



Prima Edizione della Giornata della Sicurezza Informatica in Sardegna
organizzata da
[Università di Cagliari](#) - [IBM Internet Security Systems](#) - [Tiscali Services](#) - [Sardegna Ricerche](#)

Gestione delle Identità Digitali e Controllo degli Accessi: problematiche e Soluzioni

Lucio Forastieri – Amministratore unico Sardegna IT

Pula 19 ottobre 2007, Auditorium Parco Tecnologico di Pula



La Mission di Sardegna IT

- Sardegna IT è una società “in house” della Regione Sardegna
- E’ stata costituita il 22.12.2006, ed è partecipata dalla RAS e dal CRS4
- Lo statuto prevede che la società operi per la produzione e per la fornitura di servizi strumentali alle attività della Regione, in particolare a sostegno dei processi innovativi che la Regione attuerà per i suoi uffici e per gli enti regionali ed a supporto delle collaborazioni che la Regione definirà direttamente con enti locali e con altre amministrazioni pubbliche



Cosa è un'Identità? -1-

- Non è semplicemente **CHI** si è;
- Ma è la rappresentazione di un soggetto in un determinato contesto



3



Cosa è un'Identità? -2-

- Le identità sono collezioni di dati su un soggetto e rappresentano *Attributi, Tratti e Preferenze*;
- **Attributi**: informazioni sul soggetto (es. anamnesi medica, conto bancario ecc.)
- **Tratti**: informazioni caratteristiche del soggetto, che possono variare lentamente rispetto agli attributi (es. dati anagrafici, colore degli occhi ecc.)
- **Preferenze**: informazioni che esprimono desideri (es. posto in aereo, pizza preferita ecc.)
- Genericamente si parla solo di **ATTRIBUTI**.

4



Cos'è un'Identità Digitale

Dei concetti di identità digitale (*digital identity*), identità di rete (*network identity*) o identità elettronica (*electronic identity*) esistono molteplici interpretazioni, spesso contrastanti.

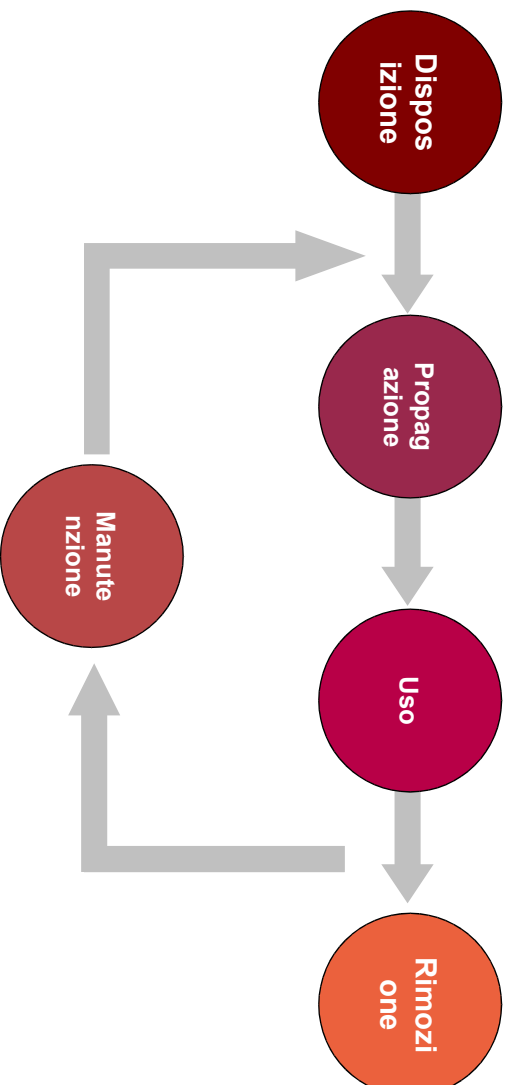
Si propone la seguente definizione:

“Network identity refers to the global set of attributes that are contained in an individual's various accounts with different service providers. These attributes include such information as name, phone numbers, social security numbers, addresses, credit records, and payment information.”

