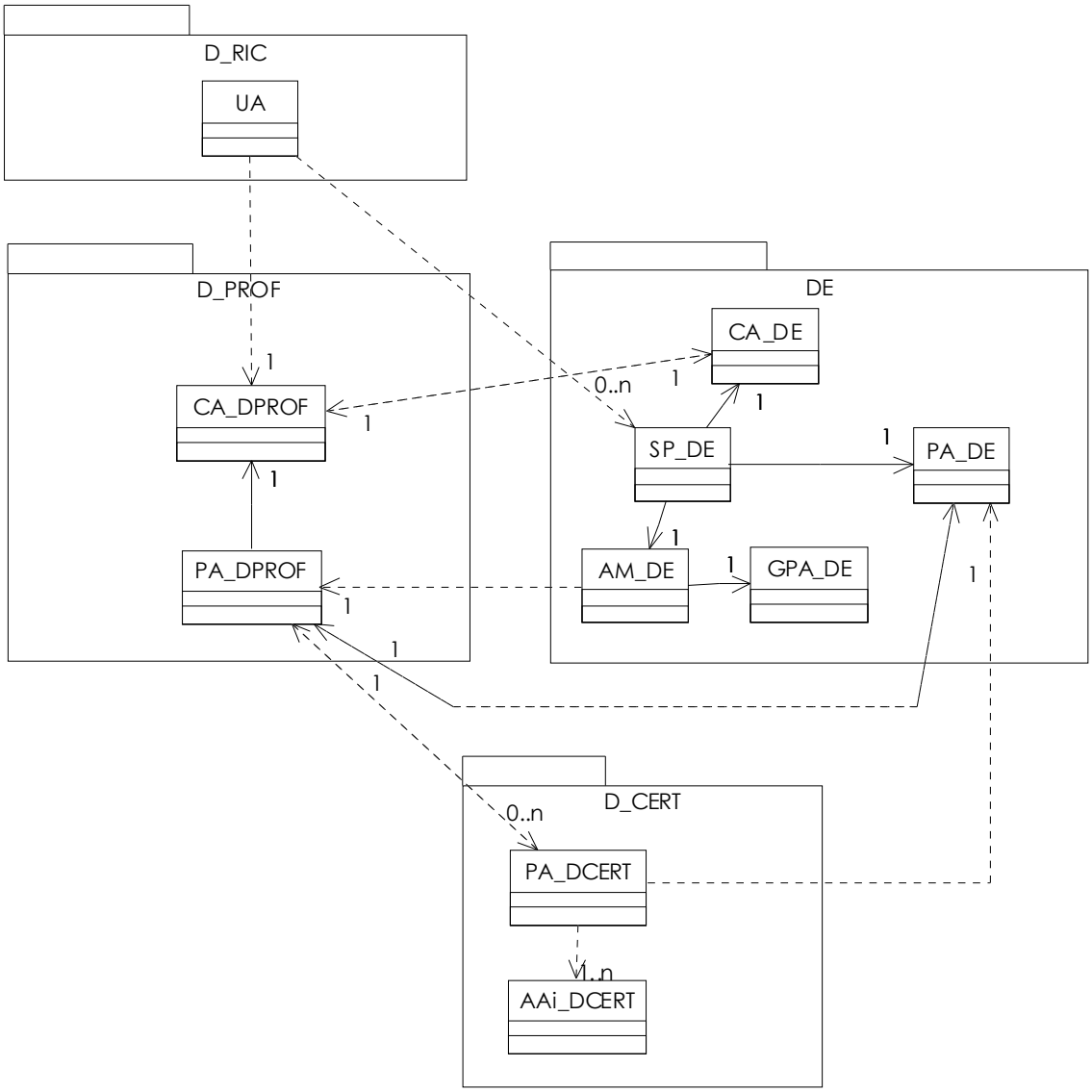

Figura 5: Relazioni intra- e inter-dominio nel modello 1

4.1.1. Interazioni nel modello 1

Nel seguito viene dettagliato uno scenario possibile nel modello 1, che copre tutte le fasi dalla richiesta di servizio, sottomessa da un utente, fino all'avvenuta autenticazione e autorizzazione inter-dominio, con la fruizione del servizio richiesto.

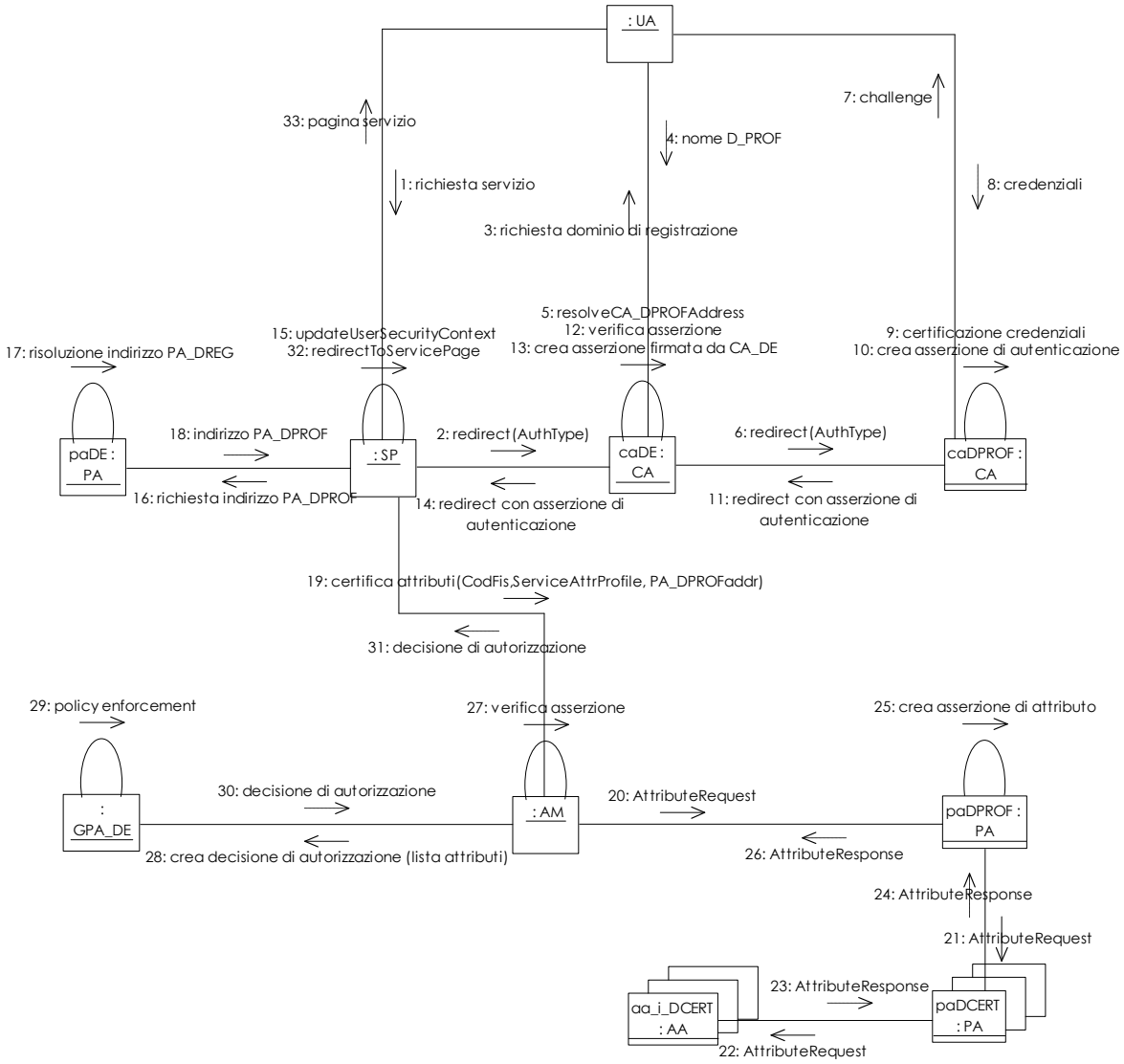

Figura 6: Scenario d'interazione nel modello 1

Nello scenario descritto in Figura 6, viene inizialmente intrapresa la fase di autenticazione dell'utente:

1. L'utente contatta un fornitore del servizio (SP) del dominio erogatore (DE) per accedere ad una delle funzionalità offerte.

2. SP riconosce che il servizio richiesto è subordinato all'autenticazione dell'utente e alla verifica del suo profilo. Pertanto per prima cosa ridirige UA sulla CA_{DE} per effettuare l'operazione di autenticazione. Durante tale redirezione viene anche indicato alla CA_{DE} che tipo di autenticazione (forte o debole) è richiesta.
3. CA_{DE} richiede all'utente qual è il proprio dominio originario, ovvero il *dominio di profilazione* in cui l'utente è stato iscritto.
4. L'utente risponde scegliendo da una lista dei domini esistenti, noti alla CA_{DE}
5. CA_{DE} risolve l'indirizzo della CA_{D_PROF}, che è competente a certificare le credenziali di autenticazione dell'utente.
6. CA_{DE} ridirige l'utente sulla CA_{D_PROF}, inoltrando la modalità di autenticazione richiesta
7. CA_{DPROF} richiede le credenziali all'utente, compatibilmente con la modalità di autenticazione richiesta.
8. L'utente fornisce le credenziali
9. CA_{DPROF} verifica le credenziali fornite
10. CA_{DPROF} produce un'asserzione di autenticazione per l'utente
11. CA_{DPROF} ridirige l'utente sulla CA_{DE} con l'asserzione di autenticazione prodotta
12. CA_{DE} verifica la validità dell'asserzione ricevuta
13. A questo punto CA_{DPROF} è in grado di autenticare l'utente, anche se questo appartiene ad un dominio esterno. Per questo produce a sua volta una nuova asserzione di autenticazione
14. CA_{DPROF} ridirige l'utente su SP, con l'asserzione di autenticazione prodotta
15. SP aggiorna le proprie strutture dati interne relative al contesto di sicurezza, annotando il fatto che l'utente richiedente è stato autenticato.

Ora è possibile procedere con le fasi di verifica delle autorizzazioni. Per questo è necessario accedere al profilo dell'utente:

16. SP chiede alla PA_{DE} l'indirizzo della PA del dominio di profilazione dell'utente
17. PA_{DE} consulta le proprie tabelle interne e risale all'indirizzo richiesto
18. PA_{DE} risponde con l'indirizzo di PA_{DPROF}
19. SP contatta l'Access Manager del proprio dominio (AM_{DE}) delegandogli il compito di recuperare le certificazioni degli attributi richiesti per la verifica dell'accesso al servizio richiesto. Viene inoltrato anche l'indirizzo della PA_{DPROF} che dovrà essere contattata.
20. AM_{DE} sa che l'utente proviene dal dominio D_PROF e quindi contatta la PA_{DPROF} sottoponendole tante AttributeRequest SAML quanti sono gli attributi da verificare
21. Per ciascuna AttributeRequest SAML ricevuta, la PA_{DPROF} effettua una nuova AttributeRequest SAML verso le PA competenti, dei domini certificanti (PA_{D_CERT}). Si noti che concettualmente la PA_{DC} potrebbero coincidere con la stessa PA_{DPROF} nel caso in cui il D_PROF fosse competente per la certificazione di alcuni degli attributi richiesti.
22. PA_{DC} contatta la $AA_{i,DC}$ competente per l'attributo i-esimo consultando il profilo dell'utente di cui è responsabile. Allo scopo inoltra una nuova AttributeRequest.

23. $AA_{i,DC}$ risponde con la certificazione dell'attributo richiesto mediante una AttributeResponse SAML.
24. PA_{DC} riceve la AttributeResponse SAML e produce a sua volta una AttributeResponse che manda alla PA_{DPROF}.
25. PA_{DPROF} riceve tutte le AttributeResponse per i vari attributi richiesti e le assembla, per creare poi una AttributeAssertion che le contiene tutte.
26. PA_{DPROF} invia l'asserzione generata, indietro a $AM_{DE.}$
27. AM_{DE} verifica l'asserzione ricevuta.
28. AM_{DE} incarica GPA_{DE} di verificare che gli attributi raccolti siano conformi al profilo del servizio, onde poter autorizzare l'utente
29. GPA_{DE} decide di autorizzare l'utente sulla base della verifica di tutti gli attributi ricevuti.
30. GPA_{DE} comunica ad AM_{DE} il risultato del processo di autenticazione e autorizzazione
31. AM_{DE} informa di questa decisione SP_{DE}
32. In caso di autorizzazione concessa, SP ridirige l'utente alla pagina del servizio e
33. SP restituisce la pagina del servizio all'utente.

4.2. Modello 2

In questo secondo modello si preserva la federazione delle CA, ciascuna delle quali mantiene un registro nel quale sono elencati i puntatori a tutte le CA degli altri domini. Tale registro non è invece più presente per le PA. In questo modo le varie AA devono essere contattate direttamente dall'esterno, ad opera di qualunque entità richiedente e senza alcun livello di intermediazione. L'unica PA concettualmente necessaria risulta essere quella del dominio di profilazione, che "conosce" l'utente, e responsabile quindi della gestione del suo profilo. Questa responsabilità però si limita alla normale gestione del profilo, senza alcuna interazione proattiva con altre entità del dominio o di altri domini. Per questo motivo, l'accesso alle varie AA viene consentito, in modo diretto, al gestore delle politiche di autorizzazione del dominio erogatore, che ha il compito di verificare che il profilo utente sia adeguato al servizio richiesto. In Figura 7 è illustrato un diagramma delle classi che mostra le relazioni interne ai domini e quelle inter-dominio. La relazione indicata tra PA_{DPROF} e le varie AA_{i,D_CERT} rappresenta il fatto che nel profilo utente mantenuto dalla PA sono memorizzati dei puntatori alle varie AA.

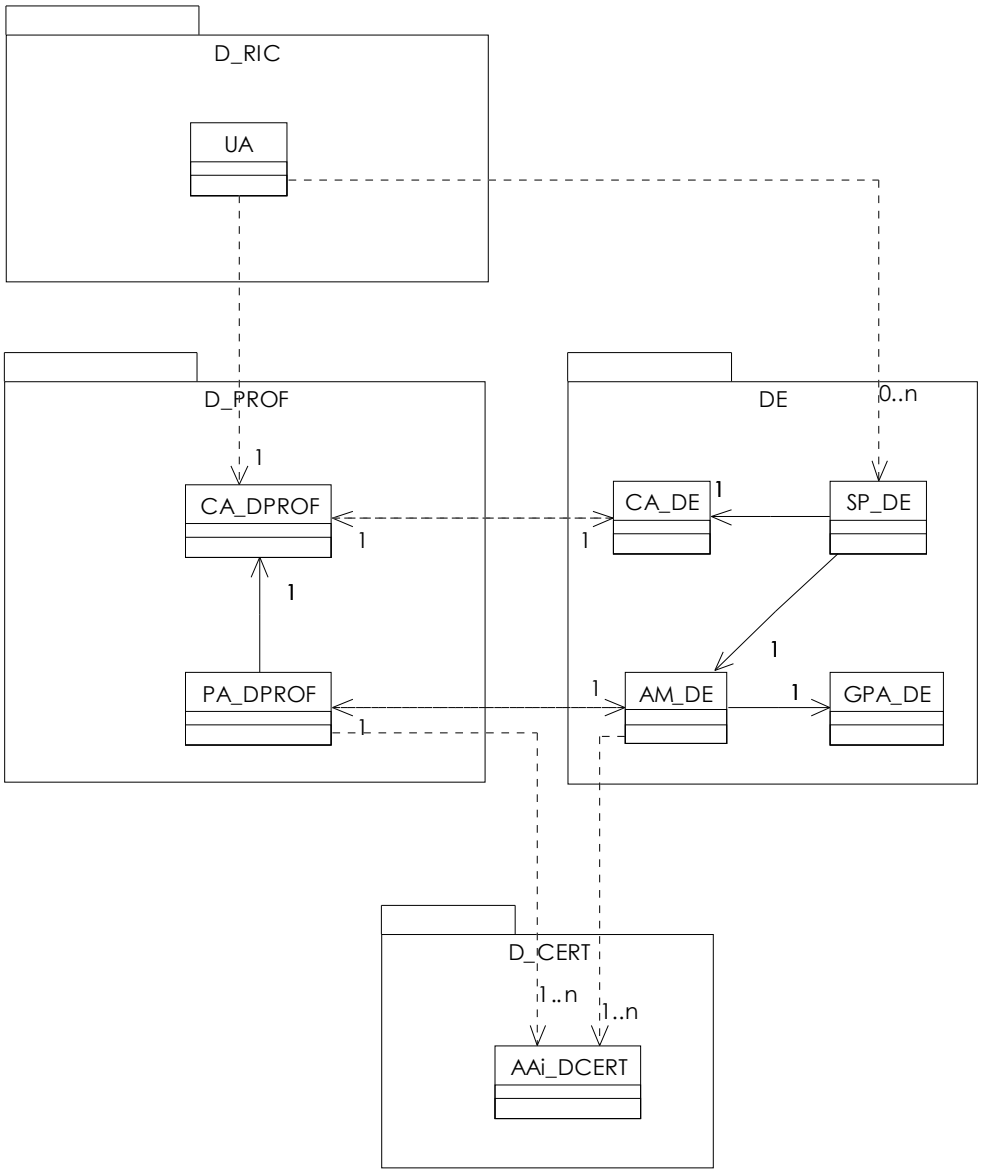

Figura 7: Relazioni intra- e inter-dominio nel modello 2

4.2.1. Interazioni nel modello 2

Analogamente a quanto fatto per il modello 1, viene di seguito presentato uno scenario completo di interazione tra le entità presenti nei vari domini del modello 2. In questo scenario i passi da 1 a 15 corrispondenti alla fase di autenticazione dell'utente coincidono con quelli del modello 1, rappresentato in Figura 6. Nei restanti si nota la variazione in cui è l'AM_{DE} che, acquisito dalla PA_{DPROF} l'elenco delle AA da contattare, procede ad interazioni dirette con esse, allo scopo di ottenere la certificazione degli attributi necessari.

