Università di Camerino
Scuola di scienze e tecnologie
Sezione informatica

Cohesion 2.0: l'esperienza della Regione Marche

D. Falcioni, F. Marcantoni, A. Polzonetti, B. Re (Università di Camerino)
S. Carota, M. L. Maggiulli, R. Piangerelli, A. Sergiacomi (Regione Marche)

Cohesion: cos'è questo!

Cohesion è il framework di autenticazione della Regione Marche, utilizzato per proteggere servizi e garantirne l'accesso agli utenti registrati, previa autenticazione, formato da un Identity Provider e un Service Provider.

FallDown!

~~SAML standard~~

HighLight!

Autenticazione con Smart Card CIE e CNS (Carta Raffaello)
Autenticazione User/Password
Autenticazione User/Password & PIN Carta Raffaello
Autenticazione di Dominio (Accesso automatico per dipendenti regionali)

Semplicità di integrazione

COHESION 2.0: REINGEGNERIZZAZIONE A SUPPORTO DI SAML 2.0

L'opera di reingegnerizzazione si è focalizzata sulla necessità di retrocompatibilità e trasparenza nell'aggiornamento in modo da avere un passaggio graduale e indolore per tutti i servizi che già integrano Cohesion.

Lato Identity Provider

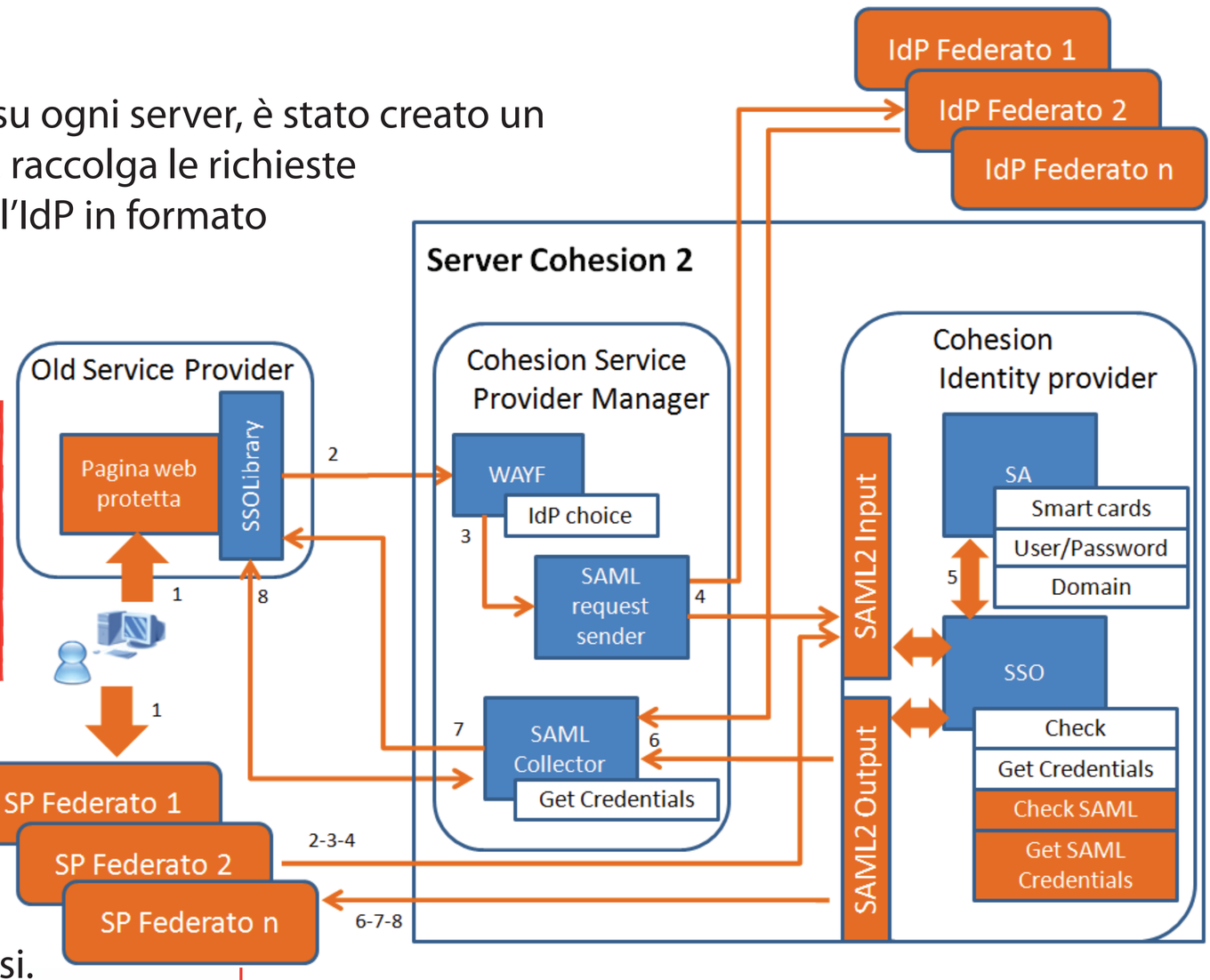
Sono stati creati ed aggiunti moduli specifici per la gestione di richieste SAML2.0 in ingresso e in uscita.
Viene gestito, oltre al proprio metadata, anche un metadata federato in cui sono presenti tutte le entità riconosciute.
I flussi interni e la gestione della sessione sono stati riadattati.

Lato Service Provider

Lasciando inalterato il lato Service Provider Installato su ogni server, è stato creato un servizio collettore che simuli le vecchie interfaccie IdP, raccolga le richieste non standard inviate dai Service Provider e le inoltri all'IdP in formato SAML2.0, facendo lo stesso per le risposte.

Elemento Disaccoppiatore!

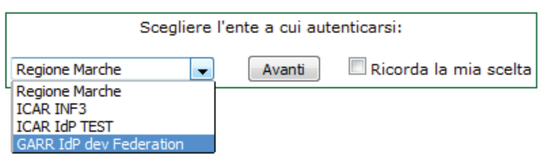
Questo nuovo componente chiamato SPManager crea una barriera tra le entità che parlano SAML2.0 e non.
Tutte le richieste inviate saranno viste lato IdP come provenienti dal SPManager il quale manterrà le associazioni per smistare correttamene la risposta al SP chiamante.



Configurazione Centralizzata!

L'SPManager integra un modulo WAYF, che legge i dati degli IdP federati, dal metadata federato, mantenuto lato IdP, e da la possibilità all'utente di sceglierea a quale Identity Provider federato autenticarsi.
La gestione della federazione non grava quindi sul Service Provider.

Servizio di autenticazione Regione Marche
Cohesion 2.0



Cohesion ha superato con successo i test pre-federazione con IDEM e l'integrazione dell'applicativo INF-3 del progetto ICAR.

Protocolli SAML2.0 supportati:
- Single Sign On in HTTP-POST
- Single Logout Protocol