Fonte Liberty Project



Ciclo di Vita di un' Identità Digitale





Problematiche delle Identità Digitali

- La complessità in continua crescita delle infrastrutture informatiche
 - la diversificazione tecnologica degli ambienti applicativi
 - l'utenza sempre più numerosa
 - la necessità di individuare con precisione compiti e responsabilità nel trattamento delle informazioni
- determinano l'esigenza di identificare ed autorizzare gli operatori in modo certo, sicuro e robusto, evitando la **frammentazione** delle credenziali che deriva dalla necessità di controllare dati e servizi su **systemi distribuiti**

7



Soluzione: Identity Management

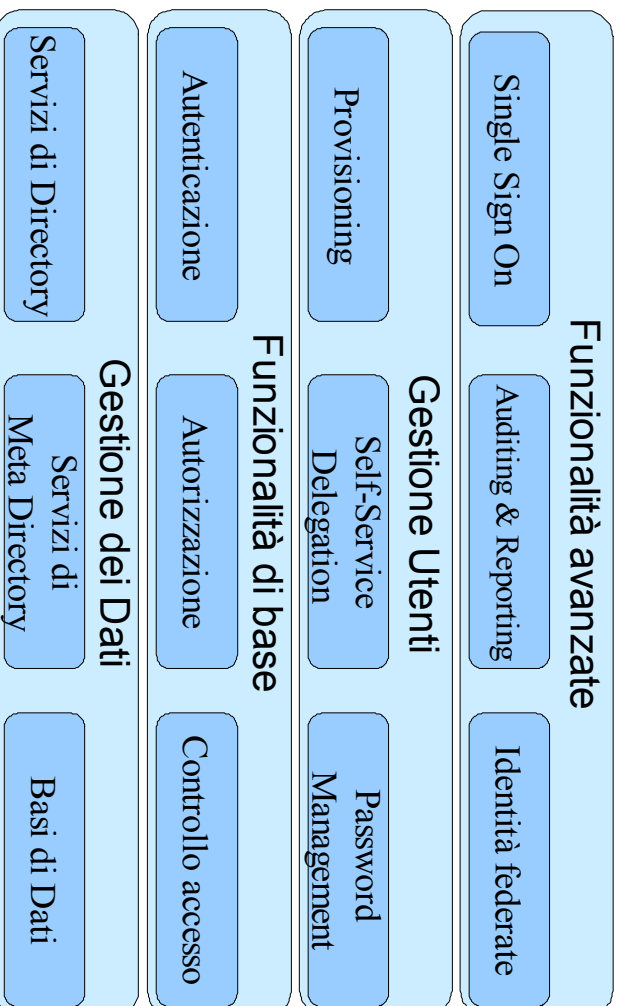
- Con **Identity Management (IM)** si intendono i sistemi integrati di **tecnologie, criteri e procedure** in grado di consentire alle organizzazioni di:
 - *facilitare gli accessi degli utenti ai servizi erogati*
 - *controllare gli accessi degli utenti ai servizi erogati*
 - *proteggere i dati personali da accessi non autorizzati*



8



Modello di un Sistema di Identity Management



9



Funzionalità di Base: AUTENTICAZIONE

- Tramite l' **Autenticazione** si verifica che l'utente dal quale si è ricevuta una certa richiesta sia realmente il mittente che sostiene di essere.
- Può essere effettuata tramite differenti meccanismi e, a seconda del meccanismo utilizzato è detta **forte** o **debole**:
 - **UID e Password, UID+PASSW+PIN, One Time Password**
 - **Certificato Digitale** (attraverso un particolare oggetto (tessera magnetica, smart card, ecc...))
 - **Caratteristiche Biometriche** (iride, impronta digitale, impronta vocale, riconoscimento del volto, ecc..).



10



Funzionalità di Base: AUTORIZZAZIONE

Autorizzazione

Definisce le regole di autorizzazione ai dati e/o alle applicazioni.

