-

Regione Toscana

Modalità di identificazione
Punto d'accesso

Documento Tecnico

Versione 1.3

FIRENZE, settembre 2011

DOCUMENTO:

Modalità di identificazione del Punto d'accesso
La redazione del documento è prevista dal D.M. n°44 del 18 aprile 2011

EMISSIONE – VERIFICA – APPROVAZIONE

	Funzione	Nome	Firma
Emissione	Responsabile tecnico Progetto "Realizzazione punto d'accesso RT"	Maria Giovanna Cuzzola	
Verifica	Responsabile Contratto	Leonardo Borselli	
Approvazione	Responsabile Contratto	Leonardo Borselli	

AGGIORNAMENTI

Versione	Data	Paragrafi Modificati	Motivo Modifica
1.0	06/06/2011		Emissione
1.01	26/06/11		Osservazioni DGSIA
1.02	14/07/11	Inserimento par 6.1, modifica capitolo 6	Osservazioni DGSIA
1.03	23/09/11	Modifica copertina,paragrafo 4.1 e 4.2; inserimento par 6.2	Osservazioni DGSIA

1 INTRODUZIONE..... 4

2 DEFINIZIONI E ACRONIMI..... 4

3 IL SISTEMA DI CERTIFICAZIONE DELL'IDENTITÀ REGIONALE..... 5

3.1 Architettura logica..... 6

3.2 Architettura fisica..... 7

4 L'ACCESSO AUTENTICATO..... 9

4.1 Autenticazione basata su PDC (Personal Digital Certificate)..... 9

4.2 Self-Registration..... 10

5 COMPONENTI DEI SOTTOSISTEMI..... 11

5.1 Sottosistema Portal..... 11

5.2 Sottosistema Role Manager..... 11

5.3 Sottosistema OpenSSO..... 12

5.4 Sottosistema Servizi applicativi..... 13

5.5 Monitoraggio dell'infrastruttura..... 13

6 INTEGRAZIONE CON IL PUNTO D'ACCESSO REGIONALE.....14

6.1 Modalità di integrazione con il Punto di Accesso "Cancelleria Telematica".....17
62 Modalità di integrazione cancelleria telematica posta elletronica certificata 20

Indice delle figure

FIGURA 1 - ARCHITETTURA LOGICA..... 7

FIGURA 2 - ARCHITETTURA FISICA..... 8

FIGURA 3 - AUTENTICAZIONE TRAMITE CERTIFICATO..... 10

FIGURA 4 - COMPONENTE OPENSSO..... 13

FIGURA 5 – USE CASE INTEGRAZIONE CANCELLERIA - ARPA..... 17

FIGURA 6 – SEQUENCE DIAGRAM ACCESSO UTENTE REGISTRATO.....18

FIGURA 7 – SEQUENCE DIAGRAM ACCESSO CITTADINO..... 19

FIGURA 8 – ARCHITETTURA FLUSSO DEPOSITO ATTI 21

1 INTRODUZIONE

Nell'ambito degli interventi a sostegno delle libere professioni Regione Toscana ha finanziato e sostenuto in questi anni il progetto denominato "Cancelleria Telematica".

Questo sistema diffuso su tutto il territorio regionale è stato adeguato su richiesta degli Uffici Giudiziari Toscani e degli Ordini degli avvocati toscani per diventare un punto d'accesso come previsto dal DM n° 44 del 18 aprile 2011.

Il presente documento, si pone come obiettivo quello di illustrare la soluzione adottata dalla Regione Toscana relativamente alla gestione delle identità digitali (identificazione informatica, come specificato nell'articolo 2 comma 1 capoverso f) dei soggetti abilitati esterni al dominio giustizia.

La soluzione che verrà illustrata è basata sul sistema ARPA, che è l'infrastruttura standard di Regione Toscana per l'autenticazione, autorizzazione e accesso ai servizi.

Il documento è suddiviso in due sezioni principali:

Il sistema di certificazione dell'identità regionale (Cap. 3)
in cui si illustrano le funzionalità dell'infrastruttura ARPA e la sua architettura logica e fisica;
Componenti dei sottosistemi (Cap. 4)
in cui sono descritti i componenti interni a ciascun sottosistema;

2 DEFINIZIONI E ACRONIMI

Adapter	Componente software che nasconde ed "adatta" l'interfaccia di un componente mostrandone un'altra all'esterno. Consente di "uniformare" l'interfaccia di accesso alle fonti dati durante il processo di discovery e verifica dei ruoli.
CNS	Carta nazionale dei servizi
CSE	Carta sanitaria elettronica
CIE	Carta identità elettronica
Fonte dati	Repository di informazione necessario al ROLE MANAGER per verificare l'assegnazione dei ruoli agli utenti attraverso specifici Adapter.
Identificazione informatica	Operazione di identificazione in rete del titolare della carta nazionale dei servizi o di altro dispositivo crittografico, mediante un certificato di autenticazione, secondo la definizione di cui al decreto legislativo 7 marzo 2005, n. 82.
Load balancer	Componente hardware o software che permette la virtualizzazione di più server su una unica entità e la suddivisione del carico su di essi.
PDC	Personal Digital Certificate
Punto di accesso	Struttura tecnologica-organizzativa che fornisce ai soggetti abilitati esterni al dominio giustizia i servizi di connessione e di trasmissione telematica dei documenti informatici relativi al processo,
SAML	Security Assertion Markup Language. Linguaggio basato su XML

	utilizzato per lo scambio di informazioni di autenticazione e autorizzazione tra domini distinti, detti Identity Provider e Service Provider
SSO	Single Sign On
Web Service	Applicazione software le cui funzionalità sono descrivibili, identificabili ed usufruibili tramite linguaggio XML; le interazioni con altre applicazioni vengono effettuate tramite scambio di messaggi basati su XML con l'utilizzo di protocolli Internet (HTTP)

3 IL SISTEMA DI CERTIFICAZIONE DELL'IDENTITÀ REGIONALE

ARPA (Autenticazione Ruoli Profili Applicazioni) è un sistema specializzato che permette ad un utente di autenticarsi una sola volta e di poter accedere poi a tutte le risorse informatiche alle quali è abilitato.

ARPA
fornisce:

- un sistema centralizzato di gestione delle identità
- un sistema scalabile, sia in termini di numero di utenze che di numero delle ap plicazioni che possono agganciarsi a esso per la gestione delle utenze
- un sistema pienamente compatibile con gli standard più diffusi, SAML v.2.0, XACLM 2.0, SOAP 2.0, e sviluppato completamente in Java Enterprise Edition (Java EE o Java J2EE)
- un sistema che garantisce la massima sicurezza, mediante il ricorso a protocolli di comunicazione sicuri (HTTPS) e opportune politiche, ampiamente configura
  bili, di accesso e visibilità dei dati.

Il sistema certifica l'utente e lo abilita ad interfacciarsi ai servizi esposti. Per garantire al meglio questa funzionalità è necessario avere massima affidabilità e sicurezza nella fase di autenticazione che può avvenire tramite *smart card* con certificato d'identità. O in maniera alternativa con username e password.

Per quanto riguarda però il progetto "Cancelleria Telematica", al fine di garantire la massima sicurezza e l'integrità dei dati e delle informazioni archiviate e veicolate presso il Data Center Regionale l'identificazione **avverrà esclusivamente tramite smartcard**

Si ricorda inoltre che, nel contesto del Piano sanitario regionale 2008-2010, in Toscana è stata distribuita a tutti i cittadini una CNS (la Carta sanitaria regionale), che garantisce il riconoscimento del titolare, tutelandone la privacy e permettendo l'accesso a tutte le applicazioni protette da ARPA, secondo le caratteristiche di profilatura legate ai ruoli degli utenti ed ai relativi diritti.

