POLITECNICO DI MILANO

Le problematiche di Identity Management per una organizzazione grande ed eterogenea

2° Convegno IDEM – Bari, 9-10 Marzo 2010

Roberto Gaffuri – Politecnico di Milano

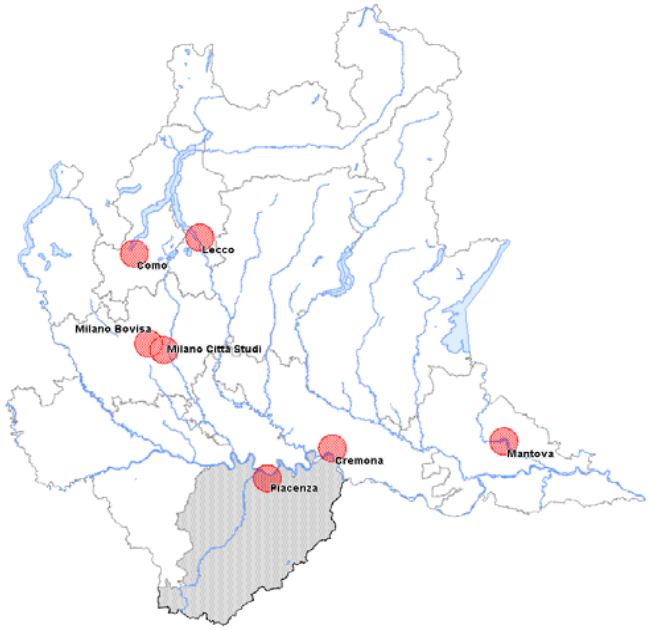
Indice

1. Caratteristiche dell'organizzazione
2. Situazione nel 2005
3. Consolidamento identità digitali, anagrafica unica e credenziali uniche
4. Modello di accreditamento
5. Autenticazione, autorizzazione e gestione dei log
6. Sviluppi futuri

Un’organizzazione grande

Molti utenti:

- 48000 studenti attivi
- 100000 laureati
- 7000 tra docenti, TA e collaboratori
- 2000 account ospiti

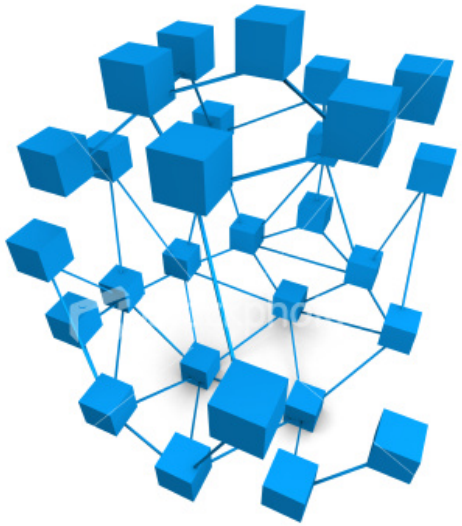


Distribuita sul territorio:

- 7 sedi : Milano, Como, Lecco, Cremona, Mantova, Piacenza

Un’organizzazione eterogenea

- 9 Facoltà (3 architettura e design, 6 ingegneria)
- 16 Dipartimenti, 7 Centri, 8 Aree dell’amministrazione centrale
- Molti progetti di cooperazione tra le strutture
- Un Area SW interna e vari centri tecnici
- Molti fornitori di IT da integrare
- Soluzioni tecnologiche eterogenee: J2EE, Windows, Open source



Situazione nel 2005 (anagrafiche)

Anagrafiche diverse:

- Censimento multiplo in diversi DB di studenti e personale
- Censimento multiplo in diverse directory
  - AD per auth Client Windows, Outlook..
  - LDAP per auth posta docenti e studenti, Proxy, client Linux
- DB satellite replicati con esportazione manuale periodica
  - Biblioteche
  - Associazione laureati..

Problemi associati:

- Accreditamento multiplo
- Poca affidabilità dei dati
- Vari punti da presidiare
- Difficoltà nella gestione del ciclo di vita dell'identità (disattivazione)
- Scarso presidio sui diritti di accesso ai servizi

Situazione nel 2005 (credenziali)

Credenziali diverse:

- In base all'uso:
  - accesso alle macchine e alla posta
  - accesso alle applicazioni
- In base alla carriera:
  - studente (1liv, 2liv, master,..ecc)
  - docente, ta. (contratto, tempo det., tempo indet.)