- E' un processo complementare all' Autenticazione.
- Pone le basi per il Controllo degli Accessi.

Da molti punti di vista, l'Autorizzazione è il fulcro attorno a cui tutta l'infrastruttura di gestione delle identità di un'organizzazione ruota.

11



Funzionalità di Base: CONTROLLO ACCESSI

E' il processo mediante il quale viene concesso o negato l'accesso a una risorsa.

Ad esempio tramite:

- Policy: l'insieme di regole che determinano chi può fare cosa.
- Schemi di autorizzazione: ACL(*Liste di controllo d'accesso*), Ruoli.

12



Funzionalità Complementari: GESTIONE UTENTI

User Provisioning

- Permette l'amministrazione degli utenti e dei loro profili al di fuori delle singole Applicazioni, tramite un'infrastruttura condivisa.

Self Service Delegation

- Permette la delega all'utente stesso relativamente all'amministrazione di alcune informazioni del proprio profilo.

Password Management

- Permette la gestione dell'autenticazione al di fuori delle singole applicazioni, tramite un'infrastruttura condivisa. Ciò tipicamente include la sincronizzazione delle password, l'aggiornamento, l'amministrazione dei profili durante l'aggiornamento.

13



Funzionalità Avanzate: SINGLE SIGN ON (SSO)

E' la possibilità per un utente di autenticarsi presso uno qualsiasi dei provider della federazione e, successivamente, di accedere ai servizi di tutti gli altri.

Più tecnicamente è l'aggregazione dei dati di identità, fondamentalmente vengono trattati come se esistesse un unico archivio centralizzato, che è il risultato di diverse soluzioni:

- Metadirectory
- Directory virtuali
- Federazione di directory

14



REGIONE AUTONOMA DELLA SARDEGNA

Sardegna IT

Funzionalità Avanzate: FEDERAZIONE

- E' una comunità di provider (SP ed IdP).
- Viene definita anche: Federation o Circle of Trust.
- Viene realizzata collegando i diversi identificatori utilizzati dai provider della federazione e relativi ad uno stesso utente.

15



REGIONE AUTONOMA DELLA SARDEGNA

Sardegna IT

Funzionalità Avanzate: Auditing & Reporting

Auditing & Reporting

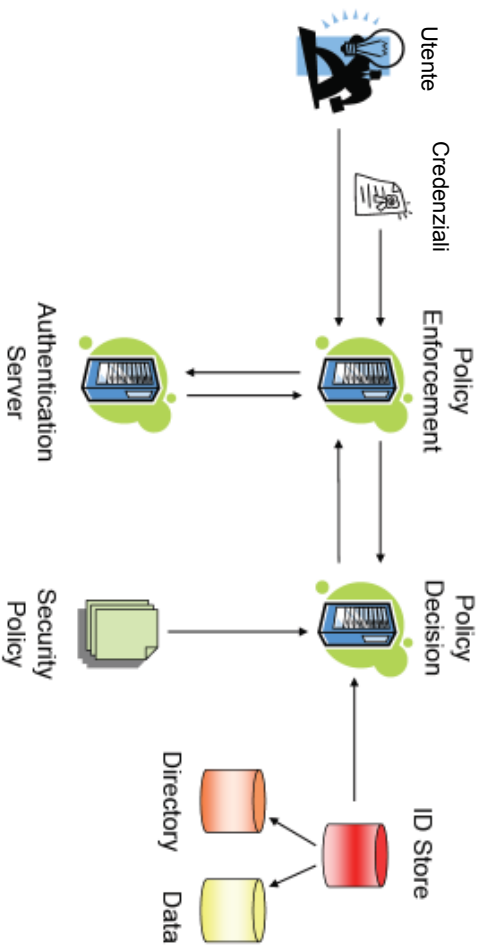
E' il processo che consente la gestione, la tracciabilità e la visualizzazione di tutte le operazioni effettuate da un utente dopo l'autenticazione.