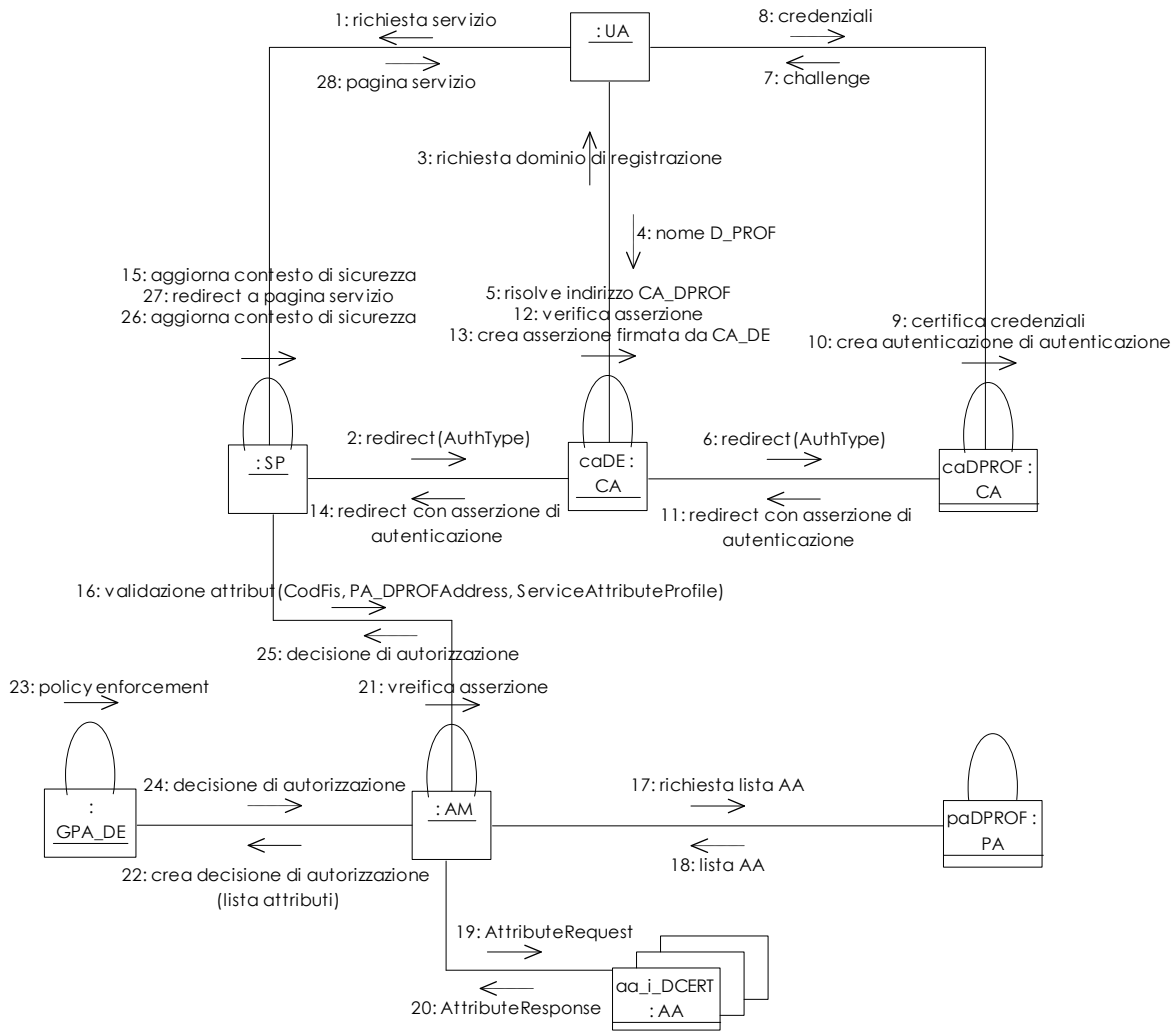

Figura 8: Scenario d'interazione nel modello 2

4.3. Modello 3

In questo modello, si ripropone la federazione tra PA, in cui ciascuna mantiene un registro che consente di indirizzare tutte le altre PA degli altri domini nella federazione. In questo modo l'unico entry-point per l'accesso ad un dominio (fatta eccezione per i SP) è fornito dalla PA, che agisce come mediatore nell'accesso sia alle AA che alle CA. Nessuna comunicazione diretta è consentita invece tra le CA di domini diversi, che non detengono più alcun registro utile a conoscere la presenza delle altre.

Per questo motivo, in questo modello le CA dei domini D_PROF e DE non si parlano direttamente, anzi, la CA_{DE} scompare, dato che non svolge più alcun ruolo, essendo sostituita dalla PA del dominio erogatore. In Figura 9, viene presentato il diagramma delle classi che illustra questa situazione, con le varie interazioni tra domini e intra-dominio.

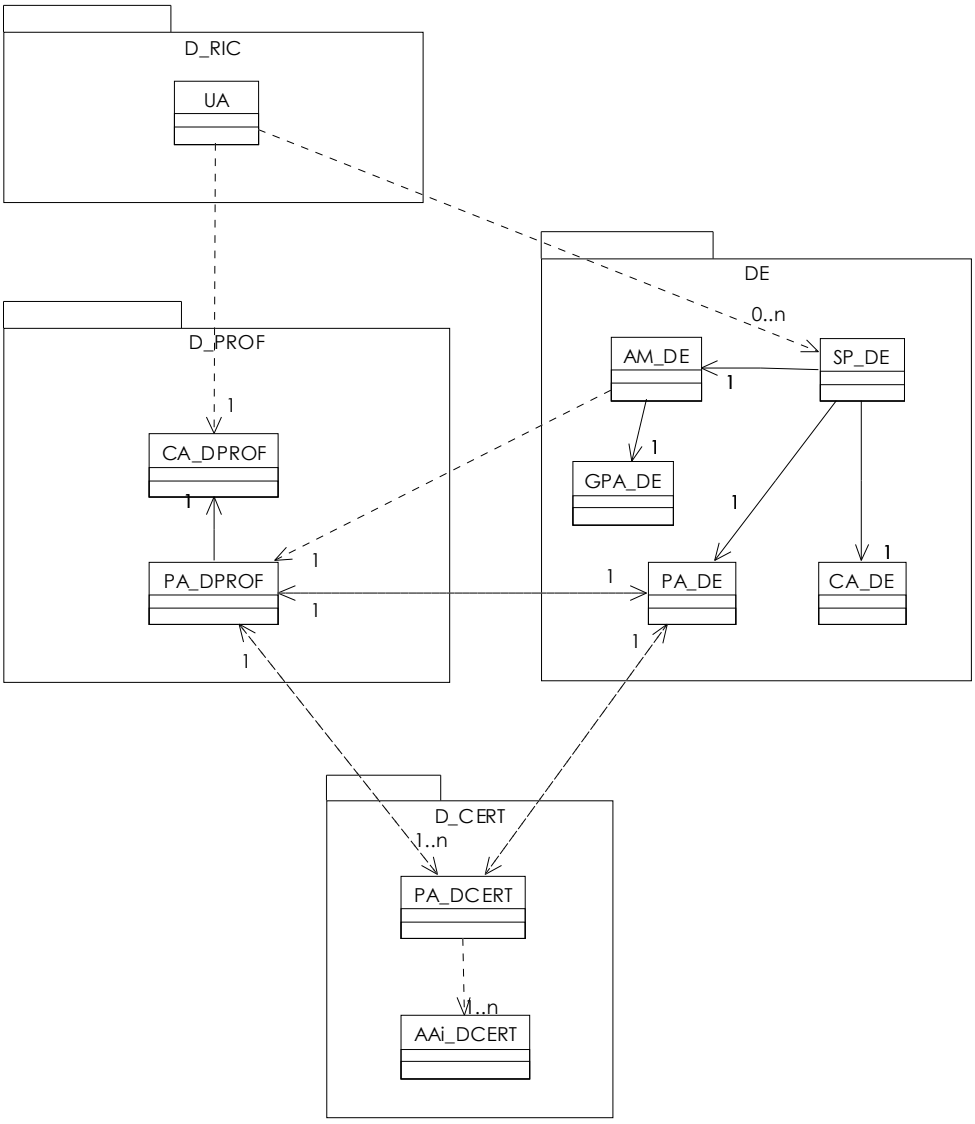

Figura 9: Relazioni intra- e inter-dominio nel modello 3

4.3.1. Interazioni nel modello 3

Lo scenario d'interazione corrispondente al modello 3 è quello descritto in Figura 10, che si differenzia da quello del modello 1 per la parte di autenticazione (messaggi da 1 a 19). In esso, il SP non contatta più la CA_{DE}, bensì fa immediatamente ricorso alla PA_{DE}, la quale richiede le informazioni sul dominio di provenienza all'utente, per poi fare a sua volta ricorso alla PA_{DPROF}, il cui indirizzo viene risolto consultando i registry di federazione. La PA_{DPROF}, a sua volta, chiederà alla CA_{DPROF} di autenticare l'utente, con la consueta sequenza di messaggi, fino ad arrivare alla produzione dell'asserzione di autenticazione e alla catena di redirezionamenti che portano l'utente indietro sino al SP, con un contesto di autenticazione valido.

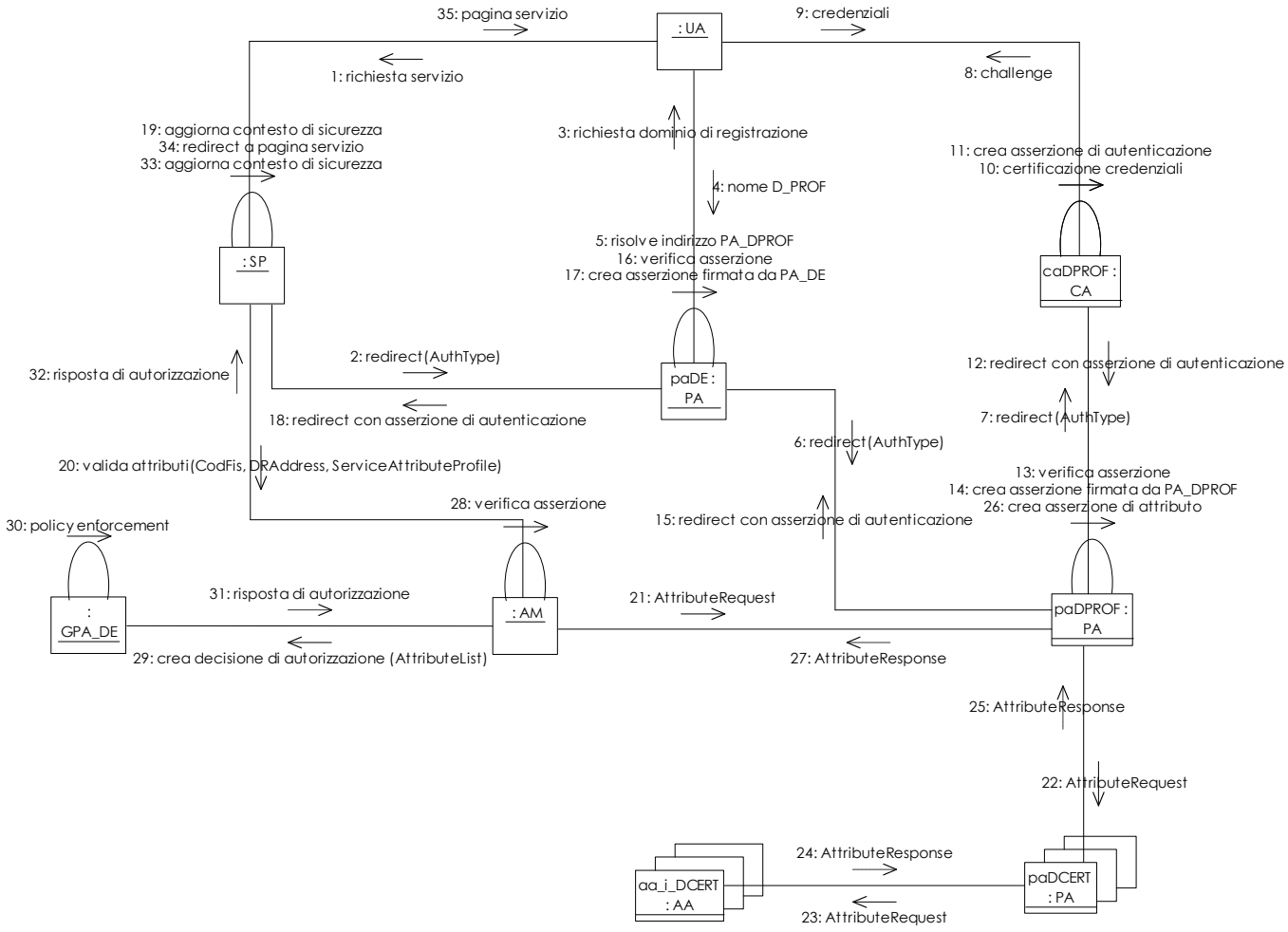

Figura 10: Scenario d'interazione nel modello 3

4.4. Modello 4

Nel modello 4, né le CA né le PA dispongono di registri per contattare direttamente le controparti in altri domini, facendo così cadere la federazione tra tali entità. Rispetto al modello precedente, le PA tornano a rivestire un più semplice ruolo di gestione del profilo, senza mascherare alcuna authority (CA o AA) competente, relativamente agli attributi memorizzati. Ogni authority deve perciò essere contattabile direttamente dall'esterno. Inoltre la PA viene privata anche del ruolo, possibile nei modelli precedenti, di entità incaricata dal SP di un dominio erogatore, di attuare parte o l'intero processo di autenticazione e autorizzazione di un utente richiedente, ruolo che viene lasciato all'AM_{DE}. Esso infatti interagisce sia con la PA_{DPROF} per ottenere l'elenco della AA da contattare, sia con le AA stesse. Come si vede anche dalla successiva Figura 11 che descrive questo modello, scompare la necessità di avere altre authority fatta eccezione per quelle responsabili di autenticare l'utente e per la PA del dominio di

profilazione, che ne mantiene il profilo. Si nota come questo modello semplifichi ulteriormente le interazioni presenti e il numero stesso delle entità inter-comunicanti, consentendo relazioni dirette tra entità di domini diversi ed eliminando qualsiasi forma di intermediazione o entry-point in ciascun dominio. Si noti che, perché AM_{DE} sia in grado di contattare la corretta PA, una volta noto il dominio di profilazione dell'utente, è necessario che esso consulti un registro nel quale siano listate tutte le PA di tutti i potenziali domini di profilazione. Dato che non è possibile conoscere in anticipo se un dominio è di profilazione per un dato utente, almeno stando sul dominio erogatore un certo servizio, ogni AM di ogni dominio in cui vengono erogati servizi, dovrà disporre di un registro delle PA e dovrà inoltre tenerlo aggiornato.

