



identità digitale federata nella P.A. italiana

Francesco Meschia
CSI-Piemonte

Definire l'Identità Digitale

- ◆ Il primo tentativo di fornire una definizione completa del concetto di identità digitale è stato fatto da Hal Abelson e Lawrence Lessig del MIT nel white paper “Digital Identity in Cyberspace”:
 - ◆ “L’insieme delle caratteristiche essenziali e uniche di un soggetto sono ciò che è in grado di identificarlo”
- ◆ Dietro questa semplice definizione si nasconde in realtà una grande complessità che è legata alla definizione di quelle che sono le sue caratteristiche uniche ed essenziali

Identity Management: due facce di una medaglia

- ◆ La gestione dell'identità digitale è un tema rilevante sia per chi la gestisce sia per chi ne è titolare
 - ◆ chi gestisce un sistema di Identity Management lo fa per mantenere il controllo e garantire la sicurezza degli accessi
 - ◆ chi possiede una identità digitale desidera tutela sulla privacy dei propri dati, desidera garanzie sul corretto uso, desidera sicurezza contro il furto della propria identità
- ◆ Storicamente il punto di vista “corporate” ha avuto maggiore rilevanza di quello dell'individuo
 - ◆ anche nell'ambito della Pubblica Amministrazione

IdM: cambia il punto di vista corporate

- ◆ Le organizzazioni si sono abituate a gestire le identità digitali dei propri membri...
- ◆ ...e a considerare l'intero tema dell'identità digitale come un fatto interno
- ◆ La situazione è cambiata a partire dal 2002: le organizzazioni hanno visto aumentare in modo prima non prevedibile le necessità di lasciare “uscire” ed “entrare” le identità digitali attraverso i confini del proprio dominio

IdM: aumenta la complessità

- ◆ Una nuova situazione si è venuta disegnando soprattutto a causa di tre fattori:
 - ◆ a seguito della “dot-com-crash” del 2000 si è manifestata una tendenza alle acquisizioni e fusioni tra imprese che ha portato alla necessità **operativa** di unificare tra loro sistemi di Identity Management precedentemente separati
 - ◆ l’aumento del ricorso all’outsourcing e offshoring ha portato a superare la visione dell’identità come fatto interno ad **una sola** organizzazione
 - ◆ più recentemente, l’emergere del cosiddetto “Web 2.0” ha messo a disposizione un gran numero di nuovi servizi rivolti alle persone, riconosciute individualmente grazie alla loro identità digitale

L'identità digitale federata

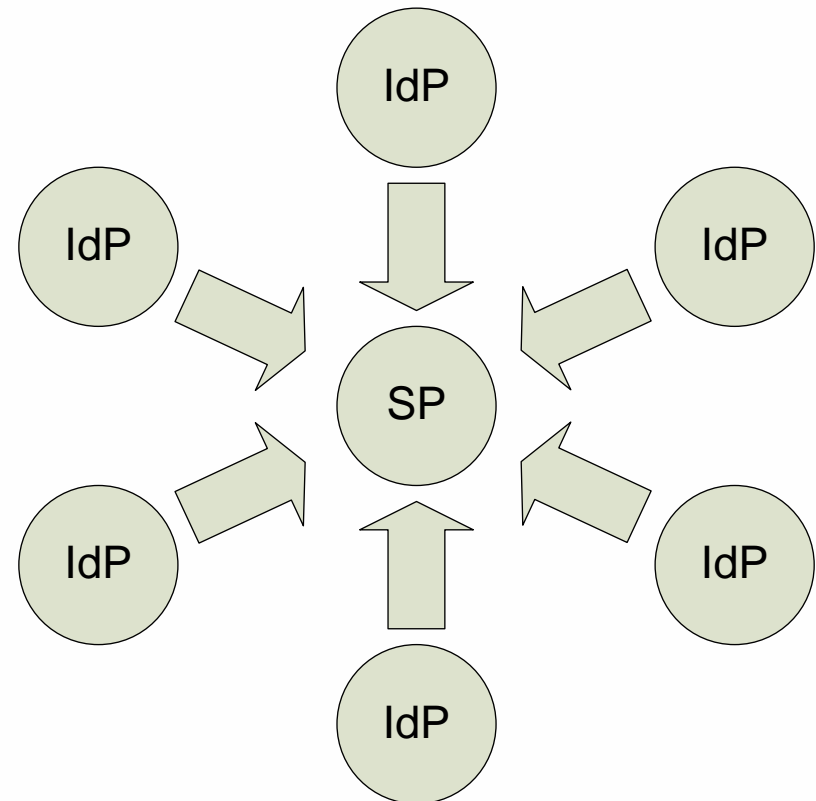
- ◆ La “***identità digitale federata***” è il nuovo paradigma che nasce dall'accettazione di questi fatti:
 - ◆ le persone si “spostano” attraverso i confini di diversi ambiti di responsabilità in modo sempre più frequente, e continuerà ad essere così in futuro
 - ◆ non è probabile che si possa giungere ad una identità digitale unificata, in qualunque ambito che non possa essere identificato con un solo dominio di responsabilità

