# Infrastruttura ARPA

## Autenticazione, autorizzazione e accesso ai servizi

| | | |
|---|---|---|
| **Redatto da** | Ugolini Grazia | Piattaforme e Infrastrutture per i servizi on-line e la cittadinanza digitale |
| **Approvato da** | Sergio Papiani | Sistema Cloud Toscano ,Infrastrutture Digitali e Piattaforme Abilitanti |
| **Versione** | 3.0 | |
| **Data emissione** | 08/09/2021 | |
| **Stato** | Approvato | |

# Sommario

## Presentazione

Regione Toscana ha realizzato una piattaforma di Access Management denominata ARPA (Accessi Ruoli Profili Applicazioni) per garantire l'accesso sicuro e unificato ai servizi on-line. ottemperando a quanto previsto dall'articolo 64 del CAD e successive integrazioni.

ARPA è ad uso sia di Regione Toscana che delle pubbliche amministrazioni toscane,

Questa infrastruttura rappresenta un punto cardine per favorire lo sviluppo e la diffusione dei servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese.

Dal punto di vista tecnologico è un servizio SAAS di autenticazione ed autorizzazione per l'accesso ai servizi online messo a disposizione delle strutture della Giunta regionale e delle PP.AA. della Toscana .

I metodi di autenticazione attualmente messi a disposizione da ARPA sono:

- **CNS :** Carta Nazionale dei Servizi
- **CIE :** Carta d'Identità Elettronica
- **SPID :** Sistema Pubblico d'Identità Digitale), aderente al DPCM 24/10/2014 e successive integrazioni (Identità Professionali e Giuridiche )
- **Login EIDAS :** nteroperabilità transfrontaliera delle identità digitali (eID )

Attraverso l'interrogazione di Attribute Authority , ARPA è in grado di costruire un profilo degli attributi qualificanti del soggetto autenticato ed appliocare profili di autorizzazione ai servizi.

Le applicazioni attualmente integrate con l'infrastruttura ARPA e realizzate da regione, enti, comuni sono fruibili da cittadini, imprese,dipendenti PA , utilizzando i metodi di autenticazione previsti dalla norma e sono sollevate dal dover affrontare problematiche come:

- gestione ed adattamento infrastruttura secondo l'articolo 64 Comma 2 del CAD e successive integrazioni;
- avere un ruolo di Soggetto Aggregatore nei confronti di AGID riguardo SPID e Attribute Authority;
- ricerca ed integrazione dei gestori di attributi qualificati, stipulando con essi apposite convenzioni;
- offrire un servizio di helpdesk di secondo livello sempre presidiato;
- garantire l'operatività della infrastruttura;
- tracciamento accessi secondo disposizioni di legge

Attraverso l'utilizzo di protocolli di federazione standard come OAuth2, OpenID Connect, SAML2 e di componenti infrastrutturali, ARPA permette la realizzazione di applicazioni come:

- applicazioni Web stateless e stateful;

- applicazioni Mobile native ed ibride, mettendo a disposizione servizi come autenticazione persistente sul dispositivo e revoca in caso di smarrimento o furto del dispositivo;
- API Rest con Policy Enforcement locale oppure attraverso API Gateway
- applicazioni per Totem
- applicazioni Desktop / TV con funzionalità di pairing per dispositivi non dotati di tastiera o CNS/ CIE

## Infrastruttura

Il core della piattaforma è una componente di identity and access management in grado di colloquiare con i servizi applicativi attraverso protocolli standard (SAML e OAUTH). A corredo vi sono:

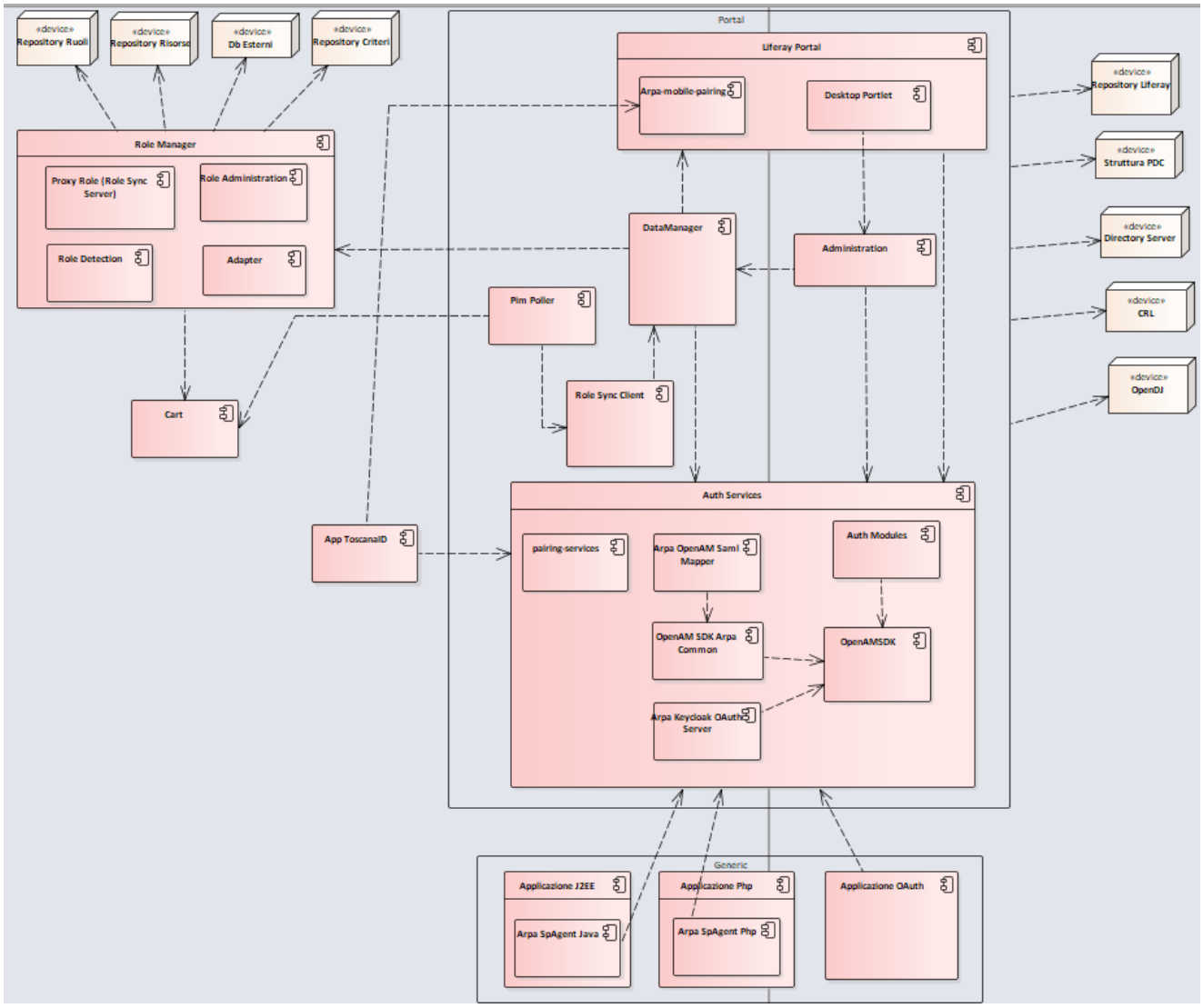
- Una componente estendibile in termini di autenticazione (al momento suono supportati tutti

gli strumenti previsti dal CAD-ossia CIE CNS Spid

- Una componente di policy enforcement point in grado di garantire il rispetto di policy dinamiche per la verifica autorizzata per l'accesso. Tale componente è implementata sia per integrazione di web application basate dunque su componenti server che per l'integrazione di single page application o app native rispondenti al paradigma dei microservizi.

- La componente per gathering delle informazioni provenienti da fonti autorevoli per la definizione di ruoli e definizione di policy di accesso basate su ruoli o tratti.

- Sistema di log e tracciatura per profili di sicurezza



## Architettura

Dal punto di vista della soluzione tecnologica, ARPA consta di una infrastruttura immateriale che solleva i team di sviluppo dalle problematiche di sicurezza, di autenticazione e qualificazione degli utenti nella realizzazione di servizi on-line.
Nel dettaglio: l'infrastruttura, riconosciuto l'utente tramite gli strumenti CNS, CIE, SPID, fornisce al servizio on line i tratti essenziali e necessari per profilare l'accesso alle singole funzioni. Per qualificare l'accesso possono essere utilizzati in mash-up basamenti informativi territoriali, servizi over SPC ed i futuri gestori di attributi qualificati previsti da SPID (Attribute Autority). Ad esempio già oggi l'infrastruttura qualifica a livello regionale il personale socio sanitario, i medici prescrittori, gli operatori della PA Locale e territoriale. Potenzialmente può qualificare soggetti iscritti ad ordini professionali o con specifici ruoli abilitanti a funzioni specifiche.

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

- **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.

### Area Role Manager

Effettua la verifica dei ruoli 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.

E' stata inoltre adattata le componente per poter interagire secondo le specifiche delle Attribute Autority Spid.

## 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 protocollo SAML e OAuth 2.0.

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.

Con riferimento all'integrazione SAML (il cui protocollo è storicamente "difficile" da manipolare senza librerie dedicate), 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.

Mentre per la parte OAuth2.0 sono stati realizzati dei progetti di esempio per i casi d'uso più comuni e con particolare riferimento al mondo Java; in ogni caso sono idealmente agnostici dal linguaggio di programmazione finale. Il protocollo OAuth2.0 è uno standard de-facto e in letteratura sono riportati numerosi esempi di utilizzo nelle più svariate piattaforme tecnologiche, tali per cui non si è ritenuto necessario realizzare particolari progetti a supporto per l'integrazione.

## 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.

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 **Sergio Papiani**

Referenti:

**ARPA Supporto:** arpa@regione.toscana.it
**Grazia Ugolini,** tel: 055 4383246; mail: grazia.ugolini@regione.toscana.it

## Riferimenti

| | |
|---|---|
| Elenco documenti aggiornato | www.regione.toscana.it/arpa |
| EIDAS Login | https://eid.gov.it |
| SPID Soggetto aggregatore | https://www.agid.gov.it/it/piattaforme/spid/soggetti-aggregatori |
| | |