3.1 Architettura logica

L'architettura logica dei sottosistemi e dei componenti è descritta nel disegno "Architettura logica" ed è composta da tre aree funzionali principali, corrispondenti ai seguenti sottosistemi:

Role manager: sottosistema che verifica che gli utenti abbiano diritto ai ruoli che dichiarano di possedere, interrogando, attraverso una serie di Adapter, le diverse fonti dati. Consente di gestire ruoli, criteri, risorse e l'associazione tra essi.

Portal: sottosistema con il compito dell'autenticazione degli utenti e del control lo degli accessi alle risorse disponibili attraverso il portale. E' responsabile della costruzione del desktop per l'utente autenticato e profilato all'interno del porta le. Comprensivo di servizio di directory.

Componenti esterne all'architettura

Servizi Applicativi (o service provider):applicazioni che utilizzano l'infrastruttura e che sono protette dai meccanismi di access management dell'infrastruttura

Fonti dati o attribute authority: servizi che, interrogati dal role manager, certifi cano ruoli e attributi utente.

Strumenti per monitoraggio proattivo dell'infrastruttura e gestione (caricamenti massivi, statistiche, etc.)

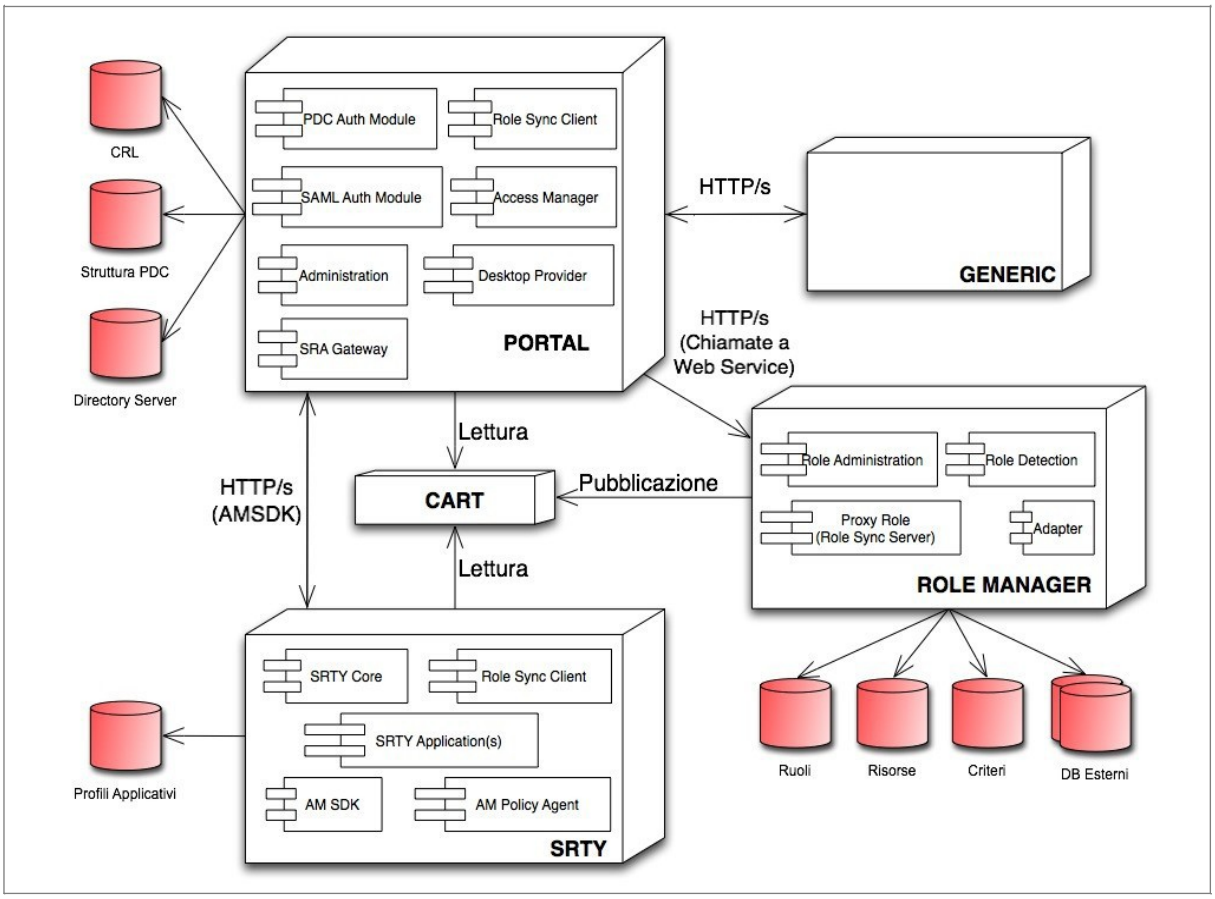


Figura 1 - Architettura logica

3.2 Architettura fisica

La figura seguente illustra l'architettura fisica della soluzione attuale. I sistemi sono acceduti attraverso il load balancer che permette bilanciamento di carico e fault tolerance in caso di fermo di un nodo.

