REGIONE BASILICATA

IMS Modellazione dei casi uso

ALLEGATO C07

REGIONE BASILICATA

DIPARTIMENTO PRESIDENZA DELLA GIUNTA REGIONALE
UFFICIO SISTEMA INFORMATIVO REGIONALE E STATISTICA

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

REGIONE BASILICATA

UFFICIO S. I. R. S.

Modellazione dei Casi d'Uso

Identity Management System

REGIONE BASILICATA

DIPARTIMENTO PRESIDENZA DELLA GIUNTA REGIONALE
UFFICIO SISTEMA INFORMATIVO REGIONALE E STATISTICA

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Controllo del documento

Identificazione documento

Titolo	Tipo	Identificatore	Nome *file*
IMS	Modellazione dei Casi d'Uso	IMS1.0	IMS_ Modellazione dei Casi d'Uso _ Marzo 2009

Approvazioni

	Nome	Data	Firma
Redatto da:	Dott.ssa Domenica Sileo	14/01/2009	
Revisionato da:	Dott. Maurizio Argoneto	15/01/2009	
Approvato da:	Dott. Giuseppe Bernardo (SI)	15/01/2009	

Variazioni

Versione	Data	Autore	Paragrafi modificati
1.1	06/2009	Dott.Maurizio Argoneto	2, 5, 5.7, 5.8

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Distribuzione

Copia No.	Nome	Locazione
1		
2		
3		
4		
5		
6		

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Indice

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

1. Introduzione

L' Autenticazione è la verifica dell' identità dichiarata da un soggetto. Tramite l'autenticazione il soggetto ricevente è sicuro sull' identità del soggetto mittente (e quindi che un impostore non si spacci per il mittente e trasmetta informazioni non vere) e viceversa il soggetto mittente è sicuro sull' identità del soggetto destinatario (e quindi che un impostore non si spacci per il destinatario e riceva informazioni non destinate a lui).

L' Autorizzazione è la determinazione, se ad un soggetto che richiede dati e/o servizi (in generale l' accesso ad una risorsa) è permesso il diritto a fare quella richiesta. In generale ad ogni soggetto sono concessi dei diritti, ad ogni risorsa sono associate delle liste di diritti (ACL, Access Control List) e quindi il processo di autorizzazione consiste nel verificare la corrispondenza tra i diritti concessi al soggetto ed il tipo di richiesta che il soggetto sta eseguendo. Una ACL è una lista dei soggetti autorizzati, in cui per ognuno sono specificati i rispettivi diritti. Il problema dell'autorizzazione è spesso identificato con quello dell'autenticazione: i protocolli per la sicurezza standard (ad esempio SSL) si basano su questo presupposto. Comunque, vi sono casi in cui questi due problemi vengono risolti con strategie differenti. Un esempio di tutti i giorni è il controllo di accesso. Un sistema di elaborazione, progettato per essere usato soltanto da utenti autorizzati, deve essere in grado di rilevare ed escludere i non autorizzati. L'accesso ad esso, dunque, viene garantito solo dopo aver eseguito con successo una procedura di autenticazione. Nel contesto dell'IT, sono stati sviluppati dei metodi crittografici (vedi firma digitale) i quali, per ora, non sono raggirabili se (e solo se) la chiave originaria, utilizzata per cifrare l'informazione, non e' stata compromessa. Questi ottimi metodi sono, almeno per ora, considerati inattaccabili. Ma non c'è, però, la certezza che essi rimangano "sicuri" per sempre. Imprevisti sviluppi matematici futuri, potrebbero rendere vulnerabile l'intera generazione moderna di algoritmi di cifratura, mettendo in seria discussione tutto ciò che è stato autenticato in passato. In particolare, un contratto digitalmente firmato non avrebbe più alcun valore nel caso che il sistema crittografico di base fosse stato 'bucato'. Particolarmente impegnativo è il compito di progettazione di una strategia di autenticazione e autorizzazione

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

per le applicazioni Web distribuite. La definizione di una tale strategia in modo appropriato nelle prime fasi di sviluppo dell'applicazione consente di ridurre molti gravi rischi in termini di protezione. Dal momento che i Web Service sono diventati un metodo molto diffuso per l'integrazione dei sistemi, i servizi sono ora esposti a Internet per l'uso da parte di clienti, partner commerciali ecc...
I requisiti operativi di questi servizi sono aumentati, e la sicurezza è spesso il più urgente di questi requisiti. Di conseguenza, il controllo e la revisione degli accessi è divenuto un punto cruciale nella costruzione di sistemi software distribuiti orientati al servizio.
L' Authentication and Authorization Infrastructure (AAI), è un meccanismo che mi permette l'autenticazione e l'autorizzazione di un utente (client) che richiede un particolare servizio ad una struttura ospitante (server) attraverso un' infrastruttura middleware che si pone fra client e server (che non hanno quindi visibilità diretta). La struttura ospitante quindi verificherà la legittimità di tale richiesta e si comporterà di conseguenza (permettendo o meno l' accesso a tale risorse).
AAI semplifica le procedure per tutte le parti coinvolte:

1. L'utente si registra, ma una sola volta, presso la sua cosiddetta Home Organization (cioè un rappresentante delle comunità di utenti come un' università, biblioteca, ospedale universitario, ecc.); la Home Organization è responsabile dell'archiviazione e dell' aggiornamento delle informazioni sull'utente.
2. L'autenticazione viene sempre effettuata dalla Home Organization dell'utente,la quale fornisce alla risorsa anche dati supplementari sull'utente, su richiesta della risorsa e con il consenso dell'utente. In tal modo, l'utente dispone di tutte le risorse abilitate AAI mediante una sola serie di credenziali. Inoltre per la risorsa, non è necessario disporre di un operatore per la registrazione dei nuovi utenti, poiché le informazioni richieste provengono direttamente dalla Home Organization dell'utente.

In base alle informazioni raccolte sull'utente, la risorsa decide se consentirne o meno l'accesso.
Shibboleth è un progetto Open Source orientato alla creazione di un'architettura per la Federated identity e single sign-on (SSO). Ciò significa che i membri all'interno della stessa federation possono condividere identity information,

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

accordarsi su una serie comune di policies, e creare un rapporto di fiducia (trust relationship). Shibboleth è progettato per essere utilizzato in browser Web, e controllare se un membro che naviga con il browser è autorizzato ad accedere ad una risorsa dislocata presso un'altra organizzazione, in base alle informazioni sull'utente che la home institution è riuscita ad ottenere. Shibboleth è basato su standard, costruito su SAML (attualmente in versione 2.0).