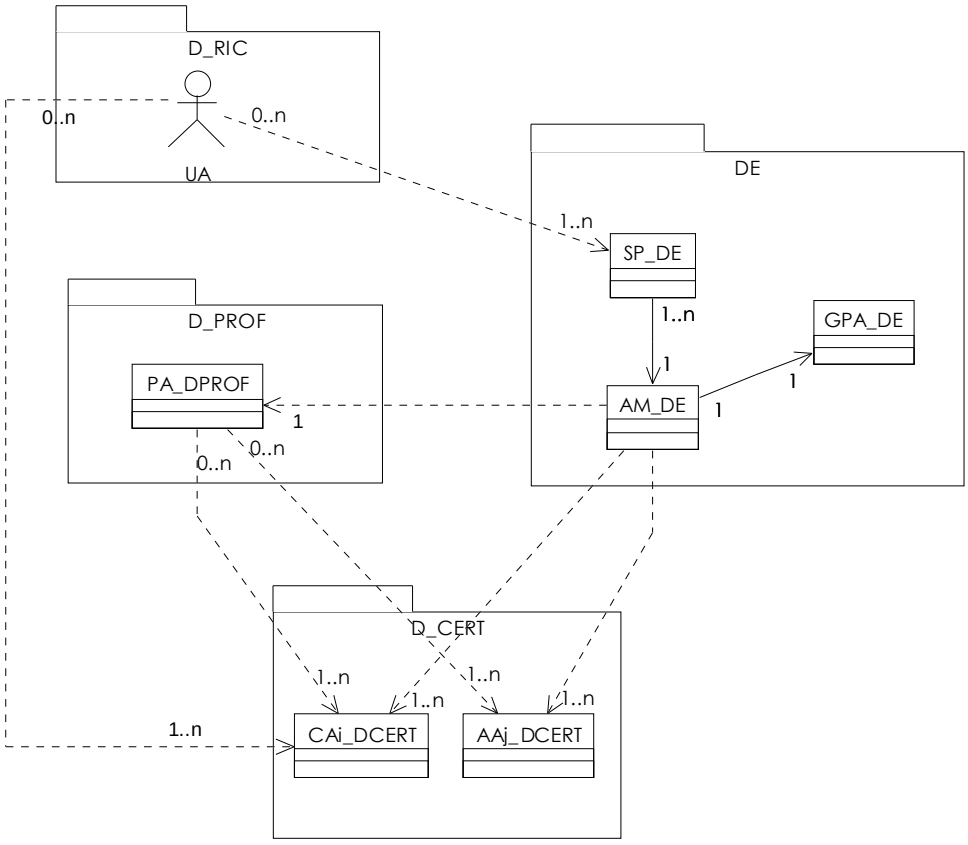

Figura 11: relazioni intra- e inter-dominio nel modello 4

4.4.1. *Interazioni nel modello 4*

Lo scenario d'interazione per il modello 4 è rappresentato nella seguente Figura 12. Si può vedere il ruolo centrale e predominante rivestito dal AM_{DE}, incaricato ora di orchestrare sia la fase di autenticazione che quella di autorizzazione. Inoltre, la CA in grado di verificare le credenziali fornite dall'utente viene estratta concettualmente dal dominio di profilazione e portata in quello di certificazione. Una CA, infatti, potrebbe afferire in generale a più domini di profilazione, in

corrispondenza di tutti gli utenti che è in grado di identificare. Per questo motivo sarebbe in teoria parte di qualunque dominio di profilazione, ma concettualmente appare meglio vederla come invece esterna a tutti e parte, come detto, del dominio appositamente creato per contenere tutte le entità certificatrici di qualche attributo presente nel profilo utente. Le credenziali, infatti, possono essere viste come degli attributi speciali per i quali è necessario contattare una particolare CA.

Date le differenze rispetto ai modelli precedenti, si fornisce di seguito descrizione dettagliata dei vari passi dello scenario.

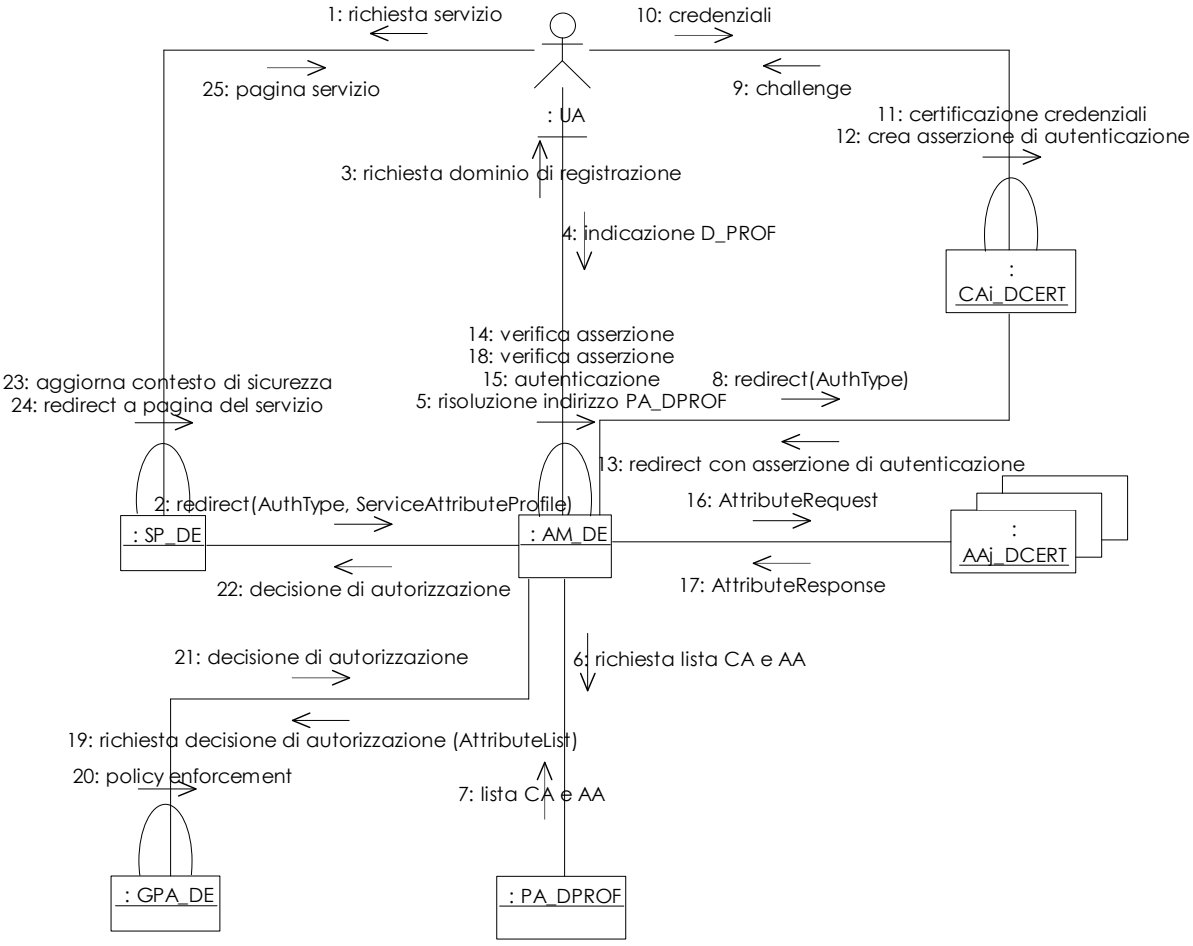

Figura 12: scenario di interazione nel modello 4

1. L'utente contatta un fornitore del servizio (SP) del dominio erogatore (DE) per accedere ad una delle funzionalità offerte.
2. Il SP non ha un contesto di autorizzazione per l'utente richiedente, e quindi dirotta la richiesta sull'Access Manager dello stesso dominio erogatore (AM_{DE}), passandogli oltre al tipo di autenticazione richiesta (username/password, PIN, ecc.) anche l'intero "profilo" del servizio che specifica, tra le altre cose, gli attributi da verificare.
3. AM_{DE} richiede all'utente qual è il suo dominio di profilazione.
4. L'utente risponde indicandone il nome (D_PROF).

5. AM_{DE} risolve l'indirizzo della PA del dominio di profilazione (PA_{DPROF}) utilizzando un registro mantenuto localmente.
6. AM_{DE} contatta PA_{DPROF} e richiede gli indirizzi di CA_{DCERT} e di tutte le AA ($AA_{i,DC}$) necessarie per consentire il policy enforcement sul servizio richiesto
7. PA_{DPROF} risponde con le informazioni richieste
8. AM_{DE} dirotta l'utente su CA_{DCERT} propagando l'informazione sulla modalità di autenticazione
9. CA_{DCERT} richiede all'utente le credenziali
10. L'utente fornisce le credenziali richieste
11. CA_{DCERT} verifica le credenziali fornite
12. CA_{DCERT} produce un'asserzione di autenticazione per l'utente
13. CA_{DCERT} ridirige l'utente sul AM_{DE} con l'asserzione di autenticazione prodotta
14. AM_{DE} verifica l'asserzione ricevuta
15. AM_{DE} autentica l'utente, ovvero stabilisce che deve procedere alla successiva fase di autorizzazione, utilizzando il profilo del servizio comunicato dal SP all'inizio dell'interazione
16. AM_{DE} effettua un certo numero di richieste di attributo alle varie AA comunicate da PA_{DPROF} al passo 7.
17. Le varie $AA_{i,DC}$ rispondono con gli attributi richiesti, inseriti in asserzioni di attributo SAML.
18. AM_{DE} verifica tutte le asserzioni ricevute dalle varie AA
19. AM_{DE} incarica GPA_{DE} di verificare che gli attributi raccolti siano conformi ai requisiti del servizio, onde poter autorizzare l'utente
20. GPA_{DE} decide di autorizzare l'utente sulla base della verifica di tutti gli attributi ricevuti.
21. GPA_{DE} comunica ad AM_{DE} il risultato del processo di autorizzazione
22. AM_{DE} informa di questa decisione SP_{DE}
23. SP_{DE} aggiorna le proprie strutture dati interne relative al contesto di sicurezza, annotando il fatto che l'utente richiedente è stato autenticato e autorizzato.
24. SP_{DE} ridirige l'utente alla pagina del servizio.
25. SP_{DE} restituisce la pagina del servizio all'utente.

4.5. Valutazione dei modelli proposti

Dopo aver presentato, nelle sezioni precedenti, quattro modelli di autenticazione e autorizzazione per il sistema federato interregionale, si intende riassumerne i tratti principali e fornire un'analisi dei principali vantaggi e svantaggi che ognuno di essi presenta.

Nel modello 1 si fa ricorso al maggior numero di entità, per i vari domini, con la doppia federazione tra CA e PA. Questo fa sì che il numero di interazioni richiesto per completare il processo di autenticazione e autorizzazione sia più lungo e complesso degli altri casi. Il dover attraversare un numero superiore di entità, da una parte sgrava attori come l'AM e le varie PA di una parte dei compiti che vengono ad assumere negli altri modelli, ma allo stesso tempo impone alle CA di mantenere un registro aggiornato, per conoscersi a vicenda, e questo non è in generale fattibile, per l'autonomia che tali soggetti dovrebbero mantenere. Una CA, infatti, in generale esiste indipendentemente dalla presenza o meno di un sistema come quello oggetto di questo documento. È bene, pertanto, ridurre il

più possibile il numero di requisiti imposti alle CA. Una federazione tra CA esiste anche nel modello 2, dove invece cade quella tra le PA. Questo modello appare quindi più snello del precedente, pur mantenendo gli stessi problemi in termini di requisiti imposti alle CA. In questo modello l'AM comincia ad assumere un ruolo di primo piano, mentre le PA scompaiono dai vari domini, fatta eccezione per il dominio di profilazione. Questo modello comincia cioè ad introdurre il fatto che l'unica PA realmente indispensabile è quella deputata alla gestione del profilo dell'utente. Tutte le altre svolgono, in altri modelli, un ruolo di intermediazione e di mascheramento rispetto ad AA presenti in domini esterni. Il modello 3 presenta un rimescolamento degli elementi considerati nei due precedenti modelli: non esiste più la federazione delle CA ma esiste quella delle PA che tornano ad avere un ruolo di primo piano. Per le considerazioni fatte, tale modello non fa che aumentare la complessità del processo di autenticazione, che dev'essere mediato dalle PA dei domini erogatore e di profilazione. Il modello 4 porta il numero delle entità in gioco al minimo indispensabile. Questo significa sia l'assenza di federazioni tra CA e PA, che l'eliminazione di tutte le PA, oltre a quella del D_PROF e di tutte le CA, tranne di quelle in grado di autenticare l'utente e quindi presenti in D_CERT. In tutti i modelli appare utile l'evidenziazione del dominio fruitore, distinto da quello di profilazione, per tenere presente che le interazioni tra il browser (UA) dell'utente debbano avvenire tra domini differenti e quindi su scala più vasta, con tutto ciò che questo comporta in termini di latenze, traffico e malfunzionamenti nella rete di comunicazione.

Nella tabella seguente sono riassunte le principali caratteristiche presentate dai modelli proposti.

Modello	# entità elementari	CoT tra CA	CoT tra PA
1	10	Sì	Sì
2	8	Sì	No
3	10	No	Sì
4	7	No	No

Tabella 1: confronto tra i modelli presentati

Complessivamente si ritiene che il modello 4 sia quello che presenti le migliori caratteristiche relativamente all'impatto su entità preesistenti (CA), al carico imposto alle varie entità in gioco e alla complessità realizzata in una interazione completa. Tale modello sarà dunque assunto come riferimento nel seguito del documento.

4.6. Considerazioni sul caching delle asserzioni

Nonostante la riduzione nel numero delle PA e l'eliminazione della federazione tra le CA porti dei benefici in termini di un modello più leggero e che presenta un impatto minore sui requisiti imposti alle authority, occorre osservare come la presenza, anche nel dominio erogatore, di una PA o comunque di un elemento facente funzioni di proxy verso AA terze, permetta di effettuare operazioni di caching delle asserzioni di attributo ricevute dalle diverse authority, in modo da poterle riutilizzare in tempi successivi, riducendo il carico generato sulle authority stesse. In realtà, per questo ruolo è possibile

utilizzare sia la PA_{DE} (ove essa esiste), che l'AM_{DE} oppure la PA_{DPROF}. Il riuso delle asserzioni può essere particolarmente utile, per la fase successiva, di interazione tra i servizi di front-end e i vari servizi di back-end retrostanti, i quali, al pari del precedente, richiedono che l'accesso ai propri servizi sia preventivamente autenticato ed autorizzato. Quanto alla scelta del dove memorizzare la cache di asserzioni ricevute, si pongono alcune alternative possibili. Mantenere una cache su CA_{DE}, PA_{DE} o AM_{DE} consentirebbe un più efficiente riuso, qualora nuove richieste di servizi erogati nello stesso DE provengano da parte di utenti diversi. Fare caching delle asserzioni su PA_{DPROF}, tuttavia, avrebbe il vantaggio di poter riutilizzare le asserzioni anche per richieste di servizi successivi, da parte del medesimo utente. Questa alternativa, tuttavia, implicherebbe automaticamente un ruolo attivo per la PA, in quanto essa non sarebbe più utilizzata soltanto per ottenere l'elenco delle authority in D_CERT da contattare (per esempio ad opera di AM_{DE}), ma sarebbe essa stessa a farsi carico di questa attività, per memorizzare poi le asserzioni ricevute in un'apposita cache. È naturalmente possibile combinare i due approcci e memorizzare una copia temporanea di tali asserzioni su tutte tali entità. È invece più difficile utilizzare il browser dell'utente (UA) per tale operazione, non trattandosi di un componente in grado di essere programmato a questo scopo. L'unico modo per avvicinarsi a tale scopo sarebbe quello di utilizzare dei *cookie* ove memorizzare le varie asserzioni durante la sessione di lavoro. Tale strumento, tuttavia, ha la peculiarità di essere riutilizzabile soltanto all'interno dello stesso dominio che l'ha creato. Per questo motivo, per fare in modo che i cookie siano scambiabili tra domini diversi, occorrerebbe fare ricorso ad un dominio centrale, noto a tutti gli altri, creando così un single point-of-failure oltre ad introdurre un elemento di centralizzazione in un modello che dovrebbe essere il più possibile distribuito e federato. In Tabella 2 sono riassunte le alternative possibili, per i vari modelli presentati.

Modello	Cache asserzioni
1	PA_{DPROF}, CA_{DE}, PA_{DE}, AM_{DE}
2	PA_{DPROF}, CA_{DE}, AM_{DE}
3	PA_{DPROF} , CA_{DE}
4	AM_{DE}

Tabella 2: Entità su cui è possibile fare cache delle asserzioni

5. MODELLO DI RIFERIMENTO PER L'AUTENTICAZIONE E AUTORIZZAZIONE NEL SISTEMA FEDERATO INTERREGIONALE

In questo capitolo, a partire dalla scelta operata, relativamente al modello di riferimento, verranno dettagliati i casi d'uso del sistema, con i relativi scenari d'interazione ad un livello di dettaglio superiore rispetto al capitolo precedente.

5.1. Casi d'uso

Nel diagramma di Figura 13 è illustrato un diagramma di casi d'uso UML che mostra gli attori e le macro attività richieste nel sistema oggetto del presente documento.

