Infrastruttura ARPA

Autenticazione, autorizzazione e accesso ai servizi

Presentazione

L'infrastruttura della Rete Telematica copre in modo capillare il territorio regionale e, su tale infrastruttura, sono ormai avviati servizi di particolare significato per l'attività degli Enti, per il sistema produttivo, per le professioni, il commercio, il turismo, la sanità e per i singoli cittadini della Toscana. La diffusione di questi servizi tende ad avanzare con rapidità e presenta alcune caratteristiche di complessità organizzativa, gestionale e amministrativa sulle quali occorre riflettere attentamente.

In particolare, è ormai acquisita, la necessità di poter disporre di strumenti e sistemi tecnologici in grado di assicurare con trasparenza, rispetto della privacy ma, al tempo stesso, rapidità operativa la certezza dell'autenticazione del soggetto (o dei soggetti) che richiedono alla Pubblica Amministrazione la fornitura di servizi sulle reti . Posto che l'infrastruttura di base esiste ormai in Toscana e che su di essa poggiano servizi garantiti, in grado di produrre e consolidare la trust and confidence che l'utente pubblico o privato ha nei confronti della Pubblica Amministrazione, il problema che si pone è quello di come garantire l'accesso sicuro all'infrastruttura e ai servizi.

I sistemi di identificazione "sicura" sono ormai molti. Quello più coerente con le tre variabili critiche – facilità di utilizzo, economia di gestione, sicurezza di impiego – corrisponde ai sistemi basati su "carte elettroniche".

In Toscana è iniziata, su impulso della Regione e della Comunità della Rete Telematica Regionale, la diffusione di una particolare "carta" a microprocessore, la Carta Nazionale dei Servizi (CNS). Va annotato che è stato recentemente approvato, sempre a livello nazionale, il decreto interministeriale per la distribuzione su tutto il territorio italiano di uno strumento in parte "alternativo" rispetto alla CNS, la Carta di Identità Elettronica (CIE) che avrà lo stesso "certificato digitale" di autenticazione e quindi sarà interscambiabile con la CNS.

Il possesso di una carta che garantisca l'identità digitale di ogni cittadino, permette l'accesso ai servizi della PA, siano essi servizi di consultazione dei propri dati o servizi interattivi, come ad esempio l'intervento sull'iter di una pratica.

Alcuni servizi hanno bisogno di una identità digitale arricchita di ulteriori informazioni quali per esempio i ruoli che ne qualifichino ulteriormente le funzioni e/o i poteri: queste informazioni sono presenti presso quelli che vengono definiti come "certificatori di ruolo", quali ad esempio gli ordini professionali, che assumono quindi un ruolo importante per l'autenticazione in rete.

Regione Toscana si è attivata per garantire anche queste informazioni con la costituzione di un sistema per l'accesso autenticato e sicuro ai servizi che prevede il coinvolgimento di questi "certificatori di ruolo".

Progetto

Regione Toscana attraverso il progetto ARPA, intende implementare una serie di servizi di autenticazione, autorizzazione ed accesso di tipo orizzontale da offrire a supporto delle applicazioni esistenti e di quelle di prossimo sviluppo.

La visione strategica di Regione Toscana mira a posizionare il Sistema ARPA , come punto di aggregazione per un insieme di servizi sia di tipo verticale (servizi applicativi) che di tipo orizzontale (servizi infrastrutturali).

I sistemi di identificazione "sicura" sono ormai molti. Quello più coerente con le tre variabili critiche – facilità di utilizzo, economia di gestione, sicurezza di impiego – corrisponde ai sistemi basati su "carte elettroniche".

Come punto di aggregazione il sistema non è isolato, ma tendenzialmente coopera e collabora con una serie di soggetti appartenenti al mondo della Pubblica Amministrazione, delle Associazioni Professionali, delle Amministrazioni che a diverso titolo e con modalità diverse utilizzano i servizi di Regione Toscana.

In questo modo il sistema ARPA è in grado di raggiungere gli obiettivi desiderati:

- Creare un punto di aggregazione per un insieme di servizi
- Consentire al Sistema di cooperare con le altre realtà
- Consentire alle P.A. toscane di: utilizzare i servizi infrastrutturali del sistema e rendere fruibili i propri servizi ad una vasta comunità di utenti

Modello Concettuale

Il soggetto o entità è un individuo (PERSONA) nella sua completezza con l'esigenza di reperire con facilità i servizi (RISORSE) offerti o di interesse in funzione delle proprie caratteristiche". L’identità del soggetto è costituita da un insieme di dati (credenziali) che consentono l’identificazione del soggetto ma non solo: esse possono rappresentare una serie di tratti o attributi che ne individuano il RUOLO ossia l’insieme delle funzioni esercitate (Dirigente, Medico, Avvocato ecc.).