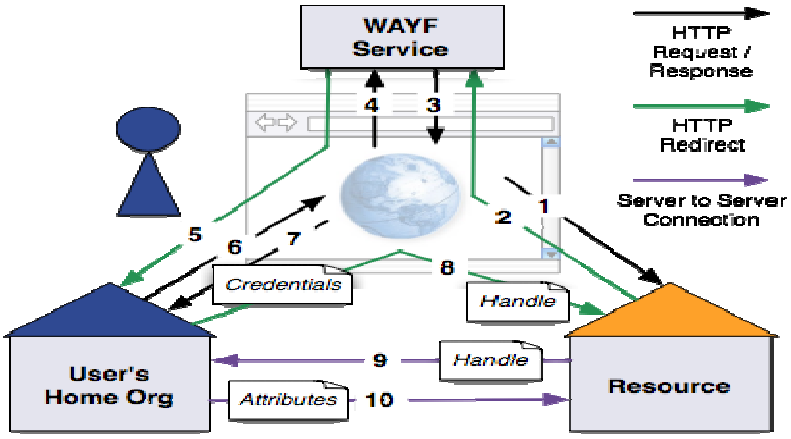
Tramite Shibboneth quando un membro di una federazione desidera accedere ad una risorsa all'interno della stessa federation, si autentica una sola volta al proprio Identity Provider (IdP). A questo punto, il suo IdP invia al Service Provider (SP) della risorsa un'asserzione SAML contenente gli attributi dell'utente. In base a questi attributi, il SP potrà consentire o negare all'utente di eseguire l'azione con la risorsa remota. Per esempio, l'utente può avere due attributi: si potrebbe dire che è uno studente dell'istituzione I, e un'altro che è registrato nel corso C. Se la security policy del SP stabilisce che gli studenti appartenenti all'istituzione I o che seguono il corso C (o che hanno entrambe le condizioni allo stesso tempo) possono utilizzare le risorse, allora il SP dovrà concedere loro l'accesso alla risorsa richiesta.

In pratica Shibboleth permette, in un contesto federale, di gestire i processi di autenticazione e autorizzazione tra un utente, la sua organizzazione di origine e la risorsa web a cui l'utente vuole accedere.

L'access management in Shibboleth è sostanzialmente gestito da tre elementi:

- un Identity Provider (IdP), gestito per esempio da un'università, che effettua l'autenticazione per i propri utenti e rilascia gli attributi, ossia le informazioni, relative a quest'ultimi a un Service Provider;
- un Service Provider (SP), ossia la risorsa web, per esempio il sito di un editore che, interagendo con l'IdP, accetta l'autenticazione proveniente da quest'ultimo e permette all'utente di usufruire di un servizio;
- un discovery service, denominato WAYF (Where Are You From), che, interpellato dall'SP, ha il compito di ridirigere l'utente sull'Idp di appartenenza, in modo che questo si possa autenticare correttamente e usufruire poi del servizio scelto.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it



La figura di cui sopra, può dare un'idea di come avvengano le cose. Nella figura, "Resource" identifica l'SP, "User's Home Org" l'IdP e il browser al centro
identifica l'utente. Seguendo le frecce si può individuare il percorso di autenticazione di un utente che vuole accedere a una risorsa:

- la richiesta (1) viene rediretta dal servizio web (SP) al sistema di WAYF (2);
- il WAYF, interagendo con l'utente (3 e 4), lo ridirige sull'Identity Provider scelto (5);
- il IdP provvede all'autenticazione (6 e 7);
- l'utente, questa volta autenticato, è indirizzato alla risorsa (8);
- il SP con una serie di connessioni (9 e 10) trasparenti all'utente, recupera dall' IdP tutti gli attributi relativi all'utente stesso.
  È interessante sottolineare alcuni concetti chiave posti alla base di una federazione Shibboleth-based:
- per lo scambio delle informazioni (i famosi attributi utente) nei processi di autenticazione e autorizzazione Shibboleth utilizza il protocollo SAML (Security Assertion Markup Language). SAML, sviluppato dalla OASIS Security Services, è in sintesi lo standard XML per lo scambio di dati sensibili, che si è imposto negli ultimi anni sulla scena internazionale;
- l'autenticazione federata presuppone una definizione di policy e standard, sia a livello legale che a livello tecnico (scambio di

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

attributi utenti con politiche di rilascio e accettazione) a cui tutti i membri e i partner della federazione devono sottostare.

In Shibboleth i componenti più rilevanti sono (Shibboleth prevede due implementazioni, una per essere incluso nell'identity provider e l'altra nel service provider):

- Identity Provider: autentica i principals e carica gli attributi, che sono rappresentati come SAML assertions. Ogni principal di una federation deve essere registrato in un IdP di quella federation.

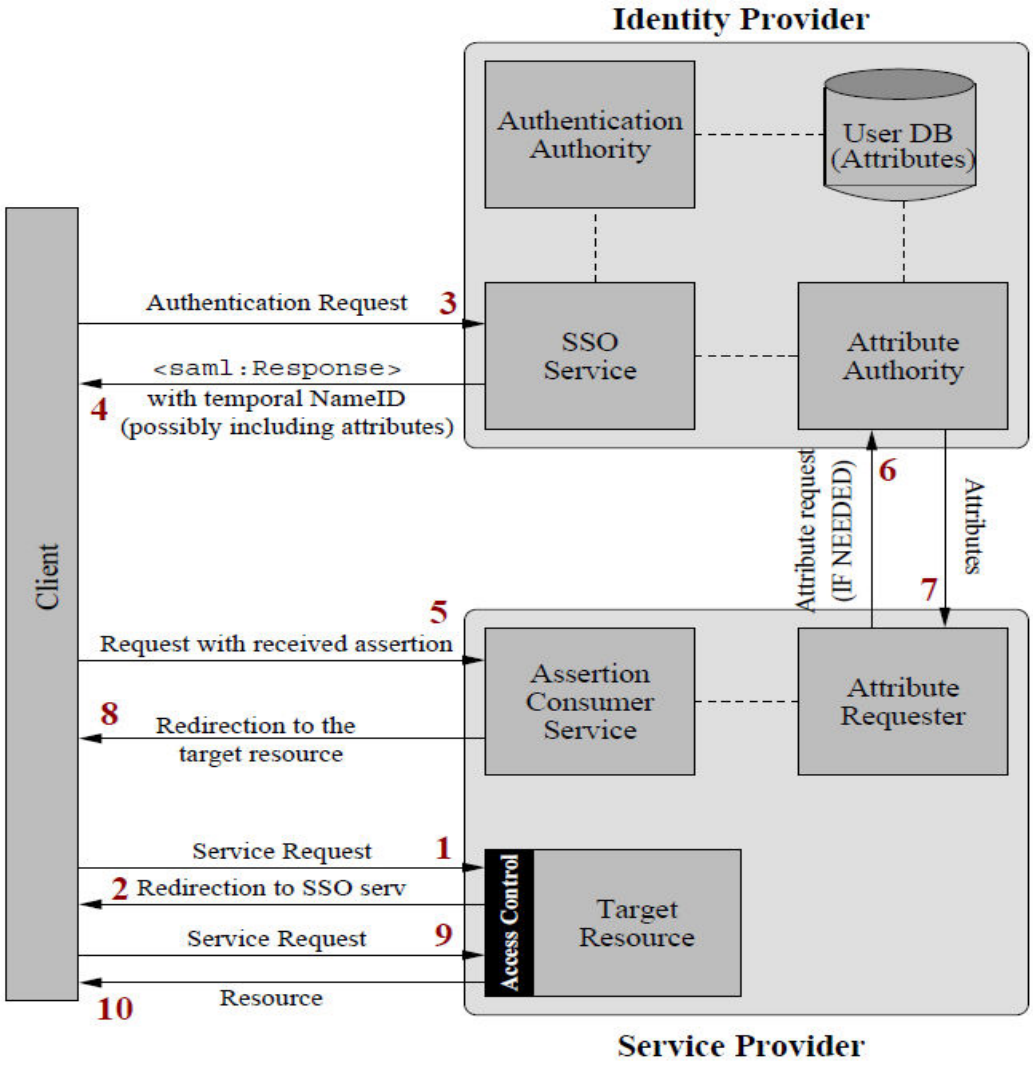
Tre entità vengono distinte nell'IdP:

