REGIONE BASILICATA

IMS – Identity Management System
Documento di visione

ALLEGATO C06

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.

Documento di Vision

Identity Management System

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	Documento di Vision	IMS01	IMS_Documento Vision_Febbraio 2009

Approvazioni

	Nome	Data	Firma
Redatto da:	Dott.ssa Domenica Sileo	12/01/2009	
Revisionato da:	Dott. Maurizio Argoneto	13/01/2009	
Approvato da:	Dott. Giuseppe Bernardo (SI)	13/01/2009	

Variazioni

Versione	Data	Autore	Paragrafi modificati
1.1	05/ 2009	Dott.Maurizio Argoneto	3.1, 6
1.1	09/2009	Dott.Maurizio Argoneto	9,9.1,10.2

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

Controllo del documento iii

Identificazione documento iii
Approvazioni iii
Variazioni iii
Distribuzione iii

1. Introduzione 6

1.1 Scopo del Documento 6
1.2 Definizioni ed Acronomi 8
1.3 Riferimenti 10
1.4 Overview 10

2. Posizionamento del prodotto (sistema) 11

2.1 Opportunità di Business 11
2.2 Definizione del Problema 11
2.3 Definizione di Posizionamento del Prodotto 12

3. Stakeholder e Utenti del Sistema 13

3.1 Sintesi degli Stakeholder 13
3.2 Sintesi degli Utenti 13
3.3 Ambiente dell'utente finale 14
3.4 Problemi chiave [percepiti dagli stakeholder] / Necessità utente 14

4. Overview del Prodotto 15

4.1 Prospettive del/la Prodotto/Soluzione 16
4.2 Sintesi delle Capacità del Prodotto 16
4.3 Ipotesi e Dipendenze 17

5. Features (Caratteristiche) del Prodotto 18

5.1 Feature 1 ..... **Errore. Il segnalibro non è definito.**
5.1.1 Featue 1.1 ..... **Errore. Il segnalibro non è definito.**
5.2 Feature 2 ..... **Errore. Il segnalibro non è definito.**

6. Altri Requisiti di Prodotto 20

6.1 Standard applicabili 25
6.2 Requisiti di sistema 25
6.3 Interfaccia utente 26
6.4 Requisiti di prestazione 26
6.5 Requisiti ambientali 26

7. Vincoli 27

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

8. Precedenze e priorità 28

9. Requisiti di Documentazione 29

9.1 Manuale utente 29
9.2 Guida interattiva 29
9.3 Guida all'installazione e alla configurazione, Read Me File 29

10. Modello generale del prodotto 30

10.1 Vista logica 30
10.2 Vista fisica 31

Riferimenti bibliografici 34

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

1. Introduzione

Publisys ha analizzato nel corso di varie riunioni le esigenze regionali in materia di **autenticazione e gestione delle identità**. In particolare ha elaborato una proposta che rappresenta una possibile visione di un sistema centralizzato regionale per la gestione delle identità. Tale proposta è stata discussa nell'ambito di vari tavoli tecnici e ha avuto un generale consenso. D'altra parte si sono evidenziate alcune problematiche da gestire, in particolare riguardanti il coinvolgimento di tutte le aziende che stanno facendo lavori su questo argomento in Regione. Va evitato infatti il rischio di sovrapposizioni nel lavoro delle tre aziende e va cercato al contrario un approccio comune che favorisca la massima collaborazione e minimizzi i costi. Per cercare di arrivare presto ad una realizzazione per la Regione che soddisfi tutti i requisiti tecnici la proposta che avanziamo con questo documento include i seguenti passi:

- Implementazione del servizio di autenticazione SAML compliant per Basilicatanet. Si tratta di implementare una componente *Identity Provider* conforme allo standard SAML 2.0 da agganciare con il repository delle utenze attuali di Basilicatanet. Questa funzionalità rappresenta il primo passo indispensabile per un'evoluzione del sistema regionale di gestione delle identità. E' inoltre una componente indispensabile che permette di attivare definitivamente i portali sviluppati da Publisys. Come da nostro progetto infatti è previsto che i nostri sistemi si autentichino all'Identity provider SAML, citato fra gli standard della Regione in un documento consultato in sede di offerta (*Specifiche tecniche e funzionali del sistema di accesso ai servizi della Regione Basilicata tramite il portale Basilicatanet.it con sistemi di autenticazione forte* del marzo 2005). Allo stato attuale però si è visto che questa componente:
  - è stata sviluppata solo a livello prototipale e non è usata da alcuna applicazione in produzione
  - è comunque compatibile con una versione vecchia di SAML, ovvero la 1.1 mentre il sistema regionale dovrebbe, anche per compatibilità con gli sviluppi ICAR, essere conforme alla versione 2.0 del protocollo.

    Supporto per arrivare alla definizione dell'architettura finale. Publisys si impegna a partecipare alle riunioni di definizione delle attività necessarie a disegnare la versione finale del sistema di Identity Management regionale. L'architettura sarà elaborata con la Regione e con i suoi fornitori. Qualora emerga la necessità di sviluppare altre componenti Publisys farà per esse delle offerte specifiche. Si allega di seguito l'analisi tecnica Publisys per il sistema di Identity Management Regionale.

1.1 Scopo del Documento

Il documento rappresenta una prima analisi delle attività da compiere per riorganizzare il sistema di autenticazione regionale. I punti da considerare sono i seguenti:

a) Definizione di un sistema di autenticazione per le applicazioni web regionali: portali, siti, etc.. Il sistema esistente è legato al portale Basilicatanet in cui vi sono oltre 120.000 utenze registrate
b) b) Realizzazione di un Identity Management System regionale per consentire l'autenticazione federata in scenari di cooperazione applicativa, in conformità alle specifiche del task INF3 di ICAR. Questo sistema deve permettere ad attori riconosciuti dalla Regione di richiedere servizi tramite l'infrastruttura di cooperazione applicativa di ICAR. INF3 in particolare copre la problematica dell'autenticazione in uno scenario SPCoop di cooperazione. Tecnicamente un tale sistema di Identity Management potrebbe anche consentire il Single Sign-On web con una federazione di siti interregionali.

La natura del sistema del punto b) è ben specificata nei suoi punti essenziali nei documenti di INF3 ma vi sono anche delle parti meno chiare, tra cui:

- chi sono esattamente i soggetti che il sistema di Identity Management regionale deve contenere. Ad esempio nei principi organizzativi di INF3 (cfr. "Sistema Federato Interregionale di Autenticazione: ORGANIZZAZIONE v. 1.0") si legge che le principali tipologie di soggetti che potranno partecipare al dominio di cooperazione così come previsto in ambito SPC sono Pubbliche Amministrazioni, Imprese singole o in forma associata (consorzi, raggruppamenti..) e Soggetti privati. In quest'ultima categoria rientrano "soggetti che operano per finalità pubbliche, esercenti di pubblici servizi (es. Poste, Banche

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

tesoriere, Enel, ANAS …)" e " soggetti abilitati a cooperare con le PPAA (es. notai e geometri con Agenzia del Territorio, trasportatori con Ag. Dogane, Banche, …)". Visto che il sistema identificherà persone fisiche ciò fa sottintendere che sarà necessaria una qualche gestione dei ruoli.

- quali sono i ruoli "ufficiali" da considerare. Qualora due PA debbano interagire sarà necessario adottare una definizione di ruoli univoca o definire delle ontologie che mappino le varie definizioni regionali tra loro. Ad esempio, immaginiamo un cittadino X, categorizzato nel sistema della Basilicata come "funzionario Regione Basilicata", che voglia interagire via SPCoop con un sistema applicativo della Regione Toscana che consente l'accesso solo a utenti con almeno ruolo "direttore settore pubblico". Da qualche parte, e in qualche modo, sarà necessario fare in modo che i due sistemi capiscano che i due ruoli sono tra loro compatibili.

Il concetto di ruolo ci permette di fare una proposta in cui le due esigenze dei punti a) e b) vanno ad unirsi tra di loro. L'idea è di lavorare ad un nuovo sistema di gestione delle identità centralizzato, basato sui ruoli, in cui il navigatore web che si registra in modalità self-provisioning viene inizialmente incluso con un ruolo di default avente i più bassi diritti possibili. All'utente sarà poi data la facoltà di richiedere la "certificazione" ovvero il riconoscimento di un ruolo di livello superiore.

Il nuovo sistema di Identity Management System Regionale (IdMS) sarà quindi realizzato secondo questi principi guida

- necessità di avere un repository unico delle identità digitali della Regione, semplificando così la gestione complessiva, valorizzando al contempo il patrimonio di utenze esistente con Basilicatanet
- possibilità di gestire un passaggio "morbido" fra il "vecchio" (Basilicatanet) e il nuovo, in modo da permettere nel frattempo di adeguare le procedure esistenti ad usare una nuova logica di autenticazione
- necessità di avere un sistema di Identity Management pronto per l'integrazione con i sistemi ICAR. Possibilità di utilizzare il sistema di identity management in una federazione, sia per scenari di cooperazione applicativa ma anche per il single sign-on web fra portali di varie Regioni
- gestire con un *processo* affidabile l'attività di identificazione dell'identità di un utente (emissione di un PIN di identificazione)
- gestire processi di autenticazione "deboli" (login/password) e "forti" (login/password/PIN; smart-card con certificato digitale).
- accesso unico (web single sign-on) alle aree ad accesso controllato dei siti web regionali. Specularmente dovrà essere possibile gestire un log-out unico. Lo standard identificato a tale proposito è SAML 2.0.
- gestire in maniera centralizzata la verifica dei ruoli dichiarati dagli utenti, mediante interazione con sistemi esterni.
- gestire in maniera unificata, conforme alle direttive che emergeranno in ICAR, il concetto di ruolo degli utenti.

Il sistema conterrà una serie di utenze provenienti da fonti diverse tra loro, tra cui citiamo:

- utenti esistenti di Basilicatanet.it
- dipendenti della Regione Basilicata contenuti nel Directory Server Regionale (Microsoft Active Directory)
- dipendenti di altre Pubbliche Amministrazioni lucane
- utenti registrati in altri sistemi di identità o database di associazioni di categoria.