Le credenziali vengono presentate ad una autorità di sicurezza che le verifica e stabilisce quali sono le risorse alle quali l’identità può accedere e quali sono le azioni che il soggetto può effettuare sulle risorse stesse.

Pertanto i componenti fondamentali di questa architettura sono:

- **Certificatore delle identità**, che nel caso di sistemi con accesso mediante strumenti di strong autentication è rappresentato dalla C.A: che ha emesso la credenziale di identificazione (certificato digitale);
- **Certificatore dei ruoli** ossia l’autorità che ha il compito di certificare che il soggetto sia effettivamente in possesso del ruolo dichiarato;
- **Autorità di sicurezza** che, sulla base delle credenziali presentate e verificate presso il certificatore di ruolo, stabilisce le politiche di accesso alle risorse.

Federazione

La soluzione proposta: Identità Federata

Elemento chiave dell’infrastruttura proposta è la capacità di interoperare con altre amministrazioni secondo il modello dell’identità federata.

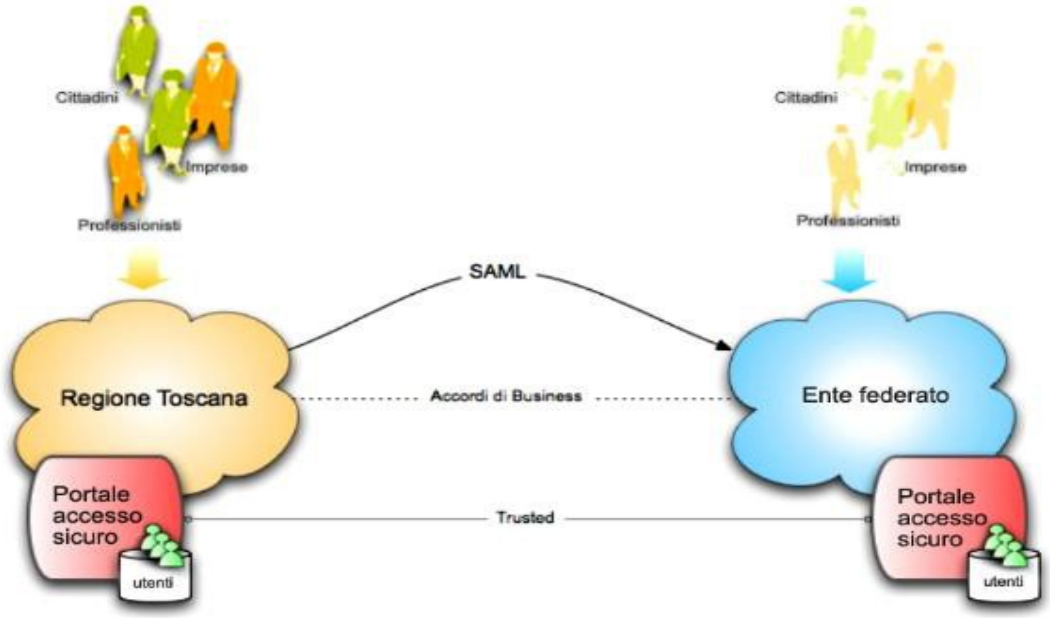
Il modello di Identità Federata, ha come obiettivo quello di erogare servizi federando le identità tra le diverse entità che offrono servizi. L'uso del termine federato è qui inteso nell'accezione di sicurezza, potendo cioè avere fiducia sulla provenienza della richiesta di servizio. Questo modello prevede due attori che concorrono a fornire un servizio all'utente:

- il Service Provider che fornisce il servizio applicativo
- l'Identity Provider che fornisce il servizio di identità

Le tecnologie e gli standard che sottendono a questo modello, consentono ad un utente riconoscito e dall' Identity Provider di utilizzare i servizi offerti da un Service Provider senza

essere nuovamente autenticato.