- Authentication Authority: concede authentication assertions ai principals. Quando un principal è autenticato, l'IdP dà una temporal "random" identity, che sarà il contenuto della field NameIdentifier nell'assertion. Questo temporal ID è chiamato Shibboleth handle. Il motivo dell'utilizzo di questo temporal ID, invece del nome dell'utente (ad es. "nome@ita.it"), è di mantenere la Privacy: l'IdP mappa internamente il random ID con il nome reale, ma la SP non sarà in grado di conoscere il nome dell'utente a meno che non sia autorizzata dall'utente stesso. Poi, il SP sarà in grado di chiedere all'IdP gli attributi di un temporal ID, e l'IP risponderà con gli attributi dell'utente corrispondente. In alternativa, l'Authentication Authority competente può includere gli attributi quando invia il messaggio di risposta dopo l'autenticazione, in aggiunta all'authentication statement (questo metodo è chiamato "attribute push"). Shibboleth non specifica quale metodo deve essere usato per l'autenticazione degli utenti. Sarà il protocol implemented nell'IdP a specificarlo (es., che potrebbe essere Kerberos, PKI, ecc.).
- Attribute Authority: controlla gli attribute assertions per un utente specifico sotto richiesta dello SP (per concedere un handle). Gli attributi di ogni utente saranno immagazzinati internamente nell'IdP, per esempio in una base di dati.
- Single Sign-On Service: Processa le richieste di autenticazione ricevute dai SP attraverso il web browser. Esso è l'entity che inizia il processo di autenticazione.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

- Service Provider: dove sono situate le risorse. Fornisce un security context per il servizio richiesto, che dà l'accesso alle risorse tramite un meccanismo di controllo delle informazioni per consentire o negare l'accesso alla risorsa. Le tre parti principali della SP sono:
  - Assertion Consumer Service: riceve l'authentication assertions generata dall'Authentication Authority dell'IdP competente, e dopo aver richiesto gli attributi dell'utente se necessario, crea un security context per l'utente sul SP.
  - Attribute Requester: Quando l'utente contatta l'Assertion Consumer Service inviando l'authentication assertion, quest'ultimo può decidere se ha bisogno di maggiori informazioni al fine di creare un security context valido (quando la SAML assertion che l'utente riceve dal suo IdP, quando l'assertion di autenticazione non contiene attributi, o per richiedere attributi supplementari a quelli necessari). L'Attribute Requester effettuerà poi lo scambio di messaggi direttamente con l'Attribute Authority dell'IdP competente, richiedendo attributi che il SP utilizzerà per decidere se l'utente deve avere accesso alle risorse o no.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it



Accesso alle risorse all'internodi una Shibboleth federation

La Figura di cui sopra illustra le azioni eseguite quando un utente richiede una risorse all'interno della stessa federation. Saranno effettuati i seguenti passi:

1. Un utente richiede una risorsa situata in un Service Provider all'interno di una federation della quale l'utente è membro. Il SP controlla se l'utente ha un security context valido (che può essere stato concesso prima in un precedente accesso dello stesso client al SP). Se esiste e se ha i necessari attributi il client riceverà la risorsa.
2. Il cliente verrà reindirizzato al suo IdP locale da dal SP.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

3. Il cliente fa una richiesta al SSO Service, specificando la risorsa. Se il principal non ha ancora un security context presso l'IdP, viene eseguita l'autenticazione e il security context viene creato. Poi, l'Authentication Authority genererà l'Authentication Statement per il client (con un temporal handle come Name ID).
4. La SSO darà una Assertion firmata al client, che contiene il suo authentication statement e includerà gli attributi.
5. Il client richiederà all'Assertion Consumer la concessione di un security context per il SP, corredandola di un'assertion ricevuta dall'IdP. L'Assertion Consumer verificherà gli statements nell'assertion. Se tutte le informazioni necessarie saranno incluse, si salterà al passo 8. Altrimenti, verrà utilizzato l'Attribute Requester per ottenere gli attributi.
6. L'Attribute Requester chiederà all'Attribute Authority alcuni attributi dell'utente (richiesti per accedere alla risorsa).
7. L'Attribute Authority otterrà gli attributi richiesti per lo specifico utente, e li restituirà al SP.
8. L'Assertion Consumer creerà un security context per l'utente al SP e reindirizzerà alla risorsa.
9. Il client richiederà il servizio nuovamente (nello stesso modo del primo step).
10. Siccome il client avrà ora un security context valido, il servizio verrà eseguito.

Tutti questi step sono eseguiti mantenendo la privacy dell'utente. Senza un meccanismo di SSO, l'utente dovrebbe mantenere un account in ogni realm dove ha accesso ad una risorsa, e fare il login ogni volta che vuole accedere ad una risorsa in un altro dominio. Shibboneth, invece, rende la gestione del lavoro di amministrazione dei realms più semplice (gli amministratori hanno solo bisogno di assistenza sugli attributi, come "PhD. student", piuttosto che sulle singole identità). L'accesso alle risorse per gli utenti diventa così più "comodo", in quanto non è necessario ricordare diversi nomi utente e password e fare login per ogni accesso. Il protocollo Shibboleth definisce i meccanismi di scambio di SAML attributes tra Identity e Service Providers, consentendo il SSO all'interno di una federation. Tuttavia, essa non specifica “standard attribute names”, ma consente ad ogni federation di definire gli attributi per essere utilizzato. Shibboleth non dice quali attributi un entity ha all'interno di una federation (ad

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

es., IDNumber, FirstName, BirthDate, …). Invece, ogni federation sceglie la serie di attributi che può essere passato ai loro subject.

1.1 Scopo del Documento

Illustrare i casi d'uso dell'applicativo e non quelli illustrati nell'introduzione che sono invece i casi d'uso che sono messi a disposizione dall'infrastruttura stessa.

1.2 Definizioni ed Acronimi

.

IP/IdP	Identity Provider. A kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles.
SAML	Security Assertion Markup Language. SAML is an XML based framework for exchanging security information.
SP	Service Provider. A role donned by a system entity where the system entity provides services to principals or other system entities, typically a web site providing services and/or goods.
SPI	Service Provider Interfaces
SSO	Abbreviation for Single Sign-On. SSO is defined as the ability of a user to authenticate once and gain access to a variety of web application resources that otherwise would have required individual authentication, with each authentication potentially requiring different set of credentials.

1.3 Riferimenti

[1] Sito di AAI URL: http://www.switch.ch/aai/docs/AAI-Flyer_en.pdf
[2] Sito di Shibboleth ProjectURL: http://shibboleth.internet2.edu/about.html
[3] Sito Standard SAMLURL: http://www.oasis-open.org/committes/security
[4] SWITCH WAYF URL: http://www.switch.ch/aai/wayf
[5] Sito di JISC URL: http://www.jisc.ac.uk/whatwedo/theme s/access_management.aspx

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

1.4 Overview

[Questa sezione riporta cosa il documento contiene e come sono organizzati i contenuti.]

