Andrea Carmignani

Global Technology Service

IT Security Architect

SPC: Interoperabilità, cooperazione applicativa e Sicurezza, il ruolo IBM

Agenda

- Il modello di **G**estione **F**ederata delle **I**dentità **D**igitale in SPCoop
- Le componenti
- Gli scenari di cooperazione Web a Web Services
- Gli Impatti sulle Pubbliche Amministrazioni
- Una RoadMap per essere “Federation Ready”

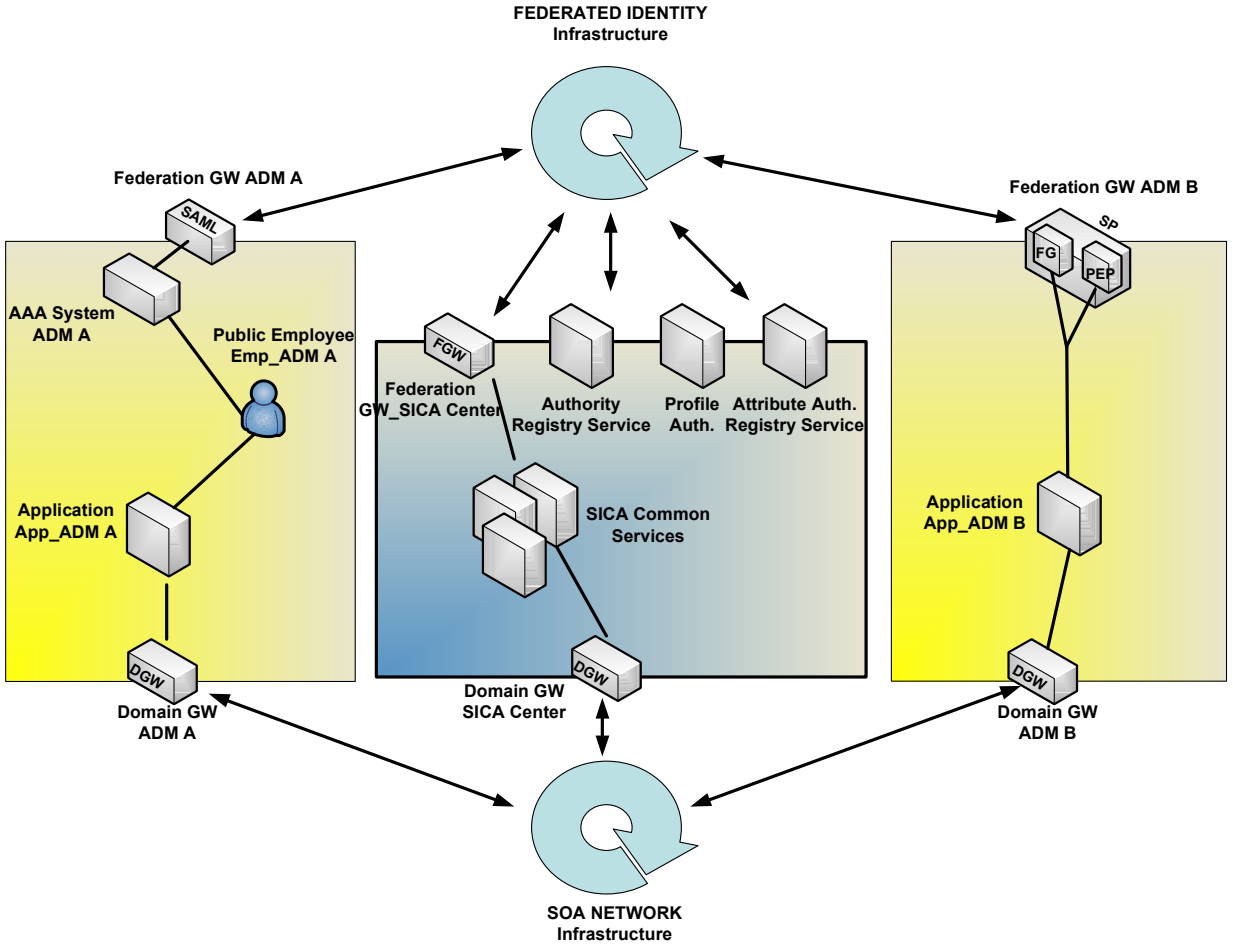
Il modello di **G**estione **F**ederata delle **I**dentità **D**igitale in SPCoop
- Esigenze -

- **Evoluzione** naturale dell'Identity management, in grado di permettere il passaggio dalla fruizione di applicazioni locali verso fruizione di applicazioni appartenenti ad altre amministrazioni ad oggi non accessibili
- **Integrazione** della sicurezza nella Cooperazione Applicativa (WEB e SOA) innalzando così la sicurezza dell'intero processo di cooperazione
- **Audit granulare** su chi accede le applicazioni appartenenti all'SPCoop

Il modello di **G**estione **F**ederata delle **I**dentità **D**igitale in SPCoop - Soluzione -

- **Approccio User Centrico**, l'utente sceglie quale profilo utilizzare per fruire del servizio;
- **RBAC,** accesso alle applicazione federate basato sui ruoli posseduti dall'utente;
- **Standard Based**, per garantire interoperabilità fra le Amministrazioni ed il CG-SICA tramite prodotti commerciale/custom ;

Modello GFID le Componenti



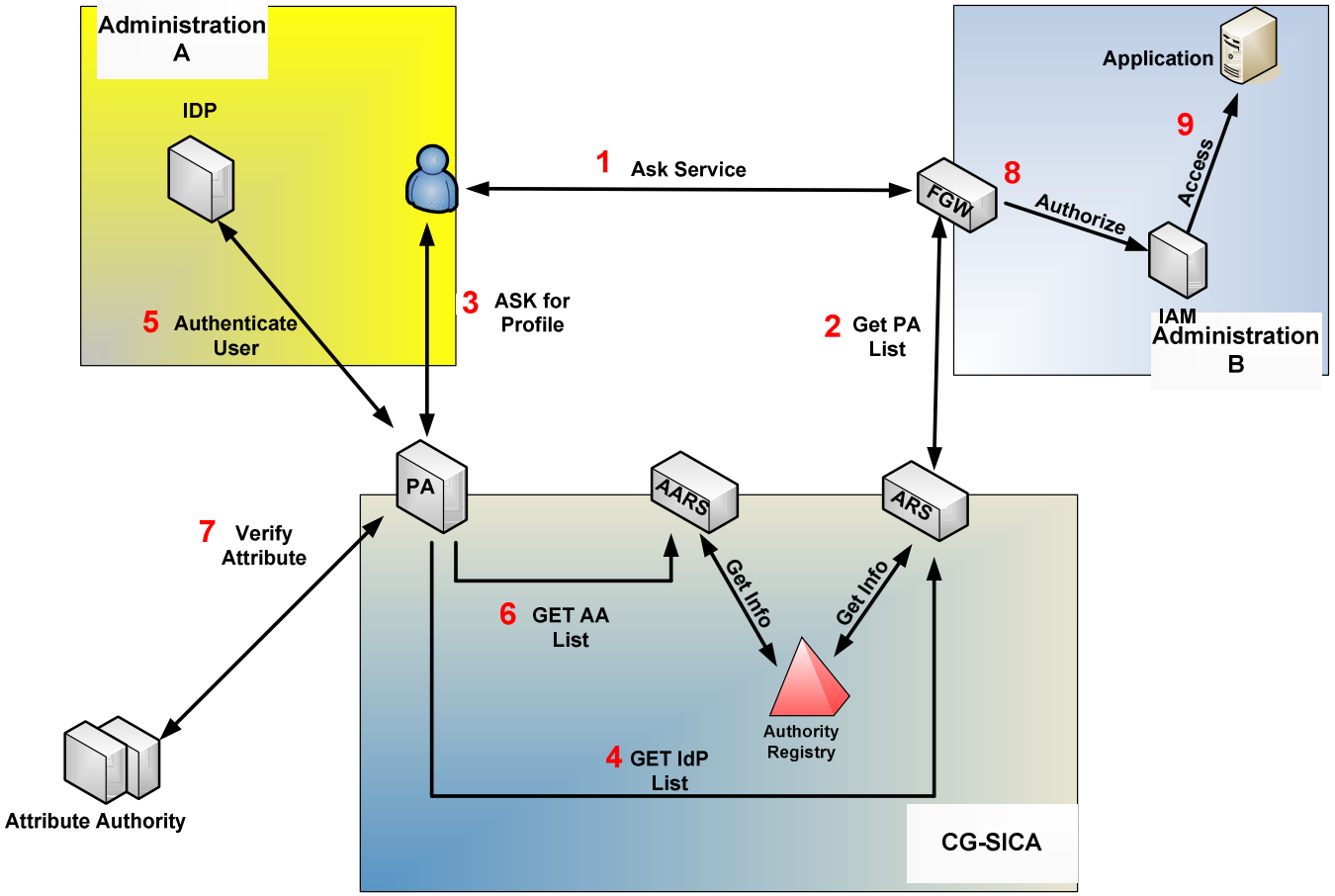
Modello GFID le Componenti

- **Service Provider:** eroga il servizio a valle di asserzioni identificative e di ruolo provenienti da un membro del dominio certificatore, è responsabile dell'erogazione del servizio e della gestione delle autorizzazioni e dell'auditing
  - Federation GW: singolo punto di contatto per tutte le richieste di accesso web alle risorse offerte
  - PeP: applica le policy di autorizzazione, prima di concedere l'accesso ai singoli servizi esposti.
- **Identity Provider**, gestisce le informazioni relative all'identità dei membri della federazione.
- **Attribute Authority**, certificare tutti o parte degli attributi componenti il profilo di un generico utente.

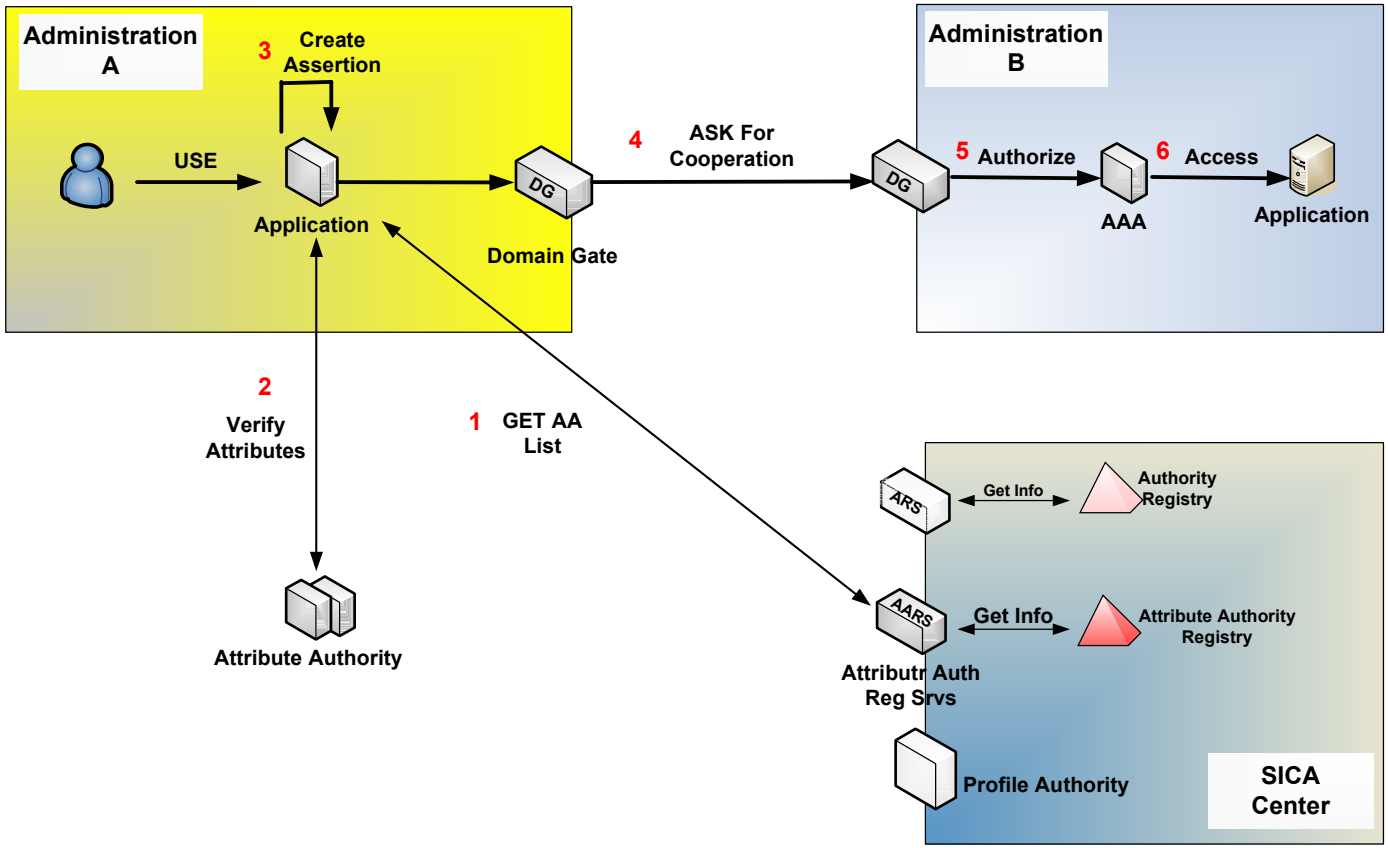
Servizi Infrastrutturali:

- **Profile Authority**, entità incaricata della gestione e manutenzione dei profili utente
- **Authority Registry Service,** fornisce la lista di tutti gli Identity Provider o le Profile Authority federate
- **Attribute Authority Registry Service,** fornisce la lista di tutte le Attribute Authority federate

Federated SSO



Cooperazione Applicativa tramite Web Services
- Verifica Attributi presso il servizio di Front End-

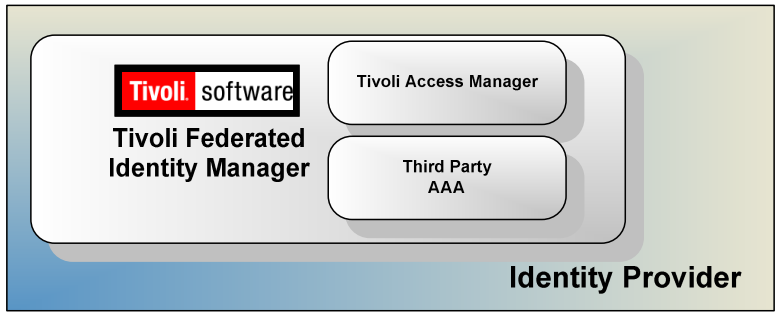


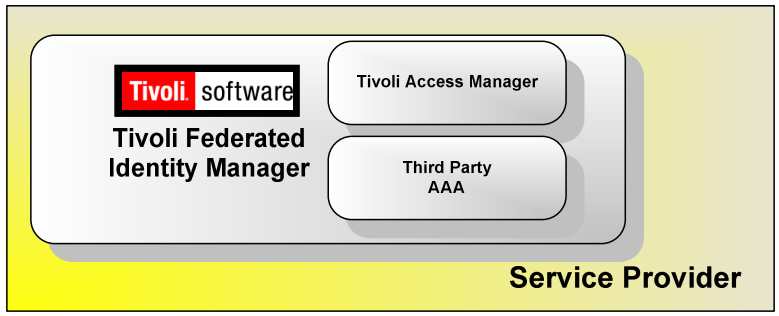
I Ruoli per un'Amministrazione all'interno della Federazione

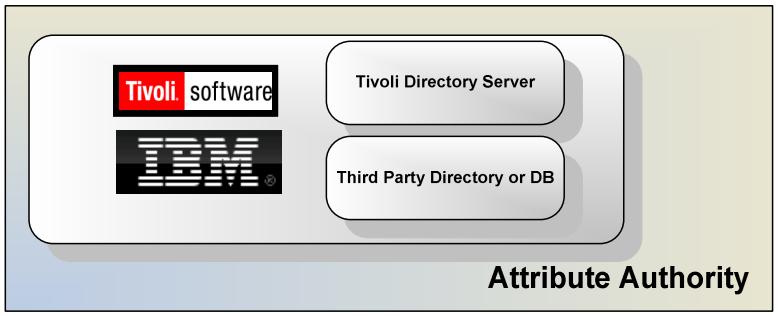
1 - Amministrazione Erogante i Servizi		
Entità	**Ruolo**	**Interfaccia**
Service Provider	Disaccoppia l'Amministrazione che offre i servizi dalla complessità della federazione stessa. E' composto da: -**Federation Gateway**, P.O.C. per tutte le richieste di accesso alle risorse offerte dall'Amministrazione -**PEP** per l'applicazione dello policy di autorizzazione prima dell'accesso ai servizi.	Accesso utente Web SAML AuthnRequest SAML AttributeQuery SAML Response Web Service per Cooperazione Applicativa
2 - Amministrazione con Utenti Federati		
Entità	**Ruolo**	**Interfaccia**
Attribute Authority	Verifica tutti o parte degli attributi componenti il profilo di un generico utente	SAML Attribute Query SAML Response
Profile Authority	Gestisce il profilo utente e prepara il portafoglio delle asserzioni	Accesso utente Web SAML AuthnRequest SAML Attribute Query SAML Response
Identity Provider	Fornisce il servizio di Autenticazione per l' End User	Accesso utente Web SAML AuthnRequest SAML Response

L’offerta IBM in Ambito Federazione

- **Portafoglio** di servizi/prodotti capaci di integrare anche prodotti forniti da terze parti (es ICAR)
- **RoadMap** per consentire ad una Amministrazione di essere "Federation/SPCoop ready" con un basso impatto sui servizi informativi e le eventuali infrastrutture AAA già presenti presso le singole amministrazioni







La roadmap IBM per essere “Federation Ready”

Analisi del contesto

Servizi

- Definizione dei Servizi da Federare
- Progettazione/Deployment/Integrazione Infrastruttura Federata
- Integrazione Infrastruttura Federata e Servizi
- Test e Certificazione dei Servizi dal CG-SICA
- Definizione Accordi di Servizio + Specifiche di Sicurezza

Utenze

- Definizione delle tipologie di utenze da Federare
- Definizione delle Authority Coinvolte in termini di Profili e Certficazioni di Ruolo
- Progettazione/Deployment/Integrazione Infrastruttura Federata
- Integrazione Infrastruttura Federata e Fonti Dati
- Test e Certificazione dei Servizi dal CG-SICA

Erogazione/Fruizione Servizi Federati

La presenza di IBM negli Standard

- **Organization for the Advancement of Structured Information Standards (OASIS):** consorzio internazionale no-profit volto a definire standard industriale per l'interoperazione SAML (1.x, 2.0), XACML, WS-Security Policy

- **World Wide Web Consortium:**
  - WS Security, WS-Policy, WS-Federation, WS-Trust, XML encryption e XML digital signature

- **Web Services Interoperability (WS-I):** organizzazione formata da diversi produttori con l'obiettivo di assicurare l'interoperabilità dei servizi Web tra tutte le piattaforme

IBM

THANK YOU

Questions

Andrea Carmignani
andrea.carmignani@it.ibm.com