Differenti profili di federazione

- ◆ Il paradigma federato costringe a ripensare i ruoli delle organizzazioni nella catena del servizio:
 - ◆ se prima **fornitori di servizio e di identità** erano la stessa organizzazione, ora appartengono a organizzazioni diverse
- ◆ I fornitori di servizio (“**service provider**”, SP) presidiano l’offerta di funzionalità applicative
- ◆ I fornitori di identità (“**identity provider**”, IdP) si specializzano nella gestione delle identità digitali
- ◆ IdP e SP cooperano sotto diversi “profili”

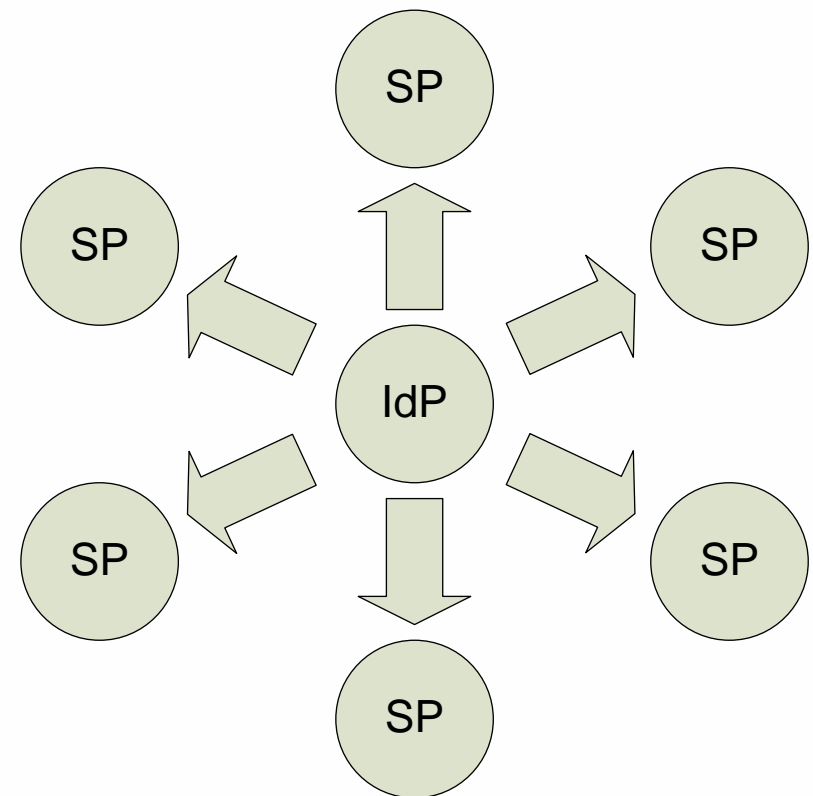
Il profilo “SP Hub”