Se nel primo caso si può ipotizzare di mantenere una logica di registrazione in modalità selfprovisioning le altre tipologie di utenza potranno invece essere importate/sincronizzate in automatico. Per evitare il rischio di collisioni tra gli ID degli utenti si può scegliere di considerare sempre anche il dominio. Ad esempio, usando il formalismo del protocollo LDAP, questo porta ad identificare gli utenti tramite un Distiguished Name (dn) simile al seguente:

- Utente della Regione: dn: uid=nome.cognome,ou=People,dc=regione,dc=basilicata,dc=it
- Utente web: dn: uid=pippo,ou=People,dc=basilicatanet,dc=it

La logica di autenticazione, così come l'organizzazione dettagliata del repository delle utenze, dovrà essere ulteriormente raffinata ma intanto questo approccio consente di proporre una visione unificata dell'IdM regionale.

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

1.2 Definizioni ed Acronomi

CDDL	Common Development and Distribution License
Circle of Trust	A circle of trust is a group of service providers who contractually agree to exchange authentication information. Each circle of trust must include at least one identity provider, a service provider that maintains and manages identity data, and provides authentication services.
DMZ	Una DMZ (demilitarized zone) è un segmento isolato di LAN (una "sottorete") raggiungibile sia da reti interne che esterne che permette, però, connessioni esclusivamente verso l'esterno: gli host attestati sulla DMZ non possono connettersi alla rete aziendale interna. Significa letteralmente zona demilitarizzata e nel modello dei firewall indica un'area della rete che non è situata né all'interno, né all'esterno del dominio protetto. Tipicamente, ai sistemi e ai dispositivi che si trovano all'interno della DMZ viene fornito un certo livello di protezione che però non viene considerato pienamente affidabile dal dominio protetto. Server Web, server proxy e banchi di modem sono spesso dislocati nella DMZ.
FAM	Federated Access Manager
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.
JAAS	Java Authentication and Authorization Service (JEE), a set of API that enables services to authenticate and enforce access controls upon users.
J2EE Agent	A J2EE agent is capable of protecting web and enterprise applications hosted by the application or portal server on which it is installed. These applications may include resources such as HTML pages, servlets, JSP, and Enterprise JavaBeans (EJB). Apart from these resources, any resource that can be accessed as a URI within a protected web application can also be secured by such agents.
Liberty	Refers to the Liberty Alliance Project (http://www.projectliberty.org/) that provides standards specifications for protocols and frameworks to facilitate network identity based services.
OpenSSO	Alias for the Open Web Single Sign-On project. This project is an open source initiative of Sun Microsystems Inc., that provides the foundation of identity services for the web platform.
Policy	A policy defines the rules that specify a user's access privileges to a protected resource. Set of rules, subjects and constraints grouped together to define authorization permissions.
Policy Agents	Policy agents are programs that police the web server or application server that hosts protected resources.
Principal	Ogni entry (utente o server) presente nel database kerberos a cui è associata una chiave segreta.
Realm	A realm is a collection of users that are controlled by the same J2EE authentication policy. Authentication domain of manageable system entities by defined privileged administrators.
REST	

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

SaaS	Software as a Service. Modello di distribuzione del software applicativo dove un produttore di software sviluppa, opera (direttamente o tramite terze parti) e gestisce un'applicazione web che mette a disposizione dei propri clienti via internet. Is a model of software deployment where an application is hosted as a service provided to customers across the Internet.
SAML	Security Assertion Markup Language. SAML is an XML based framework for exchanging security information.
SOAP	Acronym for Simple Object Access Protocol. SOAP is an open standard protocol for exchanging XML messages over a transportation protocol, such as HTTP. SOAP forms the foundation layer of the Web Services stack, providing a basic messaging framework that more abstract layers can build on.
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.
STS	A Security Token Service addresses the interoperability problem by providing a standards-based method of converting security tokens across different formats.
Web Container	"Implements the web component contract of the J2EE architecture". This contract specifies a runtime environment for web components that includes security, concurrency, life-cycle management, transaction, deployment, and other services. A web container provides the same services as a JSP container as well as a federated view of the Java EE (formerly J2EE) platform APIs.
Web Agent	Web agents are capable of protecting resources that can be hosted on the web or proxy servers on which they are installed. This protection includes any resource that can be represented as a uniform resource identifier (URI) available on the protected server. Such a protected URI can be resolved by the server to static content files such as HTML files or dynamic content generation programs such as CGI scripts or servlets hosted by an embedded servlet engine.
Web Service	A web service is a component service or application that exposes some type of business or infrastructure functionality through a language-neutral and platform-independent, network interface;
WSC	Web Service Client
WS-I	Web Services Interoperability Organization. An open industry organization chartered to establish Best Practices for Web services interoperability, for selected groups of Web services standards, across platforms, operating systems and programming languages.
WS-I BSP	WS-I Basic Security Profile. A set of non-proprietary Web services specifications, along with clarifications and amendments to those specifications which promote interoperability.
WSP	Web Service Provider
WSDL	Web Services Description Language

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

1.3 Riferimenti

[1] Sito di AAI
URL: http://www.switch.ch/aai/docs/AAI-Flyer_en.pdf
[2] Sito di Shibboleth Project
URL: http://shibboleth.internet2.edu/about.html
[3] Sito Standard SAML
URL: 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/themes/access_management.aspx

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. Posizionamento del prodotto (IMS)

2.1 Opportunità di Business

L' opportunità di business è rappresentata semplicemente dal raggiungimento degli obiettivi di progetto definiti in BAS2009 e quindi il rispetto dei termini contrattuali definiti in tale progetto.

2.2 Definizione del Problema

Il problema che si vuole affrontare con questo progetto è quello dell'autenticazione degli utenti in modalità Web Single Sign On nell'ambito dei sistemi informativi regionali. I sistemi (o i modelli) di IM possono essere classificati in base alla specifica 'filosofia' di gestione del *trust*:

IM isolato. Corrisponde al modello di IM attualmente più diffuso (è il caso della galassia di servizi erogati dalla rete Regionale sia ai cittadini che agli utenti interni). Ogni servizio ha un proprio bacino d'utenza indipendente e a ogni utente viene assegnata una credenziale distinta per ogni servizio a cui fa accesso. Questo approccio semplifica l'IM per i Service Provider (SP), ma presenta seri problemi di usabilità per gli utenti all'aumentare dei servizi utilizzati.

IM federato. La federazione dell'identità (identity federation) si può definire come l'insieme di tecnologie, standard e accordi che permettono a un insieme di SP di accettare come validi gli identificatori utente gestiti da un'altro insieme (non necessariamente distinto) di provider, detti Identity Provider (IdP). Una tale comunità di provider (SP e IdP) viene tipicamente denominata federazione (federation) o *circle of trust*. La federazione dell'identità viene realizzata collegando i diversi identificatori utilizzati dai provider della federazione e relativi a uno stesso utente. Un tale approccio implementa implicitamente il Single Sign On (SSO), ovvero la possibilità per un utente di autenticarsi presso uno qualsiasi dei provider della federazione e, successivamente, di accedere ai servizi di tutti gli altri.

IM centralizzato. Questo modello di IM è costituito essenzialmente da un unico IdP che si occupa di identificare gli utenti per conto di una molteplicità di SP. Le informazioni costituenti l'identità digitale di un utente possono anche in questo caso essere distribuite tra i provider, ma l'identificatore a essa associato è unico e gestito dall'IdP. Come il precedente, anche questo modello permette il SSO.

Il problema di	Web Single Sign On
riguarda	Tutti i cittadini e tutti gli operatori (persone che interagiscono con i sistemi informativi regionali)
L'impatto di questo è	L'impatto è solo di carattere infrastrutturale, in quanto il sistema di gestione delle identità è "cross" a tutte le applicazioni presenti
Una soluzione di successo sarebbe	Un sistema di identità basato su standard aparte con riferimento al progetto ICAR e lo standard SAML 2.0

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

2.3 Definizione di Posizionamento del Prodotto

Per	Regione Basilicata
Chi	Snellimento del processo di autenticazione ed autorizzazione all'accesso dei servizi informativi
IMS	Identity Management System

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

3. Stakeholder e Utenti del Sistema

Non sono presenti degli Stakeholder nel senso classico del termine, in quanto questo prodotto non ha nessuna connotazione funzionale particolare ma solo aspetti infrastrutturali. Le categorie di utenti coinvolte sono quindi tutti i cittadini che includono inevitabilmente anche i dipendenti e i dirigenti della Regione Basilicata.

3.1 Sintesi degli Stakeholder

[Presentare una lista sintetica di tutti gli stakeholder identificati:]

Nome	Rappresenta	Ruolo
Cittadini	Tutti i cittadini della Regione Basilicata che hanno interesse ad interfacciarsi con i sistemi informativi regionali	I Cittadini hanno il ruolo di fruitori dei servizi informativi
Dipendenti Regione Basilicata	Tutti i dipendenti della Regione Basilicata devono utilizzare l'IMS per poter accedere ai servizi dell'ente che richiedono autenticazione.	I Dipendenti hanno il ruolo di fruitori dei servizi informativi e anche di amministratori del sistema
Affiliati/appartenenti Enti Locali	Tutti gli enti del territorio potranno avere un accesso riservato all'IMS per poter accedere ai servizi che l'amministrazione Regionale mette loro a disposizione	Gli appartenenti ad altri enti locali hanno il ruolo di fruitori dei servizi informativi

3.2 Sintesi degli Utenti

[Presentare una lista sintetica di tutti gli utenti identificati:]

Nome	Descrizione	Stakeholder
<Nome del tipo di utente>	<Descrivere brevemente cosa rappresentano rispetto al sistema>	<Elenca come l'utente è rappresentato dallo stakeholder>

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

3.3 Ambiente dell'utente finale

Le componenti del sistema saranno realizzate utilizzando varie tecnologie e sviluppi ad hoc. Le più importanti sono il Directory Server da usare come repository delle utenze più uno o più framework per l'implementazione del protocollo SAML 2.0, sia lato IP che SP. Come Directory Server si può scegliere un prodotto open source come OpenLDAP o il Fedora Directory Server. Quest'ultimo sembra essere funzionalmente più completo: è un derivato del Netscape Directory Server ed ha dei template appositi per la gestione dei ruoli, cosa comoda quindi vista l'introduzione di questo concetto nel progetto. Per quanto riguarda SAML, esistono alcune implementazioni open source compatibili con la versione 2.0 dello standard. Le più complete al momento sembrano essere:

- OpenSSO: è un framework Java della SUN per la gestione delle identità. Ha anche una libreria PHP per gestire le funzionalità di Service Provider
- Lasso: è un framework piuttosto completo, sviluppato in C con estensioni in vari linguaggi, tra cui Java, Python, Perl, PHP. E' supportato anche (sebbene parzialmente) .NET.