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

2. Attori

Cittadino: utente che accede ad una risorsa protetta dall'autenticazione dell' IMS;

Dipendente: dipendente della regione basilicata che accede ad una risorsa protetta dall'autenticazione dell' IMS;

Operatore/Agente Software: utente che effettua il deploy e la manutenzione di un'applicazione web deployata sotto l'IMS;

Amministratore: utente che gestisce le applicazioni e il sistema, che definisce i ruoli e gli utenti, he associa quest'ultimi ai serivizi disponibili

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

3. Casi d'Uso

Assegnazione di Requisiti ad Attori e Casi d'Uso			
Id. Requisito	Requisito	Attore	Caso d'Uso
01	Nessuno	Cittadino	Accesso Risorsa Protetta
02	Nessuno	Cittadino	Global Logout
03	Nessuno	Cittadino	Accesso Mypage
04	Nessuno	Cittadino	Accesso ai servizi tramite la MyPage
05	Nessuno	Operatore/Agente	Registrazione Identity Provider sul SamlEngine
06	Nessuno	Operatore/Agente	Registrazione Service Provider sul SamlEngine
07	Nessuno	Operatore/Agente	Registrazione Service Provider sull'Identity Provider
08	Nessuno	Amministratore	Amministratore effettua l'accesso all'Ibasho Manager
09	Nessuno	Amministratore	Inserimento nuovo utente dall'Ibasho Manager
10	Nessuno	Amministratore	Associazione degli utenti ai servizi
11	Nessuno	Amministratore	Associazione degli utenti alle categorie
12	Nessuno	Amministratore	Definisce e scrive Policy secondo lo standard XACML
13	CU12	Amministratore	Caricamento della Policy relativa al servizio
14	CU03	Cittadino	Richiede una risorsa presente nella MyPage

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

			(implicitamente controllo della Policy tramite PolicyEngine)
15	CU14	Cittadino	Accreditamento implicito ad un servizio

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

4. Diagramma dei Casi d'Uso

Nessun diagramma prodotto

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

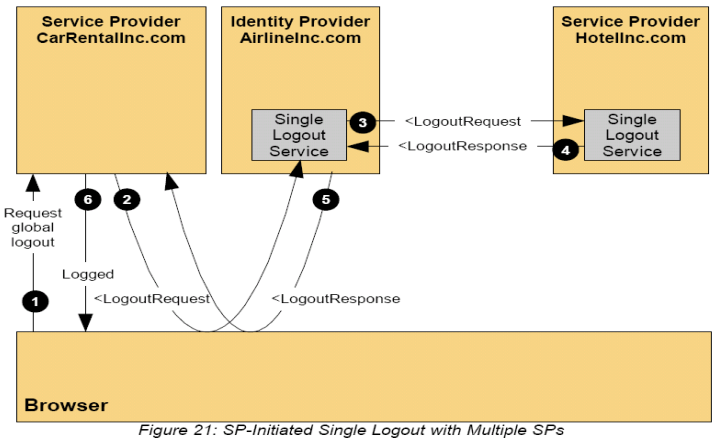
5. Documentare i Casi d'uso

Nel seguito verranno descritti i casi d'uso elencati nel paragrafo precedente

5.1 Informazioni di Base

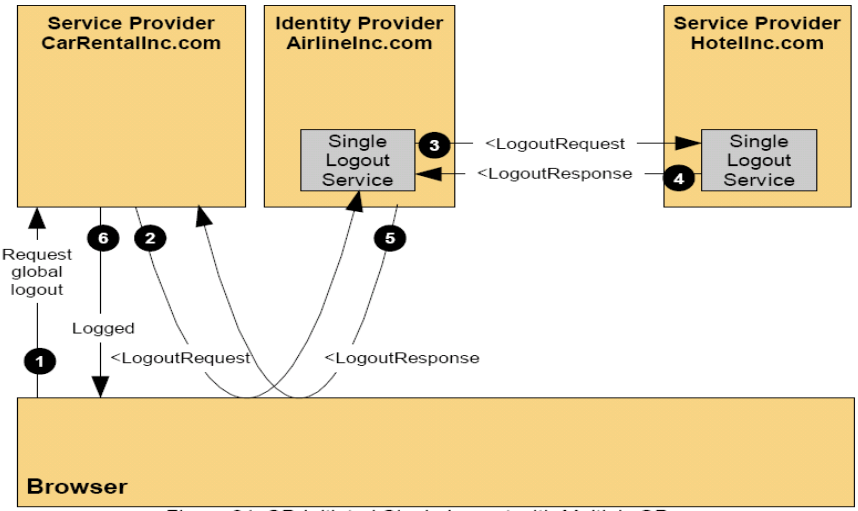
Caso d'Uso: CU01 - Accesso Risorsa Protetta	
Breve Descrizione	Il cittadino nel momento in cui tenta di accedere ad una risorsa web che si trova protetta dal sistema IMS verrà coinvolto, in modo totalmente trasparente, in un flusso di scambio di dati tra tutti i moduli che compongono il sistema d'identità atto a verificare l'accreditamento del cittadino o inoltre l'eventuale richiesta di autenticazione all' Identity Provider deputato a questa funzione.
Attori	Cittadino
Pre-Condizioni	Nessuna
Flusso Principale	1. Utente richiede una risorsa non autenticato 2. Redirezione tramite WAYF al Single Sign-On (SSO) Service [SP] 3. Richiesta del Servizio di SSO con SAMLRequest 4. Utente inserisce credenziali valide al sistema [IdP] 5. IDP costruisce l'asserzione SAML che contiene le info sull'utente loggato 6. Il sistema redirige l'utente alla risorsa richiesta [SP] 7. Un controllo di accesso verifica il rapporto Utente/SP

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

	 *Figure 21: SP-Initiated Single Logout with Multiple SPs*
Flussi Alternativi	Non ci sono flussi alternativi
Post-Condizioni per Successo	L'utente è in grado di accedere ad una risorsa protetta attraverso la MyPage
Post-Condizioni per Fallimento	Il fallimento in questo caso farebbe emergere delle lacune di carattere infrastrutturale molto importanti che comporterebbero una rivisitazione della bontà del progetto OpenSource utilizzato come base per questa soluzione.
Estende il Caso d'Uso	Non estende nessun caso d'uso
Specializza il Caso d'Uso	Non specializza nessun caso d'uso

Caso d'Uso: Cu02 - Global Logout	
Breve Descrizione	L'utente una volta autenticato presso l 'IMS ed aver acceduto alle applicazioni web a cui è stato autorizzato potrà richiedere un Global Logout che gli permetterà di terminare tutte le sessioni attive che lo riguardano e cioè effettuare il log out da tutte le applicazioni web a cui aveva acceduto tramite IMS.
Attori	Cittadino
Pre-Condizioni	Essere riconosciuto ed autenticato presso il sistema
Flusso Principale	1. Richiesta di Global Logout 2. Invio di una LogoutRequest dal SP all'Idp 3. IdP invia una LogoutRequest a tutti i SP che gestisce

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

	4. SP effettua Logout e invia una risposta all'IdP 5. IdP elabora tutte le risposte degli SP e risponde con successo 6. IdP notifica risultato dell'avvenuto Logout all'utente  *Figure 21: SP-Initiated Single Logout with Multiple SPs*
Flussi Alternativi	Non ci sono flussi alternativi
Post-Condizioni per Successo	L'utente è uscito correttamente dalla sessione autenticata precedentemente attivata
Post-Condizioni per Fallimento	Il sistema non effettua il logout e l'utente continua ad avere una sessione aperta presso IMS, che scadrà automaticamenta nel momeno del Timeout del server o della chiusura del Browser
Estende il Caso d'Uso	Non estende nessun caso d'uso
Specializza il Caso d'Uso	Non specializza nessun caso d'uso