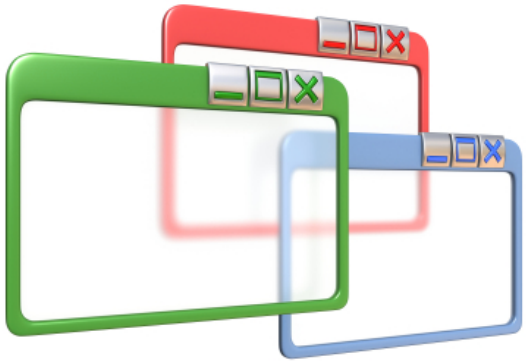
Problemi associati:

- Problemi di insicurezza (password banali, distribuzione su canali non sicuri)
- Policy diverse per ogni credenziale
- Problemi di gestione (vari punti per la gestione delle dimenticanze)
- Scarsa cooperazione tra i servizi e assenza di SSO

Situazione nel 2005 (Applicazioni)

Applicazioni sviluppate internamente (J2EE – Oracle – MS Client)

- Portale servizi amministrativi via web per lo studente
- Portale servizi amministrativi via web per docenti/ta
- Applicazioni legacy per le segreterie/amm. centrale in architettura Client/Server



Applicazioni di terze parti:

- Sistema Giuridico/Stipendi
- Protocollo Informatico di Ateneo
- OPAC bibliotecario
- Gestione di stages e tirocini
- …

Consolidamento identità digitali

Questioni affrontate:

- Come passare ad un’anagrafica unica?
- Dove tenere il master dell’anagrafica unica?
- Come gestire la riconciliazione di identità presenti in molteplici DB?
- Quali attributi propagare nelle directory?
- Come mantenere allineati il DB master, le directory, e i DB periferici?

Anagrafica unica: cosa?

Attributi di anagrafica unica:

- Credenziali uniche della persona
- Dati dell'anagrafe 'civile':
  - Persona + Residenza: valore legale
  - Recapiti: uso operativo
  - Dati di contatto: telefoni, mail, …
- Dati accademici:
  - Carriere per studenti
  - Carriere per docenti / ta
  - Ruoli/Incarichi per esterni

Anagrafica unica: come?

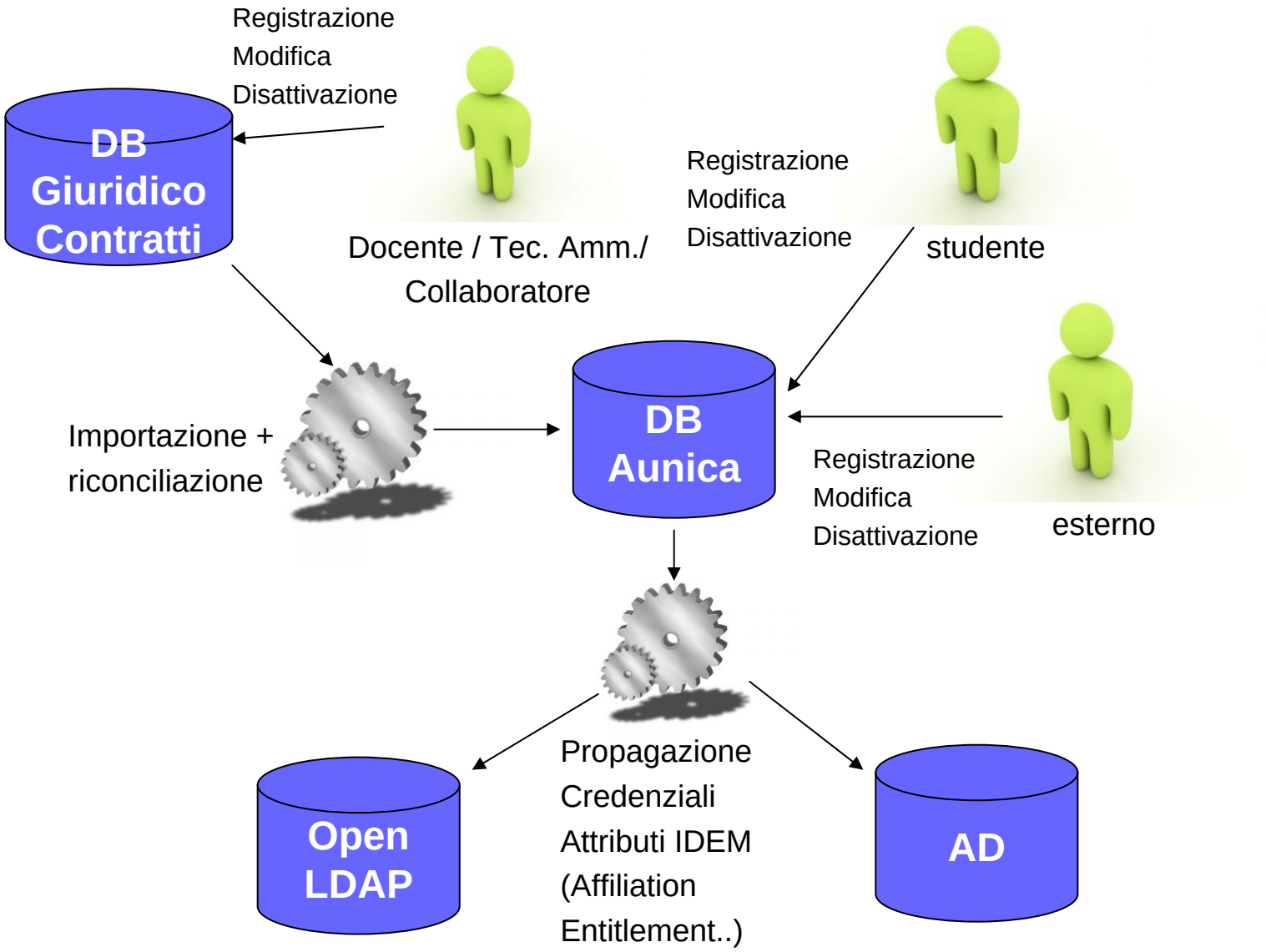
Soluzione adottata:

- Anagrafica unica su un DB master
- Propagazione verso le directory dei dati minimi necessari per autenticazione autorizzazione e mail routing (IDEM attributi)
- Propagazione verso alcuni DB satellite (che non contengono credenziali)

Componenti necessarie:

- Servizio di supporto alla riconciliazione di identità provenienti da fonti diverse
- Servizio di allineamento verso le directory schedulato e in tempo reale
- Servizio di allineamento verso alcuni DB satellite basato su web-service

Registrazione e propagazione dell'identità



Credenziali uniche

Soluzione adottata:

- Nuova credenziale unica: “Codice persona”
- Codice numerico di 8 cifre

Codice Persona vs. e-mail:

- Codice Persona precede l’assegnazione di una mail istituzionale
- L’ateneo permette mail multiple per le stesse persone (studente @mail.polimi.it, personale @polimi.it)
- Gli “esterni” non dispongono di mail istituzionale
- Accesso call center di Ateneo
  - username numerico: per praticità di inserimento
  - Pin per accesso: a differenza della password è numerico

Consolidamento: implicazioni

Questioni tecnologiche:

- Scelta del repository per anagrafica unica e della sua struttura
- Meccanismi di sincronizzazione da DB verso i directory AD / OpenLDAP
- Meccanismi di sincronizzazione con sistemi esterni

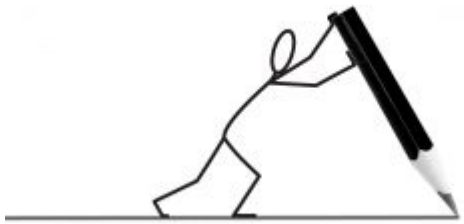
Questioni organizzative:

- Consolidamento dei processi di accreditamento
- Presidio della riconciliazione di identità provenienti da fonti differenti nel caso di sovrapposizioni (criteri di responsabilità)
- Presidio dell'interazione tra il centro e la periferia (supporto all'interazione B2B)

Propagazione attributi dell'identità verso AD e OpenLDAP

Soluzione adottata:

- Propagazione **unidirezionale** da DB AUNICA verso OpenLDAP ed Active Directory
- Blocco delle modifiche in OpenLDAP ed AD degli attributi provenienti da AUNICA



Caratteristiche OpenLDAP:

- Schemi base (LDAPv3, eduPerson, schac)
- Propagazione di eduPersonAffiliation calcolata a partire da AUNICA
- Propagazione delle e-mail di redirezione della casella istituzionale (docente/studente) come impostata nel portale personale web