Il supporto di SAML 2.0 su piattaforma Microsoft va analizzato con attenzione in quanto la strategia di Microsoft è quella di appoggiare lo standard "rivale" WS-Federation (http://www.infoworld.com/article/05/11/17/HNmssaml2support_1.html), una tecnologia che è comunque supportata da OpenSSO.

3.4 Problemi chiave [percepiti dagli stakeholder] / Necessità utente

Sistema attuale	Sistema proposto
Servizi con sistemi di autenticazione specifici	"Federazione" di servizi con Single Sign On
Utenti costretti a effettuare una o più registrazioni a seconda del numero di servizi richiesti	Unica registrazione per gli utenti
Necessità di effettuare nuovamente il processo di autenticazione per accedere a più servizi	Unica autenticazione per gli utenti
Sistemi eterogenei con numerosi "point-of-failure"	Sistema a alta affidabilità (load balancing, replica multi-master,…)
Nessuna sicurezza nell'accesso alle risorse	Criteri di sicurezza applicati all'accesso alle risorse sia applicative (Policy) che sistemistiche (SSL)

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

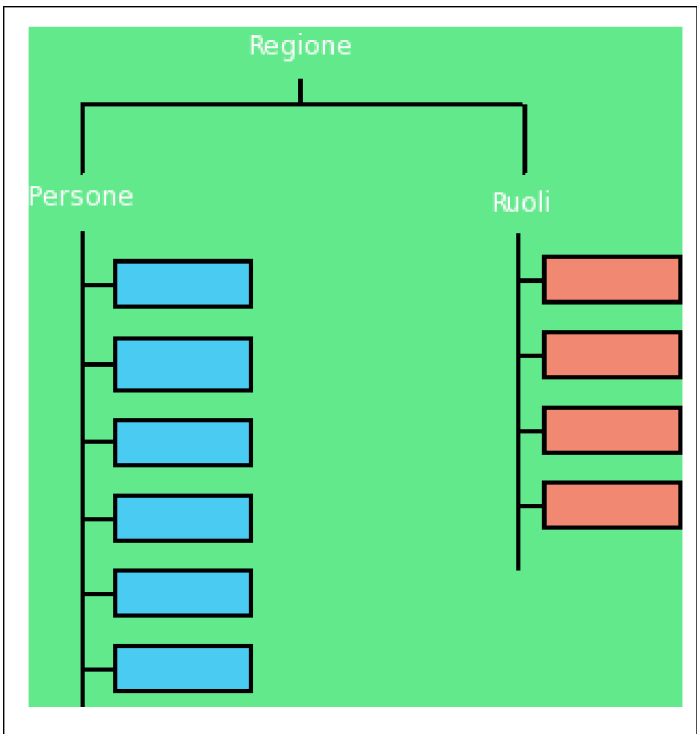
4. Overview del Prodotto

Fondamentale per implementare dei processi di e-business di una certa complessità è la necessità di accertare l'identità di un utente. Si tratta di un problema solo in parte tecnologico che è invece legato fortemente ad un processo. La distribuzione delle smart-card CIE/CNS rappresenta una possibile soluzione al problema ma va comunque considerata anche un'alternativa, da usare per quegli utenti per cui non è prevista in tempi brevi l'assegnazione di una carta. L'uso di un PIN, per rafforzare ulteriormente l'autenticazione con login e password, può essere una soluzione, tra l'altro già sperimentata in Regione per alcuni servizi (es. TriBas). Il processo deve garantire:

- l'unicità del PIN per tutti i servizi che richiedono identità forte
- la garanzia di identificare in modo certo l'utente a cui è stato rilasciato il PIN.

Il modo più sicuro per garantire l'identificazione è la distribuzione tramite pubblico ufficiale (es. tramite l'URP o l'Anagrafe del Comune di Residenza o tramite un ufficio Regionale). In questo caso il PIN, ad esempio costituito da un codice alfanumerico di 8 caratteri, potrebbe essere diviso in 2 parti. La prima metà viene inviata per posta elettronica all'utente; la seconda viene inviata, sempre per posta elettronica, ad un ufficio scelto dall'utente. Qui l'impiegato controlla il documento dell'utente con i dati indicati nella mail: in caso di riscontro positivo la seconda metà del PIN viene rilasciata.
Alla riunione del 25/7 si è anche citata la possibilità di inviare la seconda metà del PIN per posta tradizionale (strategia adottata tra l'altro dall'INPS). In questo caso è indispensabile avere un sistema automatico affidabile che controlli la correttezza delle informazioni di residenza dell'utente. Al termine del processo appena descritto l'utente acquista un Ruolo specifico (es. "Utente Certificato"). L'accesso ai servizi più delicati quindi sarà possibile solo se l'utente possiede questo ruolo e se naturalmente il processo di autenticazione con login/password/PIN è andato a buon fine. In base a quanto detto tutti gli utenti a cui viene distribuita la smart card acquisiscono automaticamente il ruolo "Utente Certificato". Approfondiamo di seguito una proposta per la gestione dei ruoli nel sistema. L'idea è mediata da un'analoga iniziativa effettuata dalla Regione Toscana in un bando del 2005. Innanzitutto a livello implementativo i ruoli saranno gestiti tramite lo stesso Directory Server LDAP che gestisce le utenze. La figura seguente mostra la strutturazione del repository LDAP. La radice dell'albero si trova, ad esempio, su “basilicata.it”, e a partire dalla radice si ha una suddivisione in due rami: ruoli e persone

- “persone” contiene le entry di tutti gli utenti registrati come indicato dalla specifica;
- il ramo “ruoli” contiene le entry che definiscono tutti i possibili ruoli che gli utenti possono assumere.



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

Il meccanismo dei ruoli oltre ad essere lo strumento utilizzato per raggruppare le entry in maniera omogenea, è essenziale nella determinazione indiretta dei ruoli, ossia la possibilità di derivare ruoli gerarchicamente inferiori contestualmente posseduti dalla singola entry. La determinazione indiretta dell'appartenenza di una entry ad un determinato ruolo può essere raggiunta utilizzando un meccanismo di incapsulamento di ruoli, che consente di creare ruoli innestati. Un ruolo innestato viene definito a partire da uno o più ruoli già esistenti applicati ad un insieme più restrittivo di entry. Ad esempio, è possibile definire il ruolo "professionista" a partire dai ruoli "avvocato", "architetto" e "medico". Questo consente di relazionare tra loro ruoli specifici unendoli in uno più generico.
E' da notare come la strutturazione ad albero dei ruoli rimanga una definizione logica che non va ad appesantire la gestione della strutturazione fisica della directory. Ad ogni utente i ruoli vengono assegnati in due modalità:

- in automatico in sede di creazione dell'utente o durante l'importazione da un repository esterno
- si lascia che l'utente indichi i suoi ruoli. Il sistema però non accetterà automaticamente le modifiche ma utilizzerà dei sistemi automatici per validare le indicazioni proposte.

Queste funzionalità sono implementate dai moduli "Gestione Ruoli" della WebGUI e "Validazione Ruoli" dello schema architetturale dell'IdMS descritto sopra. Un possibile funzionamento del sistema Web di Gestione Ruoli può essere il seguente. Intanto si tratta di un'applicazione web che deve richiedere un accesso "forte", e solo gli Utenti Certificati, in base a quanto abbiamo detto sopra, possono entrare. All'utente vengono quindi proposti i ruoli riconosciuti dal sistema. Nel momento in cui l'utente li sceglie essi non saranno automaticamente attivati ma verrà inoltrata una segnalazione al modulo "Validazione Ruoli" per far eseguire un controllo. Tale controllo dovrebbe essere possibilmente eseguito in automatico (passando via SPCoop, Web Services o legato a interazioni proprietarie con sistemi legacy, etc.): potremmo in caso prevedere anche una validazione manuale, basata sull'accettazione esplicita (in base ad workflow da definire) da parte di un responsabile. Se il processo di verifica ha successo all'utente vengono assegnati i ruoli da lui definiti; altrimenti verrà inserito in una "black-list" e il suo tentativo verrà segnalato all'amministratore del sistema. Fondamentale nella gestione dei ruoli è quindi il processo di validazione e la disponibilità di interfacce applicative autorevoli e affidabili per il controllo. Il sistema proposto dall'ufficio SIRS in questo senso può quindi costituire un punto di partenza per l'implementazione di questa funzionalità.