Caso d'Uso: CU03 - Accesso Mypage	
Breve Descrizione	Il cittadino che effettua il login tramite IMS accederà in automatico ad un'applicazione web protetta, applicazione di default associata ad ogni utente che utilizza tale sistema, nella quale sono presenti dei i riferimenti a tutte le applicazioni web alle quali il cittadino ha fatto richiesta di associazione o presso le quali possiede

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

	una registrazione. Questa applicazione è la porta d'ingresso personalizzata ai servizi del cittadino.
Attori	Cittadino
Pre-Condizioni	Essere riconosciuto ed autenticato presso il sistema
Flusso Principale	1. Utente accede alla risorsa protetta (CU01); 2. Effettua il login; 3. Visualizza la MyPage;
Flussi Alternativi	Non ci sono flussi alternativi al processo appena descritto
Post-Condizioni per Successo	L'utente accede all'applicazione protetta MyPage
Post-Condizioni per Fallimento	L'utente fallisce l'autenticazione
Estende il Caso d'Uso	Non estende nessun caso d'uso
Specializza il Caso d'Uso	Non specializza nessun caso d'uso

Caso d'Uso: CU04 - Accesso ai servizi tramite la MyPage	
Breve Descrizione	L'utente una volta effettuato il login si troverà ad interfacciarsi con l'applicazione MyPage la quale è la finestra di accesso a tutti i servizi a cui l'utente a diritto di accesso.
Attori	Cittadino
Pre-Condizioni	Essere riconosciuto ed autenticato presso il sistema ed aver acceduto alla MyPage
Flusso Principale	1. Utente accede alla risorsa protetta (CU01); 2. Effettua il login; 3. Visualizza la MyPage; 4. Visualizza l'elenco delle risorse (applicazioni web) disponibili; 5. Accede ad una o più risorse disponibili.
Flussi Alternativi	Non ci sono flussi alternativi
Post-Condizioni per	L'utente accede alle risorse a cui ha accesso

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Successo	
Post-Condizioni per Fallimento	L'utente non visualizza le risorse di cui dispone le autorizzazioni di accesso
Estende il Caso d'Uso	
Specializza il Caso d'Uso	

Caso d'Uso: CU05 - Registrazione Identity Provider sul SamlEngine	
Breve Descrizione	Questa seri di casi d'uso illustrano come sia possibile registrare un'applicazione web sotto l'IMS, renderla quindi protetta e abilitarne l'accesso solo a seguito del successo nell'autenticazione. Questo primo step serve per rendere visibile il modulo di gestione delle identità (IDP) al modulo che gestisce le transazioni SAML 2.0.
Attori	Operatore/ Agente Software
Pre-Condizioni	Essere in possesso di un'applicazione conforme agli standard definiti per l'IMS
Flusso Principale	1. Operatore seleziona IDP da elenco; 2. Associa Service Provider a IDP; 3. Inserisce informazioni utili al deploy attraverso interfaccia web;
Flussi Alternativi	Non ci sono flussi alternativi
Post-Condizioni per Successo	Registrazione avvenuta con successo
Post-Condizioni per Fallimento	Registrazione fallita
Estende il Caso d'Uso	Nessuna estensione
Specializza il Caso d'Uso	Nessuna specializzazione

Caso d'Uso: CU06 - Registrazione Service Provider sul SamlEngine	
Breve Descrizione	Questa seri di casi d'uso illustrano come sia possibile registrare un'applicazione web

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

	sotto l'IMS, renderla quindi protetta e abilitarne l'accesso solo a seguito del successo nell'autenticazione. In questo CU si registra l'applicazione web che si intende proteggere tramite IMS, presso il SamlEngine. In questo momento si selezionano tutte le informazioni relative all'applicazione in uso, il tipo di protocollo di comunicazione, e tutte le informazioni utili alla definizione dei certificati X5009 indispensabili nel processo di autorizzazione di accesso alla risorsa.
Attori	Operatore/ Agente Software
Pre-Condizioni	Essere in possesso di un'applicazione conforme agli standard definiti per l'IMS
Flusso Principale	1. Operatore avvia la procedura di registrazione; 2. Inserisce tutte le informazioni utili al deploy attraverso interfaccia web; 3. Genera il certificato e tutti i file necessari al funzionamento del processo definito nello scenario CU01
Flussi Alternativi	Non ci sono flussi alternativi
Post-Condizioni per Successo	Registrazione avvenuta con successo
Post-Condizioni per Fallimento	Registrazione fallita
Estende il Caso d'Uso	Nessuna estensione
Specializza il Caso d'Uso	Nessuna specializzazione

Caso d'Uso: CU07 - Registrazione Service Provider sull'Identity Provider	
Breve Descrizione	Questa seri di casi d'uso illustrano come sia possibile registrare un'applicazione web sotto l'IMS, renderla quindi protetta e abilitarne l'accesso solo a seguito del successo nell'autenticazione. In questo CU l'applicazione precedentemente abilitata e deploiata sotto l' IMS deve essere "presentata" all' IDP che avrà l'incarico di filtrare le richieste dirette verso questa specifica risorsa. In questo momento il servizio viene memorizzato come servizio disponibile presso il server OpenLDAP. Questo permetterà di vedere il servizio disponibile nella gestione dell'amministrazione e renderlo associabile ad uno specifico utente.
Attori	Operatore/ Agente Software

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Pre-Condizioni	Essere in possesso di un'applicazione conforme agli standard definiti per l'IMS
Flusso Principale	1. Operatore seleziona IDP da associare; 2. Associa Service Provider a IDP; 3. Inserisce informazioni utili al deploy attraverso interfaccia web;
Flussi Alternativi	Non ci sono flussi alternativi
Post-Condizioni per Successo	Registrazione avvenuta con successo
Post-Condizioni per Fallimento	Registrazione fallita
Estende il Caso d'Uso	Nessuna estensione
Specializza il Caso d'Uso	Nessuna specializzazione

Caso d'Uso: CU08 - Amministratore effettua l'accesso all'Ibasho Manager	
Breve Descrizione	Questi CU vedono l'amministratore coinvolto in tutte le operazioni di gestione del sistema IMS, come la definizione degli utenti, dei ruoli, l'associazione dei servizi disponibili alle risorse, l' associazione delle categorie agli utenti. In questo specifico CU l'amministratore del sistema effettua l'accesso all'applicazione web di amministrazione la console sempre passando per l' IMS in quanto anche questa applicazione è deploiata sotto l'IMS come se fosse una qualsiasi altra applicazione visibile soltanto ai cittadini con il ruolo di amministratore.
Attori	Amministratore
Pre-Condizioni	Nessuna
Flusso Principale	1. Amministratore effettua Login presso IMS; 2. Amministratore accede all'applicazione web di amministrazione;
Flussi Alternativi	Nessuno
Post-Condizioni per Successo	Accesso all'applicazione protetta di amministrazione
Post-Condizioni per Fallimento	Fallimento nell'accesso alla risorsa

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Estende il Caso d'Uso	Nessuna estensione
Specializza il Caso d'Uso	Nessuna specializzazione