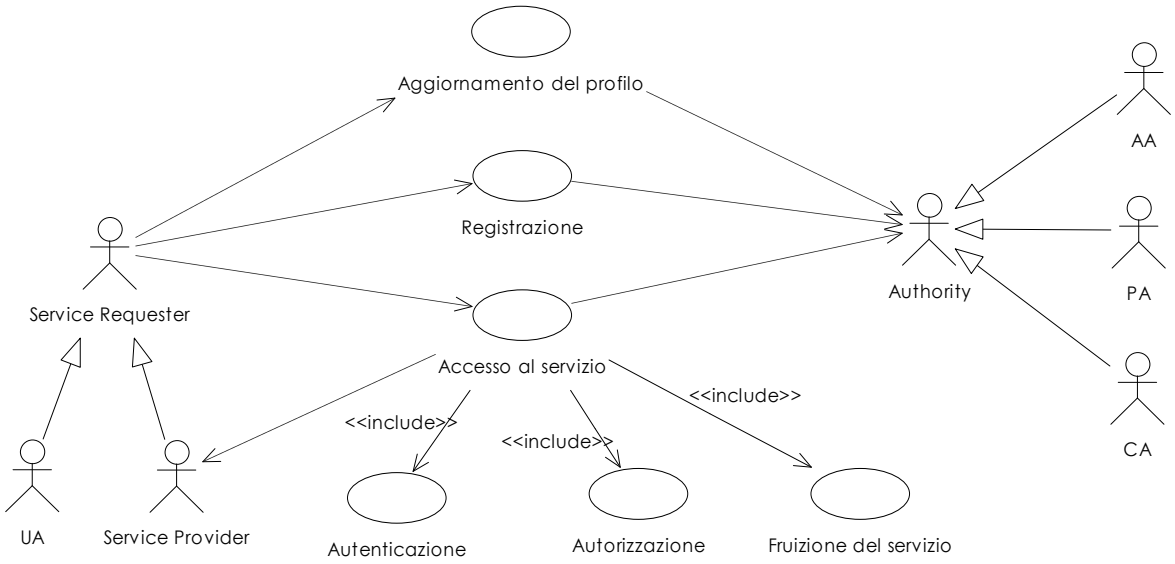

Figura 13: casi d'uso

Il caso d'uso principale è quello per l'accesso al servizio, che coinvolge tre attori: il Service Requester, una (o più) authority e un SP. Il richiedente contatta il fornitore che fa uso di un certo numero di authority certificatrici per convalidare l'accesso. Questo use case si dettaglia, come visto nei diagrammi precedenti, nelle tre sottofasi di autenticazione, autorizzazione e fruizione vera e propria del servizio. Si noti la particolarità per cui un SP può essere a sua volta un service requester. Un richiedente infatti, come detto all'inizio di questo documento, può essere sia un utente che opera mediante un browser web per contattare il front-end di un servizio, che il front-end dello stesso servizio, che deve contattare un certo numero di fornitori di servizi di back-end per completare la procedura di accesso.

Un secondo caso d'uso è quello che permette ad un nuovo utente di registrarsi presso una certa authority al fine della creazione di un nuovo profilo contenente almeno gli attributi base utili ai fini della procedura di autenticazione. Nel caso generale, tuttavia, il profilo verrà popolato anche con un certo numero di dati, ad esempio quelli anagrafici, ma potrà essere esteso anche in un secondo momento. Quest'ultima attività viene riassunta nel caso d'uso denominato "Aggiornamento del profilo" per cui un utente può accreditarsi con nuovi attributi (o qualifiche) presso una AA.

5.2. Scenario di riferimento

Nell'ambito del caso d'uso principale, ovvero quello di accesso al servizio, verrà ora ripreso e dettagliato ulteriormente lo scenario scelto come riferimento nel capitolo precedente.

In particolare è possibile notare come il componente, presente nel dominio erogatore, denominato Access Manager svolga la funzione di reperimento di asserzioni SAML da parte dei soggetti certificatori, eventualmente dirottando il browser dell'utente su di essi, quando la comunicazione non può essere mediata (es. autenticazione). Tale componente svolge quindi un ruolo centrale nel sistema di identity management. Inoltre, come preannunciato nella sezione 3.3, il SP è un'entità-wrapper, in grado di nascondere all'esterno i servizi applicativi. Esso riceve le richieste di accesso alle risorse e attiva le funzioni di autenticazione e autorizzazione, prima di inoltrare la richiesta al servizio, o risorsa, vero e proprio. Come tale, il SP colloquia da una parte con il richiedente (UA) e dall'altra con l'AM per il recupero delle asserzioni necessarie. Questo è descritto dal diagramma delle classi UML di Figura 14.

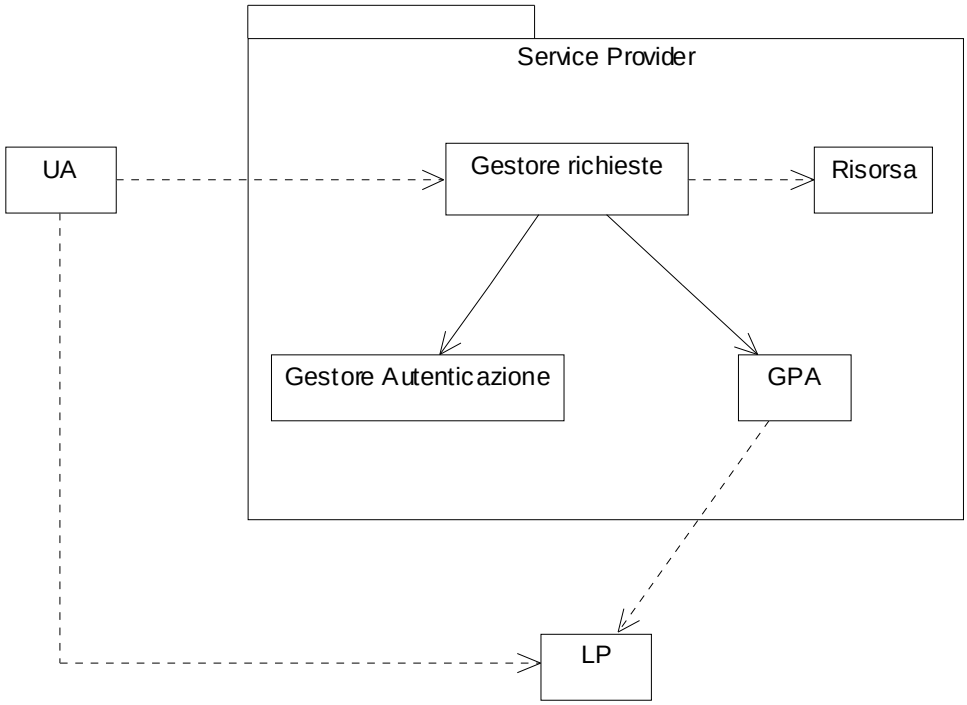

Figura 14: Struttura di un generico Service Provider

Nello scenario di riferimento adottato nel sistema INF-3 il componente AM viene chiamato "Local Proxy" (o LP), è logicamente parte del dominio erogatore e svolge funzioni di server unico per l'ottenimento dei vari tipi di asserzioni, utilizzando la notazione SAML. Esso agisce quindi da "proxy" o "façade" nei confronti del sistema di Identity Management di ICAR. Il vantaggio di questo approccio sta nel fatto che un ipotetico SP (visto come container di servizi) commerciale, SAML-ready, potrebbe usare con facilità l'infrastruttura ICAR. Riprendendo il precedente diagramma delle classi, è possibile vedere come il SP sia concettualmente composto di un Gestore delle Richieste, che resta in attesa di essere contattato dall'esterno con richieste di servizio. Successivamente, esso attiva in sequenza altri due sotto-componenti; il primo è detto "Gestore Autenticazione" e si occupa della verifica dello stato di autenticazione del richiedente, relativamente alla risorsa, o servizio, richiesta. Se necessario esso attiva la procedura di autenticazione. Il secondo è il già citato GPA, incaricato della fase di autorizzazione. Quest'ultimo interagisce con il LP per l'ottenimento delle asserzioni di attributo relative al ruolo del richiedente. Infine il Gestore delle Richieste contatta la risorsa vera e propria per attivare il servizio voluto.

Nel seguito non si farà più riferimento a dominio erogatore, di profilazione o certificatore, assumendo valido quanto già illustrato nel capitolo precedente, relativamente al modello 4. Non occorre specificare la collocazione di ciascuno di questi oggetti nel dominio fruitore o erogatore, in quanto questo modello lascia libero il richiedente di usufruire delle PA, CA e AA scelte indipendentemente dal dominio che erogherà il servizio. Occorre però postulare l'esistenza di un registro, visibile da tutte le comunità federate, che permetta l'individuazione delle URL a cui rispondano le diverse PA, CA e AA. Tale registro potrebbe essere realizzato federando tra loro più sotto-registri esistenti a livello di comunità.

In questo modo nel profilo, mantenuto dalla PA, è possibile conservare, insieme alle coppie attributo-valore, un semplice nome simbolico caratterizzante l'ente certificatore, senza specificarne l'indirizzo vero e proprio, il quale è notoriamente soggetto a variazioni.

Nella successiva Figura 15 è dettagliato lo scenario d'interazione valido per il modello di riferimento. Si noti che in tale scenario il SP non viene ulteriormente dettagliato nelle entità precedentemente illustrate; come conseguenza, il suo funzionamento interno non viene esplicitato.

Lo scenario si articola nei seguenti passi:

1. lo UA richiede una risorsa al SP
2. il SP controlla se UA è autenticato e verifica che non lo è
3. il SP genera una <AuthnRequest> SAML 2.0 destinata al LP e la invia allo UA per mezzo del binding POST
4. lo UA inoltra la <AuthnRequest> al LP
5. il LP invia allo UA una web form invitando a introdurre il proprio username qualificato o a indicare la PA desiderata
6. lo UA invia al LP la risposta
7. il LP interroga il registry per conoscere la URL del servizio PA
8. il registry risponde con la URL della PA
9. il LP interroga la PA per ottenere il nome della CA scelta dall'utente
10. la PA risponde con il nome della CA

11. il LP interroga il registry per risolvere la URL della CA
12. il registry risponde con la URL
13. il LP invia allo UA una <AuthnRequest> "proxificata" (prevista dalla specifica SAML 2.0[2]) destinata alla CA per mezzo del binding POST
14. lo UA inoltra la <AuthnRequest> alla CA
15. la CA inizia con lo UA la challenge di autenticazione
16. lo UA risponde alla challenge
17. la CA genera la <Response> e risponde allo UA secondo il binding POST
18. lo UA inoltra la <Response> al LP
19. il LP estrae l'asserzione generata dalla CA e costruisce una nuova <Response>
20. il LP invia allo UA la <Response> destinata al SP secondo il binding POST
21. lo UA inoltra la <Response> al SP

L'utente a questo punto è stato correttamente autenticato e il SP è in possesso della relativa asserzione. Lo scenario può proseguire con la verifica dell'autorizzazione:

22. il SP controlla se UA è autorizzato per l'accesso alla risorsa richiesta e verifica che non lo è ancora.
23. il SP invia una <AttributeQuery> al LP usando il binding SOAP
24. il LP determina quale sia la PA che contiene il profilo utente. Può fare questo usando una cache delle informazioni recuperate durante la fase di autenticazione, oppure è ipotizzabile che l'operazione di autenticazione inserisca nella <Response> una asserzione aggiuntiva che indica qual è la PA scelta dall'utente
25. il LP chiede alla PA il profilo dell'utente
26. la PA restituisce il profilo
27. il LP interroga il registry per conoscere le URL delle AA referenziate dal profilo
28. il registry fornisce le URL richieste
29. il LP invia alla AA una <AttributeQuery> per conoscere gli attributi posseduti dall'utente
30. la AA restituisce una <Response> con le asserzioni relative agli attributi
31. il LP estrae le asserzioni e costruisce una <Response> per il SP
32. il LP restituisce la <Response> al SP contenente le asserzioni relative a tutti gli attributi dichiarati dall'utente nel proprio profilo (portafoglio di asserzioni).
33. il SP prende la decisione in merito all'autorizzazione dell'utente
34. il SP fornisce la risorsa inizialmente richiesta.

---

[2] saml-core-2.0-os paragrafo 3.4.1.5

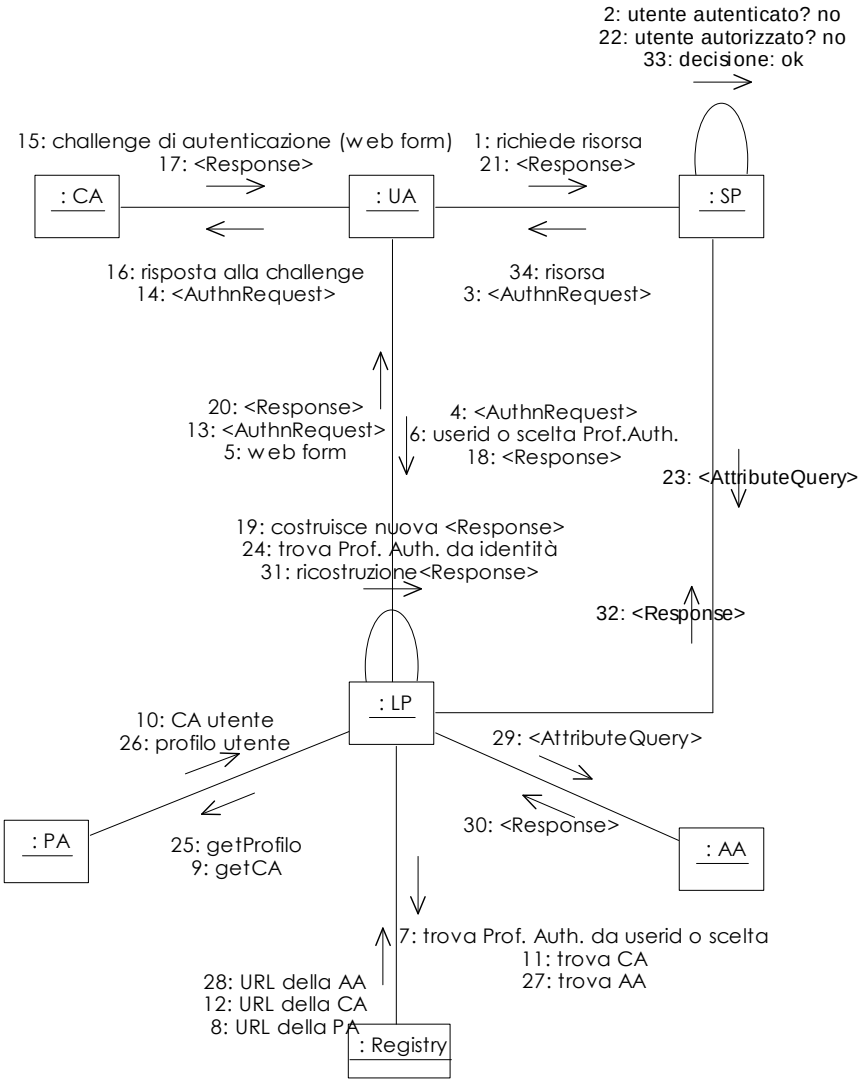

Figura 15 - Scenario di interazione – modello di riferimento

Data la descrizione di questo scenario di riferimento, appare chiaro che il punto migliore dove effettuare caching di asserzioni è proprio il proxy locale, data la sua posizione centrale rispetto alle diverse authority coinvolte. Riguardo al Registry, come detto esso deve essere noto a tutti i domini cooperanti. Per minimizzare la necessità di interventi di aggiornamento è possibile realizzare un vero e proprio registry federato, ove ogni dominio mantiene la porzione di propria competenza e referenzia le porzioni di responsabilità di domini esterni. Vi è tuttavia anche l'alternativa più semplice in cui il registry è gestito centralmente, per esempio ad opera del Responsabile del Dominio di Cooperazione. Si noti inoltre che il LP è in grado di assemblare tutte le asserzioni ricevute dai vari certificatori, all'interno di un cosiddetto "portafoglio delle asserzioni" che può essere riutilizzato più volte, limitatamente alla validità delle asserzioni ivi contenute, e che può essere inviato come unità atomica a fronte di richieste

di autenticazione/autorizzazione effettuate da servizi a valle. Si rimanda alla sezione successiva per ulteriori dettagli.

Scendendo ad un livello di dettaglio maggiore, è possibile descrivere cosa avviene all'interno del SP durante l'esecuzione dello scenario appena presentato. Il seguente diagramma di collaborazione UML presenta l'insieme delle azioni intraprese dal SP, limitando l'attenzione alle interazioni dirette con gli elementi esterni al SP stesso. Ovvero non vengono ripresi i passi dello scenario che coinvolgono le altre entità, quali il LP e i certificatori.