Caratteristiche Active Directory:

- Nessun attributo ad-hoc aggiunto negli schemi di AD
- Propagazione di appartenenza a gruppi impliciti (docenti, studenti…), che vengono mappati esplicitamente su gruppi di windows

Propagazione password verso AD ed OpenLDAP

Soluzione adottata:

- Deve avvenire in tempo reale su tutti i contenitori dell'identità che offrono autenticazione
- Per l'utente esiste un solo sistema informativo

Componenti necessarie:

- Applicazione di Ateneo per cambio password
  - Responsabile di coordinare il servizio di propagazione
- Servizio di propagazione verso LDAP
  - Propagazione real-time al cambio password
  - Con gestione del failover se nel DB le password hanno un formato compatibile con OpenLDAP (MD5/SHA/SSHA)
- Servizio di propagazione verso AD
  - Propagazione al cambio password, possibile solo la generazione contestuale DB e AD failover/riallineamento NON possibile

Integrazione con DB Esterni

Soluzione Adottata:

- WebService per aggiornamenti incrementali dei DB periferici a partire dal DB AUNICA

Vantaggi:

- Dati buoni senza ritardo
- Profili selettivi sui dati a seconda del servizio periferico
  - Quali applicazioni vedono quali attributi
- Trace completo degli accessi
- Indipendenza dai cambiamenti alle strutture dati

Accreditamento unico

Accreditamento a livello di Ateneo:

- Applicazione di Ateneo per registrazione identità per studenti ed esterni
- Procedure di importazione e riconciliazione identità in AUNICA a partire dal DB Giuridico/Contratti
- Applicazione di Ateneo per riconoscimento della persona
- Applicazione di Ateneo per rilascio e recupero delle credenziali
- Applicazione di Ateneo per modifica degli attributi anagrafici e di contatto

Riconoscimento: quando?

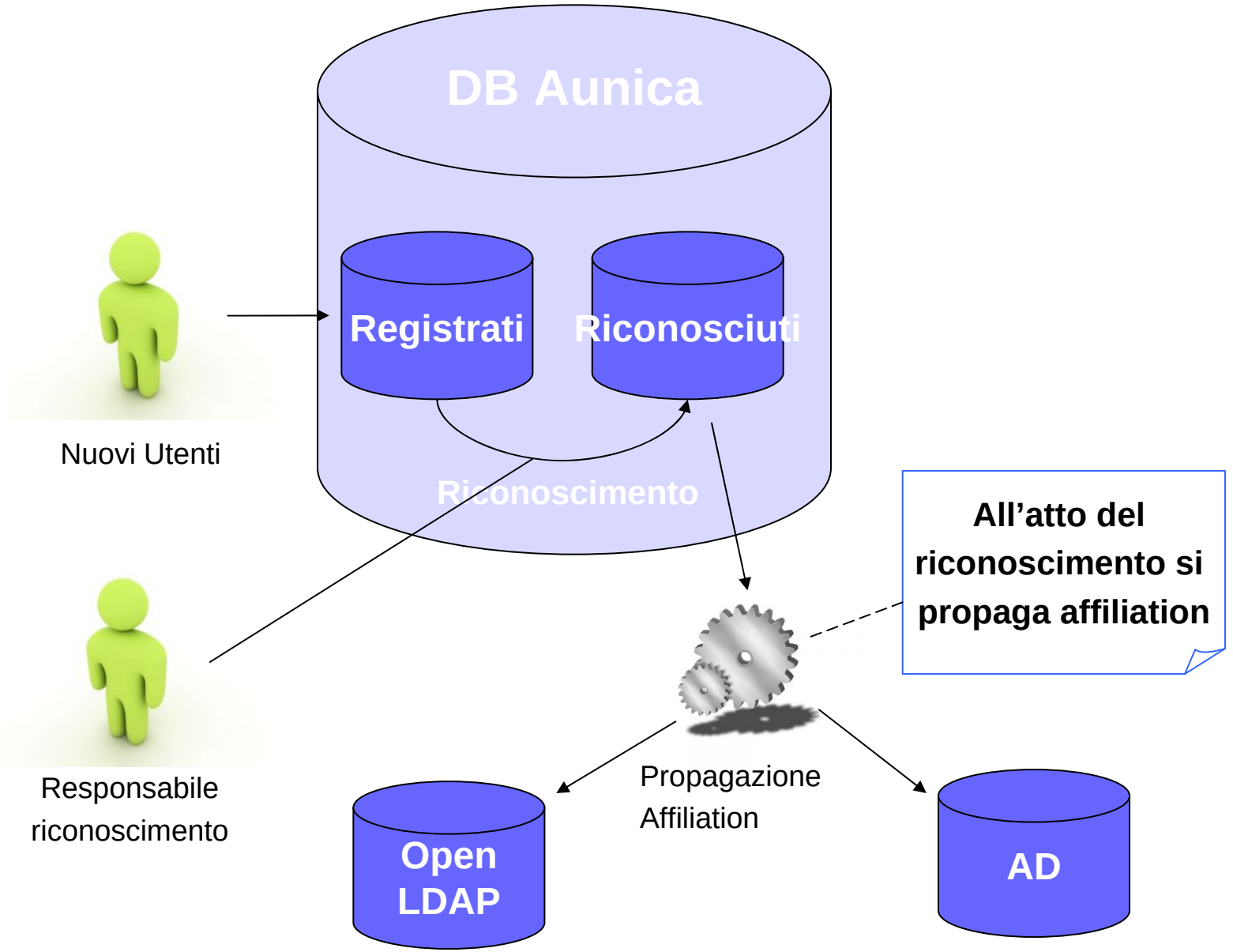
Requisiti:

- Affidabile (De Visu con documento d'identità)
- Autoregistrazione della persona
  - Pratiche pre-iscrizione per studenti (in particolare per stranieri)
  - Autoregistrazioni per ospiti (es.: x convegni)
- Abilitazione ad alcuni servizi prima del riconoscimento affidabile
- Minimizzare i passaggi delle persone da uffici dell'organizzazione
  - Sfruttare i contesti di riconoscimento già in essere (es sessioni di test di ingresso)

Conclusione:

- Registrato != Riconosciuto

Riconoscimento: effetti



Rilascio della credenziale unica

Requisiti:

- Garantire che tutti i passi siano ‘sicuri’ (nessuno possa intromettersi e ottenere le credenziali di un altro)
- Minimizzare le interazioni con uffici helpdesk di supporto (è un costo e introduce insicurezza)

Processi:

- Definire un flusso per i nuovi utenti
  - De visu (nel contesto di un riconoscimento) con stampa credenziali presso ufficio
  - Via web con URL servizio one time token sulla mail personale (non istituzionale) impostata all’atto della registrazione
- Definire un flusso di migrazione per gli utenti esistenti
  - Passaggio da vecchie a nuove credenziali

Recupero credenziali smarrite

Requisiti:

- Garantire che tutti i passi siano ‘sicuri’ (nessuno possa intromettersi e ottenere le credenziali di un altro)
- Minimizzare le interazione con Uffici di supporto

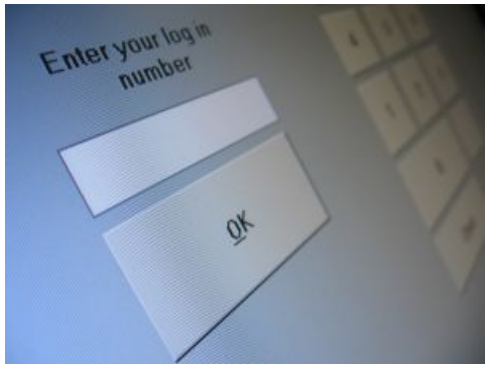
Processi:

- Modalità self-service basata su mail personale con token e domanda di sicurezza
- Modalità assistita da ufficio helpdesk con possibilità:
  - Invio token su mail personale
  - Invio token su cellulare della persona
  - Consegna De Visu con stampa nuove credenziali

Autenticazione e autorizzazione (pre Shibboleth®)

Per tutti i servizi web:

- Autenticazione basata sul sistema di Single Sign On Polimi (basato su token - WebService B2B asserzioni XML)
- Offriamo un meccanismo di autorizzazione di primo livello garantita da SSO Polimi e basata su ruoli