Caso d'Uso: CU09 - Inserimento nuovo utente dall'Ibasho Manager	
Breve Descrizione	Questi CU vedono l'amministratore coinvolto in tutte le operazioni di gestione del sistema IMS, come la definizione degli utenti, dei ruoli, l'associazione dei servizi disponibili alle risorse, l' associazione delle categorie agli utenti. In questo specifico CU l'amministratore del sistema inserisce e gestisce tutte le utenze presenti sotto il server OpenLdap configurato per lavorare in accoppiamento con il sistema delle identità in fase di sviluppo.
Attori	Amministratore
Pre-Condizioni	Nessuna
Flusso Principale	3. Amministratore effettua Login presso IMS; 4. Amministratore accede all'applicazione web di amministrazione; 5. Amministratore seleziona la funzione di visualizzazione degli utenti; 6. Amministratore inserisce nuovo utente;
Flussi Alternativi	Nessuno
Post-Condizioni per Successo	Inserimento utenti
Post-Condizioni per Fallimento	Fallimento operazione d'inserimento
Estende il Caso d'Uso	Nessuna estensione
Specializza il Caso d'Uso	Nessuna specializzazione

Caso d'Uso: CU10 - Associazione degli utenti ai servizi	
Breve Descrizione	Questi CU vedono l'amministratore coinvolto in tutte le operazioni di gestione del sistema IMS, come la definizione degli utenti, dei ruoli, l'associazione dei servizi

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

	disponibili alle risorse, l' associazione delle categorie agli utenti. In questo specifico CU l'amministratore del sistema dopo aver inserito e gestito le utenze, presenti sotto il server OpenLdap configurato per lavorare in accoppiamento con il sistema delle identità in fase di sviluppo, associa ad uno specifico utente un servizio disponibile, inserito nella fase di registrazione del servizio stesso.
Attori	Amministratore
Pre-Condizioni	Nessuna
Flusso Principale	7. Amministratore effettua Login presso IMS; 8. Amministratore accede all'applicazione web di amministrazione; 9. Amministratore seleziona la funzione di visualizzazione degli utenti; 10. Amministratore visualizza dettaglio di un utente; 11. Amministratore seleziona un servizio da un elenco di servizi disponibili e lo associa all'utente per il quale ha richiesto la visualizzazione del dettaglio.
Flussi Alternativi	Nessuno
Post-Condizioni per Successo	Associazione Utente → Servizio
Post-Condizioni per Fallimento	Fallimento operazione associazione
Estende il Caso d'Uso	Nessuna estensione
Specializza il Caso d'Uso	Nessuna specializzazione

Caso d'Uso: CU11 - Associazione degli utenti alle categorie	
Breve Descrizione	Questi CU vedono l'amministratore coinvolto in tutte le operazioni di gestione del sistema IMS, come la definizione degli utenti, dei ruoli, l'associazione dei servizi disponibili alle risorse, l' associazione delle categorie agli utenti. In questo specifico CU l'amministratore del sistema gestisce le categorie di utenti, categorie che in un secondo momento, seconda fase di sviluppo, serviranno come base per discriminare alcuni servizi o diritti di accesso.
Attori	Amministratore
Pre-Condizioni	Nessuna

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Flusso Principale	12. Amministratore effettua Login presso IMS; 13. Amministratore accede all'applicazione web di amministrazione; 14. Amministratore seleziona la funzione di gestione delle Categorie; 15. Amministratore opera sulle categorie;
Flussi Alternativi	Nessuno
Post-Condizioni per Successo	Gestione delle categorie
Post-Condizioni per Fallimento	Fallimento operazione di gestione delle categorie
Estende il Caso d'Uso	Nessuna estensione
Specializza il Caso d'Uso	Nessuna specializzazione

Caso d'Uso: Cu12 - Definisce e scrive Policy secondo lo standard XACML	

Breve Descrizione	L'utente amministratore una registrato il servizio presso il manager dell'IMS si attiva per poter scrivere la policy, obbligatoria, che andrà a definire i permessi di accesso delle utenze alle risorse. Questo principio è valido solo se la redazione di questo file viene fatta seguendo le specifiche dettate da lo standard XACML 2.0. La caratteristica principale della Policy è quella di poter essere in qualche modo una BackDoor all'accesso ai servizi. Questo genere di logica è attribuita da chi scrive la logica secondo alcune logiche di combinazione ben precisi. Di seguito riportiamo i più utilizzati:
	• Permit-Overrides
	  • Nell'insieme di regole presenti in una policy, se solamente una regola ha come effetto "Permit", il risultato della combinazione delle regole deve essere "Permit".
	  • Se invece, nessuna regola ha come effetto "Deny", e tutte le altre hanno "NotApplicable", la combinazione dovrà essere "Deny".
	  • L'effetto "Permit" ha la precendeza senza riguardo ai risultati delle valutazioni di tutte le altre regole della policy.
	  • Se si riscontra un errore durante la valutazione della condizione di una regola che ha come effetto "Permit", la valutazione continua fino alla prossima regola con effetto "Permit", se non la si trova l'intera

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

policy risulterà con effetto "Indeterminate", con allegato l'appropriato messaggio d'errore.

- Gli stessi discorsi valgono nei confronti di un PolicySet e le singole Policy appartenenti.

- Deny-Overrides
  - Nell'insieme di regole presenti in una policy, se solamente una regola ha come effetto "Deny", il risultato della combinazione delle regole deve essere "Deny".
  - Se invece, nessuna regola ha come effetto "Permit", e tutte le altre hanno "NotApplicable", la combinazione dovrà essere "Permit".
  - L'effetto "Deny" ha la precendeza senza riguardo ai risultati delle valutazioni di tutte le altre regole della policy.
  - Se si riscontra un errore durante la valutazione della condizione di una regola che ha come effetto "Deny", la valutazione continua fino alla prossima regola con effetto "Deny", se non la si trova l'intera policy risulterà con effetto "Indeterminate", con allegato l'appropriato messaggio d'errore.
  - Gli stessi discorsi valgono nei confronti di un PolicySet e le singole Policy appartenenti

Ecco di seguito un stralcio del formalismo che definisce la scrittura di una Policy

```
<xs:element name="PolicySet" type="xacml:PolicySetType"/>
<xs:complexType name="PolicySetType">
        <xs:sequence>
<xs:element ref="xacml:Description" minOccurs="0"/>
<xs:element ref="xacml:PolicySetDefaults" minOccurs="0"/>
            <xs:element ref="xacml:Target"/>
<xs:choice minOccurs="0" maxOccurs="unbounded">
<xs:element ref="xacml:PolicySet"/>
            <xs:element ref="xacml:Policy"/>
<xs:element ref="xacml:PolicySetIdReference"/>
<xs:element ref="xacml:PolicyIdReference"/>
            <xs:element ref="xacml:CombinerParameters"/>
<xs:element ref="xacml:PolicyCombinerParameters"/>
<xs:element ref="xacml:PolicySetCombinerParameters"/>
          </xs:choice>
```