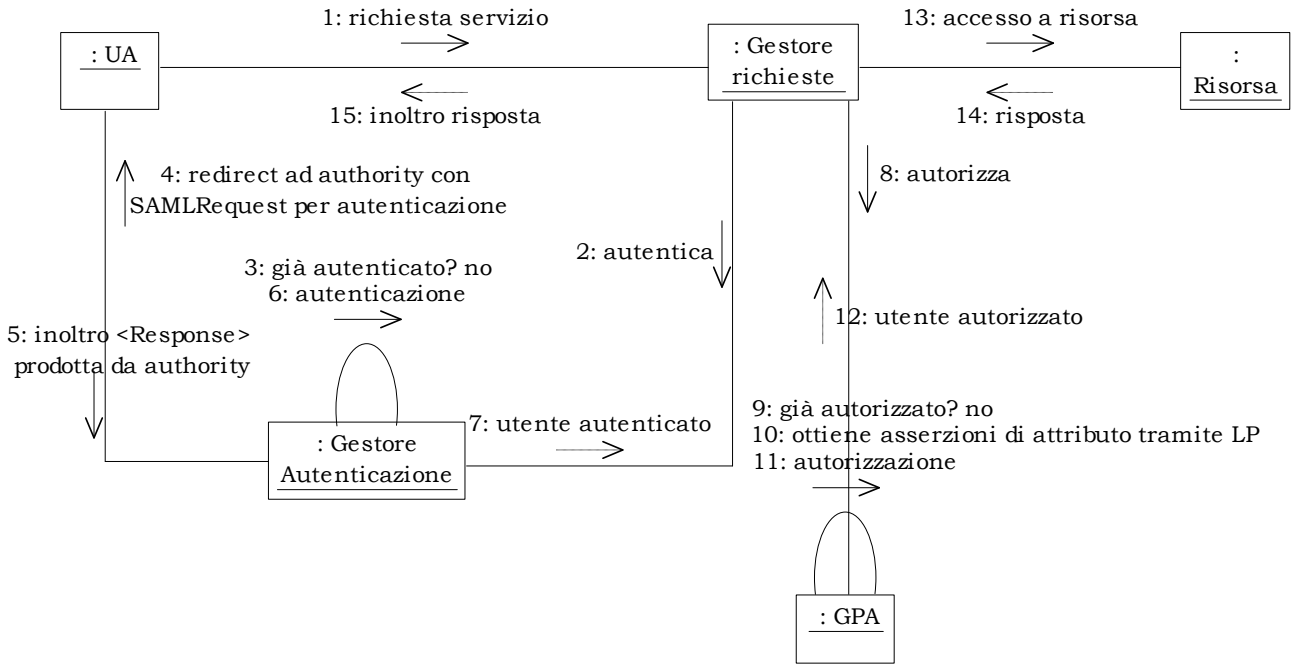

Figura 16: Dettaglio di funzionamento del Service Provider

1. UA invia la richiesta di servizio a SP, che viene raccolta dal Gestore delle Richieste.
2. Il Gestore delle Richieste richiede al Gestore Autenticazione di autenticare il richiedente
3. Il Gestore Autenticazione verifica che il richiedente non è attualmente autenticato
4. Il Gestore Autenticazione genera pertanto una SAMLRequest con la richiesta di un'asserzione di autenticazione che consegna ad UA forzandolo a presentarla al relativo certificatore (vedi scenario completo, descritto sopra per i dettagli)
5. Dopo aver fornito le proprie credenziali al relativo certificatore, UA ottiene la relativa asserzione che inoltra al Gestore Autenticazione
6. Il Gestore Autenticazione è ora in grado di autenticare l'utente
7. Il Gestore Autenticazione comunica al Gestore delle Richieste relativamente all'esito dell'autenticazione e questo procede con la fase successiva.
8. Il Gestore delle Richieste richiede al GPA di autorizzare il richiedente
9. Il GPA verifica che il richiedente non è attualmente autorizzato

10. Il GPA ottiene, mediante LP esterno (vedi scenario completo, descritto sopra, per i dettagli) le asserzioni di attributo necessarie.
11. Il GPA è in grado di autorizzare l'utente mediante tali asserzioni
12. Il GPA comunica al Gestore delle Richieste che il richiedente è ora autorizzato
13. Il Gestore delle Richieste inoltra la richiesta di servizio originale ricevuta alla risorsa
14. La risorsa fornisce una risposta al Gestore delle Richieste
15. Il Gestore delle Richieste comunica la risposta al richiedente.

Grazie alla netta suddivisione delle responsabilità delle fasi di autenticazione e autorizzazione, il modello di riferimento presenta buone caratteristiche di modularità e adattamento a varie soluzioni implementative esistenti e future. Mantenendo valido il Gestore delle Richieste, infatti, è possibile escludere o modificare/sostituire selettivamente le due parti di autenticazione e autorizzazione, e anche aggiungerne di ulteriori per coprire fasi non contemplate in questo documento (es. tracciatura delle richieste ecc.). Si osserva che, ad eccezione del protocollo di comunicazione tra GPA e proxy locale definito in questo documento, a ciascun dominio è lasciata libertà nello scegliere, per il GPA stesso, l'implementazione ritenuta più appropriata, eventualmente utilizzando sistemi esistenti.

5.3. Scenario in cooperazione applicativa

Come indicato nell'introduzione, in generale il processo di fruizione di un generico servizio erogato dal DSA (Dominio dei Servizi Applicativi, secondo la terminologia CNIPA) comporta un'interazione applicativa tra componenti applicative diverse, in modo trasparente per l'utente finale. In altri termini, a valle di una richiesta operata mediante interfacciamento web da parte di un utente (es. un cittadino) che accede ad un portale, è possibile – e in generale frequente – che tale richiesta, pervenuta ad un sistema di front-end, causi l'attivazione di ulteriori richieste per servizi di livello più basso, funzionali all'adempimento della richiesta originaria.

Si vuole affrontare qui il caso in cui un servizio di front-end abbia necessità di accedere ai servizi (detti di "back-end") erogati da sistemi posti in domini diversi dal proprio. Nell'ottica del sistema federato interregionale di autenticazione e autorizzazione, questo comporta l'insorgere di alcuni aspetti che devono essere considerati, relativamente alle garanzie di sicurezza che tali ulteriori accessi comportano.

Gli scenari presentati nel capitolo precedente, unitamente allo scenario di riferimento scelto e presentato poco sopra, prendono in considerazione un caso generico, in cui a richiedere di fruire di un servizio è un generico utente. Si è fino a questo momento assunto che l'utente richiedente agisse mediante uno user agent (o browser web). Si vedrà, tuttavia, che questa assunzione può facilmente decadere, essendo gli scenari presentati estendibili al caso di accesso da parte di un software applicativo.

Nel seguito il termine "richiedente" e "dominio richiedente" (DR) saranno usati come sinonimi di "fruitore" e "dominio fruitore", secondo la terminologia indicata in precedenza.

Come anticipato, l'alternativa all'uso di interfacce "a portale", ovvero che presuppongono la presenza di un utente umano, è quella di far uso di interfacce software, che nel modello della cooperazione applicativa coincidono spesso con le porte di dominio. Ciascun dominio erogatore, pertanto, dovrà

offrire entrambe le possibilità di accesso, nella misura in cui i propri servizi siano suscettibili di essere invocati in entrambe le modalità. Vi saranno, per contro, servizi di base e non pensati per un accesso da parte di utenti finali, per i quali l'accesso sarà consentito unicamente mediante porte di dominio, o altro tipo di interfaccia.

Allo scopo di definire uno scenario per il Sistema Federato di Autenticazione (SFA) che preveda interazioni in cooperazione applicativa, è necessario definire le modalità secondo le quali i servizi applicativi (di front-end) riescono ad accedere ad altri servizi (di back-end), situati in generale in altri domini, trasmettendo le credenziali ed eventuali altre informazioni necessarie a stabilire se sussistono le condizioni per concedere o negare l'accesso, proprio come avviene nel caso di interazione di un utente con un servizio offerto dal dominio erogatore.

A fronte di una richiesta di servizio formulata dalla porta di dominio A (porta delegata) e diretta alla porta di dominio B (porta applicativa), la seconda può accettare o rifiutare la stessa sulla base di credenziali associate alla porta stessa, che indicano ad esempio qual è il dominio di provenienza, oppure sulla base di analisi più puntuali relativamente alle caratteristiche della richiesta, come l'identità del richiedente. Il livello a cui tali controlli sono effettuati può variare in funzione degli elementi del canale di comunicazione considerati. Ad esempio, nel caso delle porte di dominio, la comunicazione avviene mediante scambio di buste di e-government in formato SOAP. Tra i vari end-point della comunicazione si assume inoltre che siano stato stabiliti opportuni livelli di accordo per garantire sufficienti livelli di servizio (SLA). A livello superiore, in fase di invocazione di servizi complessi tra domini diversi, questo livello di dettaglio viene ignorato e si assume di poter disporre di un canale affidabile, sicuro e protetto. A questo secondo livello si pone il task INF-3 del progetto ICAR, per la definizione dei meccanismi per l'interazione inter-dominio, nel sistema federato di autenticazione e autorizzazione. A livello ancora superiore, i servizi cooperano in maniera trasparente rispetto al dominio di appartenenza, sfruttando le varie funzionalità presenti e passando le informazioni di autenticazione e autorizzazione in modo automatico. Quest'articolazione in 3 livelli è riassunta dal diagramma seguente, che mostra la pila infrastrutturale di ICAR.

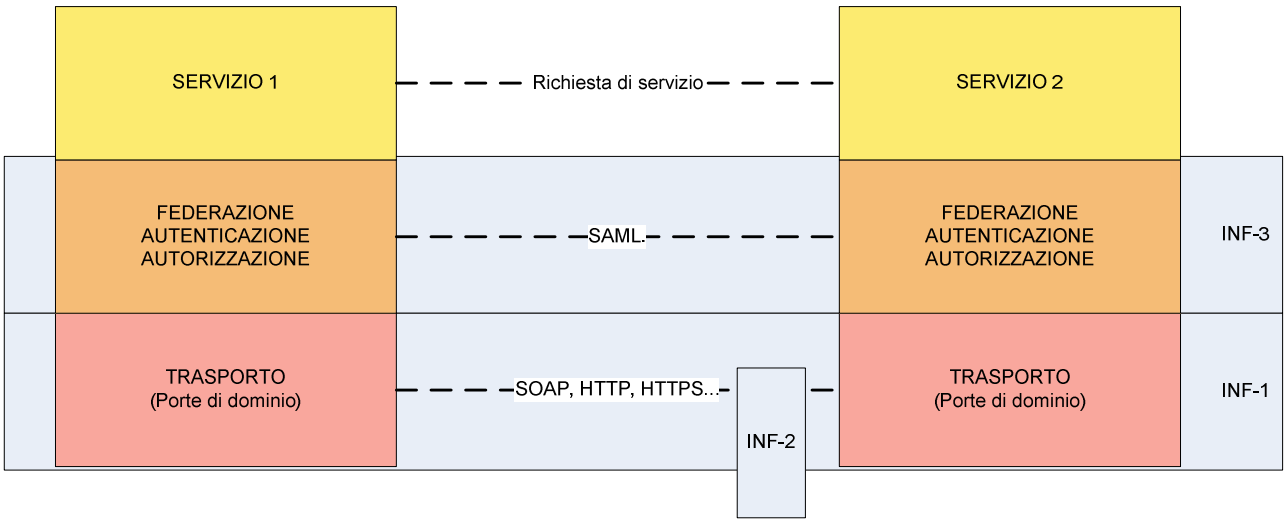

Figura 17: Pila infrastrutturale ICAR

Durante l'interazione complessa che prevede il coinvolgimento in cooperazione applicativa di uno o in generale più servizi di back-end, si assume che il sistema di front-end di INF-3 abbia collezionato un certo numero di asserzioni SAML caratterizzanti l'utente richiedente, in termini di identità e attributi. Tale portafoglio di asserzioni viene utilizzato durante la richiesta al servizio di back-end a valle, inviando tali informazioni in blocco.

Nel caso generale, il servizio di back-end richiederà a sua volta al proprio richiedente, ovvero al servizio di front-end, di autenticarsi e fornire informazioni relativamente ad alcuni attributi ritenuti indispensabili per erogare il servizio. Come si vede questo è simile a quanto illustrato sopra per quanto riguarda l'accesso mediante uno user agent, quale un browser web o altro dispositivo comandato da un utente umano. L'erogazione del servizio complessivo, così come visto dall'utente finale, può essere **sincrona** o **asincrona.** Nel primo caso l'utente invia la propria richiesta e il sistema richiedente costruisce il portafoglio delle asserzioni, identificando ed autorizzando l'utente ad accedere ai propri servizi. Successivamente il flusso operativo continuerà, spostando il focus sul servizio richiedente stesso. Questo agirà in modo automatico nei confronti del sistema nel dominio a valle. Per questo motivo non è pensabile adottare una procedura di autenticazione interattiva, in cui è l'utente (in questo caso il servizio richiedente) a fornire le proprie credenziali ad un soggetto certificatore dell'identità. Il servizio richiedente, pertanto, includerà nel portafoglio delle asserzioni un'asserzione di autenticazione SAML ottenuta in fase di setup del sistema. Allo stesso modo, tale servizio dovrà preoccuparsi di ottenere ogni ulteriore asserzione di attributo relativamente al proprio ruolo nel processo in atto, indicato come requisito da parte del servizio di back-end con cui intende colloquiare. Come indicato da CNIPA, nella descrizione delle caratteristiche di sicurezza per l'accesso ai servizi, sono definiti degli Accordi di Servizio [6], mediante l'utilizzo delle tecnologie e degli standard (ancorché tuttora in fase di definizione) relativi all'ambito dei Web Services. Alcuni di essi (WS-Policy, WS-SecurityPolicy, WS-Trust ecc.) consentono di specificare con precisione i requisiti e le regole per la fruizione di ciascun servizio. Questi Accordi di Servizio sono memorizzati in appositi registri SICA a livello generale o locale, inter-dominio.

Una volta che il servizio richiedente ha assemblato il portafoglio di asserzioni completo di tutte le informazioni necessarie, lo include nell'invocazione del servizio di back-end che lo riceverà e potrà effettuare il policy enforcement, autorizzare la richiesta e fornire la risposta.

Nella modalità asincrona, si prevede che l'utente finale si autentichi presso il servizio di front-end e ottenga in qualche modo un riscontro di attivazione del servizio, senza che esso si concluda immediatamente. Proprio come avviene per talune pratiche della Pubblica Amministrazione, la richiesta viene presa in carico da un funzionario, visto come un secondo utente, operatore del servizio di front-end, il quale proseguirà con il resto delle interazioni. In questo caso l'autenticazione del servizio richiedente su quello erogatore nel dominio di back-end può avvenire con le stesse modalità descritte negli scenari descritti nel capitolo precedente, in modo interattivo con un soggetto certificatore. Tuttavia, per evitare un eccessivo carico all'operatore responsabile della gestione del servizio richiedente (per esempio un funzionario di una pubblica amministrazione) e velocizzare e rendere così più

efficiente il processo, è preferibile agire come nel caso di interazione sincrona, in cui l'asserzione di autenticazione viene fornita automaticamente e inserita nel portafoglio delle asserzioni.

In entrambi i casi, sincrono e asincrono, infatti, si può assumere che il ruolo del funzionario o del servizio richiedente relativamente al sistema complessivo e in particolar modo relativamente al processo attuato abbia una validità temporale non breve. Ogni asserzione di autenticazione ottenuta, in ogni caso, deve essere legata alla richiesta di servizio, nel momento in cui essa viene formulata, specificando una validità temporale il più breve possibile, onde minimizzare le possibilità di intercettazione e/o alterazione del messaggio.