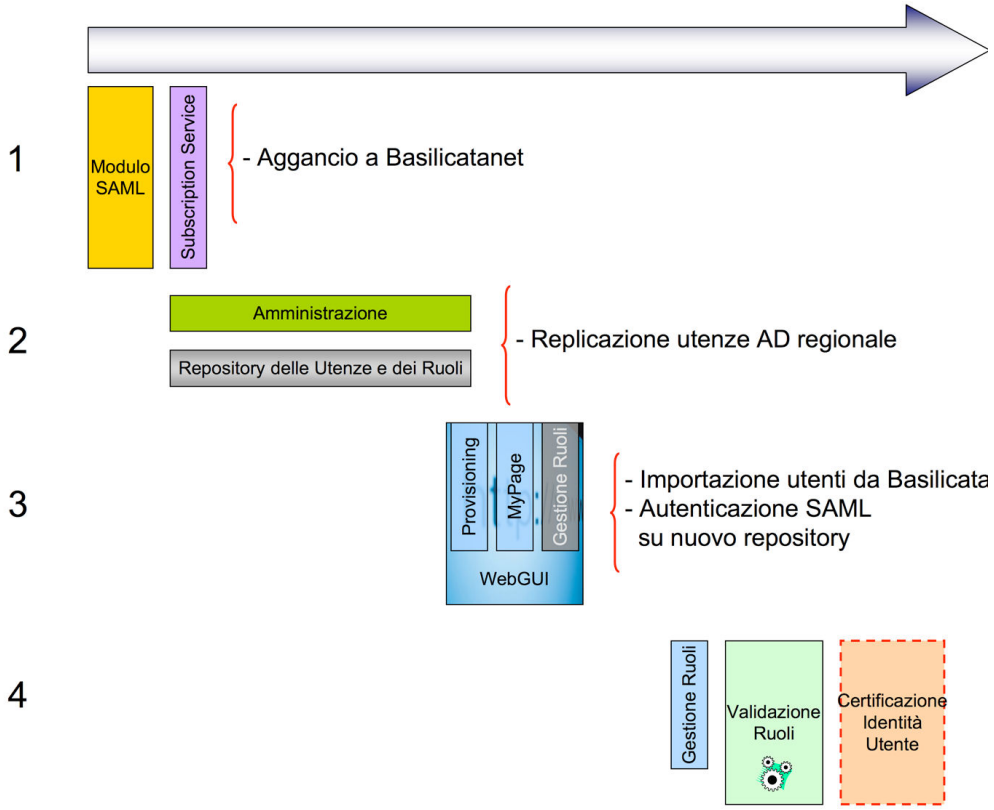
4.1 Prospettive del/la Prodotto/Soluzione

La soluzione adottata dovrà essere altamente scalabile configurabile ed integrabile con tutti i sistemi SAML2.0 Compilant per poter assolvere a pieno alle aspettativi di collettore unico delle utente, sia in termini di autorizzazione che di autenticazione ai servizi

4.2 Sintesi delle Capacità del Prodotto

L'architettura che si vuole implementare ha il vantaggio di essere modulare e di permettere perciò uno sviluppo incrementale, le cui milestone principali sono indicate nella timeline del grafico seguente.

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



Come primo passo quindi si propone di implementare il sistema di autenticazione basato su SAML che nella sua prima incarnazione si appoggerà all'attuale repository delle utenze di Basilicatanet. Verrà implementato sia il servizio di autenticazione (IP) che delle librerie di alto livello che semplificano lo sviluppo delle funzionalità lato SP. In questa prima fase verranno sviluppate due librerie, una per le applicazioni Java e un'altra per quelle .NET. Seguirà quindi un porting graduale dei meccanismi attuali di autenticazione di Basilicatanet e degli altri portali regionali per utilizzare queste librerie e la nuova logica. Nella seconda fase viene implementato il Directory Server con le funzionalità di amministrazione. La terza fase è invece quella più delicata perché prevede il passaggio in produzione del nuovo sistema e l'utilizzo esclusivo di quest'ultimo per le autenticazioni. E' indispensabile quindi che ogni sistema abbia migrato la sua logica di autenticazione. Gli utenti di Basilicatanet verranno importati nel nuovo sistema e anche la posta elettronica andrà ad autenticarsi al nuovo repository. Come dicevamo prima nel nuovo sistema gli utenti di Basilicatanet avranno nella login in automatico un suffisso "@basilicatanet.it". Modificando opportunamente le configurazioni del sistema di posta attuale (server SMTP e POP) l'aggiunta del suffisso potrebbe essere fatta automaticamente, evitando quindi di richiedere agli utenti di modificare la configurazione dei loro applicativi. A questo punto potrà anche essere attivata la sincronizzazione automatica tra l'Active Directory dei dipendenti regionali e l'IdMS regionale (funzionalità meta directory). L'ultimo passo è quello in cui viene aggiunta la gestione dei ruoli e l'attivazione del processo di verifica dell'identità di un utente.

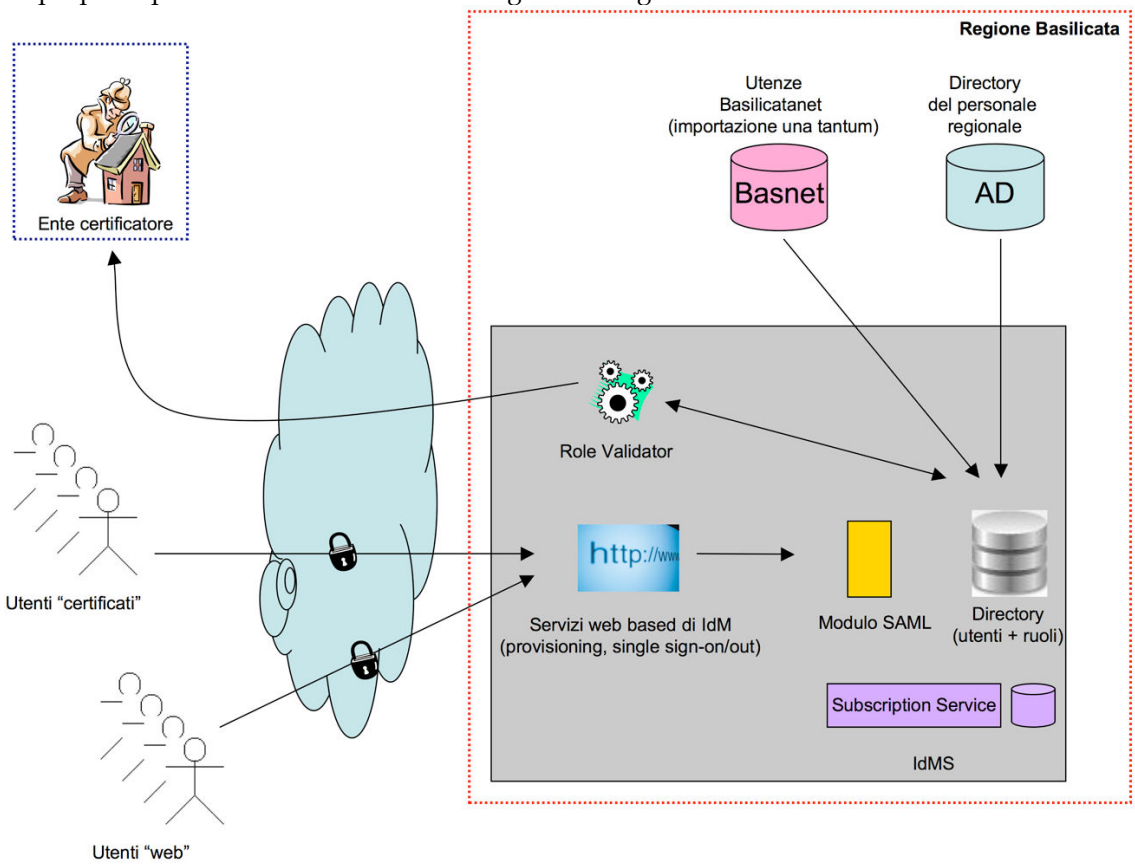
4.3 Ipotesi e Dipendenze

[Elencare tutti i fattori che riguardano le caratteristiche definite nel Documento di Visione. Elenca le ipotesi che, se modificate, produrranno cambiamenti nel Documento di Visione. Per esempio, un'ipotesi può stabilire che uno specifico sistema operativo sarà disponibile per l'hardware previsto per il prodotto software. Se il sistema operativo non è disponibile, il Documento di Visione dovrà essere cambiato.]

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

5. Features (Caratteristiche) del Prodotto

Lo scenario proposto può essere sintetizzato dal diagramma seguente:



Al centro c'è il Repository (Directory Server) che deve contenere i dati sulle persone fisiche secondo questa logica:

- informazioni necessarie per l'identificazione univoca dell'utente e per la sua autenticazione
- dati generali sull'utente: il repository deve contenere il "minimo comune multiplo" dei dati sull'utente che possono essere utilizzati dai vari sistemi che si appoggiano ad esso
- gestione dei ruoli associati all'utente.

Il repository dovrà essere unico per tutte le utenze della Regione e verrà alimentato, una tantum o di continuo, da altri sistemi regionali (in logica meta directory). Si deve appoggiare a sistemi esterni per consentire una verifica automatica dei ruoli dell'utente.

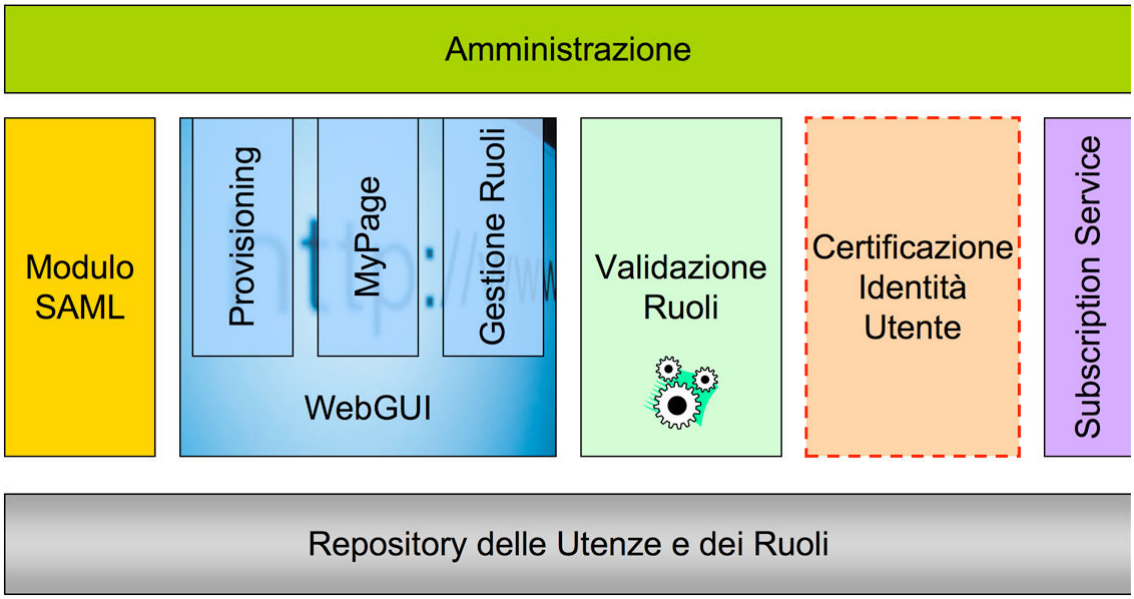
Modulo fondamentale del sistema è la componente che gestisce l'autenticazione e il web single sign on compatibile con lo standard SAML 2.0.