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

	<xs:element ref="xacml:Obligations" minOccurs="0"/> </xs:sequence> <xs:attribute name="PolicySetId" type="xs:anyURI" use="required"/> <xs:attribute name="Version" type="xacml:VersionType" default="1.0"/> <xs:attribute name="PolicyCombiningAlgId" type="xs:anyURI" use="required"/> </xs:complexType>
Attori	Amministratore
Pre-Condizioni	Non ci sono precondizioni
Flusso Principale	1. Amministratore accede al tool di scrittura che desidera sul proprio computer; 2. Amministratore definisce la policy secondo quelle che sono le tipicità della propria applicazione e decide i permessi di accesso alla risorsa sulla base dei ruoli e sulla base di specifiche condizioni create sulla base dei dati di profilazione definiti nell'IMS. Potrebbe per esempio decidere di non consentire l'accesso agli utenti che hanno meno di 18 anni etc etc; 3. La policy viene salvata nel sistema e da questo momento è pronta per essere caricata sul sistema in accoppiata con il servizio che sarà protetto appunto da questa Policy.
Flussi Alternativi	Non ci sono flussi alternativi
Post-Condizioni per Successo	L'utente è uscito correttamente dalla sessione autenticata precedentemente attivata
Post-Condizioni per Fallimento	Il sistema non effettua il salvataggio del file di policy
Estende il Caso d'Uso	Non estende nessun caso d'uso
Specializza il Caso d'Uso	Non specializza nessun caso d'uso

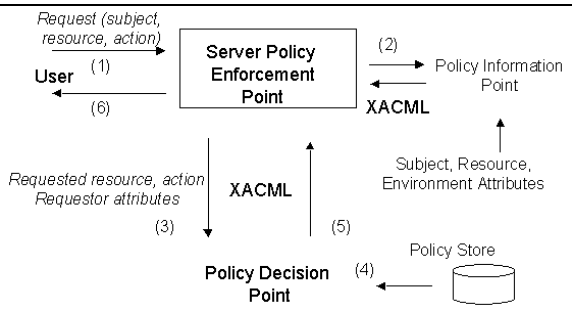
Caso d'Uso: Cu13 - Caricamento della Policy relativa al servizio

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

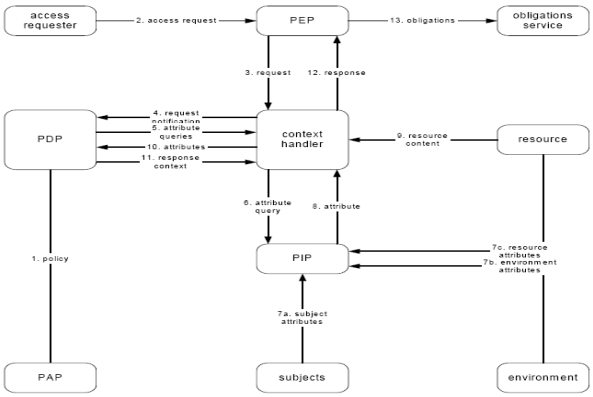
Breve Descrizione	L'utente amministratore una registrato il servizio presso il manager dell'IMS si attiva per poter caricare la policy, obbligatoria, che andrà a definire i permessi di accesso delle utenze alle risorse. Questo principio è valido solo se la redazione di questo file viene fatta seguendo le specifiche dettate da lo standard XACML 2.0
Attori	Amministratore
Pre-Condizioni	Essere riconosciuto ed autenticato presso il sistema e tutto quello previsto nello scenario descritto da CU12
Flusso Principale	1. Amministratore accede al pannello di gestione dei servizi; 2. Amministratore accede in modifica sui dati del servizio sul quale intende operare e inserisce la Policy nel sistema; 3. La policy viene salvata nel sistema e da questo momento ad ogni accesso alla risorsa il sistema controllerà la validità dell'incrocio dei dati di richiesta con la policy appena salvata. 4. Amministratore effettua logout.
Flussi Alternativi	Non ci sono flussi alternativi
Post-Condizioni per Successo	L'utente è uscito correttamente dalla sessione autenticata precedentemente attivata
Post-Condizioni per Fallimento	Il sistema non effettua il salvataggio del file di policy
Estende il Caso d'Uso	Non estende nessun caso d'uso
Specializza il Caso d'Uso	Non specializza nessun caso d'uso

Caso d'Uso: Cu14 - Richiede una risorsa presente nella MyPage (implicitamente controllo della Policy tramite PolicyEngine)	
Breve Descrizione	L'utente cittadino che accede ad un servizio nella MyPage, implicitamente deve passare per la validazione del PolicyEngine che ha il compito di valutare il matching tra la richiesta dell'utente (espressa in XACML) e la Policy definita per il servizio del quale si è cercato l'accesso. Questa valutazione avrà come risultato una condizione che determinerà l'accesso o la negazione all'accesso per la risorsa interessata.

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it



Data flow model della richiesta di accesso ad una risorsa con interessamento del PolocyEngine:



XACML Request

Questi documenti rappresentano un'ipotetica richiesta che può essere sottomessa al PDP, sulla quale vengono poi definite una o più policy.

Queste informazioni di richiesta vengono rappresentate attraverso un "contesto di richiesta".

Il documento XACML che definisce questo contesto, deve avere come root l'elemento <Request>, che rappresenta la richiesta alla risorsa.

XACML Response

Una volta che il richiedente effettua una richiesta per eseguite un'azione su di una particolare risorsa, e una volta che a questa richiesta vengono applicate delle policy dal PDP, il Context Handler deve produrre una risposta adeguata per il richiedente.

Anche la risposta è definita attraverso un documento XACML, composto dagli elementi del namespace per il contesto di richiesta (xacml:context).

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

	XACML Result L'elemento <Result> rappresenta un'unica decisione di autorizzazione per l'accesso alla risorsa specificata nell'attributo ResourceId. Un risultato può includere una serie di obblighi che devono essere rispettati dal PEP. Se il PEP non capisce o non può rispettare un obbligo deve comportarsi come se il PDP abbia negato l'accesso alla risorsa chiesta. <xs:complexType name="ResultType"> <xs:sequence> <xs:element ref="xacml-context:Decision"/> <xs:element ref="xacml-context:Status" minOccurs="0"/> <xs:element ref="xacml:Obligations" minOccurs="0"/> </xs:sequence> <xs:attribute name="ResourceId" type="xs:string" use="optional"/> </xs:complexType>
Attori	Cittadino
Pre-Condizioni	Essere riconosciuto ed autenticato presso il sistema e tutto quello previsto nello scenario descritto da CU03
Flusso Principale	1. Cittadino accede alla MyPage; 2. Cittadino accede ad un servizio al quale è interessato; 3. Il sistema tramite il PolicyEngine valuta la Request dell'utente con la Policy e "decide" se quell'utente può o non può accedere alla risorsa da lui richiesta. 4. Punto di diramazione: a. Decisione PERMIT: l'utente accede correttamente alla risorsa; b. Decisione DENY: l'utente viene respinto e non potrà accedere alla risorsa. 5. L'utente fa Logout ed esce dal sistema
Flussi Alternativi	I flussi alternativi si evidenziano nell'esito del PolicyEngine e sono descritti come "Punto di diramazione" nel flusso principale al punto 4
Post-Condizioni per Successo	L'utente è uscito correttamente dalla sessione autenticata precedentemente attivata

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Post-Condizioni per Fallimento	Nessuna
Estende il Caso d'Uso	Non estende nessun caso d'uso
Specializza il Caso d'Uso	Non specializza nessun caso d'uso