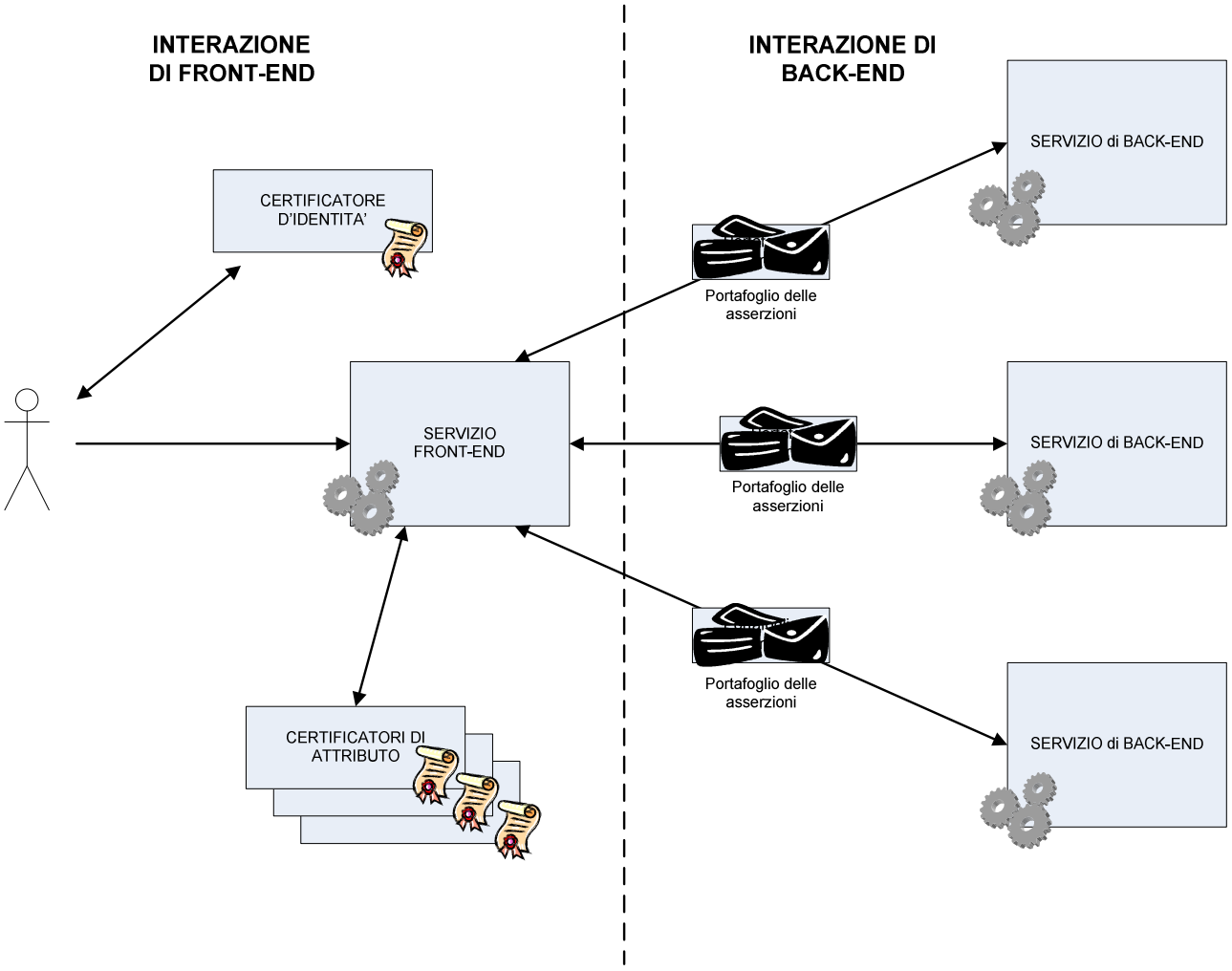

Figura 18: Schema generale interazioni di front-end e back-end

Nel diagramma di Figura 18 viene illustrato uno schema generale con le varie interazioni presenti nella prima e nella seconda fase di accesso al servizio da parte dell'utente finale. Si noti come il servizio richiedente operi come delegato dell'utente, nei confronti dei vari servizi erogatori in altrettanti domini di back-end. In questo senso l'identità e gli attributi principali forniti a questi ultimi per l'autenticazione e autorizzazione saranno relativi a dati propri del servizio richiedente che fa da intermediario. Tuttavia il portafoglio delle asserzioni contiene anche i dati reperiti originariamente per l'utente finale. Tali dati,

seppure non strettamente necessari per l'accesso al servizio di back-end, vengono comunque inclusi nel portafoglio, dato che potranno essere utilizzati dalla logica del singolo servizio.

Grazie alla propagazione dell'intero portafoglio di asserzioni ai vari servizi di back-end, a questi ultimi non è richiesto di consultare alcuna autorità di certificazione per sopperire a dati mancanti. Questo consente di aggirare eventuali problemi legati al fatto che gli stessi certificatori sono visti come servizi che richiedono a loro volta autenticazione e autorizzazione per l'accesso. Può accadere infatti che un dato servizio di back-end, appartenente ad un dominio remoto, non goda dei privilegi sufficienti per ottenere certificazioni relative ad un soggetto (servizio richiedente) appartenente ad un dominio diverso. Il servizio di back-end utilizzerà unicamente il proprio gestore delle politiche di autorizzazione che potrà effettuare il policy enforcement con i soli dati ricevuti.

5.3.1. Le entità interagenti nello scenario in cooperazione applicativa

Nel diagramma delle classi UML di Figura 19 sono raffigurate le entità coinvolte in un generico scenario d'interazione inter-dominio, in cooperazione applicativa. In tale diagramma vengono utilizzati alcuni stereotipi UML, definiti ad-hoc, per caratterizzare la semantica dei messaggi scambiati dalle diverse entità in gioco. Tali stereotipi decorano le relazioni di dipendenza ed associazione indicate, allo scopo di dettagliare la semantica dei messaggi scambiati tra le entità che sono istanze delle classi rappresentate nel diagramma. Maggiori informazioni al riguardo saranno fornite più avanti in questa stessa sezione.

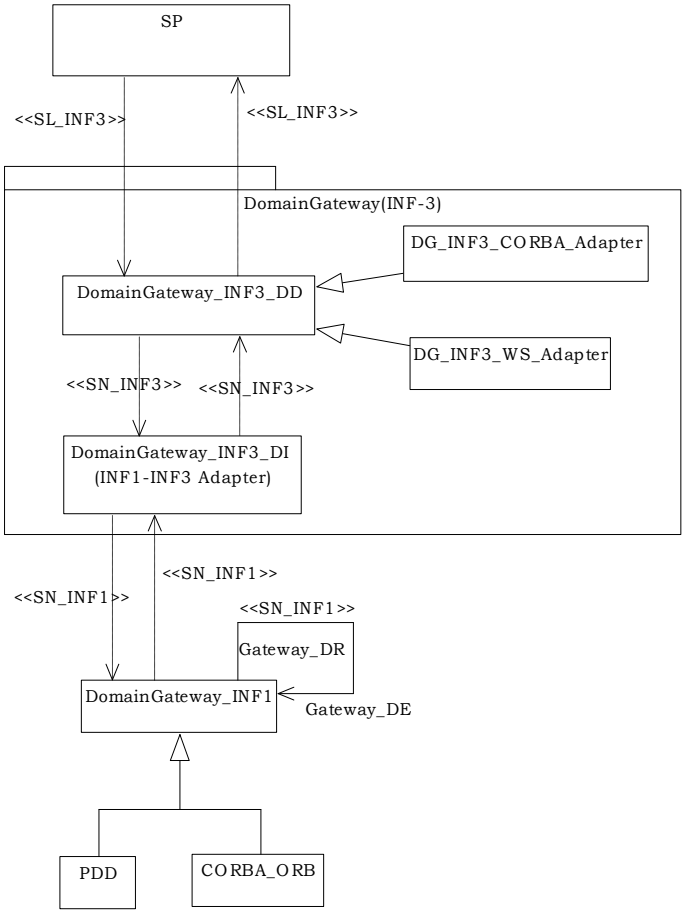

Figura 19: Entità coinvolte nello scenario di cooperazione applicativa

In esso, oltre al SP, rappresentante sia quello presente nel dominio fruitore che quello nel dominio erogatore, sono indicati i cosiddetti Gateway di Dominio, ovvero i componenti che svolgono le funzioni di interfaccia tra due domini informatici distinti, e attraverso i quali fluiscono tutti i messaggi scambiati tra essi. In particolare si è voluta mantenere la strutturazione e distinzione delle diverse responsabilità in carico al sistema di autenticazione e autorizzazione federata (INF-3) rispetto a quelle del sistema di trasporto a livello più basso (INF-1).

Il gateway di dominio a livello INF-3 è presentato dettagliandone i sotto-componenti. Esso infatti si articola nel gateway dipendente dal dominio e in un adattatore, indipendente dal dominio, tra il formato dei messaggi secondo il livello INF-3 e quello secondo il livello INF-1.

Si consideri, infatti, che il generico SP presente in un certo dominio, potrebbe supportare diversi tipi di interazione distribuita con altri sottosistemi. Questo significa, ad esempio, che un dato SP potrebbe non dialogare via protocollo SOAP su HTTP come i Web Services, ma per esempio attraverso un protocollo CORBA o altro standard. Affinché esso possa utilizzare l'infrastruttura ICAR e quindi il sistema per l'autenticazione e l'autorizzazione federata, e possa quindi inviare messaggi all'esterno del proprio dominio, a servizi ugualmente eterogenei, è prevista la componente domain-dependent, in grado di adattarsi a vari standard d'interazione. Nel diagramma è pertanto evidenziato come tale parte si

specializzi in alcune varianti (adapter) di cui l'adapter CORBA e quello per Web Services (WS) sono solo due esempi.

A valle di tale sezione vi è la parte domain-independent del gateway di dominio a livello INF-3, ovvero quella in grado di colloquiare, senza preoccuparsi dei dettagli specifici dei singoli domini/servizi, con la parte di trasporto sottostante, indicata come gateway a livello INF-1.

Questo componente, al di fuori delle responsabilità del task INF-3, ha la funzione di instaurare il canale di comunicazione inter-dominio, assicurandone, come già accennato, opportune caratteristiche di sicurezza, affidabilità, qualità ecc. In particolare, si è preferito non vincolare questo componente ad alcuna implementazione specifica: come indicato, il gateway INF-1 generico si può specializzare in un qualunque numero di sistemi specifici, quali le Porte di Dominio (come da documentazione CNIPA SPCoop) oppure ORB CORBA o altri ancora.

Il gateway di dominio a livello INF-1 colloquia con la propria controparte nel dominio di destinazione (come indicato dall'autoanello nel diagramma) e propaga le informazioni passandole ai corrispondenti strati superiori (INF-3) in modo speculare a quanto avviene nel flusso di messaggi "all'andata". Questo sarà dettagliato meglio nei successivi diagrammi di collaborazione.

Di seguito vengono descritte le semantiche dei messaggi scambiati tra le entità in gioco.

- **SL_INF3: semantica locale dello strato INF-3**. Corrisponde alla semantica, locale a ciascun dominio, utilizzata per le invocazioni di servizio. Ad esempio la semantica associata ad un'invocazione CORBA (es. tipo e posizione dei parametri, ecc.) è diversa da quella per un'invocazione di Web Services. In tale semantica è previsto il trattamento del portafoglio delle asserzioni, a livello applicativo, ovvero insieme all'invocazione di un certo metodo di un servizio. A titolo di esempio, nel caso di un'invocazione SOAP di un Web Services, nella parte *BODY* del messaggio possono essere contenuti entrambi i tipi di informazioni: oltre ai parametri applicativi dell'invocazione può essere contenuto il portafoglio di asserzioni, come ulteriore parametro.
- **SN_INF3: semantica neutrale dello strato INF-3**. La semantica locale, proprio perché peculiare di ciascun dominio/servizio deve essere trasformata in una semantica indipendente dal dominio, in grado di essere compresa con certezza da qualunque controparte allo stesso livello, in un altro dominio. In particolare, nel caso di Web Services, si assume che secondo questa semantica il messaggio SOAP sia organizzato con il portafoglio di asserzioni inserito nella sezione WS-Security della parte *HEAD*, mentre l'invocazione vera e propria con i parametri viene inserita nella parte *BODY*.
- **SN_INF1: semantica neutrale dello strato INF-1**. Il messaggio con semantica SN_INF3 viene trattato come messaggio opaco dallo strato INF-1 che lo deve recapitare a destinazione. Lo strato INF-3, pertanto, indicherà unicamente il dominio di destinazione e il messaggio stesso allo strato INF-1, secondo questa semantica. Nel caso di Porte di Dominio, il messaggio trasferito sarà di tipo SOAP, nella cui parte *BODY* è inserito il messaggio in semantica SN_INF3, opaco allo strato INF-1. A sua volta, infine, INF-1 potrà aggiungere qualsivoglia struttura di controllo, sicurezza ecc. alla parte *HEAD* di questo messaggio, per gli scopi di trasporto.

Tutti i sopraccitati stereotipi, pertanto, associano la semantica dettagliata con l'invio di un messaggio, come sarà chiarito nei successivi diagrammi di collaborazione.

5.3.2. Scenario generale d'interazione in cooperazione applicativa

In Figura 20 viene riportato un diagramma di collaborazione UML che illustra l'intero scenario in cooperazione applicativa che è stato accennato sopra, dettagliandone tutti i passi.

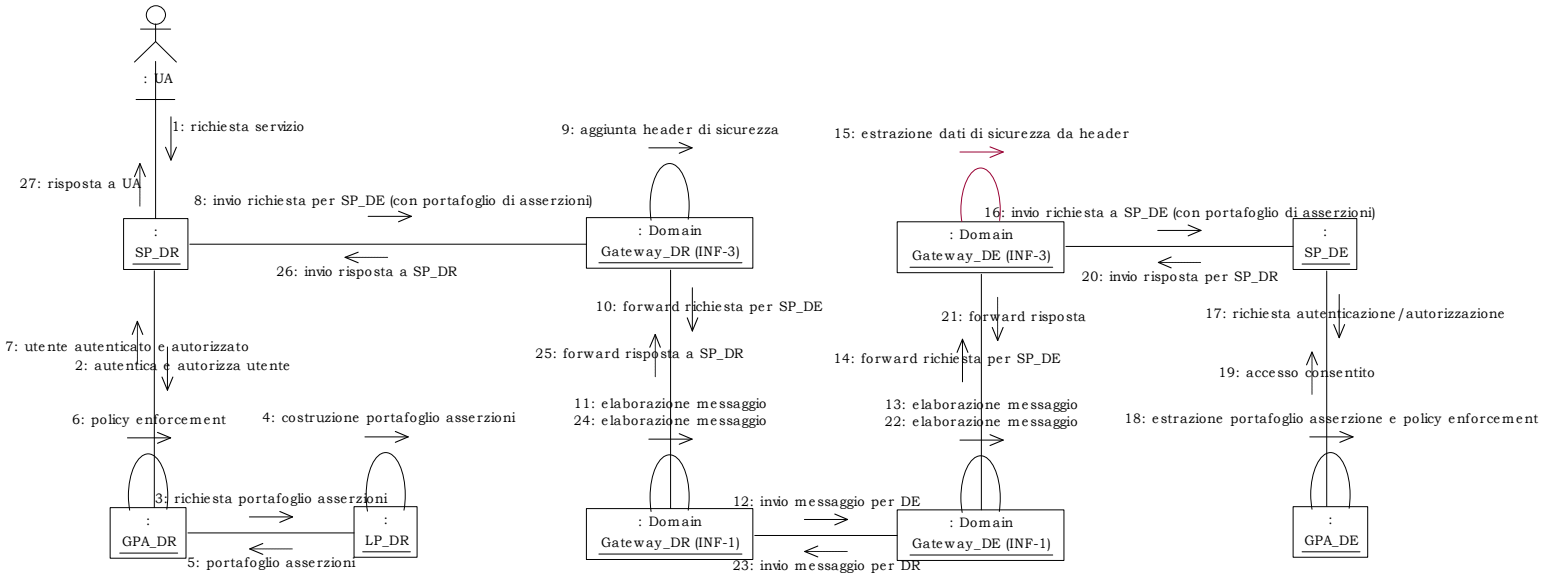

Figura 20: Scenario generale di interazione con cooperazione applicativa

Lo scenario comprende, come è possibile vedere, anche una parte iniziale d'interazione con un utente umano, che opera mediante il proprio browser web o altro dispositivo di accesso. Tale interazione viene riassunta in un numero di passi inferiore rispetto allo scenario di riferimento illustrato nella Sezione 5.2, al solo scopo di illustrare lo scenario completo, a partire da una richiesta utente, fino al coinvolgimento di tutte le altre entità in gioco. In particolare, si tenga presente che nel diagramma il componente GPA rappresenta in realtà anche i già citati Gestore Richieste e Gestore Autenticazione e che pertanto ne assume le funzionalità. Nel dettaglio, lo scenario si articola nei seguenti passi:

1. UA contatta un servizio (di front-end) SP_DR.
2. SP_DR accede all'infrastruttura di autenticazione e autorizzazione del proprio dominio per verificare che l'utente abbia diritto all'accesso. Per fare questo interroga il componente GPA_DR.
3. GPA_DR accede al profilo del servizio e passa il controllo al proxy locale LP_DR, richiedendo il reperimento di un certo numero di certificazioni di autenticazione e attributo.
4. LP_DR contatta vari certificatori (quest'interazione non è esplicitata) e costruisce un portafoglio delle asserzioni.
5. LP_DR restituisce a GPA_DR il portafoglio delle asserzioni.
6. GPA_DR utilizza tale portafoglio per effettuare il policy enforcement ed abilitare l'utente all'accesso a SP_DR.