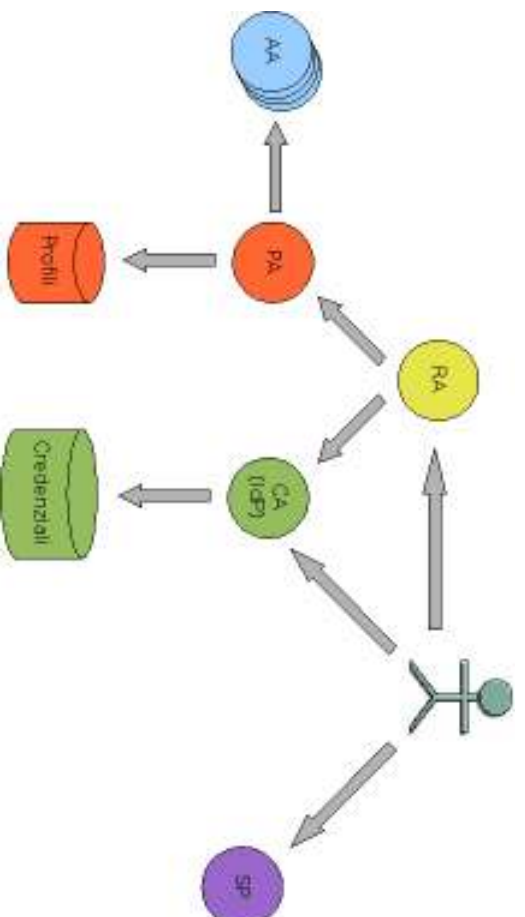
16



Architettura di un sistema IM



Attori in gioco





Attori in gioco: REGISTRATION AUTHORITY (RA)

Registration Authority (RA) e Provisioning

La Registration Authority (RA) si occupa di raccogliere e verificare le informazioni relative agli utenti (provisioning).

La certificazione delle informazioni di identità può avvenire secondo tre modalità:

- Il riconoscimento a vista del soggetto effettuato da un addetto incaricato dall'Ente mediante esibizione di un documento di identità valido.
- In base all'Art. 45 del DPR n. 445, 28 dicembre 2000 mediante invio via fax o posta del modulo di registrazione sottoscritto, accompagnato dalla copia fotostatica di un documento di identità valido.
- Per via telematica tramite compilazione sul sito dell'ente ed invio del modulo di registrazione da parte di un utente, che si è autenticato al servizio di registrazione utilizzando la CIE o una CNS.

19



Attori in gioco: ATTRIBUTE AUTHORITY (AA)

Attribute Authority (AA)

Il componente Attribute Authority ha il compito di certificare i singoli attributi che formano il profilo utente memorizzato dalle Profile Authority.



20



Attori in gioco: PROFILE AUTHORITY (PA)

Profile Authority (PA)

Il componente Profile Authority memorizza e gestisce i profili degli utenti.

Ciascun profilo utente può contenere diversi attributi utente, ciascuno dei quali riferenzia la Attribute Authority in grado di certificarlo.



21



Attori in gioco: CERTIFICATION AUTHORITY (CA)

Certification Authority (CA) o Identity Provider (IdP)

L'Identity Provider garantisce il riconoscimento dell'utente di cui crea e conserva le credenziali consegnate al diretto interessato.

Di norma è un soggetto di fiducia esterno e gestisce tutta la fase di autenticazione.

Il componente Identity Provider è conforme all'omonima entità prevista dalle specifiche SAML, cioè rappresenta l'entità in grado di certificare l'identità di un utente a seguito di una fase di autenticazione.



22



Attori in gioco: USER AGENT (UA)

User Agent (UA)

E' l'applicazione che, per conto dell'utente richiede l'accesso ad una risorsa protetta

The screenshot shows the SardegnaIT website interface. At the top, there are navigation tabs for 'Comuni sardi', 'Cittadini', and 'Presidi'. Below this, there are sections for 'COMUNI SARDI' with a dropdown menu, 'ACCEDEI AI SERVIZI' with input fields for 'cod. fiscale o P.IVA' and 'Inserisci codice', and a 'password' field. There are also links for 'Recupera dati di accesso', 'Registrazione | Attivazione', and 'SERVIZI AL CITTADINO'. A large red arrow points to the 'ACCEDEI AI SERVIZI' section. At the bottom, there is a 'TOSAP' section with an image of a person at a computer and text about public spaces and taxes.