Se gli scenari di cooperazione prevedono inoltre un accesso ai servizi ristretto a specifiche categorie di utenza, caratterizzate dal possesso di una determinata qualifica o ruolo ,il problema si arricchisce della necessità di instaurare rapporti di mutua fiducia in merito all'attribuzione di queste qualifiche oltre alla necessità di verificare che la semantica della stessa qualifica sia la medesima in entrambi i domini.



Regione Toscana aderisce al progetto interregionale ICAR e quindi al sistema interregionale di autenticazione (TASK-INF 3) e dunque partecipa al processo con cui verranno definite a livello interregionale :

- le informazioni utili a identificare il soggetto richiedente un determinato servizio
- gli attributi utili a determinare l'abilitazione all'accesso
- le modalità con cui verranno veicolate le informazioni sui soggetti richiedenti credenziali nelle interazioni tra domini di cooperazione applicativa

Delega delle funzioni

Il sistema consente la funzionalità di delega.

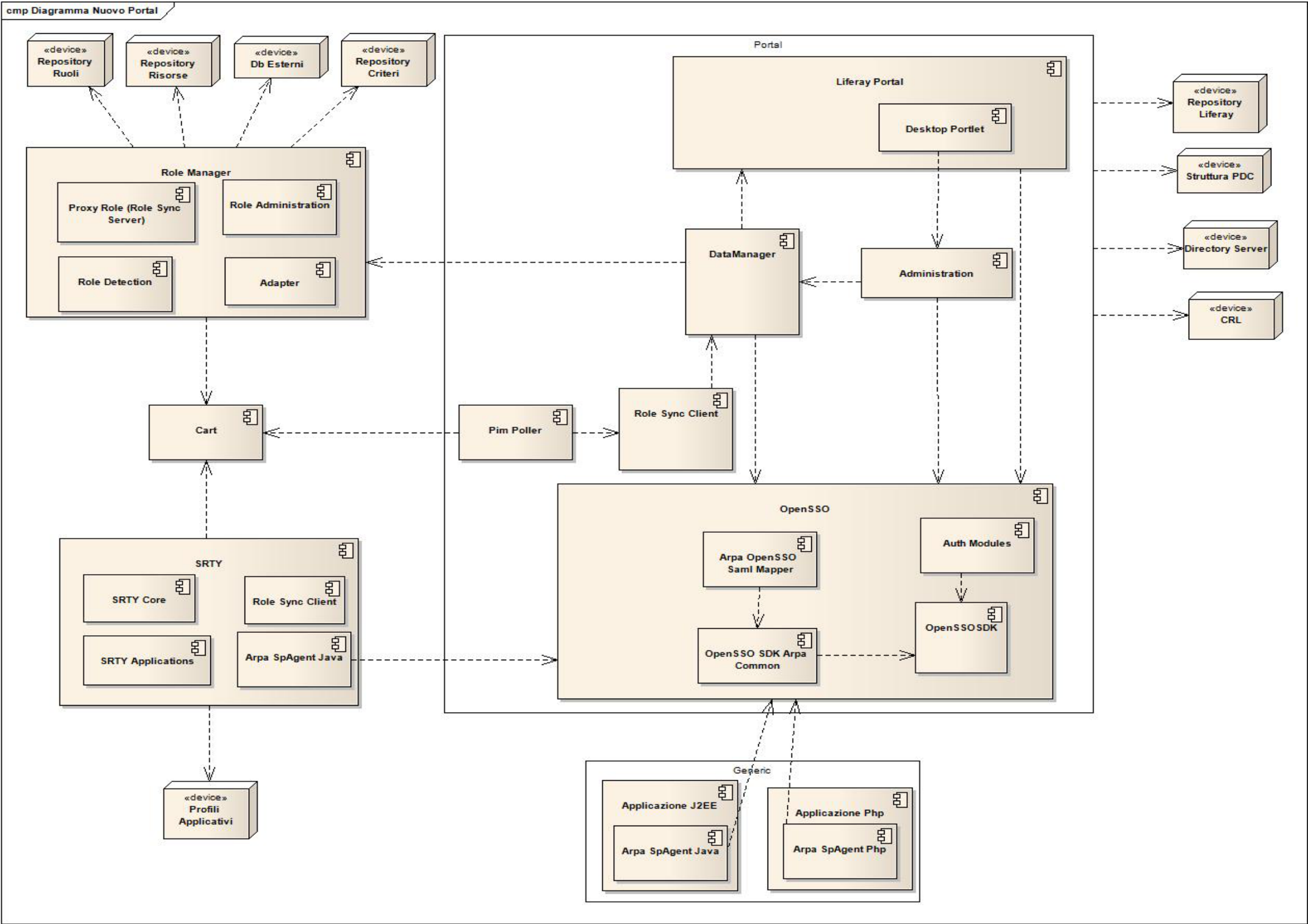
La delega permette ad un utente (delegato) di accedere, per un periodo di tempo determinabile, ad una risorsa o a tutte le risorse assegnate ad un certo ruolo con le credenziali e privilegi di un altro utente (delegante).