7. GPA_DR comunica a SP_DR che l'utente è abilitato e trasmette l'intero portafoglio delle asserzioni insieme a questa comunicazione. N.B.: si assume che tutti i SP del sistema INF-3 siano in realtà dei wrapper dei servizi elementari che supportano, e in particolare siano in grado di comprendere e gestire i portafogli di asserzioni ottenuti dal sistema federato.
8. Per eseguire correttamente la propria logica applicativa, SP_DR necessita di contattare un secondo servizio, chiamato SP_DE, situato in un altro dominio, detto dominio erogatore del servizio, o di back-end. Per questo SP_DR genera un'invocazione di servizio che trasmette al gateway del proprio dominio, a livello INF-3. Si noti che a questo punto il dominio DR è diventato il dominio richiedente di un nuovo servizio.
9. Il gateway del dominio richiedente a livello INF-3 inserisce in una struttura WS-Security (o altra struttura) il portafoglio delle asserzioni ricevuto da SP_DR.
10. Il gateway del domino DR a livello INF-3 passa il messaggio siffatto al gateway del dominio DR, a livello INF-1, per il trasporto.
11. Il gateway del dominio DR a livello INF-1 elabora il messaggio secondo le modalità che ritiene più opportune per ottimizzarne il trasporto.
12. Il gateway del dominio DR a livello INF-1 spedisce il messaggio alla propria controparte nel dominio DE.
13. Il gateway del dominio DE a livello INF-1 effettua le operazioni di elaborazione del messaggio, opposte a quelle effettuate dalla propria controparte all'andata, ricostruendo il messaggio originale.
14. Il gateway del dominio DE a livello INF-1 invia il messaggio ricostruito al gateway del dominio DE a livello INF-3.
15. Il gateway del dominio DE a livello INF-3 riceve il messaggio ed estrae il portafoglio delle asserzioni dalla sezione WS-Security (o altra struttura) del messaggio, riportandolo al livello di invocazione, secondo la semantica supportata dal servizio destinazione SP_DE.
16. Il gateway del dominio DE a livello INF-3 invia il messaggio di invocazione (es. SOAP + portafoglio di asserzioni) al SP_DE.
17. SP_DE richiede al sistema federato di autenticazione e autorizzazione INF-3 un controllo sull'identità e ruolo del richiedente. Per fare questo comunica il portafoglio delle asserzioni a GPA_DE.
18. GPA_DE effettua il policy enforcement per SP_DE, utilizzando le asserzioni contenute nel portafoglio. Si ricorda che tali credenziali recano l'impronta del Responsabile del Dominio di Cooperazione, che abilita tutti i certificatori del circuito di domini interoperanti e federati. GPA_DE, pertanto, attribuisce il corretto valore e fiducia a tali asserzioni.
19. Se i dati ricevuti lo consentono, GPA_DE comunica a SP_DE che il richiedente è abilitato all'accesso. Si noti che ora il richiedente di SP_DE è il SP_DR e NON l'utente tramite il dispositivo di accesso UA. Questo significa che nel portafoglio delle asserzioni ricevuto, il policy enforcement coinvolgerà soltanto quelle asserzioni che sono relative a dati del servizio SP_DR o del suo operatore (es. funzionario comunale).
20. Con questa interazione inizia il flusso di messaggi di risposta. SP_DE risponde al gateway del dominio DE a livello INF-3, con un messaggio diretto a SP_DR.

21. Il gateway del dominio DE a livello INF-3 inoltra la richiesta al gateway del dominio DE a livello INF-1 per il trasporto.
22. Come nel flusso di andata, il gateway del dominio DE a livello INF-1 elabora il messaggio aggiungendo qualsivoglia struttura di controllo nella sua intestazione.
23. Il gateway del dominio DE a livello INF-1 inoltra il messaggio alla propria controparte nel dominio DR.
24. Il gateway del dominio DR a livello INF-1 riceve ed elabora il messaggio, invertendo le operazioni della propria controparte in DE e ricostruendo il messaggio di risposta per SP_DR.
25. Il gateway del dominio DR a livello INF-1 invia al gateway del dominio DR a livello INF-3 il messaggio di risposta diretto a SP_DR.
26. Il gateway del dominio DR a livello INF-3 inoltra il messaggio di risposta al SP_DR.
27. Infine, SP_DR, dopo eventuali ulteriori attività, crea la risposta per UA.

Come è possibile vedere dal dettaglio dei passi di questo scenario, si è voluto nascondere i dettagli delle interazioni tra i componenti del gateway di dominio a livello INF-3, come illustrate nella sezione precedente. Ai fini di una comunicazione end-to-end, infatti, è importante osservare ciò che i vari livelli passano agli altri. I dettagli dell'interazione tra i domain gateway, invece, con l'indicazione delle semantiche utilizzate durante le varie interazioni sono illustrati nel diagramma di collaborazione di Figura 21, seguente.

In esso appare evidente la strutturazione a "pila protocollare", come già illustrato in Figura 17, in cui i servizi di livello applicativo comunicano idealmente con i servizi di qualunque dominio federato, sfruttando i servizi offerti a livello sempre più basso dagli strati INF-3 e INF-1.

Senza ripetere puntualmente l'elenco dei passi, che corrisponde ad un sottoinsieme di quelli già elencati sopra, si vuole qua evidenziare come entrambi i SP utilizzino una semantica locale a livello INF-3, che corrisponde ad una conoscenza del portafoglio delle asserzioni (qualora presente), in aggiunta ai dettagli dell'invocazione di servizio. La semantica locale viene prima mutata in una neutrale dallo strato di adattamento (domain dependent) del livello INF-3, e poi in una seconda, neutrale, a livello INF-1 dallo strato domain independent. A livello basso INF-1 colloquia con la propria controparte. Quest'interazione, nel caso di utilizzo di Porte di Dominio, corrisponde ad un invio di una busta di e-Government, secondo direttive CNIPA. L'interazione prosegue poi, a risalire, fino a raggiungere il SP di destinazione, utilizzando semantiche in ordine opposto al precedente.

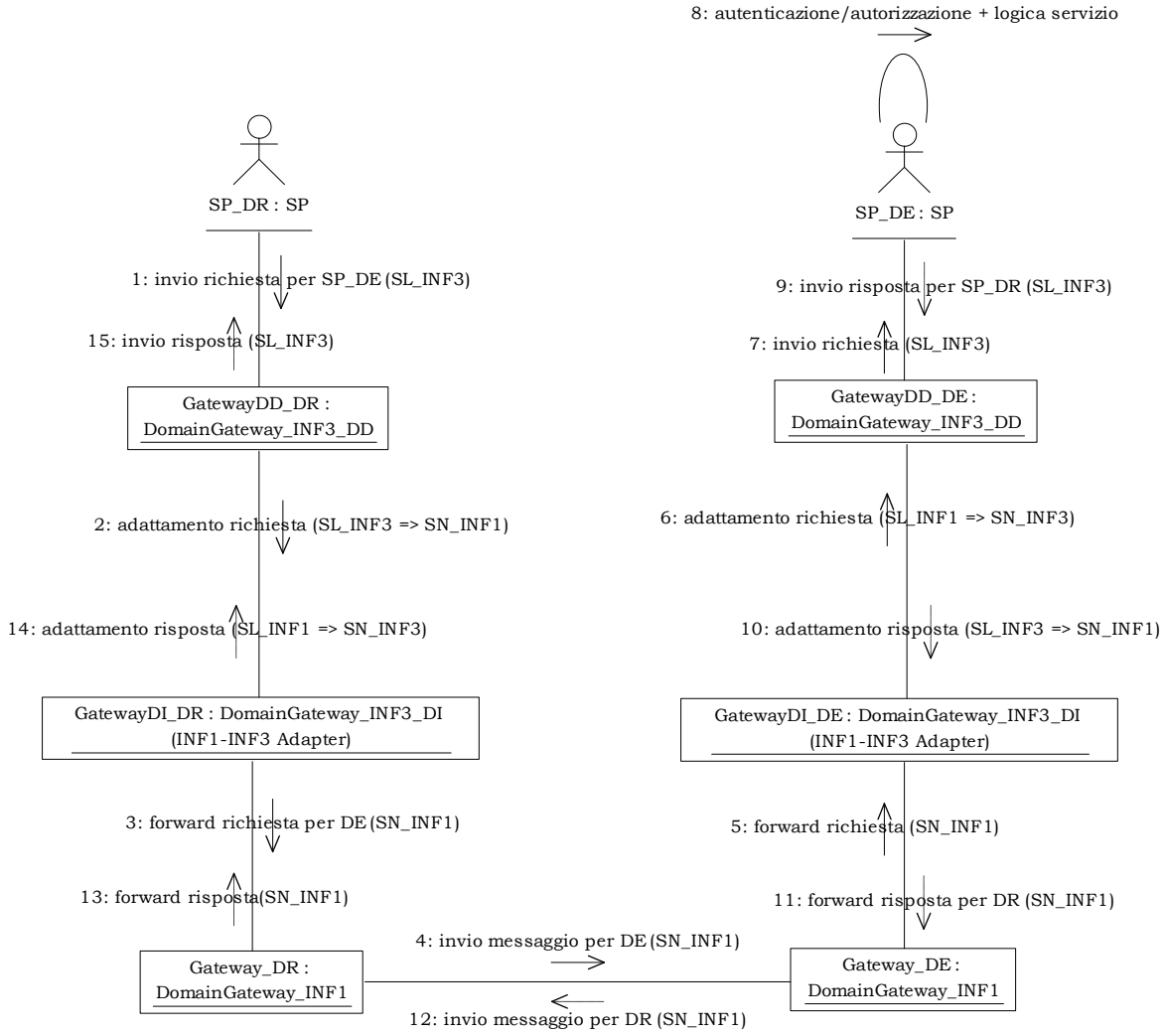

Figura 21: Dettaglio interazioni in cooperazione applicativa tra domain gateway

Un discorso analogo vale per il flusso dei messaggi di risposta, nel senso opposto, anch'esso descritto in figura.

6. TECNOLOGIE DI RIFERIMENTO

In questo capitolo verranno illustrate alcune delle tecnologie che si ritengono più utili per supportare la realizzazione degli scenari individuati, nell'ambito del sistema federato di autenticazione e autorizzazione.

Astraendo, come detto, dai dettagli tecnologici alla base della comunicazione a basso livello tra interfacce quali le porte di dominio, ci si concentra sullo scambio dei token di sicurezza, ovvero delle asserzioni di autenticazione, attributo e autorizzazione, necessarie per abilitare gli utenti alla fruizione dei servizi nei vari domini a disposizione.

Come già menzionato nelle sezioni precedenti, verrà utilizzato il linguaggio SAML per la codifica e il trasferimento delle asserzioni. Si farà ricorso invece allo standard XACML per formalizzare le policy di autorizzazione adottate presso i vari SP. Ulteriori standard riguardano i meccanismi alla base delle relazioni di trust e sicurezza, codifica dei messaggi e firma, in fase di definizione nel mondo dei Web Services. Si fa qui riferimento ad alcuni standard della classe WS-*, quali WS-Policy, WS-SecurityPolicy, WS-Trust, ecc. Sebbene promettenti per risolvere problemi quali la formalizzazione dei requisiti di sicurezza di un generico servizio, tuttavia essi non presentano ancora sufficienti caratteristiche di maturità e non hanno ancora raggiunto un livello di standardizzazione e diffusione tale da poter essere adottati estensivamente. Ciononostante, essi costituiscono la base di partenza e il loro sviluppo sarà seguito con attenzione, per recepire qualunque evoluzione che li porti in una migliore condizione di utilizzazione. Il supporto di strumenti (tool, API, editor, ecc.) ad oggi esistenti per tali specifiche è pressoché inesistente, cosa che contribuisce a limitarne fortemente l'adozione. Viceversa, lo standard WS-Security, utilizzato per la protezione dei messaggi SOAP di invocazione di Web Services, costituisce come già indicato nelle sezioni precedenti, lo standard di riferimento da cui partire per il trasporto delle richieste di servizio. In particolare, esso fornisce il meccanismo di base per l'aggiunta di token di sicurezza SAML nei messaggi SOAP che sarà utilizzato anche nel sistema INF-3 per includere informazioni complesse quali il portafoglio delle asserzioni. Tale standard non verrà ulteriormente dettagliato in questo documento. Si rimanda pertanto, per ulteriori dettagli, ai relativi documenti di specifica [7].

6.1. SAML

La notazione SAML, creata nel 2002 dall'ente di standardizzazione OASIS, consiste in un framework basato su XML e indipendente dai vendor, per lo scambio di informazioni di sicurezza, dette "asserzioni", tra business partner via Internet.

SAML è stato pensato per consentire molta di quella interoperabilità che si è dimostrata assolutamente necessaria tra i prodotti di sicurezza e i sistemi di gestione degli accessi sicuri ai siti Web. Lo scopo di SAML è realizzare un framework unificato che sia in grado di trasmettere le informazioni di sicurezza dell'utente che interagisce con un sistema, in modo da realizzare una lingua franca delle credenziali di sicurezza che permetta di scambiare informazioni senza modificare i sistemi di sicurezza esistenti.

Inoltre, SAML è stato progettato per funzionare sui meccanismi di trasporto più comuni, come HTTP, SMTP, FTP e alcuni framework XML, come SOAP ed ebXML. Fornisce un metodo standard per definire l'autenticazione dell'utente, le autorizzazioni e gli attributi all'interno di un documento XML.

Gli attori previsti dalla specifica della notazione sono entità che emettono asserzioni, dette "asserting party" e altre entità che le richiedono e ne fanno uso per gli scopi di autenticazione e autorizzazione, dette "relying party". Tale distinzione ben si adatta agli scopi della presente trattazione sul sistema federato di autenticazione e autorizzazione, dato che, di fatto, gli asserting party coincidono con i certificatori di identità e attributo, mentre i relying party sono le entità che li interrogano, come il Local Proxy dello scenario di riferimento.

Le componenti principali della notazione SAML sono le seguenti.

- **Asserzioni**. Presenti in tre tipi diversi, sono dichiarazioni di fatti riguardanti l'utente, sia esso una persona fisica o un sistema hardware/software. Le asserzioni di autenticazione richiedono che un utente provi la propria identità. Le asserzioni di attributo (attribute assertion) contengono i dettagli specifici dell'utente, come il ruolo assunto in un'organizzazione. I permessi (authorization decision statements) identificano invece quali operazioni un utente può compiere (per esempio l'accesso ad una data pagina di un servizio).
- **Protocolli**. Definiscono come si richiedono e ricevono le asserzioni contattando un asserting party; sono costituiti da successioni di SAML request e SAML response, a loro volta in formato di messaggi XML. Le request comprendono dati sui soggetti dei quali viene richiesta una asserzione, mentre nelle response sono presenti le asserzioni richieste.
- **Binding**. Forniscono i dettagli esatti su come i vari protocolli definiti possono essere mappati nei protocolli di trasporto, come SOAP su HTTP.
- **Profili**. Corrispondono ad un certo numero di scenari d'uso, nei quali è definito come le asserzioni, i protocolli e i binding vengono utilizzati in modo combinato per raggiungere gli scopi per i quali tali scenari sono stati pensati. Esempi di profili sono quello per effettuare il single sign-on tra vari servizi cross-dominio, quello per identificare l'asserting party usato da un certo soggetto e uno per formulare query di asserzioni utilizzando un binding sincrono come SOAP.

La notazione SAML, in sé, non autentica o autorizza gli utenti. Essa è il mezzo con il quale le varie entità citate, chiamate anche authentication/authorization server, rilasciano attestati comprovanti certe caratteristiche di taluni soggetti. In questo senso, i certificatori esterni all'infrastruttura e con essa interagenti mediante cooperazione applicativa vengono ad essere degli authorization server, in quanto ricevono richieste di asserzioni di attributo ove gli attributi in questione corrispondono ai ruoli degli utenti, che devono essere certificati.

Come accennato, la specifica SAML definisce alcuni protocolli, ovvero sequenze di messaggi, ad esempio per la richiesta/risposta di asserzioni. È presente, a questo scopo, una notazione per formalizzare tali richieste e tali risposte in XML. In particolare si noti che laddove gli end-point della comunicazione sono in grado di interagire mediante scambio di messaggi SOAP (es. le porte di dominio), le richieste e le risposte SAML vengono inserite nella sezione "body" delle buste SOAP. Un attributo importante specificato insieme a ciascuna asserzione è l'istante temporale di emissione, oltre naturalmente al soggetto che l'ha emessa. Ogni asserzione dispone a sua volta di una parte header e di

una parte body. Nella prima vengono inserite informazioni quali l'issuer e il subject a cui tale asserzione si riferisce e delle condizioni di validità. Ciascuna asserzione infatti è considerata valida soltanto all'interno di un ben specificato intervallo temporale. Questo consente, tra l'altro, di impedire che asserzioni dotate di un livello di criticità elevato, quali sono le asserzioni di autenticazione, vengano intercettate e riutilizzate più volte da parte di soggetti che non ne hanno titolo. Nella parte "body", invece, possono essere inseriti più statement, di vario tipo (autenticazione, attributo, autorizzazione).

Inoltre, le asserzioni SAML possono essere utilizzate anche come token nell'ambito dello standard WS-Security, per proteggere i dati veicolati da messaggi SOAP. In questo caso le asserzioni SAML contengono informazioni quali le chiavi usate per firmare digitalmente il contenuto (body) del messaggio SOAP del quale fanno parte, nella sezione header.

Nel Marzo 2005 il consorzio OASIS ha rilasciato la versione 2.0 dello standard SAML. Tale versione rappresenta un'evoluzione della precedente versione 1.1 a cui unisce contributi provenienti dalla specifica degli scenari di federazione dello standard Liberty Alliance Federation Framework (Liberty ID-FF) [5]. Quest'ultimo standard prevede alcune modalità secondo cui realizzare la federazione delle credenziali con cui vari soggetti si identificano presso vari sistemi. Secondo gli scenari definiti in Liberty Alliance, è possibile realizzare il single-sign-on con identità federate tra diversi sistemi, consentendo agli utenti di fornire una sola volta le proprie credenziali. La convergenza di tali scenari con quelli in via di definizione all'interno di SAML 1.1 ha portato alla maturazione dello standard SAML 2.0 che comprende tutti questi aspetti, oltre ad apportare alcune correzioni alla sintassi dei linguaggi XML utilizzati per rappresentare le asserzioni e i protocolli di richiesta/risposta con cui esse vengono veicolate.

