

ARCHITETTURA DI SICUREZZA DEL PROGETTO CRS-SISS: REGIONE LOMBARDIA

Mario Martinelli
Riccardo Ranza

Il sottosistema di Single Sign On & User Management (SSO/UM) ha un ruolo essenziale nel progetto Carta Regionale dei Servizi - SISS (CRS-SISS) in quanto realizza il livello di coordinamento applicativo della sicurezza (autenticazione e autorizzazione). Esso consente all'utente, cioè all'operatore socio sanitario, di presentarsi una sola volta all'extranet, anziché tante volte singolarmente a ciascun servizio richiesto. La chiave di accesso all'extranet, cioè lo strumento che consente di presentarsi all'extranet è la smart card della CRS-SISS.

Lo stesso sottosistema consente al gestore della CRS-SISS di amministrare unitariamente e coerentemente le autorizzazioni all'accesso degli utenti a tali servizi.

Il sottosistema gestisce il caso di servizi applicativi, sia in architettura client server che web browsing.

L'architettura prevede che l'utente, all'inizio del suo operare col SISS, inserisca la smart card e dia origine alla fase di Identificazione & Autorizzazione (I&A) Primaria. Questa consiste in una interazione fra il modulo di sicurezza locale alla sua postazione ed il server di SSO ed è preliminare ad ogni azione successiva. Il modulo locale e il server di SSO realizzano l'autenticazione sfruttando le componenti crittografiche della smart card.

In esito all'I&A Primaria, il modulo locale ottiene la credenziale dell'utente firmata dal server di SSO. La credenziale definisce essenzialmente il ruolo dell'utente e la sua struttura di appartenenza (cosiddetto contesto funzionale): si noti che un operatore che ricopra più incarichi nell'ambito della socio sanità dovrà esplicitare all'atto della

I&A Primaria l'incarico svolto in quel momento, in modo tale che il server di SSO selezioni automaticamente la giusta credenziale.

La successiva scelta di un servizio applicativo dell'extranet si può estrinsecare in due modi differenti, rispettivamente nel caso di soluzione applicativa client server oppure basata su web.

Si noti che il servizio applicativo dell'extranet consiste nell'esposizione (e quindi nella visibilità ed accessibilità) sul front end di competenza (ovvero porte applicative del Dominio Centrale, dell'AO, ...) del punto di accesso al servizio applicativo residente all'interno del sistema informativo (ovvero intranet) dell'Ente/Struttura (p.e. i Servizi Centrali del Dominio Centrale, il CUP dell'AO, ...).

Applicazioni client server

In questo scenario la credenziale è fornita dal client al server applicativo a cura dello strato infrastrutturale ("middleware") di Cooperazione, nell'ambito dell'I&A Secondaria che i due elementi (client e server) fanno fra loro, senza coinvolgere l'utente ma col supporto del modulo di sicurezza locale. Tale credenziale metterà in condizione il modulo di sicurezza del server di consentire o negare l'accesso di quell'utente al servizio applicativo (come meglio descritto nel seguito).

Il caso è descritto nella figura che segue:



Applicazioni basate su web

Il caso è descritto nella figura che segue:



In questo scenario, il browser della postazione dell'utente realizza l'I&A Secondaria col Web Server, senza coinvolgere l'utente ma col supporto del modulo di sicurezza locale. Sulla base di tale I&A, il modulo di sicurezza del web server ottiene dal server di SSO la credenziale dell'utente, che nell'ambito dell'I&A Secondaria che realizza col server applicativo e per tramite dello strato infrastrutturale ("middleware") di Cooperazione, viene fornita al server stesso. Tale credenziale metterà in condizione il modulo di sicurezza del server di consentire o negare l'accesso di quell'utente al servizio applicativo (come meglio descritto nel seguito).

Autorizzazione all'accesso al servizio

Come si evince dalla figura che segue, ciascun server applicativo installa un modulo di sicurezza (detto Distributed Credential Controller) il quale a sua volta è popolato a partire dal server di SSO con le informazioni che lo concernono relative all'autorizzazione all'accesso ai servizi applicativi locali (cosiddette Access Control List). Tale popolamento viene realizzato automaticamente alla partenza del modulo stesso ed in caso di variazioni nella Base Dati Sicurezza del server di SSO.

Questo modulo di sicurezza consente o nega l'accesso sulla base del confronto fra credenziale dell'utente e ACL.



Amministrazione

L'attività di amministrazione consiste principalmente nell'opportuna definizione dell'utente nella Base Dati Sicurezza (SIB: Security Information Base) e nello stabilire una relazione fra ciascun utente (o loro aggregazioni) ed i servizi applicativi consentiti.