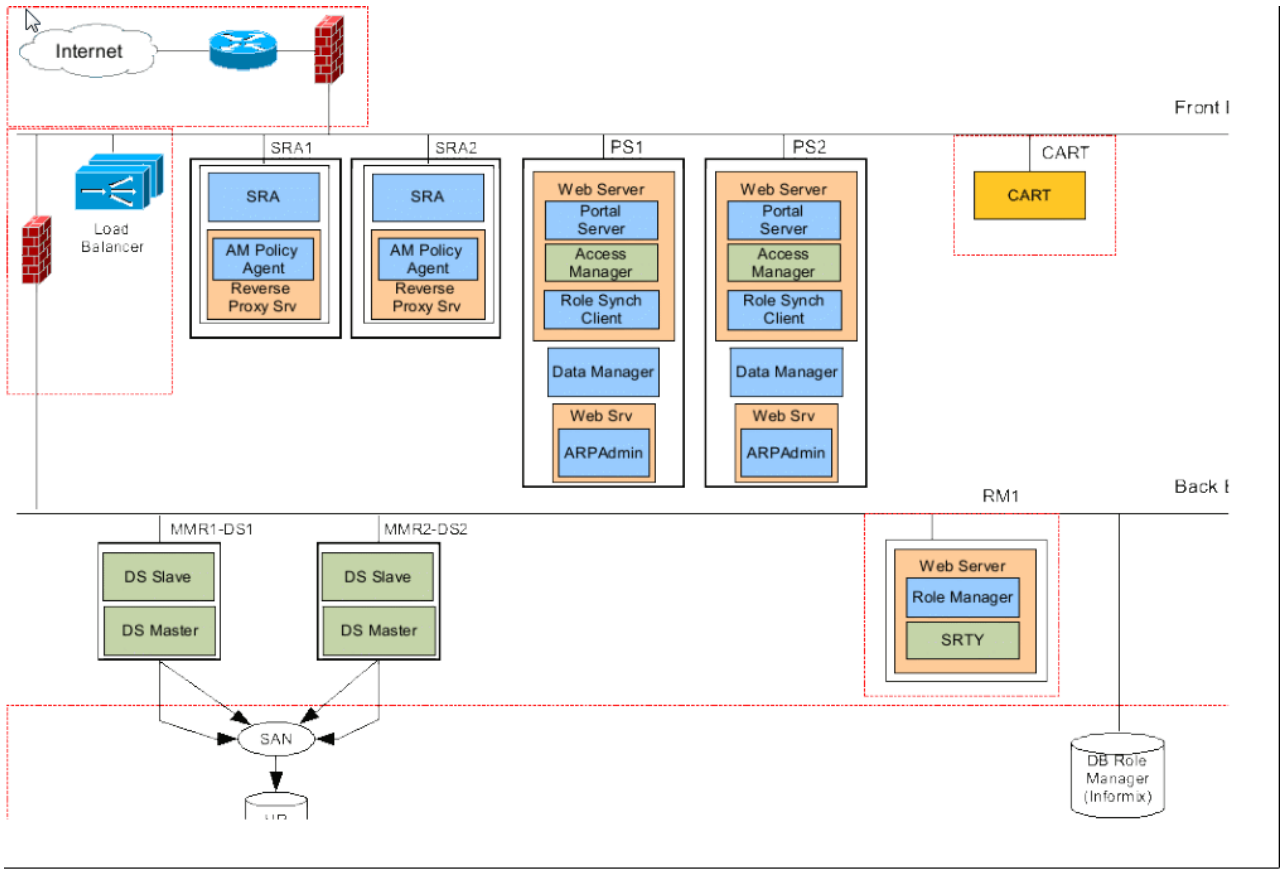


Figura 2 - Architettura fisica

La soluzione distribuisce i principali componenti dell'architettura logica di ARPA, su una serie di sistemi distribuiti tra la rete di Front End e quella di Back End. La rete di Front End è visibile dalla Intranet/Internet o in qualche modo raggiungibile da una richiesta di connessione del client (browser), mentre la rete di Back End è visibile solo dalla rete di Front End.

E' importante rilevare come l'intera infrastruttura è caratterizzata da completa ridondanza ad ogni livello (dispositivi, sistemi, componenti software) ed assenza di single-point-of-failure, per garantire la continuità di servizio.

4 L'ACCESSO AUTENTICATO

4.1 Autenticazione basata su PDC (Personal Digital Certificate)

L'autenticazione basata su PDC prevede il riconoscimento di carte CNS e CIE. Il sistema è in grado di autenticare ed autorizzare tutti gli utenti che tentano l'accesso al sistema presentando un PDC valido.
Un avvocato non autenticato accede a Cancelleria Telematica (punto d'accesso regionale) presentando un PDC (CNS o CIE); il sistema valida il certificato verificando che non sia scaduto e che sia firmato da una CA riconosciuta. Il sistema considera riconosciute e valide tutte le CA registrate in fase di configurazione nel suo database dei certificati. Se la verifica effettuata fallisce l'intero processo di autenticazione fallisce. L'elenco dei certificati è aggiornato con la lista dei certificati dei certificatori autorizzati da DigitPA.

Viceversa, nel caso in cui il PDC è validato con successo, si da inizio al vero e proprio processo di riconoscimento implementato dall'Access Manager mediante i meccanismi di autenticazione predisposti.

In questo contesto si inserisce l'interazione tra l'albo telematico degli ordini degli avvocati e l'infrastruttura di autenticazione. Nell'ambito di ARPA sono definiti, dal componente role-manager ,i ruoli istituzionali e la fonte dati da interrogare per l'attribuzione del ruolo corretto all'utente avvocato loggato. Le fonti dati vengono interrogate tramite opportuni adapter. Vedi oltre: par. 6 - Integrazione con il punto d'accesso regionale

Nel caso in cui il certificato risulti scaduto, oppure in un formato non valido, oppure revocato, il processo di autenticazione fallisce.
Il certificato passa quindi al primo modulo di autenticazione, CheckCertificateModule, che ne verifica la validità in termini di scadenza e revoca; in particolare, se il certificato non risulta scaduto ed in un formato sintatticamente corretto, viene verificato che non sia presente in alcuna lista di revoca legata al suo ente emettitore.

Il secondo passo della catena di autenticazione dipende da come l'utente abbia deciso di accedere al sistema: utilizzando una CNS o una CIE.

Nel caso in cui un utente abbia deciso di utilizzare una CNS, il modulo che entra in gioco è PDCAuthModule, altrimenti CIEAuthModule.

Entrambi questi moduli di autenticazione hanno come principale obiettivo quello di recuperare le informazioni utente a partire dai certificati ed altre informazioni inviate con questi.
Nel caso delle CIE, il certificato è accompagnato da ulteriori dati utente recuperati dalla carta.
I passi successivi, come il primo, sono indipendenti dal tipo di carta utilizzata per l'accesso e quindi si procede allo stesso modo, sia nel caso dell'utilizzo di una CIE, sia nel caso dell'utilizzo di una CNS.
Il controllo successivo è la verifica dell'esistenza, nel Directory Server di portale, di un utente che abbia l'attributo uid uguale al valore del codice fiscale presente nel certificato appena validato: se l'utente esiste, il processo di autenticazione termina con successo altrimenti parte il processo di self-registration. Una volta terminato con successo il processo di autenticazione, viene mostrato il desktop dell'applicazione ed i servizi offerti.