- ◆ Uno dei profili di cooperazione più semplici è quello in cui un SP si avvale dei servizi di Identity Management offerti da più IdP
 - ◆ la “federazione” è l’ambito, fiduciario e contrattuale, che lega l’SP al centro della stella agli IdP



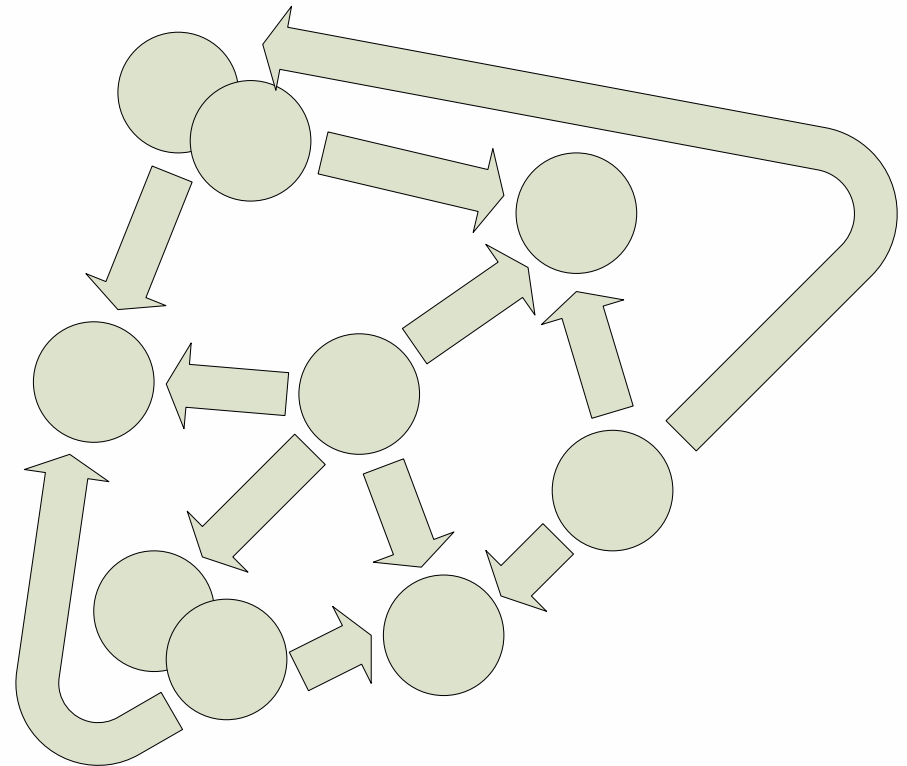
Il profilo “IdP Hub”

- ◆ Un altro semplice profilo di collaborazione è quello in cui un IdP offre i propri servizi a diversi SP
 - ◆ la federazione lega l'IdP a tutti i SP che desiderano trarre vantaggio dalla capacità di identity management dell'IdP



Il profilo “multi-provider”

- ◆ A un livello di maturità maggiore si situa il profilo “multi-provider” che vede una molteplicità tanto di IdP quanto di SP, legati in una federazione ampia
 - ◆ la federazione è un ambito fiduciario in cui ci si accorda su un insieme di regole comuni e un comune modello di trust e di responsabilità
 - ◆ si parla di “circle-of-trust”



Il profilo “multi-provider”

- ◆ Questo profilo è considerato lo scenario a cui possono tendere, al raggiungimento di un adeguato livello di maturità, le federazioni di tipo hub-and-spoke
- ◆ Il **circle-of-trust** diventa un circolo virtuoso in cui ogni organizzazione può agire da SP o da IdP in modo non preclusivo, asserendo determinati attributi e fornendo servizi in base agli attributi asseriti da altre autorità
- ◆ E' il profilo tipico per le federazioni tra le P.A., che agiscono sia con ruolo di IdP sia con ruolo di SP



differenti strategie ed esempi di federazione

La federazione: checklist

- ◆ Un progetto di federazione necessita di stabilire regole tecniche tra le parti
- ◆ Occorre innanzi tutto una **sintassi** comune
 - ◆ che specifichi la forma degli oggetti scambiati
- ◆ Subito dopo occorre una **grammatica** comune
 - ◆ che indichi quale significato attribuire agli oggetti
- ◆ Infine occorre una **semantica** comune
 - ◆ che indichi quali profili di interazione e casi d'uso vengono previsti
- ◆ Diversi progetti possono definire in modo differente le singole “parti del discorso”