Il sistema avrà un'interfaccia web per consentire agli utenti:

- la registrazione in logica self-provisioning
- l'accesso ad una pagina personalizzata "MyPage" da cui poter modificare la password, i dati personali, verificare i servizi a cui è sottoscritto, ovvero i siti ad accesso controllato presso cui ha richiesto l'accesso. Eventualmente l'accesso alla MyPage è da inibire (in tutto o in parte delle sue funzionalità) per gli utenti che provengono da sistemi di autenticazione esterni (es.Active Directory Regionale). Non deve essere possibile ad esempio che un dipendente regionale possa modificare i suoi dati personali dalla MyPage: si genererebbe così una discordanza con quanto memorizzato nell'Active Directory regionale. Sul concetto di "Servizio" si rimanda alle considerazioni di un successivo paragrafo.
- la gestione dei suoi ruoli (si veda di seguito).

Trasversali alle varie funzioni ci sono poi i moduli di gestione e amministrazione. Riassumendo, le componenti del sistema sono quelle indicate nel diagramma seguente.

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



Contrariamente a quanto si possa pensare l'approccio proposto consente di essere introdotto gradualmente nell'architettura complessiva regionale, per risolvere intanto alcuni problemi di autenticazione dei portali in corso di sviluppo. Per dettagli sui passi di implementazione si veda di seguito la timeline proposta.

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

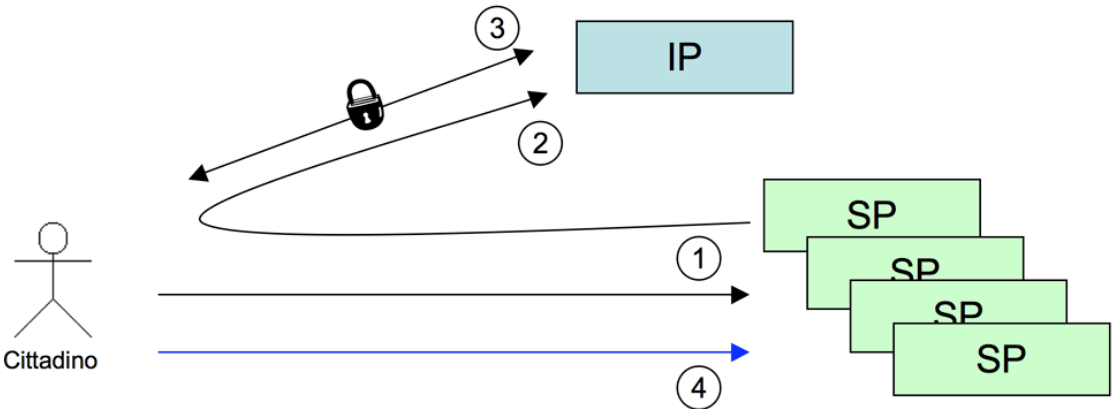
6. Altri Requisiti di Prodotto

Generalità

E' già stato concordato in varie riunioni di abbracciare lo standard SAML 2.0 per la gestione del Web Single Sign-On (SSO). Tre sono i *profili* (per usare la terminologia SAML) che vanno sicuramente implementati1:

- Web Browser SSO Profile
- Single Logout Profile
- Assertion Query/Request Profile: che permette di interrogare l'IdMS per ottenere informazioni (attributi) su un utente.

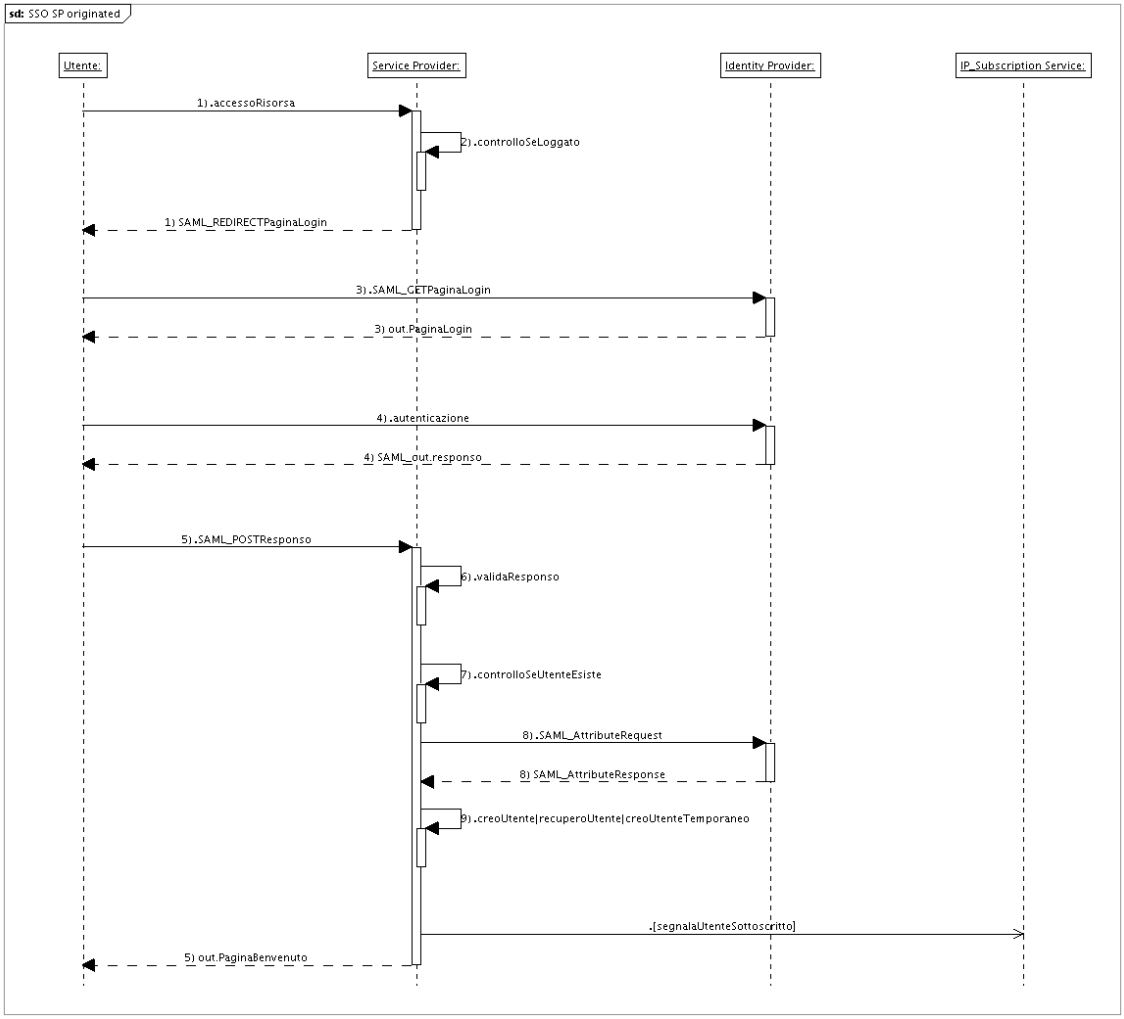
Nel linguaggio SAML si identificano l'*Identity Provider*, che certifica l'identità di un utente, e i *Service Providers*, ovvero i siti web a cui un utente vuole accedere per ottenere un servizio. Gli scenari di accesso sono di due tipi: *SP-initiated* e *IP-initiated*. Il primo caso, il più frequente, si ha quando un utente accede direttamente al SP per richiedere un servizio. Nel secondo caso invece l'utente accede prima all'IP, si autentica, e da qui accede ad uno dei vari SP disponibili. Descriviamo nel dettaglio il primo caso.



- Al passo 1 l'utente accede al SP. Il SP si accorge (secondo una sua logica personale, indipendente da SAML) che l'utente non si è autenticato.
- (passo 2) Genera allora una ridirezione HTTP (HTTP Status 302 o 303) al servizio di login dell'IP secondo le specifiche SAML. In particolare sarà specificata la richiesta di autenticazione (AuthnRequest) e verrà indicata la URL di ritorno (attributo RelayState).
- (passo 3) L'utente si autentica all'IP secondo varie logiche (ad esempio invio login/password su sessione HTTPS). L'IP, riconosciuto l'utente, produce (specifiche SAML) una pagina che contiene un form HTTP con associata un'azione POST verso il SP.
- (passo 4) L'utente accede al SP, che verifica la Response SAML ricevuta via POST e fa accedere l'utente.

Tecnicamente questo è lo scenario più semplice di accesso SAML: in alcuni casi potrà essere sostituito da una logica diversa (POST/Artifact Binding), sempre prevista dallo standard, in cui la prima richiesta tra SP e IP deve viaggiare tramite una POST e non tramite una redirect. Questo si rende necessario quando l'attributo RelayState supera gli 80 bytes previsti dalla specifica o se si vuole mescolare in una stessa interazione l'autenticazione di un utente con la richiesta di un numero variabile di suoi attributi. I passi eseguiti in questa fase di autenticazione sono descritti dal sequence diagram seguente.