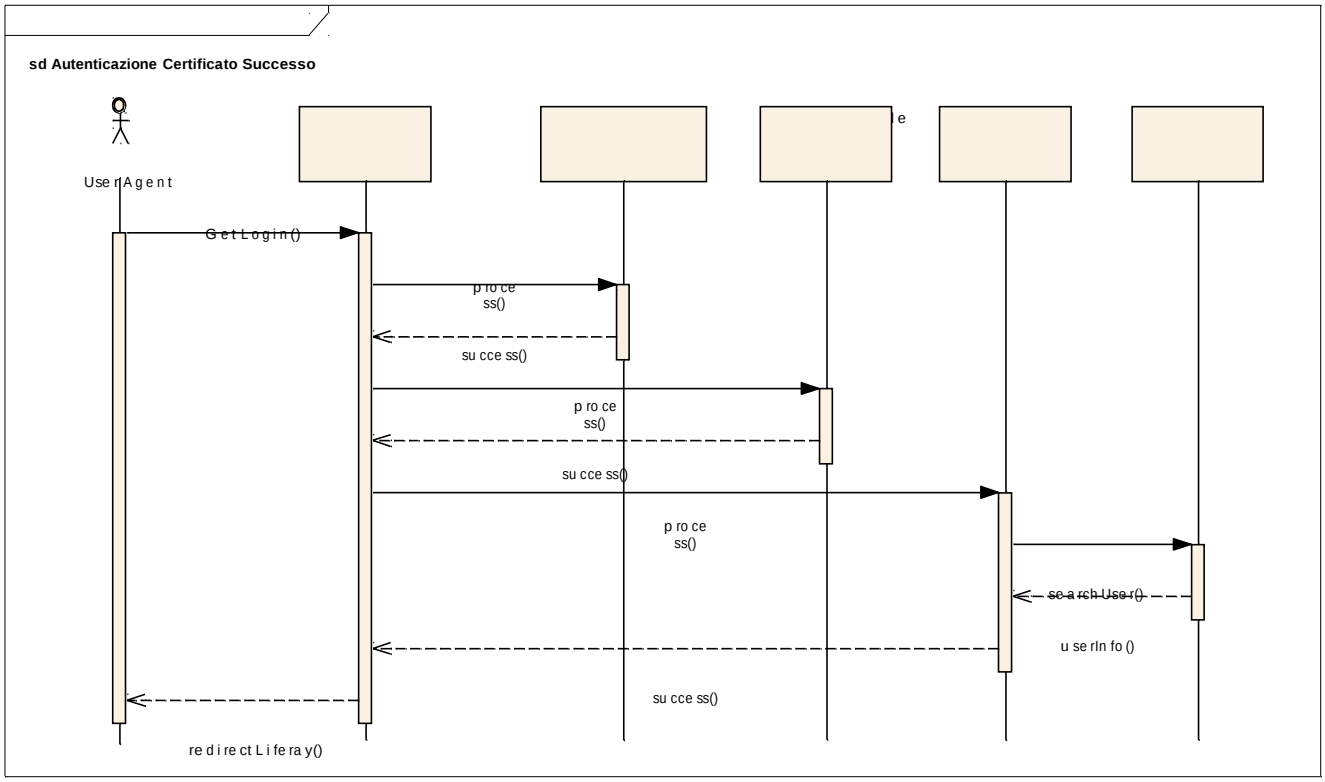


Figura 3 - Autenticazione tramite certificato

4.2 Self-Registration

Il processo di self-registration ha luogo quando, al termine di una procedura di autenticazione basata su PDC avvenuta con successo, l'utente, titolare del certificato validato, non sia presente sul Directory Server del portale.

Il processo di self-registration fa parte del processo di autenticazione e quindi come tale deve essere sviluppato come modulo di autenticazione dell'Access Manager. In particolare, il modulo in questione è RoleAuthModule .

In fase iniziale il RoleAuthModule recuperera tutti i ruoli definiti dal ROLE MANAGER e li presenta all'utente mediante una form HTML.

A questo punto, l'utente sceglie i ruoli tra un elenco e li invia all'Access Manager che li passa a sua volta al modulo di autenticazione. Ad esempio ad un avvocato si presenteranno il ruolo avvocato e cittadino se poi è un avvocato della Regione Toscana anche il ruolo di dipendente Regionale
L'Access Manager li processa verificandone la veridicità: esso infatti verifica tutte le coppie ruolo/utente, per ogni ruolo scelto, appoggiandosi al DataManager che implementa richieste ai web service esposti dal ROLE MANAGER.
Se la verifica dei ruoli va a buon fine l'account relativo all'utente è creato nel Directory Server.

In attesa di un responso del processo di verifica delle coppie ruolo/utente, l'utente può soltanto accedere ad un desktop temporaneo.

5 COMPONENTI DEI SOTTOSISTEMI

5.1 Sottosistema Portal

Il sottosistema include i seguenti componenti:

Desktop Provider: Costruisce il desktop personalizzato per l'utente in base al suo ruolo.

PDC Auth Module: Il Personal Digital Certificate (PDC) Module è la componente che implementa il requisito di autenticazione basata sulla verifica della validità del certificato digitale inviato dall'utente in fase di richiesta di servizio (accesso al portale); tecnicamente è quello che si definisce un modulo di autenticazione del portale.

SAML Auth Module: È la componente che implementa il requisito di autentica zione basata sulla verifica di asserzioni SAML (Security Assertion Markup Lan guage).

Administration: Fornisce le funzionalità di amministrazione del sistema.

Role Sync Client: Legge / interpreta / gestisce i messaggi pubblicati dal Role Sync Server sincronizzando le informazioni opportune, relative a ruoli, risorse e attributi, nel Directory Server.

Access Manager: Si occupa di fornire le funzionalità di autenticazione e controllo degli accessi e fornisce l'identità dell'utente ai servizi applicativi che fanno uso di AMSDK

OpenSSO: Componente che, utilizzando AMSK, ottiene l'identità dell'utente e la invia ai servizi applicativi che fanno uso di SpAgent

SRA Gateway: La componente che è in grado di fornire la protezione in termini di sicurezza di accesso a tutte le altre.

Gestione Informazioni Utenti: L' applicazione di back-office per la gestione delle informazioni degli utenti. Realizzata in Java modifica le info utente memorizzate sul servizio di directory.

5.2 Sottosistema Role Manager

Il sottosistema include i seguenti moduli

Role Detection: Si occupa principalmente di verificare l'appartenenza di un utente, ad un determinato ruolo. L'utente è identificato attraverso il proprio Co

dice Fiscale.

Il modulo di Role Detection espone due servizi:

- Check Role: Esegue la verifica di cui sopra (veridicità dei ruoli). Per ogni ruolo valido restituisce gli attributi valorizzati per l'accesso alle applica zioni da esso autorizzate.
- Find Role: Restituisce l'elenco dei ruoli definiti nel sistema.
- Il modulo di Role Detection, nel processo di verifica e discovery dei ruoli, può avvalersi di uno o più Adapter in base ai criteri definiti per ciascun attributo.

Proxy_Role (Role Sync Server): Pubblica i messaggi di notifica corrispondenti alla creazione, modifica e cancellazione di ruoli nel ROLE MANAGER.

Role Administration: Consente ad una specifica figura di amministratore, l'Am ministratore dei Ruoli, la gestione dei ruoli, delle risorse e dei criteri.

Adapter: Il modulo espone dei servizi di base al modulo di Role Detection, con un'interfaccia ben definita, al fine di consentire l'interrogazione delle fonti dati esposte dai Certificatori di Ruolo. Le modalità di utilizzo di un Adapter rispetto, a quali fonti dati contattare, quali credenziali d'accesso utilizzare, quali attributi recuperare sono definite in fase di configurazione dei criteri.

5.3 Sottosistema OpenSSO

OpenSSO agisce da Identity Provider nei confronti dei soggetti pubblici che non dispongono di un proprio meccanismo di autenticazione. In questo modo viene garantita la centralità del meccanismo di autenticazione ed autorizzazione. OpenSSO deve essere visto logicamente come un'estensione del blocco PORTALE per permettere la generazione delle asserzioni SAMLv2.

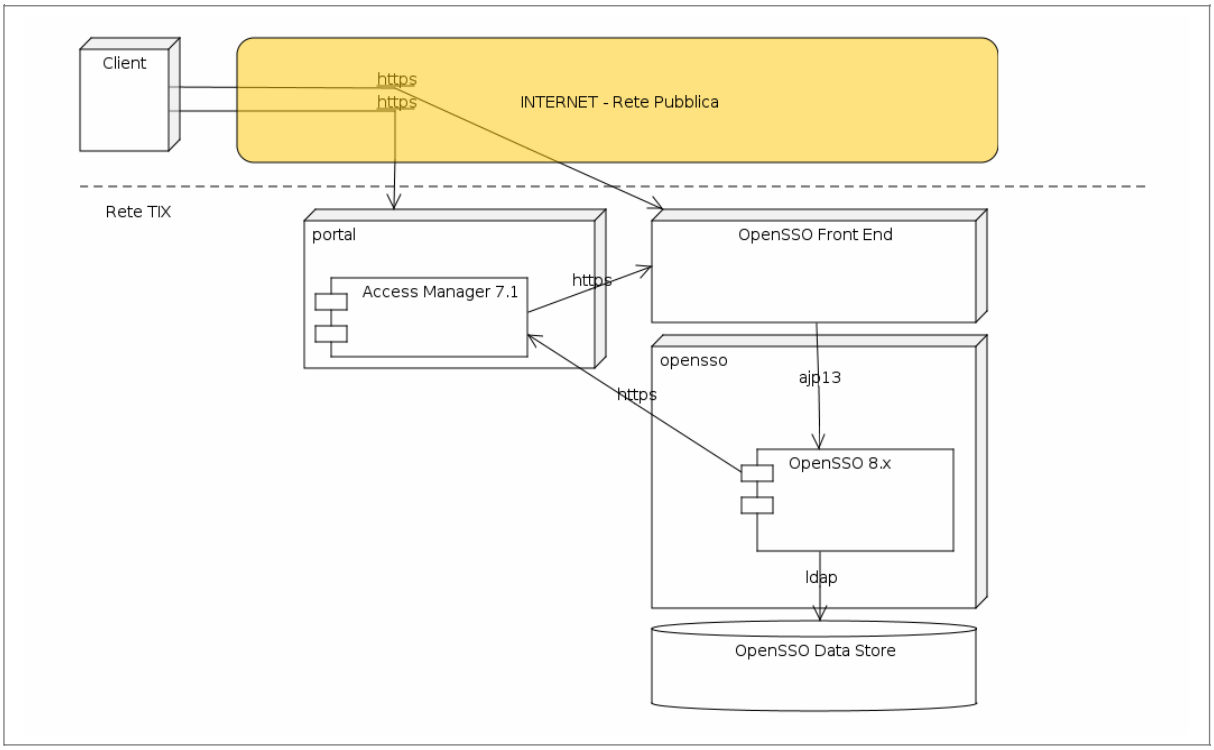


Figura 4 - Componente OpenSSO

5.4 Sottosistema Servizi applicativi

E' composto dai servizi applicativi integrati con l'infrastruttura. L'integrazione delle applicazioni e dei servizi web con il sistema di autenticazione e autorizzazione adottato dalla Regione Toscana richiede il rispetto di alcune caratteristiche di base che devono essere rispettate affinché l'applicazione possa integrarsi con ARPA, che comunque hanno un impatto minimo con la struttura dell'applicazione stessa. Le modalità di integrazione previste sono:

AMSDK: il servizio applicativo accede al componente access manager

SPAGENT: il servizio applicativo è protetto dal componente Spagent che costi tuisce un preprocessore in grado di gestire il colloquio basato su SAML con il componente OpenSSO

Reverse Proxy: il servizio applicativo è protetto dal componente SRA Gateway

5.5 Monitoraggio dell'infrastruttura

E' implementato un sistema specifico di test e misure che consente la verifica del buon funzionamento delle componenti applicative dell'infrastruttura complessiva. Tale sistema si riferisce ai singoli nodi/componenti che sono generati da apposite funzioni esposte dagli stessi nodi/componenti.

Altre misure sono invece orientate alla creazione di statistiche d'uso della infrastruttura. Tali misure vengono realizzate tramite sonde che analizzano e collezionano le informazioni nel tempo. Le misure vengono realizzate mediante script che verranno resi disponibili e dovranno essere adattati alla nuova infrastruttura.

Il sistema è in grado di monitorare anche le componenti esterne alla infrastruttura centrale (fonti dati e servizi).

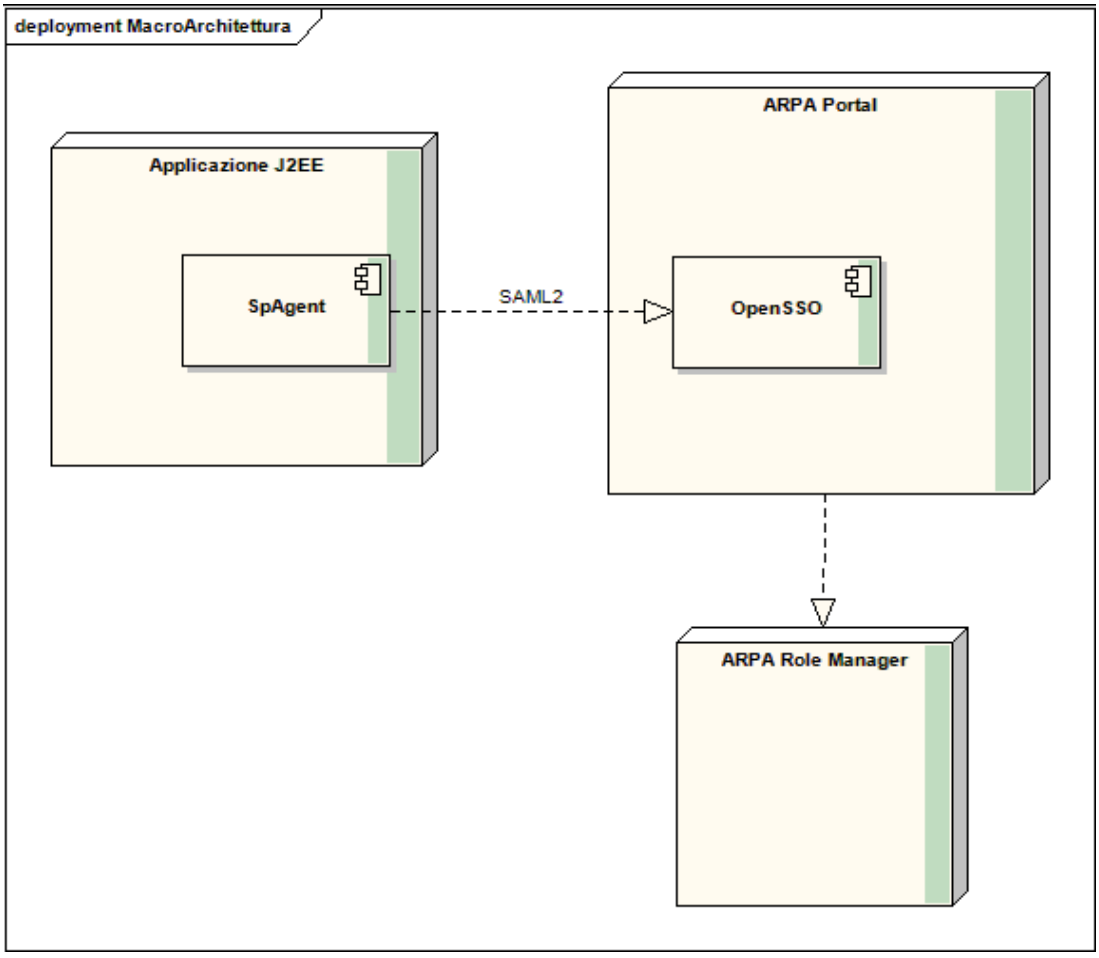
6 INTEGRAZIONE CON IL PUNTO D'ACCESSO REGIONALE

Nell'ambito del progetto l'integrazione col sistema ARPA seguirà due direttrici fondamentali:

- L'utilizzo dei servizi di autenticazione e profilazione forniti da ARPA, per il riconoscimento degli utenti ed il loro accesso al punto d'accesso regionale sulla base dei ruoli posseduti;
- La realizzazione di *fonti dati* dai consigli dell'ordine degli avvocati ad uso dell'infrastruttura ARPA (in particolare del componente Role Manager, che all'interno di ARPA assume appunto il ruolo di Gestore dei Ruoli).

L'integrazione dell'applicazione avviene installando l'SpAgent e le relative librerie, ed implementando il codice applicativo che realizza il mapping tra le informazioni trasmesse da ARPA (utenti e ruoli) ed i meccanismi di prolifazione propri del punto d'accesso regionale.

L'SpAgent è sostanzialmente un filtro J2EE che, impiantato nel container in cui è istallato il punto d'accesso regionale , la protegge da accessi non autorizzati e consente di fruire dei servizi di *autorizzazione* e *policy enforcement* di ARPA. Il tutto avviene attraverso scambio di asserzioni standard SAML2 con l'infrastruttura centrale di ARPA (in particolare col componente OpenSSO all'interno del blocco PORTAL), dove sono implementate tutte le funzionalità di riconoscimento delle credenziali dell'utente e verifica dei ruoli.



In ARPA, la fonte dati è un componente che viene interrogato dal Role manager per l'attribuzione dei ruoli agli utenti loggiati, attraverso opportuni *adapter*, a seconda dell'interfaccia applicativa (protocollo e formati) offerta dalle fonti dati stesse.

Il punto d'accesso regionale utilizza la soluzione in cui l'implementazione delle fonti dati è basata web services.

La comunicazione tra il punto d'accesso regionale e l'albo dei consigli dell'ordine degli avvocati avverrà secondo RFC n° 146 di Regione Toscana.

Nel caso si verifichino modifiche ai valori di uno o più attributi all'interno della fonte dati per uno o più utenti verrà utilizzato l' RFC 156, che standardizza le modalità con cui l'albo degli avvocati trasmette le variazioni al Role-Manager, il quale a sua volta provvederà a valutarne l'impatto sui ruoli ed a propagare ai vari sottoscrittori (tipicamente, il blocco PORTAL di ARPA) le eventuali variazioni avvenute sui ruoli.

Di seguito lo schema XSD per la fonte dati proveniente dal consiglio dell'ordine degli avvocati

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
<xs:element name="avvocati">
<xs:complexType>
<xs:sequence>
<xs:element maxOccurs="unbounded" ref="avvocato"/>
</xs:sequence>
<xs:attribute ref="xsi:noNamespaceSchemaLocation" use="required"/> </xs:complexType>
</xs:element>
<xs:element name="avvocato">
<xs:complexType>
<xs:sequence>
<xs:element ref="cognome" minOccurs="1" maxOccurs="1"/>
<xs:element ref="nome" minOccurs="1" maxOccurs="1"/>
<xs:element ref="cf" minOccurs="1" maxOccurs="1"/>
<xs:element ref="specializzazione" minOccurs="1" maxOccurs="1"/>
<xs:element ref="studio_legale" minOccurs="0" maxOccurs="1"/>
<xs:element ref="indirizzo_studio" minOccurs="1" maxOccurs="1"/>
<xs:element ref="comune_studio" minOccurs="1" maxOccurs="1"/>
<xs:element ref="provincia_studio" minOccurs="0" maxOccurs="1"/>
<xs:element ref="cap_studio" minOccurs="0" maxOccurs="1"/>
<xs:element ref="telefono_studio" minOccurs="1" maxOccurs="1"/>
<xs:element ref="fax_studio" minOccurs="0" maxOccurs="1"/>
<xs:element ref="cellulare" minOccurs="0" maxOccurs="1"/>
<xs:element ref="ente" minOccurs="0" maxOccurs="unbounded"/>
<xs:element ref="messaggio" minOccurs="0" maxOccurs="1"/>
<xs:element ref="email" minOccurs="1" maxOccurs="1"/>
<xs:element ref="data_iscrizione_albo" minOccurs="1" maxOccurs="1"/>
<xs:element ref="foro_appartenenza"/ minOccurs="1" maxOccurs="1">
<xs:element ref="cassazionista" minOccurs="1" maxOccurs="1"/>
<xs:element ref="data_iscrizione_cassazionisti" minOccurs="0" maxOccurs="1"/>
<xs:element ref="validita" minOccurs="1" maxOccurs="1"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="cognome" type="xs:string"/>
<xs:element name="nome" type="xs:string"/>
<xs:element name="cf" type="xs:string"/>
<xs:element name="specializzazione" type="xs:string"/>
<xs:element name="studio_legale" type="xs:string"/>
<xs:element name="indirizzo_studio" type="xs:string"/>
<xs:element name="comune_studio" type="xs:string"/>
<xs:element name="provincia_studio" type="xs:string"/>
<xs:element name="cap_studio" type="xs:integer"/>
<xs:element name="telefono_studio" type="xs:integer"/>
<xs:element name="fax_studio" type="xs:integer"/>
<xs:element name="cellulare" type="xs:integer"/>
<xs:element name="ente" type="xs:string"/>
<xs:element name="messaggio" type="xs:string"/>
<xs:element name="email" type="xs:string"/>
<xs:element name="data_iscrizione_albo" type="xs:date"/>
<xs:element name="foro_appartenenza" type="xs:string"/>
<xs:element name="cassazionista" type="xs:boolean"/>
<xs:element name="data_iscrizione_cassazionisti" type="xs:date"/>
<xs:element name="validita" type
```

6.1 Modalità di integrazione con il Punto di Accesso "Cancelleria Telematica"

L'utente può accedere al Punto di Accesso in due modalità:

1. Attraverso il sistema Portale Sicuro
2. Direttamente sull'applicazione

Entrambi gli ingressi utilizzano per l'autenticazione il modulo ARPA realizzato da Regione Toscana. Le modalità di interazione e autenticazione sono analoghe, di seguito diamo una descrizione della prima modalità; la seconda è analoga.

L'utente accede al modulo di autenticazione di Regione Toscana (ARPA) con la smart card e dichiara il proprio ruolo. Nel caso in cui dichiara di appartenere ad uno dei ruoli certificati dal Role Manager (avvocato, CTU,…) viene verificato attraverso il modulo Certificatore di Ruolo di ARPA se effettivamente appartiene a quel ruolo. In caso affermativo l'utente può accedere ai sistemi di Cancelleria Telematica. Nel caso in cui l'utente non appartiene a nessuno dei ruoli certificati viene censito come cittadino e la sua utenza viene gestita dai profili applicativi di Cancelleria Telematica.

Le modalità di interazione sono:

- *Accesso al sistema per un utente registrato*. L'utente registrato accede al sistema accesso sicu ro e dichiara il proprio ruolo. Il Role Manager verifica le credenziali e, se necessario interroga il certificatore di ruolo, concede o meno l'accesso settando gli attributi che verranno poi gestiti dal l'applicativo Cancelleria Telematica;
- *Accesso al sistema per l'utente Cittadino*. il cittadino accede al sistema accesso sicuro e il role manager verifica le sue credenziali (smart card) e concede l'accesso al sistema.

Di seguito i casi d'uso del modulo di integrazione tra Cancelleria Telematica e ARPA

Accesso utente registrato. L'utente accede al portale dei servizi sicuri di Regione Toscana utilizzando la smart card, viene interrogato il Role Manager per verificare se l'utente appartiene a quel ruolo e se è ancora valido (per esempio nel caso si tratti di un avvocato occorre verificare che non sia stato sospeso o interdetto,

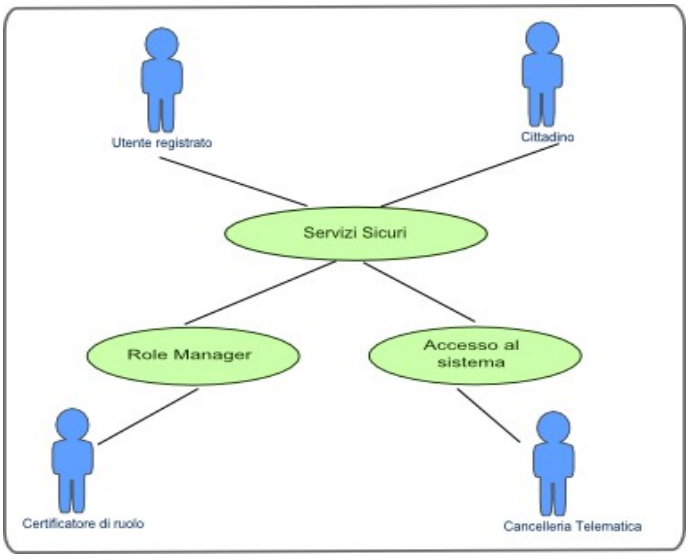


Figura 5 – Use Case integrazione Cancelleria - ARPA

in questo caso negherà l'accesso). Il Role Manager invia gli attributi dell'utente a Cancelleria Telematica che farà accedere l'utente alle funzionalità in base alla mappatura con il profilo applicativo.

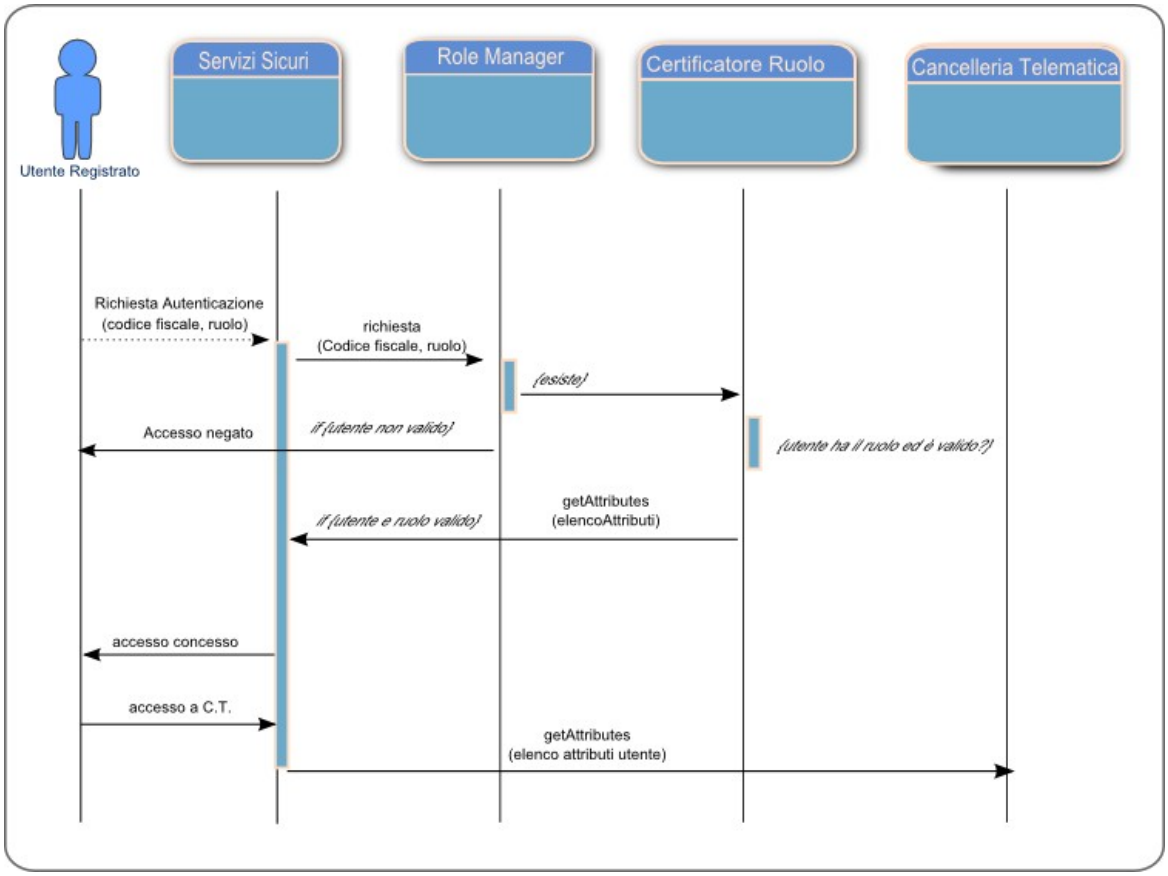


Figura 6 – Sequence Diagram Accesso utente registrato

Accesso cittadino. L'utente accede al portale dei servizi sicuri di Regione Toscana utilizzando la smart card e accede al sistema Cancelleria Telematica come cittadino. nel caso in cui il suo codice fiscale corrisponda a un profilo diverso non ancora inserito nel Role Manager sarà l'applicazione Cancelleria Telematica a provvedere alla profilazione e alla presentazione delle funzionalità in modo appropriato.

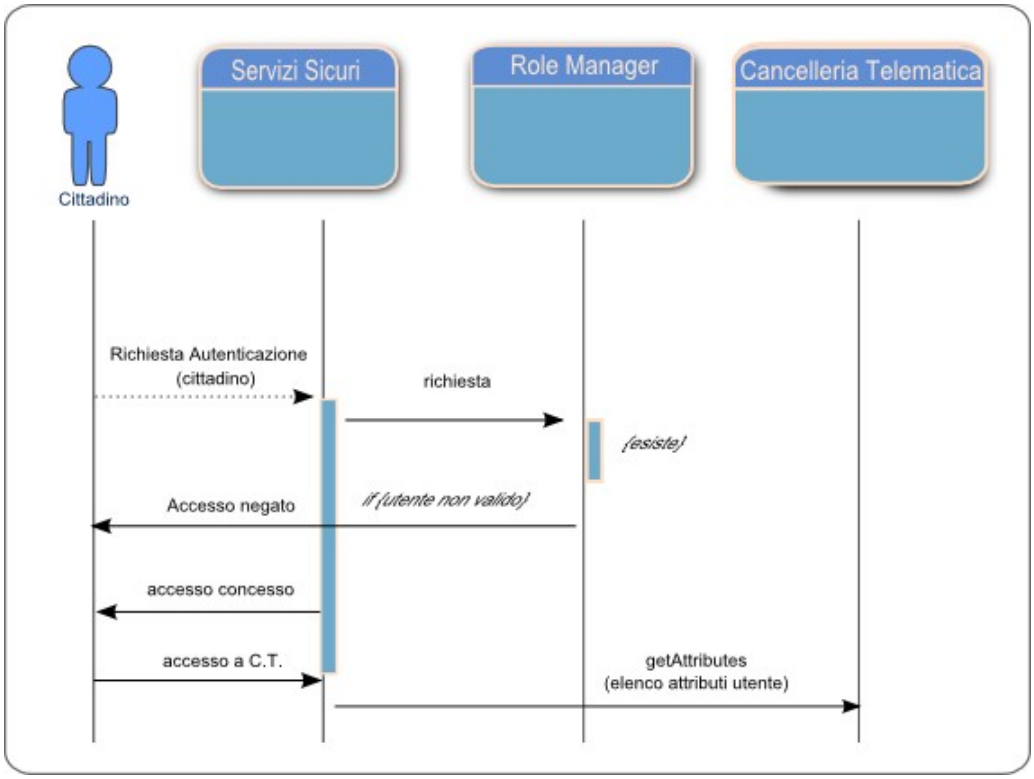


Figura 7 – Sequence Diagram
Accesso cittadino

6.2 Modalità di integrazione cancelleria telematica posta elletronica certificata

La cancelleria telematica per fornire un servizio più semplice e intuitivo ai professionisti è integrata con il flusso PEC sia in entrata che in uscita dagli uffici giudiziari.

L'architettura per il flusso di deposito atti da un avvocato verso un ufficio giudiziario è descritta nella fig 8. in cui si evidenziano le seguenti componenti

- Cancelleria Telematica;
- Pubblicatore GWPEC;
- Proxy GWPEC;
- Infrastruttura di Cooperazione Applicativa;
- Gateway PEC;
- LDAP.
-

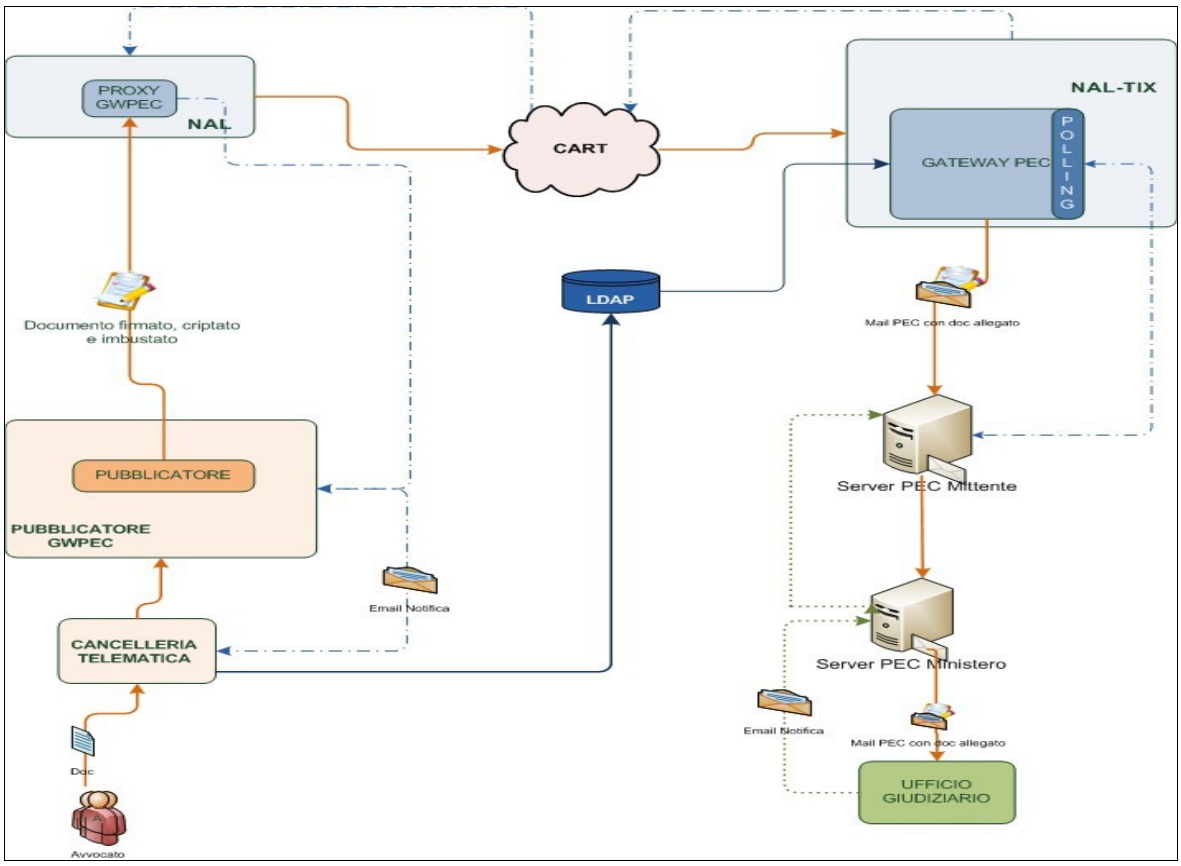


Figura 8: Architettura flusso deposito atti

Pubblicatore GWPEC

Il Pubblicatore GWPEC, consente l'invio dei documenti per il deposito degli atti. Il sistema verificherà la presenza di documenti da depositare. Nel caso in cui ci sia un documento da depositare, si occupa di criptarlo e di imbustarlo secondo le specifiche tecniche definite dal Ministero della Giustizia.

Il modulo si occuperà inoltre di ricevere le notifiche e depositarle nel database di CancelleriaTelematica per la loro gestione

Gateway PEC

Il Gateway PEC è il modulo che si occupa di inoltrare le mail con l'allegato preparato. Il messaggio oltre all'allegato dovrà contenere anche l'indicazione del mittente (casella mail PEC dell'avvocato) Il gateway recupera questa informazione del mittente nell'LDAP e inoltrare la mail .

Il modulo di polling installato su questo componete è implementato utilizzando una tabella di appoggio in cui vengono inserite le mail da cui si attende una notifica. Nel momento in cui sono state ricevute tutte e quattro le notifiche la mail (riga della tabella) può essere marcata, in modo tale da non far più parte delle mail da verificare. Questo modulo ha anche il compito di intercettare i biglietti di Cancelleria (per esempio lo spostamento di una udienza).

LDAP

Contiene le informazioni degli avvocati necessarie per l'invio, indirizzo pec, server di posta, credenziali per l'accesso alla mail.

Flusso Deposito Atti

Il flusso per i deposito atti attraverso la PEC è il seguente:

Il professionista che vuole depositare un atto attraverso il sistema Cancelleria Telematica si collega al sistema viene riconosciuto e autorizzato ad accede al fascicolo a cui l'atto si riferisce e inserisce il file firmandolo digitalmente.

Il sistema imbusta il documento criptandolo secondo le specifiche definite dal Ministero della Giustizia ed invia una mail PEC all'indirizzo dell'ufficio giudiziario competente La mail inviata ha come indirizzo mittente quello di PEC del professionista.

La mail viene; i sistemi ministeriali intercettano la mail ed effettuano i controlli formali (sulla correttezza del formato e della cifratura). L'ultimo controffo viene effettuato dal cancelliere sul sistema SICID

Questo flusso produce 4 mail di notifica:

1. Presa in carico. Il server di posta certificata mittente nel momento in cui prende in carico la mail invia al mittente una notifica di presa in carico.
2. Avvenuta consegna. Sempre il server di posta certificata mittente quando consegna al server di posta certificata destinatario la mail invia una notifica di avvenuta consegna.
3. Controlli formali superati. I sistemi ministeriali intercettano il messaggio ed effettuano i controlli formali sulla mail. Al termine delle verifiche viene inviata una

mail con l’esito dei controlli. La data di superamento delle verifiche formali costituisce la data ufficiale di deposto dell’atto.

4.Accettazione dell’atto . Il cancelliere al termine delle verifiche sul documento, accetta il documento e il sistema ministeriale invia la mail di avvenuta accettazione. A questo punto può essere inviato il biglietto di cancelleria e l’atto può essere reso disponibile alla controparte.

Il sistema Cancelleria Telematica intercetta, utilizzabdo il modulo polling , tali notifiche e le mostra utilizzando una maschera web e rende visibile lo stato dell'invio.