L'emergere degli standard

- ◆ A partire dal 2002 sono nate diverse iniziative che mirano alla costruzione di un sistema completo e coerente per la gestione dell'identità digitale federata
- ◆ Al momento si individuano quattro principali approcci:
 - ◆ l'approccio *Liberty Alliance*
 - ◆ l'approccio *OASIS-SAML*
 - ◆ l'approccio *WS-Federation*
 - ◆ l'approccio *Transport Layer Security*

La convergenza non tecnica

- ◆ Ciò che gli standard non dettano sono le condizioni ***non-tecniche*** che deve avere la federazione per poter funzionare:
 - ◆ quali sono le *relazioni di fiducia* tra le parti?
 - ◆ come si garantisce la *fiducia* end-to-end?
 - ◆ come si garantisce la *privacy* dell'utente?
 - ◆ come *scala* la federazione all'accoglimento di nuovi membri?
- ◆ Questo è l'elemento che qualifica un progetto di federazione rispetto ad un altro

I progetti di identità federata nella P.A.

- ◆ A partire dalla prima fase di e-gov sono emerse iniziative volte alla federazione delle basi di identità di diverse amministrazioni
 - ◆ il progetto **IRIDE** ha permesso ai servizi di e-gov piemontesi di accettare diversi formati di credenziali (approccio TLS + estensioni locali)
 - ◆ il progetto **People** ha costruito un circolo fiduciario “bottom-up” tra una numeroso gruppo di Comuni italiani (approccio SAML 1.1 + estensioni)
 - ◆ i progetti **SIRV-INTEROP** e **INTERPRANA** hanno costituito una federazione tra Comuni e ASL delle Regioni Veneto e Friuli-Venezia-Giulia (approccio SAML 1.1 + estensioni)
 - ◆ il progetto **ICAR** sta disegnando l’ambito fiduciario federato tra le Regioni aderenti (approccio SAML 2.0)

Serve ancora l'identità federata in Italia?

- ◆ Anche se il sistema-Paese si avvia a disporre di uno strumento unico nella Carta di Identità Elettronica, rimangono diverse ragioni per la sussistenza di progetti di federazione
 - ◆ necessità di gestire il periodo transitorio fino alla compiuta diffusione della CIE
 - ◆ necessità di offrire alternative all'autenticazione crittografica, fino a quando la soglia di ingresso tecnologica per i cittadini non sia scesa abbastanza
 - ◆ consapevolezza che l'identità di un individuo è più complessa di quanto rappresentato su una carta, e comprende informazioni con cicli di vita diversi e certificate da soggetti diversi



l'identità federata nel progetto ICAR

Il progetto ICAR-INF3

- ◆ ICAR (Interoperabilità e Cooperazione Applicativa tra le Regioni) è un progetto della II fase di e-Gov
- ◆ Il progetto ICAR ha avuto il merito di vedere nell'identità digitale federata il presupposto per accrescere l'impatto dei servizi di e-Government
- ◆ Uno dei task interni al progetto (denominato INF3) ha il compito di attuare questo presupposto attivando la ***federazione dell'identità digitale tra le regioni***
- ◆ Ci si è subito resi conto del fatto che il compito presenta sfide architettoniche, tecnologiche e organizzative

