

## Sistemi di gestione dell'identità federata e ACM

Sistemi di gestione dell'identità federata e ACM .....	1
1 Identity Management .....	2
Identità digitale federata.....	2
Il modello .....	2
Identità digitale (Digital Identity - DID).....	2
Emettitori di Identità (Identity Issuer - IDIS).....	3
Erogatori di servizi (Service Provider - SP) .....	3
Federazione .....	3
Federazione di emettitori di identità.....	3
Federazione di erogatori di servizi.....	3
Federazione di identità .....	3
Acquisizione dell'identità (Identity Acquirer - IDAC).....	3
Instradamento (Identity Router - IDR) .....	3
Autenticazione (Authentication Service - AS).....	3
Controllo di accesso (Access Control - AC) .....	3
2 ACM e le identità federate.....	4
ACM in un ambito federato.....	4
Identità in ACM.....	4
ACM e i sistemi di identità federata .....	5
Esperienze di integrazione: SIRAC.....	5
Bibliografia e link .....	6

# 1 Identity Management

Internet non ha meccanismi precisi per identificare "chi comunica con chi": è sempre mancata cioè una **infrastruttura per la gestione delle identità**, e di conseguenza le imprese, le Pubbliche Amministrazioni e le singole persone hanno nel tempo dovuto sviluppare una serie di soluzioni isolate, parziali e spesso incompatibili per risolvere i loro contingenti **problemi di identificazione nelle transazioni**.

Imprese e Pubbliche Amministrazioni si trovano comunque ad affrontare il problema dell'identificazione degli individui, spesso chiedendo loro il rilascio di molte informazioni personali, generando di conseguenza anche **problemi di privacy**. Tendono infatti a confrontarsi due approcci o punti di vista teoricamente opposti: quello dell'organizzazione che gestisce le identità, e che ha l'obiettivo di garantire la sicurezza degli accessi, e quello dell'individuo, che chiede garanzie sull'utilizzo della propria identità digitale, e tutela della privacy.

Il problema è acuito dalla volontà di migliorare la capacità di erogare servizi semplificando i processi; volontà che impone oggi alle imprese ed alla Pubblica Amministrazione la necessità, senza precedenti, di **condividere in maniera sicura informazioni sensibili per cooperare con servizi online interoperabili**.

Infatti le transazioni via web hanno ormai reso **evanescenti i confini** che separano le diverse organizzazioni, consentendo un **flusso di servizi trasversale rispetto ai domini di competenza ed alle tecnologie di supporto**: in tale modello di servizi distribuiti è inoltre fondamentale adottare meccanismi in grado di **garantire la privacy e la protezione dei dati personali**.

La gestione delle identità on-line deve essere quindi riconsiderata.

## *Identità digitale federata*

La gestione dell'identità può essere sempre meno vista come un problema solo interno alle singole organizzazioni: le persone infatti, mentre effettuano transazioni, "si spostano" sempre più attraverso i confini di **diversi ambiti di responsabilità** corrispondenti ad altrettante organizzazioni.

Il paradigma di **identità digitale federata** nasce come risposta all'esigenza che le organizzazioni hanno di cooperare condividendo dati, partendo dal presupposto che il traguardo di una identità digitale "unica", trasversale ai vari domini, è poco realistico.

## *Il modello*

In letteratura esistono **modelli di identità digitale federata** molto simili.

Nel seguito vi è il tentativo di presentarne uno unificato in cui si sono evidenziati tutti i possibili soggetti/componenti. La terminologia non fa riferimento diretto ad uno specifico modello ed ha una validità riferita a questa presentazione: componenti omonime con altri modelli potrebbero avere ruoli non identici.

### **Identità digitale (Digital Identity - DID)**

Per identità si intende un **insieme di informazioni che consentono di distinguere una entità da un'altra in modo univoco**: in una identità digitale, questo insieme di informazioni è espresso in forma digitale.

Se queste informazioni hanno un valore relativo ad un contesto si parla di identità locale (a detto contesto). Esempi: la coppia nome/cognome, il codice fiscale, un certificato digitale, l'impronta digitale della retina o del pollice.

#### **Emittitori di Identità (Identity Issuer - IDIS)**

Un aspetto fondamentale nella gestione delle identità come più sopra definita, è la **certezza che ad essa corrisponda l'entità titolare**, unitamente al fatto che sia nella piena disponibilità dello stesso. Gli IDIS garantiscono questa associazione e gestiscono la sua validità. Esempi: La Regione Lombardia, per dare piena validità alla Carta Regionale dei Servizi da lei emessa ha richiesto ai Cittadini lombardi di presentarsi agli uffici postali per farsi identificare.