Essendo l'ultima versione dello standard SAML molto recente, ad oggi non esistono ancora delle valide implementazioni, né sotto forma di editor, né sotto forma di librerie di programmazione (API) che ne consentano un fattivo utilizzo in prodotti e prototipi reali. Nella sezione successiva vengono riportate alcune informazioni su una libreria esistente, con supporto alla versione 1.1 di SAML.

6.1.1. OpenSAML

OpenSAML (www.opensaml.org) è un insieme di librerie che implementano la specifica SAML di OASIS (versioni 1.0 e 1.1).

Le librerie OpenSAML sono state realizzate e sono mantenute dal consorzio Internet2 come parte del progetto Shibboleth (http://shibboleth.internet2.edu). Sono disponibili in versione Java e C++ e sono distribuite con licenza Apache. Queste librerie forniscono una visione ad oggetti e di alto livello dei diversi elementi definiti dalla specifica SAML, nascondendo allo sviluppatore i dettagli del processo di firma e verifica del documento XML che rappresenta una specifica asserzione e le problematiche di costruzione delle varie componenti di un'asserzione. La libreria OpenSAML utilizza le librerie Apache XMLSecurity e XMLBeans.

6.1.2. Uso di SAML per il sistema di autorizzazione e autenticazione federata (INF-3)

La notazione SAML è utilizzata, all'interno del sistema di autenticazione e autorizzazione, per descrivere le informazioni di sicurezza scambiate tra le varie entità (authority, SP, ecc.) presenti nei vari domini informatici definiti in questo documento. In particolare, i vari certificatori di ruolo (attributo) e d'identità sono visti come server SAML, in grado cioè di ricevere delle richieste secondo il protocollo definito dallo standard. Essi forniscono in risposta una o più asserzioni di autenticazione o attributo, utilizzate per decidere sull'accesso degli utenti ai servizi disponibili. Nella seguente Figura 22 è riportato il diagramma delle classi che illustra come SAML è utilizzato dal servizio di raccolta delle certificazioni, rappresentato nello scenario di riferimento descritto nella Sezione 5.2 con il nome di Local Proxy.

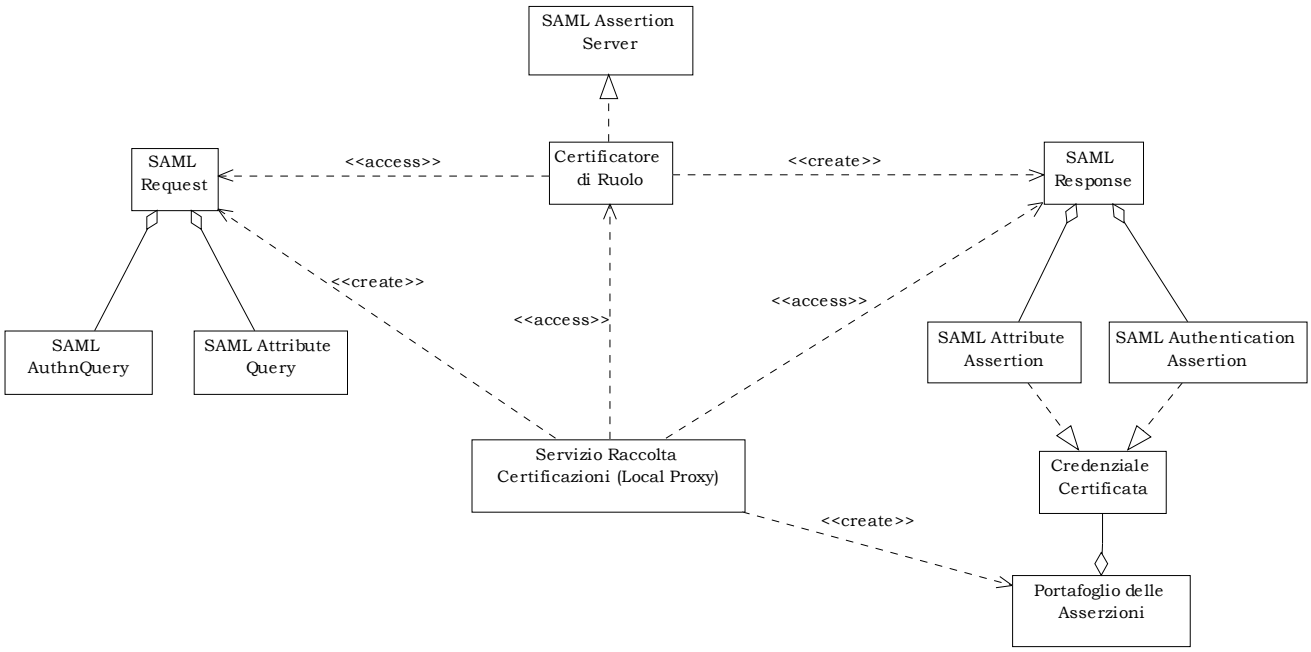

Figura 22: Entità coinvolte per la certificazione delle credenziali

Tale servizio accede ai vari certificatori di ruolo sottoponendo loro varie richieste (SAML Request) che possono riguardare sia informazioni di identificazione (SAML AuthnQuery) che di ruolo (SAML Attribute Query). I vari certificatori, ricevono tali richieste e producono delle risposte (SAML Response) contenenti sia asserzioni di autenticazione che di attributo che, insieme concorrono a formare le credenziali certificate, inserite dal proxy locale nel più volte citato "portafoglio delle asserzioni".

6.2. XACML

Lo standard XACML (eXtensible Access Control Markup Language) è un altro standard, basato su XML, definito dal consorzio OASIS e ha lo scopo di definire la sintassi e la semantica di un linguaggio per esprimere e valutare politiche di controllo di accesso. La versione attuale di questo standard è la 2.0, del Febbraio 2005. I lavori su SAML e XACML iniziarono quasi contemporaneamente, essendo visti come strettamente correlati, anche se nel seguito la loro evoluzione è proceduta in modo indipendente, anche se può esserne fatto un uso congiunto, come accade nel sistema INF-3.

Tra i principali linguaggi esistenti per la definizione di politiche di controllo di accesso, XACML si distingue per il fatto di essere stato definito come standard, versatile all'impiego in svariati campi applicativi e non è invece legato, come spesso accade per altre soluzioni, ad uno specifico contesto. Inoltre già nella sua versione base, senza necessità di particolari estensioni, il linguaggio si presenta già abbastanza flessibile e potente, supportando numerosi tipi di dato e algoritmi per combinare i risultati di differenti politiche di controllo di accesso.

Il linguaggio XACML definisce, come SAML, un protocollo di richiesta/risposta, ove le richieste indicano la volontà di accedere a particolari risorse (es. servizi). Le risposte comunicano la decisione presa, che può essere di permesso, diniego o rimanere indeterminata. Gli elementi costituenti del linguaggio XACML sono i seguenti:

- **Policy**: sono le politiche di accesso viste come insiemi di regole (rule) e algoritmi per la combinazione di regole. Lo scopo di questi ultimi discende dal fatto che, dal momento che una politica potrebbe contenere più regole, le quali potrebbero sortire decisioni diverse e contrastanti, è necessario riconciliare queste differenze nei risultati e produrre un'unica decisione finale. Esempi di algoritmi sono quello per cui se esiste nella politica anche soltanto una regola che vieta l'accesso, allora la decisione globale è di divieto.
- **Target**: è un insieme di condizioni su alcuni elementi, quali il soggetto a cui si applica la policy di cui il target è parte, la risorsa richiesta ed un'azione richiesta su tale risorsa, da parte del soggetto indicato. Tali condizioni servono per consentire di stabilire un legame tra una certa politica e una data richiesta di accesso. Se tutte le condizioni di un certo target sono soddisfatte, allora viene applicata la rispettiva regola che decide sull'accesso alla risorsa.
- **Rule**: sono le regole elementari contenute nelle politiche, definite come insieme di un target, un effetto (o decisione) e una condizione. Se la condizione è soddisfatta, viene restituita la decisione (permesso o divieto) di accesso alla risorsa indicata.
- **Policy set**: è un insieme di politiche unitamente a un algoritmo di combinazione delle decisioni prodotte dalle politiche. Ad un livello superiore viene ripetuto ciò che accade per le regole all'interno di una policy. L'algoritmo di combinazione serve per conciliare differenti risultati di diverse politiche di accesso relative alla stessa risorsa.

Oltre a tali concetti, XACML fa uso di mattoni elementari per effettuare le sue valutazioni sulle politiche, che sono attributi e valori in cui memorizzare i dati relativi ai soggetti richiedenti, alle risorse ecc., oltre ad alcune funzioni di calcolo e combinazione.

Tutti gli elementi sopraindicati concorrono alla definizione delle politiche di accesso secondo una sintassi XML definita mediante opportuni schemi nell'ambito dello standard.

La specifica XACML definisce inoltre alcuni ruoli standard, nel processo di enforcement delle politiche di accesso, necessari per l'attuazione dello stesso: i principali sono il "Policy Enforcement Point" (PEP) e il "Policy Decision Point" (PDP). Il primo riceve le richieste di accesso alle risorse protette e si preoccupa anzitutto di recuperare tutte le informazioni relative agli attributi e ruoli dei soggetti che richiedono l'accesso. Queste ultime informazioni possono essere trasferite direttamente come asserzioni SAML utilizzando uno dei profili definiti per tale standard. Lo scenario di autorizzazione, sulla base delle politiche definite in XACML, è descritto dal diagramma di collaborazione UML di Figura 23.

Una volta che il PEP è in possesso della richiesta e dell'insieme di asserzioni (portafoglio) utile a prendere una decisione sui diritti di accesso del richiedente, eventualmente accedendo anche ad altri tipi di informazioni addizionali, esso passa il controllo al PDP che si incarica di prendere tale decisione. Il PDP accede alla definizione delle politiche di controllo di accesso relative alla risorsa richiesta e le valuta rispetto alle asserzioni pervenute. Infine informa il PEP della decisione presa, in modo tale che quest'ultimo consenta o neghi l'accesso al richiedente. Tale scenario è riportato nel diagramma di collaborazione seguente.

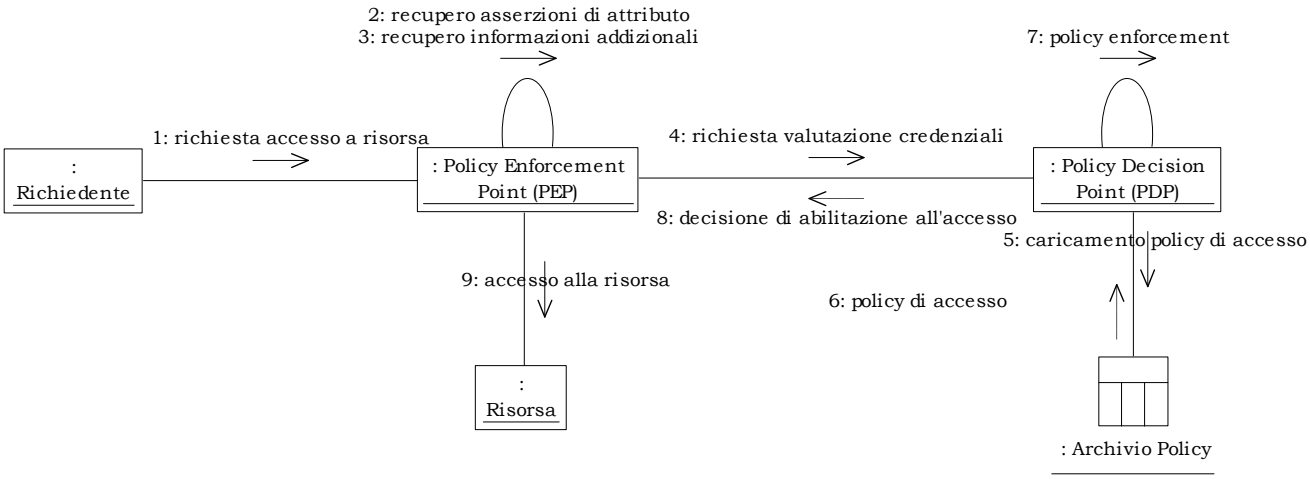

Figura 23: Policy enforcement mediante XACML

6.2.1. Implementazione Sun XACML

Esistono pochi strumenti software disponibili per sfruttare appieno le potenzialità di questa specifica. Uno dei più completi è realizzato da Sun Microsystems, che ha realizzato una prima versione di una API open source in linguaggio Java per il supporto alla specifica XACML 1.x (1.0 e 1.1). È richiesta una versione 1.4.0 o successiva del linguaggio Java per il corretto funzionamento e utilizzo dell'API. Nel Gennaio 2005 questa libreria è stata estesa con il supporto di alcune caratteristiche della versione 2.0 del linguaggio. È reperibile tramite il circuito SourceForge, all'URL http://sunxacml.sourceforge.net.

6.2.2. *Uso di XACML per il sistema di autorizzazione e autenticazione federata (INF-3)*

Come illustrato nello scenario di riferimento ed in quello di cooperazione applicativa, il sistema INF-3 effettua le operazioni di autorizzazione sulla base di credenziali certificate, contenute in un portafoglio delle asserzioni, costruito dall'entità detta Proxy Locale. In tutti gli scenari, l'entità responsabile di effettuare il policy enforcement per la fase di autorizzazione e consentire o negare l'accesso ai servizi richiesti è stato indicato con il termine "Gestore delle Politiche di Autorizzazione" o GPA. A livello concettuale, tale entità svolge le funzionalità corrispondenti ai ruoli PEP e PDP definiti da XACML. Si osserva che l'uso della specifica sintassi e struttura di messaggi secondo lo standard XACML avviene a valle dell'interfaccia costituita dal PEP, in particolare per la comunicazione tra PEP e PDP e ad opera del PDP per ottenere la definizione delle politiche di controllo di accesso da altre entità. Dal punto di vista del sistema INF-3, il gestore delle politiche di autorizzazione presenta un'interfaccia in grado di ricevere il portafoglio delle asserzioni e l'indicazione su qual è il servizio a cui si intende accedere. Tali richieste non sono formattate secondo lo standard XACML che, come detto, interviene dopo. L'effettiva progettazione e implementazione del GPA non è tuttavia in alcun modo vincolata da quanto definito dalla specifica XACML, salvo per il protocollo di comunicazione con cui il GPA richiede al proxy locale le asserzioni di attributo. Essendo il proxy locale un SAML server, tale protocollo dovrà conformarsi alla specifica di tale linguaggio.

7. ACRONIMI

AA	Attribute Authority (vedi anche: D*, Dominio)
AM	Access Manager (vedi anche: D*, Dominio)
CA	Certification Authority (vedi anche: D*, Dominio)
CoT	Circle of Trust
D*	Dominio, in particolare: • D_{PROF} o D_PROF: dominio di profilazione • D_F o DF: dominio fruitore • D_E o DE: dominio erogatore • D_{CERT} o D_CERT: dominio certificatore • D_R o DR o D_RIC: dominio richiedente (sinonimo di DF) • DSA: dominio dei servizi applicativi
GPA	Gestore delle Politiche di Autorizzazione (vedi anche: D*, Dominio)
LP	Local Proxy
PA	Profile Authority (vedi anche: D*, Dominio)
PDD	Porta di Dominio
PIN	Personal Identification Number
RDC	Responsabile del Dominio di Cooperazione
SFA	Sistema Federato di Autenticazione
SL_*	Semantica Locale (es. riferita allo strato INF-1 o INF-3)
SN_*	Semantica Neutrale (es. riferita allo strato INF-1 o INF-3)
SP	Service Provider (vedi anche: D*, Dominio)
UA	User Agent

8. BIBLIOGRAFIA

[1] J. Hughes and E. Maler, Security Assertion Markup Language (SAML) 2.0 Technical Overview Working Draft 06, 3 June 2005, Oasis http://www.oasis-open.org/committees/download.php/12938/sstc-saml-tech-overview-2.0-draft-06.pdf

[2] M. Gudgin et al., SOAP Version 1.2 Part 1: Messaging Framework, W3C Consortium, 24 June 2003, http://www.w3.org/TR/soap

[3] CNIPA, Specifiche della busta di e-government, 21 Aprile 2004, http://www.cnipa.gov.it/site/_files/4.SPC_Busta e-Gov v.1_0-21-04-2004.pdf

[4] ICAR-INF3, Sistema Federato Interregionale di Autenticazione: Organizzazione, versione 1.0, Ottobre 2005.

[5] T. Wason et al, Liberty ID-FF Architecture Overview, version 1.2 errata-v1.0. http://www.projectliberty.org/specs/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf

[6] CNIPA, Sistema Pubblico di Connettività e Cooperazione, "Sistema pubblico di cooperazione: Accordo di Servizio - versione 1.0", 14 Ottobre 2005. http://www.cnipa.gov.it/site/_files/SPCoop-AccordoServizio_v1.0_20051014.pdf

[7] K Lawrence, C. Kaler, D. Flinn, OASIS Web Services Security (WSS) TC, OASIS Consortium, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss