Garantire la Sicurezza nella Cooperazione Applicativa:

Strumenti a supporto, stato dell'arte, casi pratici

Andrea Carmignani
Senior IT Architect

Security Day 2010

Agenda

- Il significato della Identity Propagation
- Standard a supporto
- Il trend della cooperazione applicativa in europa
- Lessons learned

Nuovi Driver di Business e Tecnologici richiedono nuove strategie per la gestione e la propagazione dell'identità digitali

Driver di Business:

- Outsourcing;
- Iniziative di business basate su modelli di collaborazione;
- Fusioni Aziendali;
- Software as a Service (SaaS);

Driver tecnologici:

- Service Oriented Architecture;
- Cloud Computing;
- Virtual Desktop;

Il Significato della Federazione

•Dal punto di vista formale, con il termine Federazione si intende

a) La capacità di un'organizzazione di riconoscere ed autorizzare identità esterne al proprio perimetro organizzativo

b) La relazione esistente fra due entità

c) Un'associazione comprendente un qualsiasi numero di Service Provider ed Identity Provider

•La Federazione richiede un'infrastruttura di Trust su cui i modelli di Business Federati vengono implementati

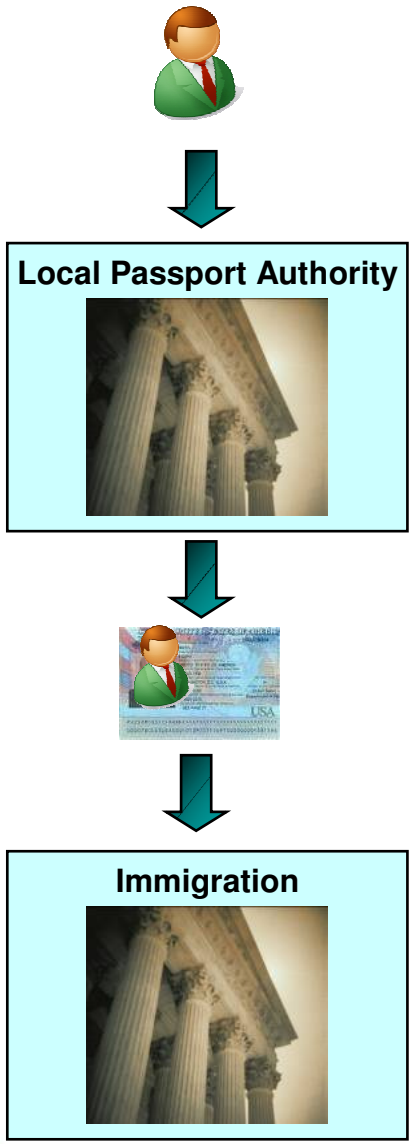
I modelli di Business devono contemplare:

•Scenari di cooperazione adottati;

•Agreement su tipologia formato e sintassi dei dati da trasmettere

Un esempio di Federazione - Il passaporto

- **L'identità federata è come il passaporto**
  - Ne esiste uno per ogni nazione
  - Ognuno ha un solo passaporto
- **Esiste un Trust fra le nazioni**
  - Il passaporto è accettato da nazioni straniere
  - Il passaporto verifica la nostra identità all'estero
- **Per andare all'estero quindi serve un passaporto**
  - Ottenuto dalle autorità locali
  - Previa verifica dell'identità



Il significato della sicurezza nei Web Services

Assicurarsi che:

- Solo chi è propriamente autenticato ed autorizzato possa eseguire chiamate ai web services
- I messaggi siano protetti in termini di integrità e confidenzialità durante il trasporto e se necessario anche durante l'archiviazione,
- Le applicazione siano protette dai comuni attacchi nei confronti degli stack SOAP/XML
- L'infrastruttura e le applicazioni S.O.A. siano progettate con in mente la sicurezza sin da subito in modo da prevenire incidenti di sicurezza, perdita di dati, frodi, sabotaggio.

Il design e l'implementazione di alcuni Security Building Block dovrebbero essere considerati sin dall'inizio

Building Block

- **Access control** – Identificare chi voglio nel mio "Cerchio della Fiducia" e con quale livello di fiducia
- **Identity Propagation** – Mantenere l'Identità di chi ha iniziato la transazione
- **Audit** – Gestire i log per la Compliance alle leggi vigenti.
- **Identity and Access Management (I&AM)** – Integrare l'infrastruttura IAM all'interno dell'architettura SOA per gestire le identità digitali
- **Confidentiality & Integrity controls** – Utilizzare integrità e confidenzialità dove necessario per proteggere i dati di business.

Gli standard sopperiscono la mancanza di sicurezza all'interno di SOAP

	Transport Layer	Message Layer
Identification / Authentication	HTTP Authentication SSL/TLS Authentication	WS-Security SAML / XKMS
Authorization	(using authenticated identity against directory or similar)	WS-Authorization SAML / XACML
Confidentiality	SSL/TLS Encryption	XML-Encryption
Integrity	SSL/TLS Encryption	XML-Signature XML Schema Validation
Accountability / Non-repudiation		XML-Signature WS-Security / XKMS
Administration	Policy Infrastructure	Policy Infrastructure

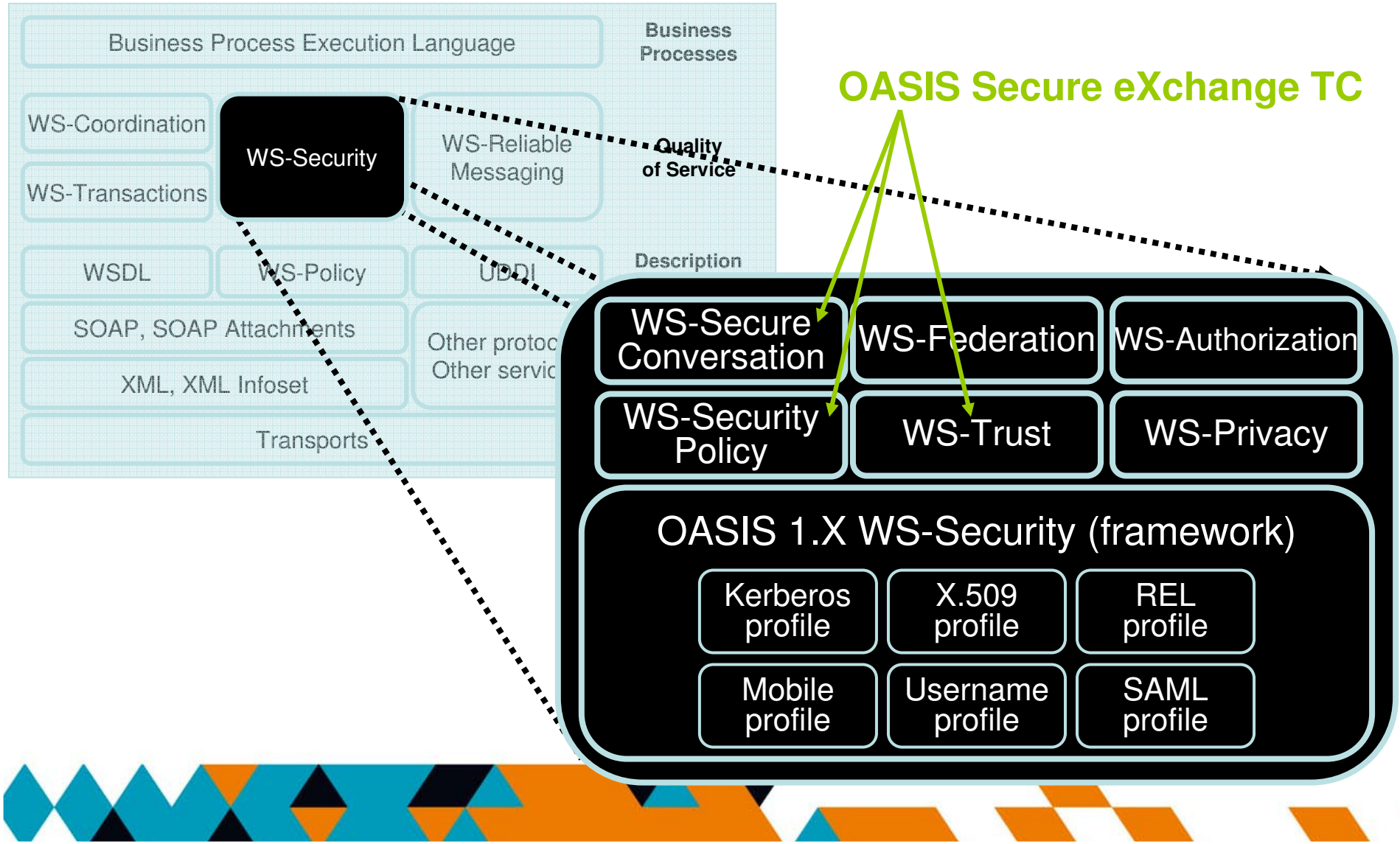
Transport Layer Security

- Sicurezza peer-to-peer. Deve essere ristabilita in ogni Hop.
- Protezione a livello di sessione

Message Layer Security

- Protegge il messaggio ed il suo contenuto.
- La protezione persiste anche in multi hop

Web Services e SOA Security



Lo standard WS-Security offre diversi metodi di Autenticazione ad oggi tutti implementabili

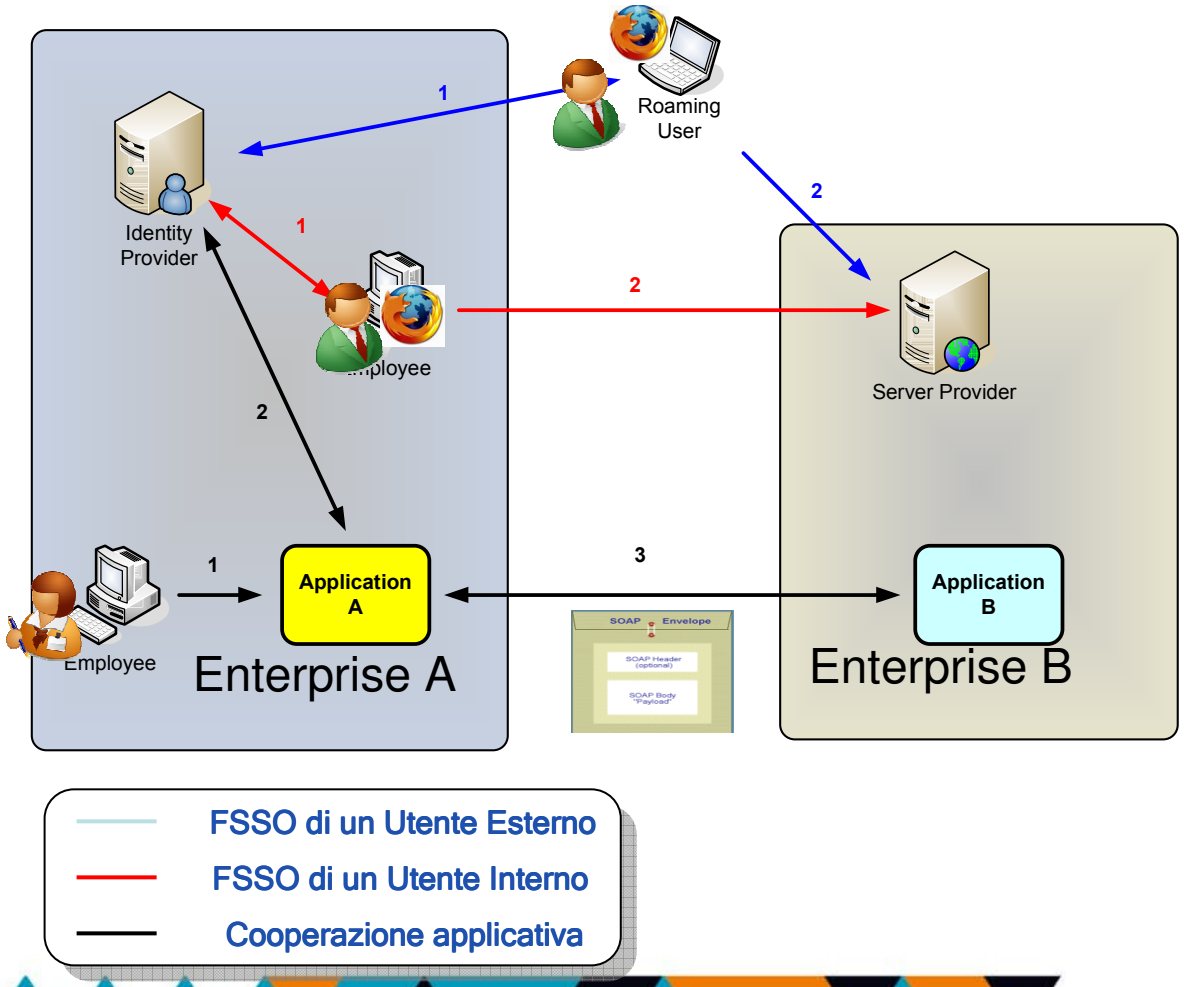
Accesso Locale Debole, tramite UID e PWD

Accesso Locale Forte, tramite Certificato Digitale X.509v3

Accesso Federato Debole, l'asserzione SAML deve avere un authentication context che indichi l'avvenuta autenticazione tramite UID e PWD

Accesso Federato Forte, l'asserzione SAML deve avere un authentication context che indichi l'avvenuta autenticazione tramite X509v3

F-SSO e Cooperazione applicativa come scenari tipici



Identity Provider è responsabile della gestione delle Identità degli utenti

1. Crea/Gestisce le credenziali
2. Gestisce il ciclo di vita delle utenze
3. Autentica gli utenti
4. E' il "Garante" riguardo l'identità degli utenti

Service Provider controlla l'accesso ai servizi

1. Ha piena fiducia nelle asserzioni di Identità provenienti dall'IdP
2. Fornisce accesso basato sulle asserzioni ricevute
3. Gestisce solo attributi utente locali

La Cooperazione nella Pubblica Amministrazione – Il Trend Europeo

Trattato Lisbona 2007 – Conferenza eGovernment Europea:

- Ogni paese dell'Unione europea **deve garantire interoperabilità con ogni stato membro (cross border interoperability);**
- Ogni paese deve agire per ridurre la burocrazia (reduction of administrative burdens) per il cittadino; quest'ultimo deve avere **accesso semplificato ai servizi dell'amministrazione pubblica;**

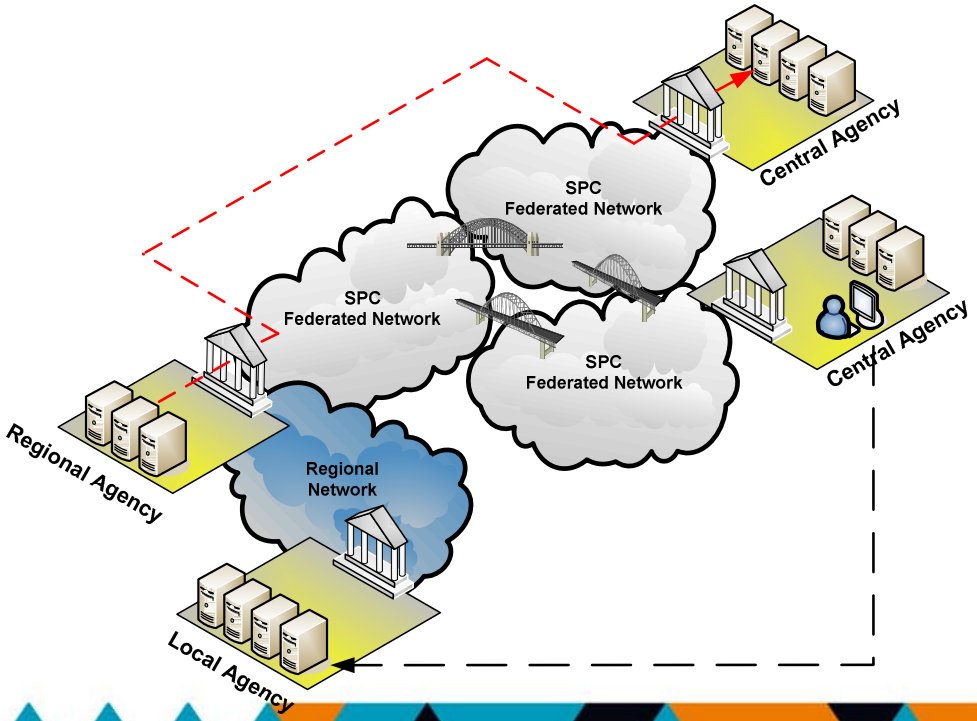
Conseguenze:

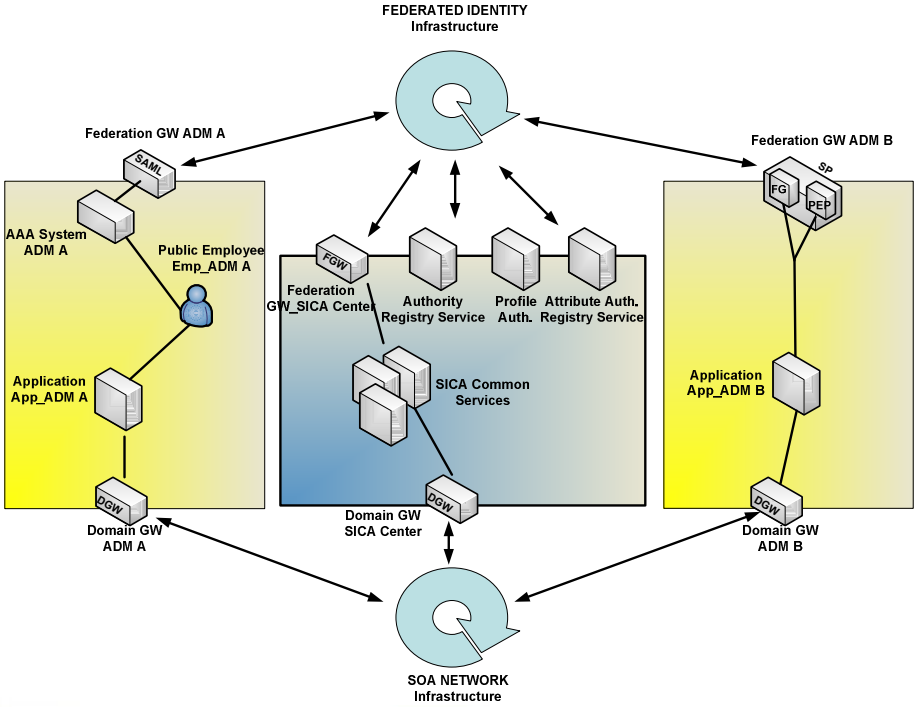
- **Ogni paese membro** si deve dotare di un **framework per l'interoperabilità** che permetta alle sue agenzie, ai suoi cittadini e ad ogni partner di **interagire con standard e politiche condivise**;
- Anche il **piano industriale per l'innovazione E-Gov 2012** richiede esplicite azioni per **l'evoluzione** e **l'adozione** della cooperazione applicativa;

La Cooperazione nella Pubblica Amministrazione – L'esperienza Italiana

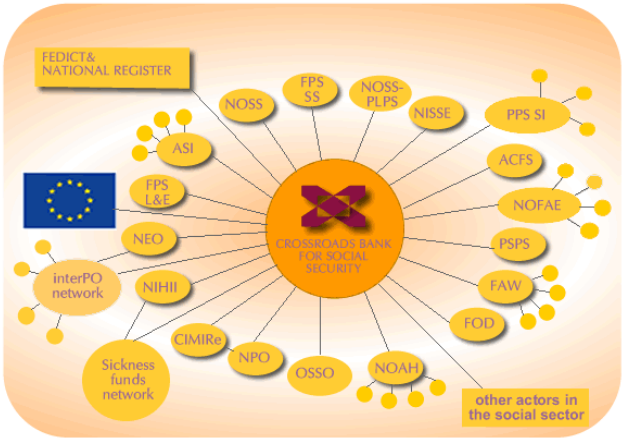
L'Italia dal canto suo ha sviluppato il **Sistema Pubblico di Connettività (SPC)**

Uno degli obiettivi dell'SPC è proprio quello di **garantire la federazione delle infrastrutture IT della Pubblica Amministrazione**





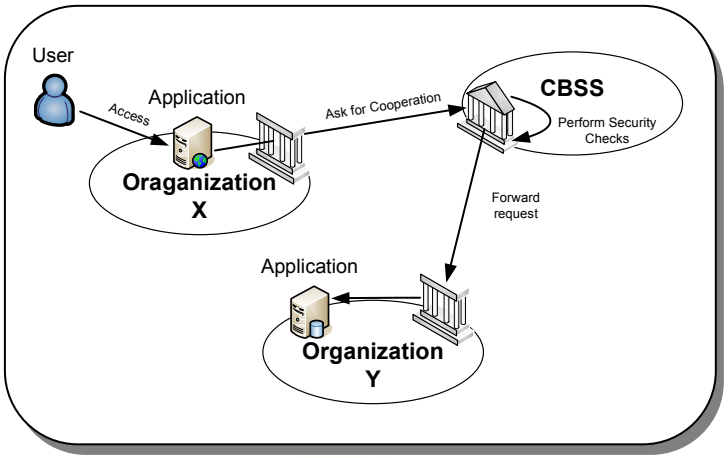
La Cooperazione nella Pubblica Amministrazione – l'esperienza BeNeLux



The Belgian social security consiste di:
•3 sistemi di previdenza;
•4 sistemi di assistenza;
•3.000 istituzioni sono responsabili per la Social Security Belga;
•Più di 10.000.000 utenze;

Obiettivo della CBSS:
• supportare il sistema previdenziale tramite l'utilizzo di nuove tecnologie così da snellire la burocrazia esistente;

•Promuovere una cooperazione basata sulla privacy e la sicurezza dei dati degli utenti;



L'utilizzo di un nuovo paradigma per la gestione delle identità causa cambiamenti in vari ambiti

- Privacy
- Audit
- Mind-set,
- Necessità di nuovi skill e tecnologie

Come fare Audit in un mondo federato?

Chi è responsabile in caso di frode?

L'IDP autentica l'utente ma non ha visione della azioni intraprese sull'SP

- Deve garantire che il processo di identificazione ed autenticazione sia robusto e conforme agli accordi sanciti (es: metodo di autenticazione)

L'SP non necessariamente conosce i dettagli riguardo l'identità dell'utente a cui sta erogando il servizio (es: Matricola, Codice Fiscale, Stringa Alfanumerica complessa a piacere)

- Deve garantire che il profilo autorizzativo sia corretto rispetto agli accordi di business sanciti con i partner

Il classico log di autenticazione ed accesso al servizio è diviso fra IdP e SP

L'approccio classico confinato all'interno di una sola azienda deve evolversi anch'esso verso un approccio federato e cooperativo

All'interno degli agreement con i partner ci dovrebbero essere almeno:

- i casi e le modalità con cui accedere alle informazioni inerenti i log altrui;
- le responsabilità di ognuno dei partner per quanto concerne la sicurezza e la privacy dei dati;

Le informazioni di Audit ora divengono anche uno strumento di charging!

Possibili fattori inibitori verso una veloce adozione della federazione

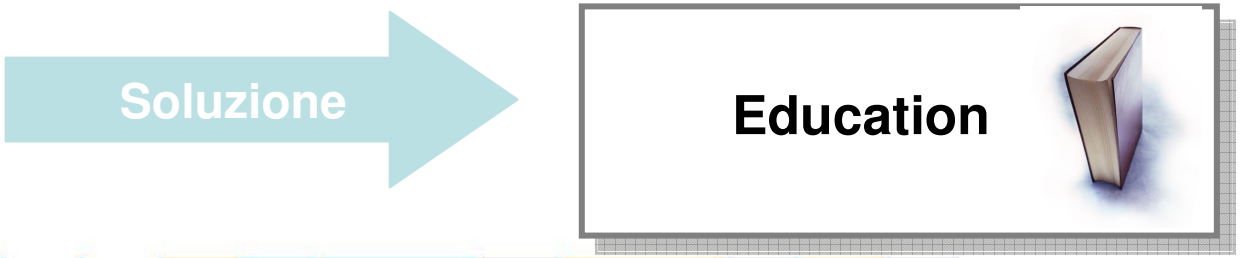
Ad oggi le difficoltà più diffuse nell'adozione delle cooperazione applicativa si possono riassumere in:

•Difficoltà nel definire effettivi scenari di utilizzo,
- molte volte il mindset dei clienti è radicato in una gestione centralizzata delle utenze e dei servizi

•Scarsi skill riguardo gli standard alla base della federazione:
- SAML, Liberty Alliance, Shibboleth;
- Ws-Security, WS-policy, Ws-Security Policy, WS-Federation;

•Sbagliato utilizzo degli standard,
- il connubio dei punti precedenti tende a far utilizzare gli standard per scopi non propriamente idonei;

•Prodotti non sempre maturi per supportare le visione di business del cliente;



Enterprise 2.0,propagare l'identità diviene una esigenza di business

Business Process-as-a-Service

salesforce.com experience success.

SIEBEL CRM OnDemand

SuccessFactors Business Execution Software

Sempre più società offrono i propri prodotti CRM e ERP come servizi "remotizzati"

Application/Software-as-a-Service

Google Apps

icloud

Crescono nuove offerte di prodotti di
- virtual desktop,
- remote communication & collaboration

E-Government Service

CBSS Crossroads Bank for Social Security

IDManagement.gov

CNIPA Centro Nazionale per l'Informatica nella Pubblica Amministrazione

A livello internazionale le amministrazioni stanno promuovendo inziative di E-Government Federato

Infrastructure as Service

IBM

amazon web services™

Sun microsystems

TELECOM ITALIA

I grandi player tecnologici cominciano ad offrire servizi virtualizzati di Storage e Computing

Quanto la cooperazione sicura è un effettivo beneficio?

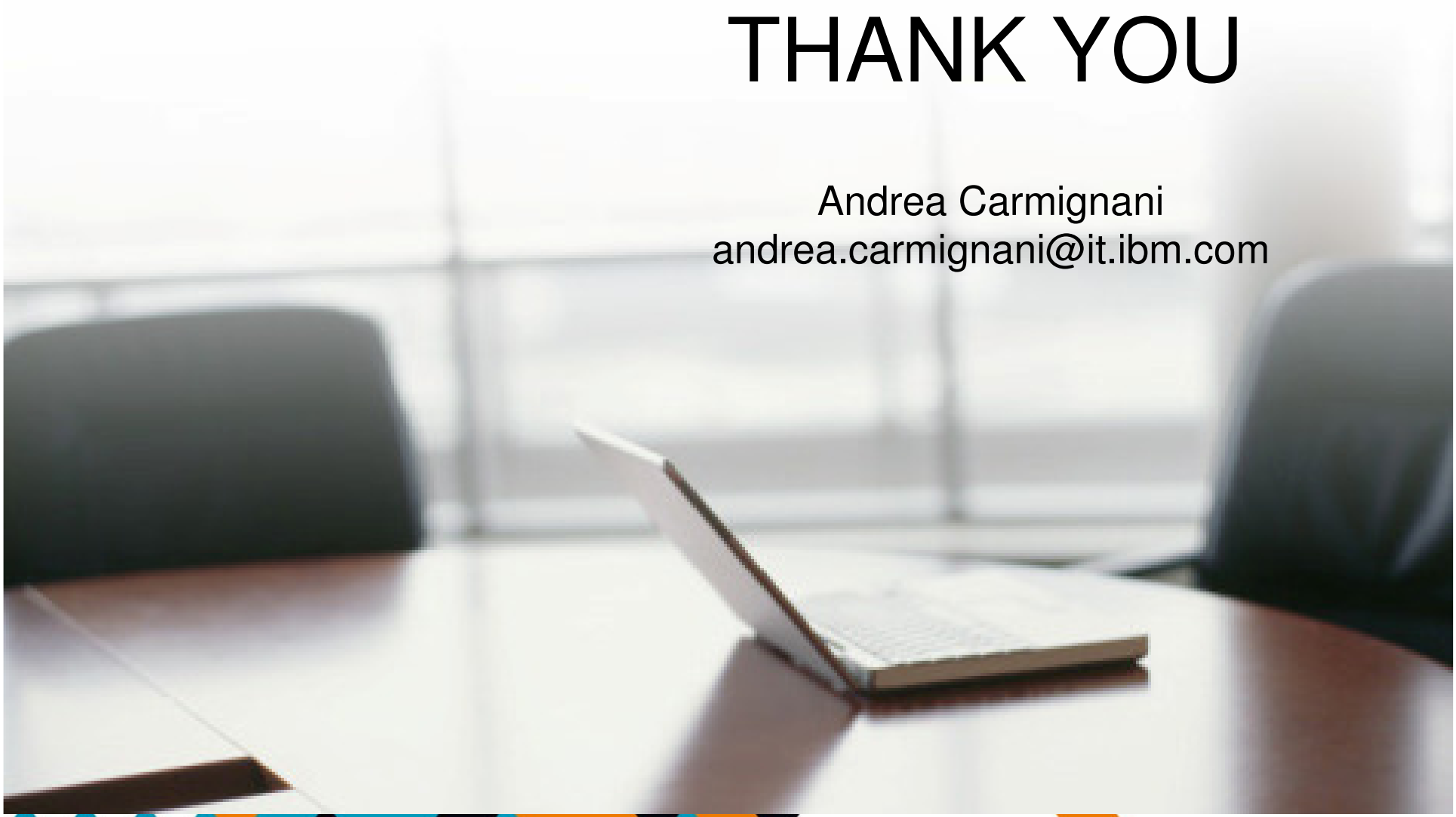
Nonostante gli impatti, che naturalmente l'adozione di una nuovo paradigma introduce, la gestione federata delle identità digitali all'interno della cooperazione applicativa è un fattore abilitante in termini di:

Riduzione dei costi:

- minori costi di gestione dell'Identity Management tramite;
- riduzione della complessità associata allo sviluppo delle applicazioni;
- riuso dei servizi IT esistenti;
- possibilità di outsourcing;

Aumento dell'efficienza:

- integrazione dei processi di business;
- sicurezza End-to-End nei processi di Cooperazione;
- time to market;
- quality of service (user experience);



THANK YOU

Andrea Carmignani
andrea.carmignani@it.ibm.com