#### **Erogatori di servizi (Service Provider - SP)**

Sono i soggetti che **erogano servizi individuali** (che necessitano cioè di indentificazione) a cui il titolare di una identità vuole accedere. Esempi: una PAL che eroga il servizio di pagamento tributi o di rilascio permessi di circolazione.

#### **Federazione**

Per federazione in generale si intende l'associazione formata dall' **accordo di più parti**. In questo caso si possono distinguere diverse tipologie di federazioni.

##### *Federazione di emittitori di identità*

Associazione finalizzata alla amministrazione distribuita e/o decentralizzata delle identità digitali.

##### *Federazione di erogatori di servizi*

Gli erogatori di servizi si associano in un circolo fiduciario (circle of trust) con il quale stipulano un accordo di "circolazione" delle autenticazioni.

##### *Federazione di identità*

In questo caso si intende la possibilità per l'utente di collegare (federare) le proprie identità locali in un'unica identità federata (in questo caso si parla anche di network identity).

#### **Acquisizione dell'identità (Identity Acquirer - IDAC)**

L'identità digitale viene presentata ad un **soggetto preposto all'acquisizione della stessa**. Tale soggetto può acquisire identità in relazione a diversi SP per conto di diversi IDIS.

#### **Instradamento (Identity Router - IDR)**

L'identità acquisita deve essere **instradata al servizio di autenticazione connesso con l'emittitore della stessa**. Tale instradamento logico è di fatto una mappatura tra gli emittitori di una identità e i servizi di autenticazione da loro ammessi (e con loro connessi). Tipicamente l'instradamento è operato attraverso una informazione di reindirizzamento del titolare verso uno dei AS accettati.

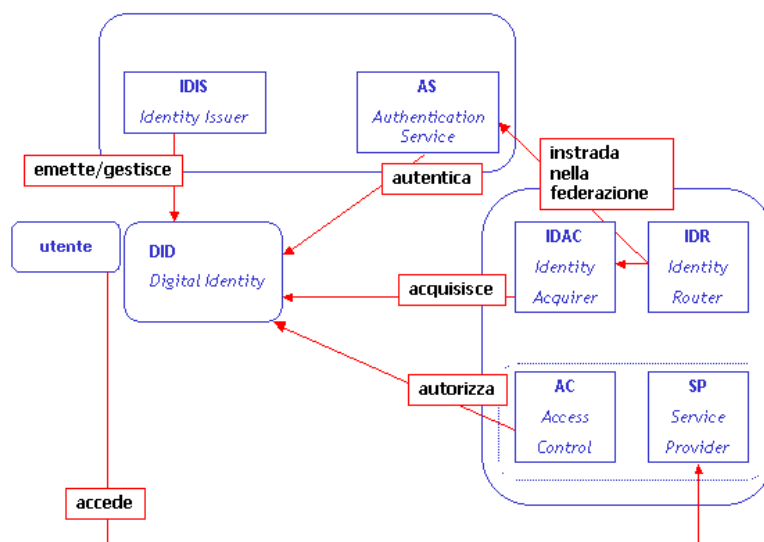
#### **Autenticazione (Authentication Service - AS)**

Il servizio di autenticazione **verifica** con il processo legato alla specifica identità e allo specifico emittitore la **veridicità** e la **validità** dell'identità presentata.

L'architettura in questione cioè non impone uno specifico schema di autenticazione.

#### **Controllo di accesso (Access Control - AC)**

L'accesso ad uno specifico servizio è regolamentato da un **sistema di controllo dell'accesso** che si basa sull'identificazione autenticata.



## 2 ACM e le identità federate

### *ACM in un ambito federato*

Il Content Management System ACM nasce come strumento per la gestione dei contenuti per la organizzazione di pubblicazioni multicanale (Web, Smartphone, PDA Voce).

Fin dalle prime versioni di ACM era possibile con una unica installazione gestire redazioni completamente distinte che incidevano su database dei contenuti virtualmente separati. A tali ambienti redazionali è stato dato il nome di Istanze.

Tali funzioni sono state implementate consci dell'esigenza che - ovunque vi sia una Organizzazione che ha in carico la gestione di più portali - si pone la questione della loro gestione "federata" sia essa intesa generalmente come "coordinamento" tra i diversi portali o, più precisamente, come capacità di utilizzare sistemi di identità federata.