Il delegante indica il delegato, il periodo di validità della delega e se la delega ha valore su tutte le risorse associate al ruolo o alle singole risorse.

Il sistema registra la delega e inoltra alle risorse sia le credenziali del delegato che del delegante permettendo quindi ai singoli servizi di effettuare la corretta profilazione applicativa e, eventualmente, di registrare le operazioni effettuate in delega.

Architettura di ARPA: la soluzione realizzata

l risultato è la costruzione di un portale per l'accesso sicuro alle risorse applicative che consente di centralizzare l'accesso degli utenti, rafforzandolo di strumenti di autenticazione sicuri quali le smart card ,offrendo all'utente un desktop personalizzato sulla base del proprio ruolo. L'interazione tra il portale ed il modulo di gestione dei ruoli consente di disaccoppiare il controllo accessi basato sui ruoli dalla gestione delle banche dati utilizzate per la validazione dei ruoli stessi.


cmp Diagramma Nuovo Portal
«device»
Repository
Ruoli
«device»
Repository
Risorse
«device»
Db Esterni
«device»
Repository
Criteri
Portal
Liferay Portal
Desktop Portlet
«device»
Repository
Liferay
«device»
Struttura PDC
«device»
Directory Server
«device»
CRL
Role Manager
Proxy Role (Role Sync
Server)
Role Administration
Role Detection
Adapter
DataManager
Administration
Cart
Pim Poller
Role Sync Client
OpenSSO
Arpa OpenSSO
Saml Mapper
Auth Modules
OpenSSOSDK
OpenSSO SDK Arpa
Common
SRTY
SRTY Core
Role Sync Client
SRTY Applications
Arpa SpAgent Java
«device»
Profili
Applicativi
Generic
Applicazione J2EE
Arpa SpAgent Java
Applicazione Php
Arpa SpAgent Php

Il modello architetturale su cui si dispiega il sistema è costituito da tre Aree :

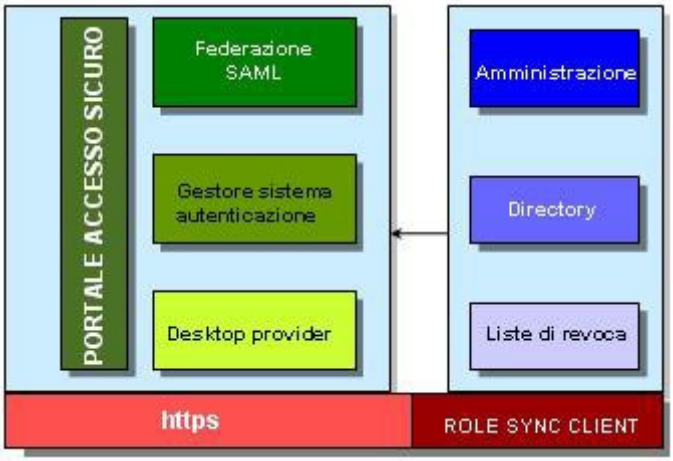
- **Access Provider**, che fornisce l'accesso agli utenti garantendo i servizi di autenticazione , autorizzazione e controllo accessi;
- **RoleManager** che garantisce la corretta associazione utente/ruoli;
- **Area Servizi** che è costituita dalle risorse applicative disponibili; tra queste le risorse che saranno in grado di fornire il corretto profilo applicativo all'utente sulla base delle sue credenziali così come fornite dall'area portale e valorizzate dall'area Role Manager.

Access Provider

Responsabile della fase di autenticazione e controllo degli accessi, autentica i propri utenti attraverso certificati digitali personali (PDC) e visualizza per ognuno di loro un desktop di portale il cui contenuto varia in funzione dei ruoli attribuiti all'utente stesso.

Il desktop utente mostra solo le risorse abilitate all'utente.