23



Attori in gioco: SERVICE PROVIDER (SP)

Service Provider (SP)

Il Service Provider eroga i servizi e esiste a prescindere dal sistema di autenticazione

The screenshot shows a collage of various web pages from the SardegnaIT website. It includes pages for 'Comuni sardi', 'Cittadini', and 'Presidi'. There are also pages for 'Comuni sardi' and 'Cittadini' with different content, and a page for 'Presidi' with a photo of a person. The pages are arranged in a grid-like fashion, showing different parts of the website's interface.

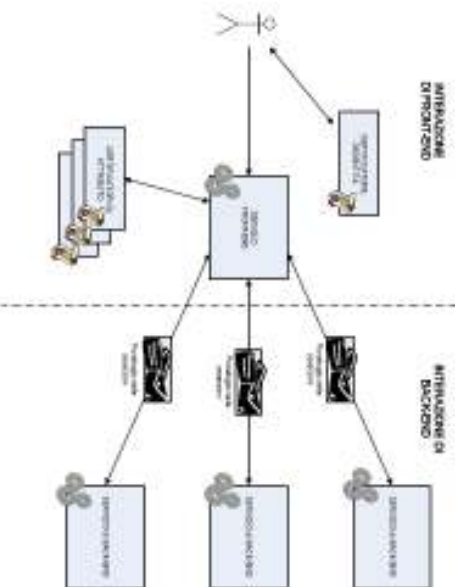
24



Autenticazione di applicazioni

Il processo di fruizione di un servizio, comporta un'interazione applicativa tra componenti applicative diverse, in modo trasparente per l'utente finale.

In altri termini, a valle di una richiesta da parte di un utente è possibile, e in generale frequente, che tale richiesta, causi l'attivazione di ulteriori richieste per servizi di livello più basso, funzionali all'adempimento della richiesta originaria.



25



Consigli per l'implementazione di una soluzione di IM: COSA FARE *

- Scrivere applicazioni snelle, per semplificare i processi
- Implementare il più possibile architetture IM centralizzate sia per applicazioni legacy che nuove.
- Privilegiare l'utilizzo dell' autenticazione forte.
- Implementare un repository centralizzato per l'auditing (event log).
- Includere i costi di auditing nell'investimento per l'IM

* Fonte: **GARTNER** - The Do's and Don'ts of Identity and Access Management - Aprile 2006

26



Consigli per l'implementazione di una soluzione di IM: **COSA NON FARE ***

- Evitare l'uso di un singolo Identity Provider.
- Non basarsi su una singola enterprise directory.
- Non usare la Profile Authority per il Provisioning
- Evitare di integrare tutto in un'unica applicazione.
- Non sperare che il Single Sign On (SSO) funzioni perfettamente in tutte le applicazioni.
- Non preoccuparsi di avere Identità federate a meno che non diano evidenti benefici.
- Evitare di implementare un proprio sistema IM se non è strettamente necessario, e comunque, cercare di renderlo semplice.

* Fonte: GARTNER - The Do's and Don'ts of Identity and Access Management - Aprile 2006

27



Esempi di Soluzioni IM commerciali



IBM Tivoli



HP Identity management Solutions



Novell Identity Manager



Sun Java System Identity Manager



Oracle Identity Manager



REGIONE AUTONOMA DELLA SARDEGNA

Sardegna IT

SOLUZIONI IM Open source



Liberty Alliance Project



Bandit project



The Open Web SSO project



Diamelle Technology's
OpenIAM



Shibboleth software



SSOCircle.com

29



REGIONE AUTONOMA DELLA SARDEGNA

Sardegna IT

DOMANDE ????

30