Generalmente la gestione federata può spaziare dalla condivisione dell'infrastruttura IT, alla progettazione coordinata, all'aggiornamento ecc., e pone una serie di problematiche precise (si veda la documentazione di ACM in tema di Portali Federati).

Alcune tipologie di organizzazione che potrebbero affrontare problematiche simili sono Università, Pubbliche Amministrazioni Centrali e Locali (Ministeri, Regioni, Province, Comunità montane...), Grandi Aziende, Medie Aziende con struttura capillare di produzione e distribuzione, ASL e Ospedali.

Nel seguito si descrive come ACM possa utilizzare sistemi di identità federata.

### *Identità in ACM*

ACM è composto essenzialmente da due servizi: uno riguarda la contribuzione delle informazioni e la configurazione della loro fruizione e l'altro è la fruizione stessa.

Mentre il primo è incondizionatamente sottoposto a controllo di accesso gestito internamente dall'applicazione, per cui necessita di identificazione, il secondo gestisce solo opzionalmente l'accesso ad informazioni riservate.

Nell'ambito della fruizione è inoltre integrato in ACM un **modulo di integrazione applicativa (ATP)** che può condizionare a sua volta l'accesso alle applicazioni integrate in funzione dell'identità dell'utente.

### *ACM e i sistemi di identità federata*

ACM nasce nel 2001 prima della nascita di queste problematiche: ciononostante la sua architettura è stata successivamente modificata in modo tale da **consentire l'utilizzo di sistemi di identificazione ed autenticazione** differenti da quello incorporato.

Sulla base di questa potenzialità sono integrabili sistemi come **Shibboleth, Lasso o OpenSSO**.

A riprova di questo può essere portato un caso reale: il portale dei servizi del comune di Pavia.

### *Esperienze di integrazione: SIRAC*

Ariadne ha curato la parte di integrazione applicativa tra i servizi che il comune di Pavia espone al cittadino.

Come primo passo, utilizzando **ACM (Ariadne Content Manager)** e le specifiche librerie di **integrazione applicativa** ha reso **omogenee le interfacce e le modalità di autenticazione ed accesso** - con Single-Sign-On - alle varie applicazioni, realizzando così una **federazione locale di identità** tra sistemi eterogenei.

A questo punto il comune di Pavia si è trovato nella classica posizione in cui si trovano i gestori tradizionali di servizi in ambienti di identità non federata: dover accentrare e gestire tutte le problematiche di emissione/certificazione dell'identità, il ciclo di vita relativo, il sistema di autenticazione e così via. Affrontare e gestire queste problematiche non è semplice per una Pubblica Amministrazione che deve approntare uffici e personale a tal fine.

La soluzione definitiva è stata attuata quindi con il secondo passo: **l'utilizzo di un sistema federato di gestione delle identità che consentisse al comune di Pavia di delegare (circle-of-trust) tali incombenze**.

In ambito di e-gov in Italia le pubbliche amministrazioni possono scegliere di utilizzare il framework **SIRAC (Servizio infrastrutturale di Registrazione e Autenticazione di Comunità)**, nato nell'ambito del più vasto progetto People, che implementa un sistema di identità federata indipendente dall'emittitore e dagli schemi di autenticazione.

Nel caso del comune di Pavia è stato scelto di appoggiarsi alla **Regione Lombardia** come emittitore della **Carta Regionale dei Servizi (CRS)** e permettere al cittadino di autenticarsi in maniera "debole" - cioè con username e password - o "forte" - cioè con l'uso di tale carta.

Il sistema di controllo di accesso di ACM è stato quindi interfacciato ai sistemi di autenticazione di SIRAC, realizzando così un portale di informazioni e servizi per il cittadino che può identificarsi attraverso una delle modalità accettate.

## *Bibliografia e link*

- "Identità Digitale Federata nella P.A. italiana", Francesco Meschia, FORUM PA 2007  
[http://www.forumpa.it/forumpa2007/convegni/relazioni/1300\\_francesco\\_meschia/1300\\_francesco\\_meschia.pdf](http://www.forumpa.it/forumpa2007/convegni/relazioni/1300_francesco_meschia/1300_francesco_meschia.pdf)
- <http://www.project-liberty.org/>
- <http://www.oasis-open.org/>
- <https://www.prime-project.eu/>
- <http://shibboleth.internet2.edu/>
- <http://lasso.entrouvert.org/>
- <http://www.pingidentity.com/>
- <http://www.progettopeople.it/>
- <http://www.progettoicar.it>