L'utente, selezionando una risorsa contenuta nel proprio desktop di portale, accede alle funzionalità da questa esposte.



L'infrastruttura attraverso la componente PDC si fa carico della verifica del certificato digitale in possesso del cittadino. Tale verifica (stato del certificato) è estesa a tutte le CNS emesse dalle PA nazionali.

Area Role Manager

Effettua la verifica dei ruoli dichiarati dall'utente.

La certificazione del ruolo viene effettuata attraverso l'interrogazione di una o più fonti dati da cui reperire le informazioni necessarie a soddisfare i criteri di appartenza al ruolo (Certificatori di Ruolo).

Si prevede inoltre che ciascun ruolo abbia la possibilità di avere associate delle informazioni aggiuntive denominate "attributi".

Compito dell'Area Role Manager è dunque anche la valorizzazione di tali attributi.

Il codice fiscale, i ruoli posseduti e i relativi attributi costituiscono le credenziali utente.

La componente è progettata per essere altamente flessibile e poco invasiva sulla logica dei certificatori di ruolo oltre che per adattarsi alla tecnologia scelta per esporre le informazioni.

In fase di configurazione dell'are RoleManager è possibile :

- indicare quali sono i soggetti autorevoli per la valorizzazione di attributi;
- indicare la tecnologia da utilizzare per l'interrogazione (esempio web services , Ldap, Database ...);
- specificare la logica con cui le informazioni devono essere aggregate e/o interpretate

per la certificazione dell'appartenenza di un utente ad un ruolo.

i certificatori di ruolo interagiscono con il Role Manager secondo regole definite da RFC146 e RFC156 come previsto dal sistema e.toscana compliance.

Area Servizi

Questa Area, sulla base delle credenziali presentate e verificate tramite RoleManager, applica le politiche di accesso alle risorse. Le risorse mediante attraverso le componenti fornite accedono alle credenziali utente ed hanno la possibilità di applicare regole per la profilazione applicativa ossia per stabilire quali sono le azioni che il soggetto può effettuare sulle risorse stesse.

L'area servizi è in grado di colloquiare con l'Access Provider che fornisce le politiche di accesso e le credenziali utente.

Nel modello di dispiegamento è prevista la possibilità di avere più aree servizi distribuite.

Questa modalità di dispiegamento offre il vantaggio di centralizzare la sola fase di autenticazione ed autorizzazione , mentre la fase di erogazione del servizio può avvenire in modalità diretta (accesso diretto alle risorse).

Risorse Integrabili

L'integrazione dei servizi in ARPA avviene secondo il modello SAML.

Regione Toscana ha sviluppato una serie di componenti che possono essere incluse dalle PA nei propri applicativi, rendendo dunque semplice l'attività di integrazione con l'infrastruttura regionale.

Tali componenti sono disponibili per gli ambienti J2EE e PHP. Per la documentazione si veda la sezione dedicata.

Grazie a queste componenti il processo di integrazione risulta ampiamente semplificato.

Certificatori di ruolo

I Certificatori di Ruolo, rappresentano le entità che espongono le fonti dati attraverso cui verificare/reperire i ruoli e gli attributi ad essi associati. Riferendosi alla terminologia adottata dal progetto ICAR , i certificatori di ruolo corrispondono alle "autorità di certificazione delle qualifiche " o AA (attribute authority).

Regione Toscana curerà i rapporti con altre pubbliche amministrazioni, albi e ordini professionali per la realizzazione di queste funzionalità di certificazione .

Le credenziali utente così realizzate costituiscono di fatto "l'identità digitale" dell'utente collegato, autenticato ed autorizzato dal sistema ARPA.

I Servizi esposti dai certificatori di ruolo sono acceduti alla componente RoleManager

i certificatori di ruolo interagiscono con il Role Manager secondo regole definite da RFC146 e RFC156 come previsto dal sistema e.toscana compliance.

Contatti

Direzione Generale Organizzazione, Settore "Infrastrutture e Tecnologie per lo Sviluppo della Società dell'Informazione", Responsabile **Laura Castellani**

Referenti di progetto:

- **ARPA project:** arpa-project@regione.toscana.it
- **Grazia Ugolini,** tel: 055 4383246; mail: grazia.ugolini@regione.toscana.it
- **Luca Bonuccelli,** tel: 055 4383122; mail: luca.bonuccelli@regione.toscana.it