- ◆ Prendere in considerazione casi d'uso rappresentativi
 - ◆ interazioni **G2C/G2B** e **G2G** in cooperazione applicativa
- ◆ Modellare il contesto organizzativo di riferimento
 - ◆ quali **soggetti** sono coinvolti
 - ◆ quali **relazioni** coinvolgono i soggetti
 - ◆ come si propagano le relazioni di **fiducia**
- ◆ Modellare il contesto tecnologico di riferimento
 - ◆ quali **oggetti informatici** rappresentano i soggetti della federazione
 - ◆ quali **dati** vengono scambiati
 - ◆ come vengono garantite **privacy, sicurezza e fiducia**

ICAR: il problema dell'autenticazione

- ◆ Come può l'ente erogatore del servizio accertare l'identità dell'utente?
 - ◆ risposta tradizionale: usando una procedura di autenticazione che permette all'utente di dimostrare il possesso di un dato "segreto" noto solo all'utente stesso e all'ente (identity management locale)
 - ◆ risposta federata: l'ente ripone fiducia nell'assunzione di responsabilità da parte di un identity provider che riconosce l'utente (identity management delegato)

ICAR: schematizzazione del modello

- ◆ Gli enti che decidono di federarsi nel quadro di cooperazione ICAR entrano a far parte dell'ambito fiduciario comune (*circle of trust*)
- ◆ Grazie all'esistenza di questo ambito fiduciario è possibile sgravare i domini delle P.A. dal compito di *identity e attribute provisioning*
 - ◆ perché questo compito può essere svolto da domini specializzati (**domini certificatori**)
 - ◆ la fiducia si mantiene perché i certificatori sono accreditati e convalidati all'interno del **dominio di cooperazione** che rappresenta ICAR

ICAR: schematizzazione del modello

- ◆ Gli utenti (cittadini o intermediari) si rivolgono ai ***certificatori di identità*** riconosciuti per farsi registrare ed ottenere le credenziali
 - ◆ questa funzione potrà tipicamente essere svolta dalle attuali ***Certification Authority***
- ◆ Rivolgendosi poi ai ***certificatori di attributo*** potranno ottenere le attestazioni digitali delle proprie qualifiche
 - ◆ ***ordini*** ed ***albi professionali*** potranno fornire questo servizio
- ◆ Identità ed attributi diventeranno parte del ***profilo*** dell'individuo, che potrà essere gestito grazie a servizi di comunità detti ***certificatori di profilo***

ICAR: user-centrismo e profilo utente

- ◆ “**User-centric-identity**” è una parola-chiave che richiama un concetto: riportare sotto il controllo dell’utente la sua identità in rete
- ◆ La “federazione classica” viene vista come un modo in cui il controllo viene in realtà sottratto all’utente
 - ◆ perché i diversi attori si scambiano “fuori banda” informazioni sull’individuo senza che questi lo sappia
- ◆ L’utente di un sistema user-centrico ha invece il controllo su ciò che di lui si vede in rete

ICAR: user-centrismo e profilo utente

- ◆ L'idea originale (Dick Hardt, 2005) è stata accolta come una visione sostanzialmente **contraria** alla federazione corporate-centrica
- ◆ In realtà ICAR propone una sinergia tra esigenza di federazione e esigenza di privacy dell'utente
- ◆ Il “profilo” permette all'utente di decidere ciò che di lui si vede in rete
 - ◆ fatte salve, ovviamente, verifiche per **obblighi di legge**

Bibliografia e link

- ◆ H. Abelson, L. Lessig, “Digital Identity in Cyberspace”, MIT, 10 December 1998
- ◆ E. Norlin, A. Durand, “Federated Identity Management”, PingID Network Inc., December 2002
- ◆ Liberty Alliance Project, <http://www.projectliberty.org>
- ◆ Shibboleth Project, <http://shibboleth.internet2.edu>
- ◆ OASIS, <http://www.oasis-open.org>
- ◆ Identity 2.0 blog, <http://www.identity20.com>
- ◆ Progetto ICAR, <http://www.progettoicar.it>