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



Qui vale la pena di soffermare l'attenzione su alcuni dei passi eseguiti (chiamate 7, 8 e 9 del diagramma) che riguardano il modo in cui il SP gestisce le informazioni dell'utente, in particolare se deve memorizzare in maniera persistente i dati in una sua struttura utente. Si pensi ad esempio ad un'applicazione di Content Management (che è un SP nel nostro caso) che deve tenere traccia dei suoi utenti per associare loro le politiche di utilizzo del sistema. Si tratta ovviamente di informazioni specifiche del SP, che non devono quindi essere gestite centralmente. In questo caso il SP, dopo la fase di autenticazione SAML, deve verificare se l'utente esiste già nel suo sistema: in caso positivo recupera i dati dal proprio repository interno (*recuperoUtente*) e lo fa entrare.
Altrimenti deve creare l'utente (*creoUtente*): potrebbe a questo punto aver bisogno di alcune informazioni che richiede, sempre via SAML, all'IP. Dati ulteriori (legati alla natura specifica del SP) potranno poi ulteriormente richiesti all'utente in questo suo primo accesso. Naturalmente, per evitare problemi di disallineamento, si potrebbe scegliere di non replicare mai nei repository interni dei SP i dati gestiti centralmente dall'IP. In questo dopo ad ogni autenticazione ci sarà una richiesta SAML di attributi tra il SP e l'IP.
Nel sequence diagram è poi indicata l'ulteriore azione "SegnalaUtenteSottoscritto", tra parentesi quadre per indicare che si tratta di un'azione opzionale. E' stata introdotta per gestire il concetto di Servizio. Nel nostro caso per **Servizio** si intende essenzialmente un sito a cui un utente si iscrive. Conviene tenere traccia centralmente dell'associazione Utente <-> Servizio in modo da poter sapere sempre a cosa si è iscritto un utente. Questo è utile per vari motivi:

- motivi legati alla privacy: se un utente richiede la cancellazione dei suoi dati l'operazione deve essere ripetuta anche nei siti a cui lui si è sottoscritto se tengono traccia di sue informazioni
- sincronizzazione tra il Repository dell'IP e i SP in caso di modifica dei dati dell'utente. Il problema può essere ridotto al minimo evitando, con la modalità descritta sopra, di conservare in locale i dati dell'utente gestiti centralmente

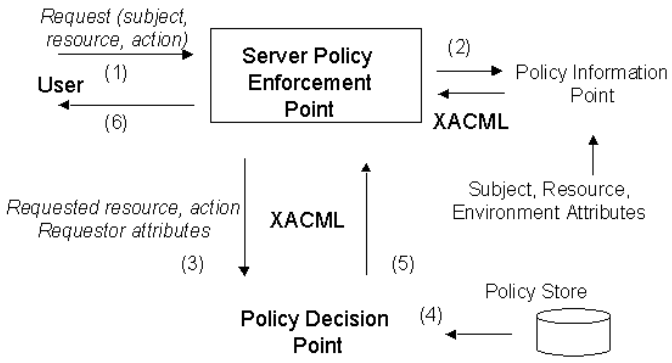
Viale della Regione Basilicata n° 4
85100 Potenza
tel 0971/668335
fax 0971/668954
ufficio.sirs@regione.basilicata.it

- possibilità di implementare logiche centralizzate di "Desottoscrizione" di un servizio. Si dà così all'utente, tramite la MyPage, di desottoscriversi da un sito che non interessa più, provocando in esso la cancellazione dei suoi dati.
- possibilità di elaborare statistiche sull'uso che gli utenti fanno dei sistemi regionali.

La componente Subscription Service dell'IdMS gestisce le problematiche appena descritte. Naturalmente nel caso in cui il SP non abbia la necessità di memorizzare i dati dell'utente (ad esempio perché non deve gestire delle preferenze personali) ad ogni accesso verrà creato un utente temporaneo, che sarà eliminato al logout dell'utente o dopo un certo periodo di inutilizzo (*creoUtenteTemporaneo*). SAML tra l'altro offre degli interessanti meccanismi per garantire la privacy di un utente, ad esempio permettendo l'uso di pseudonimi nei SP in modo da nascondere il più possibile l'identità gestita dall'IP.

Sicurezza

XACML eXtensible Access Control Markup Language è un linguaggio di Policy, utilizzato per descrivere i requisiti generali del controllo degli accessi a risorse distribuite (xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"). Un linguaggio per gestire gli accessi a risorse, che permette di sapere quando una data azione su di una risorsa può essere compiuta o meno e di interpretarne un eventuale risultato. Ecco un esempio di funzionamento del Policy Engine di Ibasho:



PEP

E' quell'entità di sistema che effettua il controllo sugli accessi, facendo richieste di decisione e facendo rispettare le decisioni di autorizzazione. Livello logico che protegge la risorsa richiesta (posta su file system distribuito o web server che sia)

PIP

E' l'entità di sistema che ha la funzione di archivio dei valori dei vari attributi di risorsa, azione o ambiente. Esso fornisce i valori degli attributi al context handler.

PDP

E' l'entità di sistema che valuta le policy applicabili e produce la decisione di autorizzazione per l'esecuzione dell'azione sulla risorsa richiesta. Quando un utente cerca di accedere ad una risorsa, il PEP ne definisce gli attributi ed assegna al PDP il compito di decidere se autorizzare o meno la richiesta. La decisione è presa in base alla descrizione degli attributi dell'utente.

Context Handler

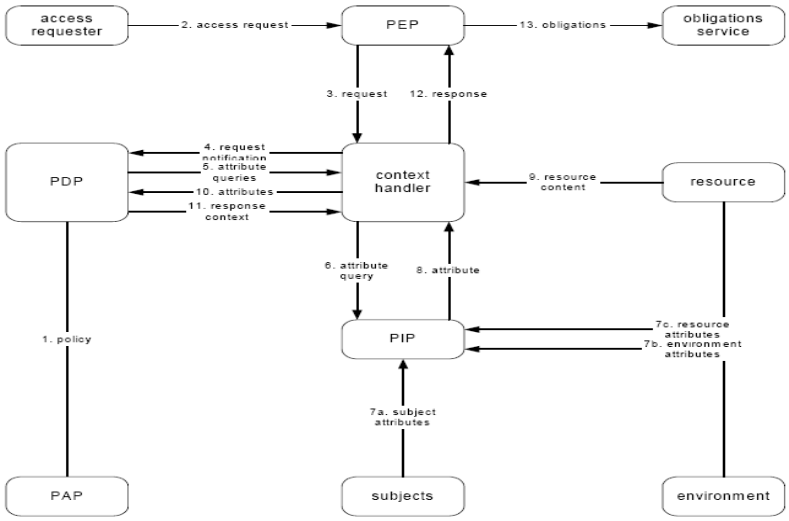
E' l'entità di sistema che converte la richiesta dal suo formato nativo al formato canonico XACML e viceversa e che permette la comunicazione tra tutte le altre componenti del sistema.

Data Flow Model

Situazione di base: qualcuno vuole effettuare un'azione su di una risorsa. Questo il flusso delle operazioni:

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

- Il PAP scrive policy singole o set di policy e le rende disponibili al PDP. Questi set di oggetti rappresentano le politiche per uno specifico target;
- Chi richiede l'accesso alla risorsa, effettua una richiesta al PEP;
- Il PEP manda la richiesta al Context handler aggiungendo attributi per la risorsa, l'azione e il sistema;
- Il context handler, prima richiede gli attributi dal PIP, poi costruisce una richiesta XACML e la manda al PDP;
- Il PDP valuta le politiche allegate alla richiesta;
- Infine ritorna la risposta (con inclusa la decisione di autorizzazione) al context handler;
- Il context handler traduce la risposta e la ritorna al PEP;
- Il PEP fa rispettare gli obblighi dati dalla decizione di autorizzazione;
- Se l'accesso è permesso, quindi, il PEP autorizza il richiedente ad accedere alla risorsa, altrimenti gli nega l'accesso;



Accreditamento ai servizi

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 del sito di Basilicatanet e vuole partecipare alle attivtà 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 delle policy stesse. In tale circostanza l'applicativo che viene raggiunto dal cittadino, e che quindi ha superato il controllo di sicurezza, hai due scenari complementari:

- Il cittadino non esiste quindi lo creo sul db dell'applicativo, lo autentico;
- Il cittadino già esiste e lo autentico al sistema;

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

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.

Integrazione dei sistemi esistenti

Concludiamo questo paragrafo con la descrizione di un componente che si è reso necessario realizzare nello sviluppo del sistema di Single Sign On e cioè il sistema d'integrazione. Come già accennato esistono delle casistiche particolari in cui il componente Guard sviluppato in Java per il progetto Ibasho non si può inserire all'interno della web application che offre i servizi che devono essere integrati nel sistema SSO. Queste problematiche si possono riassumere con i seguenti casi:

- Incompatibilità delle librerie con l'ambiente di distribuzione: si sono verificati diversi casi in cui il server contiene una versione dell'ambiente Java troppo datato o le librerie adottate da Ibasho entrano in conflitto con quelle del server.

- Incompatibilità dell'ambiente di sviluppo: in questo caso non è questione di librerie Java ma di tecnologie e linguaggi di programmazione diversificati come ad esempio applicazioni scritte in .NET oppure in php.

- Impossibilità di effettuare le chiamate interne tra i server: in questo filone ricadono le situazioni che vedono i server posti su reti diverse tra le quali si interpongo dei firewall o altre strutture che impediscono le comunicazioni tra le chiamate interne delle componenti Guanxi.

- Impossibilità di modifica alle applicazioni preesistenti: questo avviene solitamente quando si chiede di modificare le web application sviluppate da altre aziende che non intendono modificare le librerie all'interno dei loro prodotti. In questo caso si cerca di offrire un componente software più leggero per l'integrazione con il sistema di single Sign On che non preveda l'utilizzo di librerie aggiuntive al di fuori di quelle J2EE standard.

Integrazione con sicurezza DEBOLE (WRAPPER)

L'idea di fondo della soluzione adottata è la creazione di una applicazione dedicata al Tunneling delle richieste di autenticazione. Questo significa che l'applicazione che definiremo client demanderà il processo di autenticazione utente ad una diversa applicazione che definiremo tunneling attraverso una apposita richiesta http. Questa applicazione tunneling ritornerà quindi l'elenco dei dati di profilazione utente alla applicazione client. Questa soluzione è orientata ad un'integrazione delle applicazioni tramite una sorta di wrapper che effettuerà una redirect, dopo l'autenticazione con l'IMS, all'applicazione da proteggere attraverso l'invocazione di una FORM POST in HTTPS. In questo scenario è fondamentale definire delle politiche di sicurezza aggiuntive a quelle offerte dal framework di SingleSignOn, come un filtro sugli indirizzi IP "certificati/attendibili" dai quali ricevere connessioni etc. La segretezza del canale di comunicazione che si instaura tra l'applicazione web del servizio e l'applicazione di tunneling viene garantita dall'utilizzo del Secure Sockets Layer attraverso chiamate con protocollo https.