Caso d'Uso: Cu15 - Accreditamento implicito ad un servizio	
Breve Descrizione	Le strategie di accreditamento ai servizi prevedono due scenari differenti e possono essere riassunti in questo modo: accreditamento diretto e accreditamento indiretto. **Accreditamento diretto** Nel caso dell'accreditamento diretto una volta che l'utente accede e che ha superato il controllo del PDP, basato sulla validità della Policy di richiesta e sulla base della policy definita dal servizio, ha a tutti i diritti per accedere a tale risorsa e come tale deve poter essere anche registrato in modo trasparente. Per esempio se un cittadino ha intenzione di accedere alla Comunity di un sito e vuole partecipare alle attività e ai servizi esposti su tale sito, dato che tale applicazione prevede una policy di accesso a tutti i cittadini, non dovrà fare richiesta esplicita di registrazione ma la sua richiesta di autorizzazione è implicita nel controllo della policy stessa. In tale circostanza l'applicativo che viene raggiunto dal cittadino, e che quindi ha superato il controllo di sicurezza, hai due scenari complementari: 1. Il cittadino non esiste quindi viene creato sul db dell'applicativo e immediatamente viene autenticato; 2. Il cittadino già esiste e viene autenticato; **Accreditamento indiretto** Nel caso dell'accreditamento indiretto una volta che l'utente accede e si presenta come nel caso di sopra, e nelle stesse condizioni di permesso dell'accesso,l'applicativo può decidere di trattare l'accesso alla sua applicazione nel modo più "custom" possibile. Potrebbe infatti decidere di creare automaticamente un utente come "pending" nella propria applicazione, o chiedere all'utente di integrare alcuni dati di specifiche e mirata utilità. Questo perché ci possono essere dei casi in cui è necessario attribuire dei ruoli, localmente all'applicazione, al cittadino e/o al dipendente che fa richiesta di una certa applicazione e questo presupporrebbe una "mediazione" nella validazione di un utente che non è possibile definire in modo automatico e attraverso processi deterministici.
Attori	Cittadino

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Pre-Condizioni	Essere riconosciuto ed autenticato presso il sistema e tutto quello previsto nello scenario descritto da CU14
Flusso Principale: accreditamento diretto	1. Cittadino accede alla MyPage; 2. Cittadino accede ad un servizio al quale è interessato; 3. Il sistema tramite il PolicyEngine valuta la Request dell'utente con la Policy e "decide" se quell'utente può o non può accedere alla risorsa da lui richiesta. 4. Decisione PERMIT: l'utente accede correttamente alla risorsa; 5. Il cittadino raggiunge l'applicativo. A questo punto sono due i possibili scenari in cui può incappare il cittadino: a. non esiste quindi viene creato sul db dell'applicativo e immediatamente viene autenticato; b. già esiste e viene autenticato; 6. L'utente fa Logout ed esce dal sistema
Flussi Alternativi: accreditamento indiretto	1. Cittadino accede alla MyPage; 2. Cittadino accede ad un servizio al quale è interessato; 3. Il sistema tramite il PolicyEngine valuta la Request dell'utente con la Policy e "decide" se quell'utente può o non può accedere alla risorsa da lui richiesta. 4. Decisione PERMIT: l'utente accede correttamente alla risorsa; 5. Il cittadino raggiunge l'applicativo. A questo punto gli scenari potrebbero essere molteplici inquanto l'applicativo potrebbe richiedere all'utente anche informazioni aggiuntive o sottoporlo a procedure particolari che prescinderebbero dalla responsabilità del sistema di gestione delle identità: a. Procedura CUSTOM; 6. L'utente fa Logout ed esce dal sistema
Post-Condizioni per Successo	L'utente è uscito correttamente dalla sessione autenticata precedentemente attivata
Post-Condizioni per Fallimento	Nessuna
Estende il Caso d'Uso	Non estende nessun caso d'uso
Specializza il Caso d'Uso	Non specializza nessun caso d'uso

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

5.2 Scenario Base

Lo scenario base è descritto nella sequenza dei passi presente nel paragrafo precedente

5.3 Varianti allo Scenario Base

Non si riscontrano varianti rilevanti agli scenari previsti e precedentemente descritti

5.4 Interfacce Utilizzate nel Caso d'Uso

Le interfacce utilizzate sono quelle web per la parte di amministrazione della gestione dell' IMS e per la parte di interazione del cittadino e script e funzionalità manuali di modifica di file di configurazione per la parte dei casi d'uso riservata agli operatori.

5.6 Ulteriori Requisiti

Non esistono requisiti diversi da quelli già specificati

5.7 Altre Informazioni

Pianificazione	CU01 – Previsto per Giugno 2009
Priorità di Sviluppo	Molto Alta
Frequenza Prevista di Esecuzione	Ad ogni modifica

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Pianificazione	CU02 – Previsto per Giugno 2009
Priorità di Sviluppo	Molto Alta
Frequenza Prevista di Esecuzione	Ad ogni modifica

Pianificazione	CU03 – Previsto per Giugno 2009
Priorità di Sviluppo	Media
Frequenza Prevista di Esecuzione	Ad ogni modifica

Pianificazione	CU04 – Previsto per Giugno 2009
Priorità di Sviluppo	Media
Frequenza Prevista di Esecuzione	Ad ogni modifica

Pianificazione	CU05 – Previsto per Giugno 2009
Priorità di Sviluppo	Media
Frequenza Prevista di Esecuzione	Ad ogni modifica

Pianificazione	CU06 – Previsto per Giugno 2009
Priorità di Sviluppo	Media
Frequenza Prevista di Esecuzione	Ad ogni modifica

Pianificazione	CU07 – Previsto per Giugno 2009

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Priorità di Sviluppo	Media
Frequenza Prevista di Esecuzione	Ad ogni modifica

Pianificazione	CU08 – Previsto per Giugno 2009
Priorità di Sviluppo	Media
Frequenza Prevista di Esecuzione	Ad ogni modifica

Pianificazione	CU09 – Previsto per Giugno 2009
Priorità di Sviluppo	Media
Frequenza Prevista di Esecuzione	Ad ogni modifica

Pianificazione	CU10 – Previsto per Giugno 2009
Priorità di Sviluppo	Media
Frequenza Prevista di Esecuzione	Ad ogni modifica

Pianificazione	CU11 – Previsto per Giugno 2009
Priorità di Sviluppo	Media
Frequenza Prevista di Esecuzione	Ad ogni modifica

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

Pianificazione	CU12 – Previsto per Settembre 2009
Priorità di Sviluppo	Molto Alta
Frequenza Prevista di Esecuzione	Al caricamento del servizio

Pianificazione	CU13 – Previsto per Settembre 2009
Priorità di Sviluppo	Alta
Frequenza Prevista di Esecuzione	Al caricamento del servizio e ad ogni modifica delle regole del servizio

Pianificazione	CU14 – Previsto per Settembre 2009
Priorità di Sviluppo	Alta
Frequenza Prevista di Esecuzione	Ad ogni interazione dell'utente con il sistema

Pianificazione	CU15 – Previsto per Settembre 2009
Priorità di Sviluppo	Bassa
Frequenza Prevista di Esecuzione	Ad ogni accesso ai nuovi servizi installati nell'IMS

Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

5.8 Problemi Aperti

Problemi Aperti	
Id. Problema	Descrizione
01	Aumento della sicurezza relativa all'integrazione dei sistemi