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

Questo è lo scenario più comune e tendenzialmente quello che nel medio lungo periodo sarà quello più utilizzato. È infatti possibile integrare con il sistema di autenticazione un qualunque Service Provider sviluppato con Shibboleth 2.0. Questa soluzione permette di integrare qualsiasi Web server che gira su qualsiasi piattaforma e/o sistema operativo e permette quindi di integrare anche applicazioni sviluppate con tecnologie molto differenti (PHP, .NET etc). Il nostro Idp è in grado quindi di rispondere a tutte le chiamate e le interrogazioni fatte tramite asserzioni SAML 2.0 su protocollo HTTPS sia in configurazione HTTP Redirect e http Post Binding. Le istruzioni ed il software per l'installazione di un service provider così descritto sono reperibili al seguente indirizzo: https://spaces.internet2.edu/display/SHIB2/Installation .

Di seguito vengono forniti i metadati per la configurazione dei vostri ServiceProvider già configurati per il funzionamento con l'IMS. Unica personalizzazione consiste nella definizione e configurazione degli attributi generati dall'IDP che desiderate siano visibili (in Session) nella vostra web application e il setting della variabile EntityID che sarà quella che vi verrà fornita in seguito alla registrazione del SP presso l' Idp della Regione Basilicata (Ved. Paragrafo). Per la configurazione del vostro SP si rimanda alla documentazione ufficiale di Shibboleth 2.0 https://spaces.internet2.edu/display/SHIB2/Home

6.1 Standard applicabili

Le componenti del sistema saranno realizzate utilizzando varie tecnologie e sviluppi ad hoc. Le più importanti sono il Directory Server da usare come repository delle utenze più uno o più framework per l'implementazione del protocollo SAML 2.0, sia lato IP che SP. Come Directory Server si può scegliere un prodotto open source come OpenLDAP o il Fedora Directory Server. Quest'ultimo sembra essere funzionalmente più completo: è un derivato del Netscape Directory Server ed ha dei template appositi per la gestione dei ruoli, cosa comoda quindi vista l'introduzione di questo concetto nel progetto. Per quanto riguarda SAML, esistono alcune implementazioni open source compatibili con la versione 2.0 dello standard. Le più complete al momento sembrano essere:

- OpenSSO: è un framework Java della SUN per la gestione delle identità. Ha anche una libreria PHP per gestire le funzionalità di Service Provider
- Lasso: è un framework piuttosto completo, sviluppato in C con estensioni in vari linguaggi, tra cui Java, Python, Perl, PHP. E' supportato anche (sebbene parzialmente) .NET.

Il supporto di SAML 2.0 su piattaforma Microsoft va analizzato con attenzione in quanto la strategia di Microsoft è quella di appoggiare lo standard "rivale" WS-Federation (http://www.infoworld.com/article/05/11/17/HNmssaml2support_1.html), una tecnologia che è comunque supportata da OpenSSO.

6.2 Requisiti di sistema

Non si evidenziano particolari requisiti di sistema. È necessario che le macchine deputate ad ospitare tale sistema siano preferibilmente Linux con JDK Java 5.x o superiori preinstallato, PHP 5.x e una configurazione di base di OpenLdap.

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

6.3 Interfaccia utente

L'interfaccia utente prevista è quella Web per le applicazioni di gestione del server OpenLdap e interfacce a Script peril deploy e la configurazione delle applicazioni Service Provider Deployate sotto l'infrastruttura dell' IMS.

6.4 Requisiti di prestazione

Al momento non si evidenziano particolari vincoli inerenti le prestazioni.

6.5 Requisiti ambientali

[Requisiti ambientali possono includere condizioni di uso, ambiente utente, disponibilità di risorse, gestione e recupero degli errori, aspetti di manutenzione.]

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

7. Vincoli

Non si evidenziano vincoli relativi alla progettazione e allo sviluppo fatta eccezione per le specifiche tecniche e tecnologiche derivanti dal lavoro del CNIPA in ambito di Identità federate e dal progetto ICAR per la definizione di un'infrastruttura di eGov basata su standard aperti.

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

8. Precedenze e priorità

Le priorità sono quelle di sviluppare in primo luogo tutta la parte relativa al Web Single Sign On rispettando gli standard di SAML 2.0 e successivamente sviluppare il modulo di gestione delle identità federate per l'interfacciamento con il mondo ICAR.

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

9. Requisiti di Documentazione

È necessario che insieme alla documentazione in analisi sia consegnata anche tutta la documentazione delle specifiche tecniche relative agli standard già citati come SAML2.0, XACML 2.0 etc.

9.1 Manuale utente

Il Manuale utente sarà una guida, corredata da opportuni software a supporto , per gli sviluppatori che dovranno attenersi a direttive ben specifiche per poter essere "IMS Compilant". Sarà necessario inoltre una guida per le attività di deploy della web application sotto l' IMS. Questo documento prende il nome di *"BAS2009-INTEGRAZIONE-IdMS-1.4"*.

Il progetto tecnico è invece esplicitato in un altro documento che prende il nome di *"IMS-ProgettoTecnico-v.1.0"*

9.2 Guida interattiva

Non è prevista nessuna guida interattiva.

9.3 Guida all'installazione e alla configurazione, Read Me File

Riconducibile alla guida, manuale utente discusso sopra.

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

10. Modello generale del prodotto

[In questa sezione si fornisce una caratterizzazione generale del prodotto sia dal punto di vista logico che fisico, in modo da evidenziare le principali connessioni tra i suoi macro-componenti e la loro localizzazione sull'hardware designato.]

10.1 Vista logica

L'immagine che segue presenta una visione complessiva del modello della proposta, di cui si discute subito i principi fondamentali, mentre i dettagli delle componenti software che compongono la piattaforma e i principi di progettazione saranno affrontati nei paragrafi che seguenti.

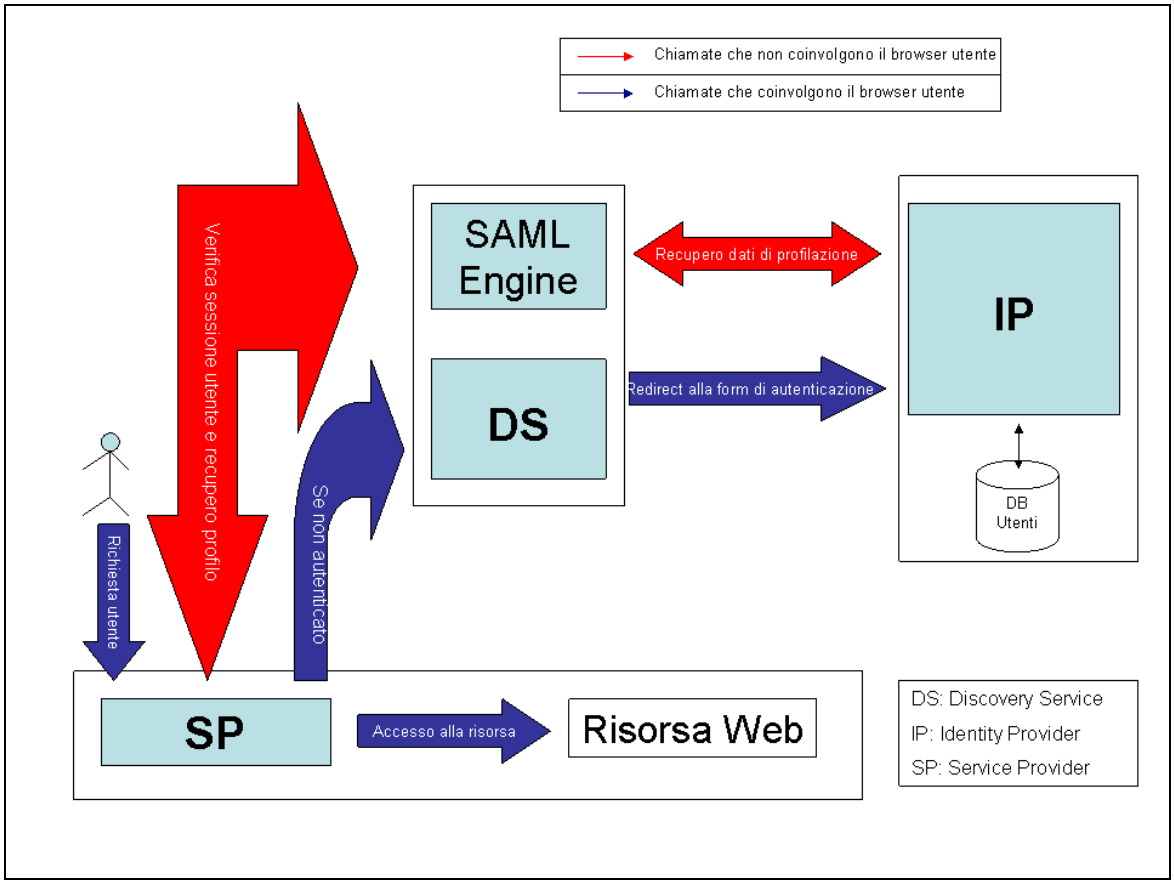


Figura 1 - Modello SSO

Service Provider 1

- Ogni richiesta utente a una risorsa viene intercettata dal Service Provider (SP).
- Il SP chiede all'Engine SAML informazioni sul profilo utente.
- L'Engine SAML verifica che la richiesta provenga da un SP valido.

Discovery Service

- Se l'utente non è già stato autenticato si chiede all'Engine SAML l'indirizzo del server che eroga il Discovery Service (DS).
- Il browser mostra all'utente l'elenco dei possibili Identity Provider (IP).

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

- L'utente viene rediretto alla pagina di login Single Sign On (SSO).

Identity Provider

- L'utente inserisce le proprie credenziali attraverso il browser (oppure si autentica tramite CIE, CNS o altro).
- Le credenziali vengono verificate da IP.
- Se l'autenticazione ha esito positivo l'Engine SAML attiva la sessione utente.

Attribute Authority

- I dati utente vengono estratti dal repository degli utenti (anagrafica unica?) attraverso il modulo Attibute Authority.
- Il risultato viene trasmesso all'Engine SAML

Service Provider 2

- L'Engine SAML decodifica i dati del profilo utente e li invia al SP.
- L'Engine SAML notifica al SP che l'utente può accedere alla risorsa richiesta.
- Il browser dell'utente viene reindirizzato alla pagina web richiesta.

10.2 Vista fisica

Una volta disposti i vari componenti middleware, il passo successivo è stato progettare e implementare l'architettura logica e applicativa. Oltre alle scelte architetturali, è stato necessario frazionare le risorse e disporle in base alle esigenze tecnologiche e di traffico delle applicazioni da sviluppare. In questo capitolo e per ogni suo paragrafo, verranno chiariti i concetti di **scalabilità, sicurezza, disponibilità e affidabilità** e di come questi si siano realizzati attraverso politiche di bilanciamento del carico, clustering, riciclo delle sessioni, replica e backuping dei database e trasporto sicuro delle informazioni (HTTPS). Verrà, inoltre, illustrata l'idea di sleeper applicativo secondo cui in un cluster composto da n server applicativi ve n'è almeno uno inattivo che entra in funzione soltanto quando almeno uno di quelli attivi non passa in stato di fault, garantendo sempre e comunque una ripartizione equa del carico tra i componenti.

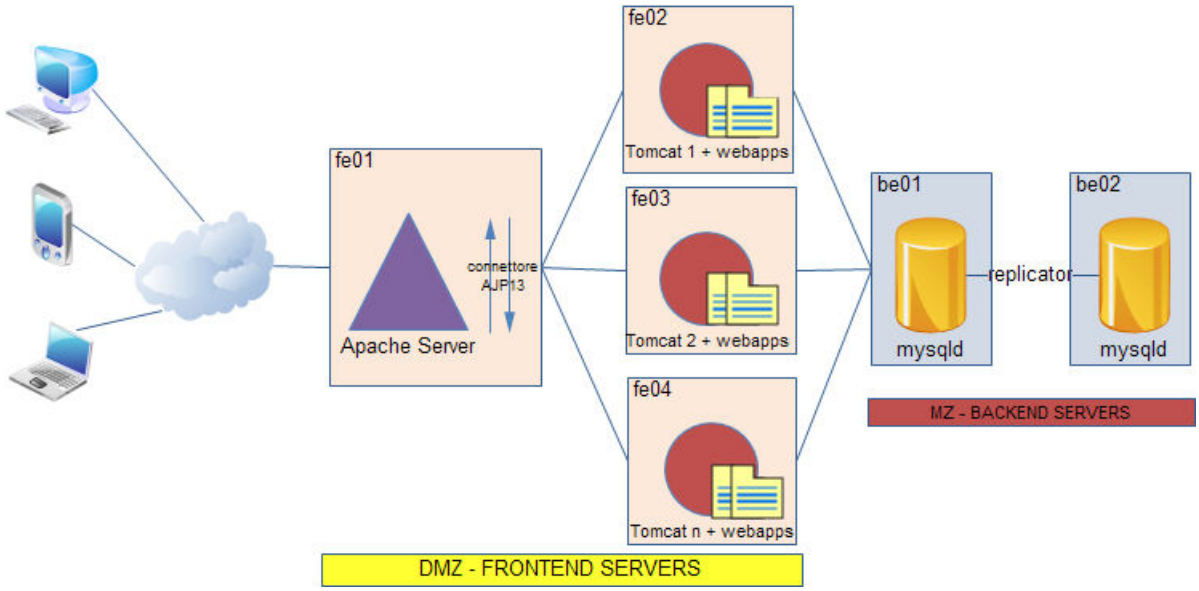
Nel resto del capitolo questi concetti, insieme a quelli del capitolo precedente, serviranno a illustrare l'architettura implementata per le applicazioni sviluppate. In particolare sono state tracciate due distinte geometrie applicative, la prima volta a ospitare l'IMS e la seconda i siti istituzionali di nuova e vecchia implementazione. Questo problema si risolve rendendo l'architettura scalabile e tollerante ai guasti (fault tolerance) e i servizi "altamente disponibili" (high avalaibility).

Con il termine scalabile ci si riferisce, in termini generali, alla capacità di un sistema di "crescere" o "decrescere" in funzione delle necessità o delle disponibilità. La scalabilità può essere verticale o orizzontale. Quella verticale si ottiene incrementando le risorse hardware di un calcolatore (essenzialmente RAM, CPU e/o dischi). In questo contesto l'aumento della capacità computazionale non cresce linearmente all'aumentare delle risorse, ma è comunque limitato dall'hardware e dai programmi in esecuzione. La scalabilità orizzontale si realizza con un cluster di calcolatori. L'aumento delle esigenze computazionali, derivante dall'incremento delle richieste dei servizi, viene soddisfatto aggiungendo nuovi nodi al cluster.

Con il concetto di "alta disponibilità", in inglese high avalaibility, si intende la capacità di un sistema di

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

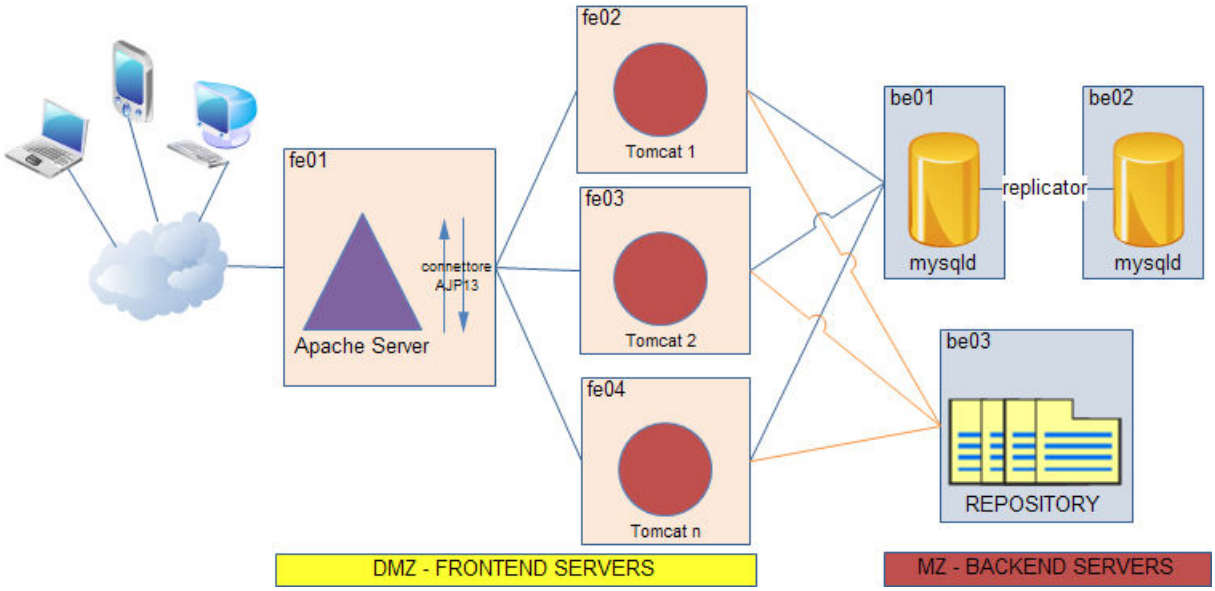
garantire la continuità nell'erogazione dei servizi. Nell'ambito di un cluster, nel caso in cui un nodo si blocchi, il carico delle richieste che il nodo inattivo non può più processare viene reindirizzato verso gli altri nodi del sistema. La ridondanza dei nodi definiti in un cluster ha come obiettivo l'eliminazione dei punti deboli del sistema (i così detti "single point of failure") attraverso procedure automatiche che mantengono i nodi sincronizzati tra loro. In un tale contesto la tolleranza ai guasti (fault tolerance) è un aspetto che assume un'importanza rilevante. Maggiore è il numero degli elementi di un sistema, maggiore è la probabilità che ciascuno di essi possa andare in fault, determinando un'interruzione del servizio. Ciò rende la tolleranza ai guasti un requisito fondamentale al crescere dei sistemi distribuiti. Le tecniche sottostanti alla creazione di un cluster (alta disponibilità, bilanciamento e scalabilità) permettono a un sistema distribuito di garantire elevati livelli di fault tolerance.



Per il momento, pur non entrando nel merito delle tecniche di clustering e bilanciamento del carico, possiamo affermare che un modello così strutturato garantisce un'elevata scalabilità dei servizi. Volendo migliorarlo ulteriormente, si potrebbe pensare di ottimizzare la distribuzione delle applicazioni all'interno dell'architettura. Guardando il diagramma precedente, ci si accorge che a ogni Tomcat corrisponde un insieme di applicazioni, ovvero che ogni applicazione è replicata per ciascun Tomcat del cluster. Ciò oltre a introdurre un'elevata ridondanza, rende estremamente macchinose le operazioni di deploy, in quanto si ha la necessità di replicare manualmente qualunque operazione per tutti i Tomcat, pena il disallineamento delle informazioni nel sistema. Se è vero che uno scenario di questo tipo può essere considerato tollerabile in un piccolo ambiente di produzione, è altrettanto vero che in un'architettura con un elevato numero di nodi o applicazioni, diventa estremamente complicata qualunque operazione di manutenzione delle webapps. L'idea, dunque, è quella di centralizzare le applicazioni, creando un vero e proprio repository da cui i tomcat possano attingere. Con un sistema di questo tipo, inserendo, per esempio, una versione aggiornata di una webapp all'interno del deposito unico, le modifiche sarebbero immediatamente disponibili per tutti i Tomcat. L'unico problema di questo modello è che, mentre i tomcat continuano a rispettare i principi di scalabilità, le applicazioni rischiano di essere indisponibili completamente nel caso in cui dovesse passare in fault la macchina di repository. Tuttavia il problema si risolve eleggendo come macchina di repository una all'interno della MZ, quindi un nodo altamente affidabile dell'architettura.

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

Il modello finale è il seguente:



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

Riferimenti bibliografici

[Questa sezione fornisce l'elenco di tutti i documenti referenziati all'interno del Documento di Visione. Ciascun documento viene identificato mediante il titolo, la data di pubblicazione, l'organizzazione che l'ha prodotto, il sito web da cui è stato prelevato.]