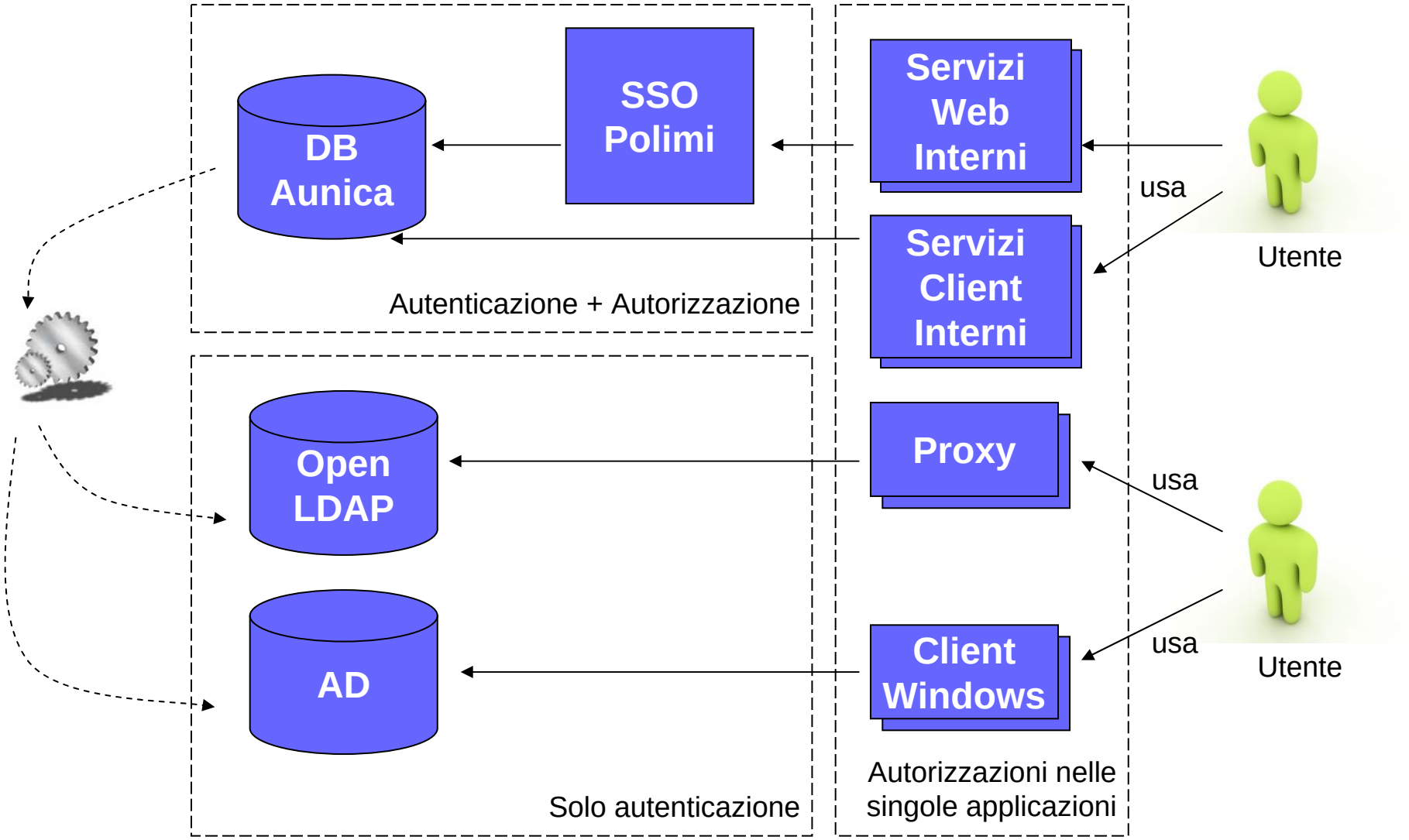
Per i servizi non web o preesistenti e non modificabili:

- Autenticazione via DB per Client MS
- Autenticazione in OpenLDAP: per posta studenti, proxy, Client Linux
- Autenticazione in AD per Client Windows, Suite Microsoft (Outlook, SharePoint, Client Management)

Conserviamo nel DB:

- Catalogo di tutte le applicazioni (interne ed esterne)
- ACL che indicano quali utenti (ruoli/gruppi) possono accedere a quali applicazioni

Autenticazione e autorizzazione (pre Shibboleth®)



Consolidamento del Logging accessi/eventi

Requisiti:

- Log di tutti gli accessi ai servizi
- Log delle azioni chiave all'interno dei servizi
- Ricostruire le azioni dell'utente in una sessione di SSO

Complessivamente:

- Log centralizzato dell'intero percorso d'uso attraverso le varie applicazione
- Il logging è consolidato pertanto si possono applicare:
  - regole di privacy, di conservazione dei dati, di auditing,
  - si possono fare dei report

Autenticazione e autorizzazione (con Shibboleth®)

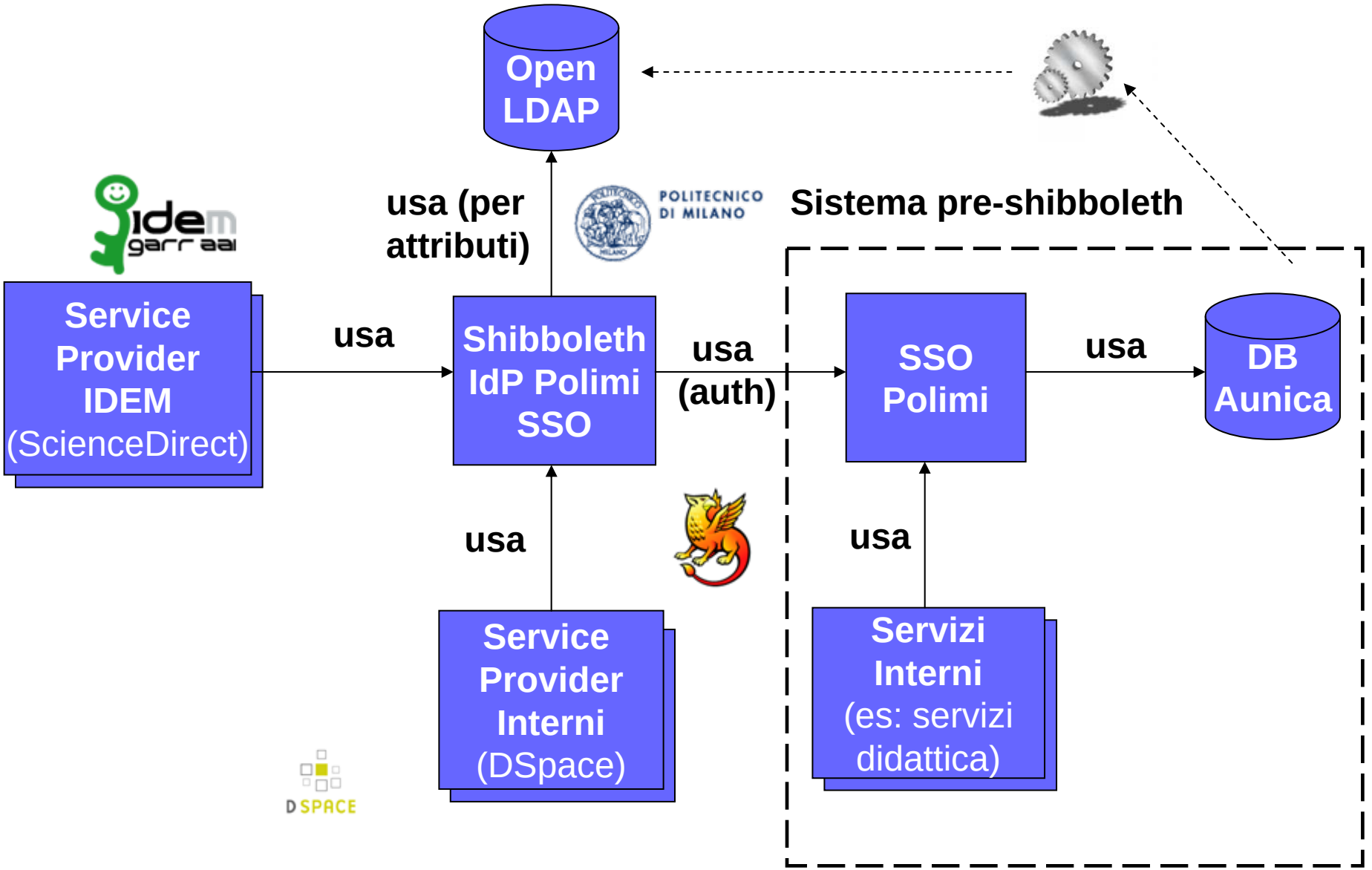
Due livelli di SSO:

- **SSO Polimi:**
  - Verso le applicazioni interne in standard Polimi

SSO SAML:

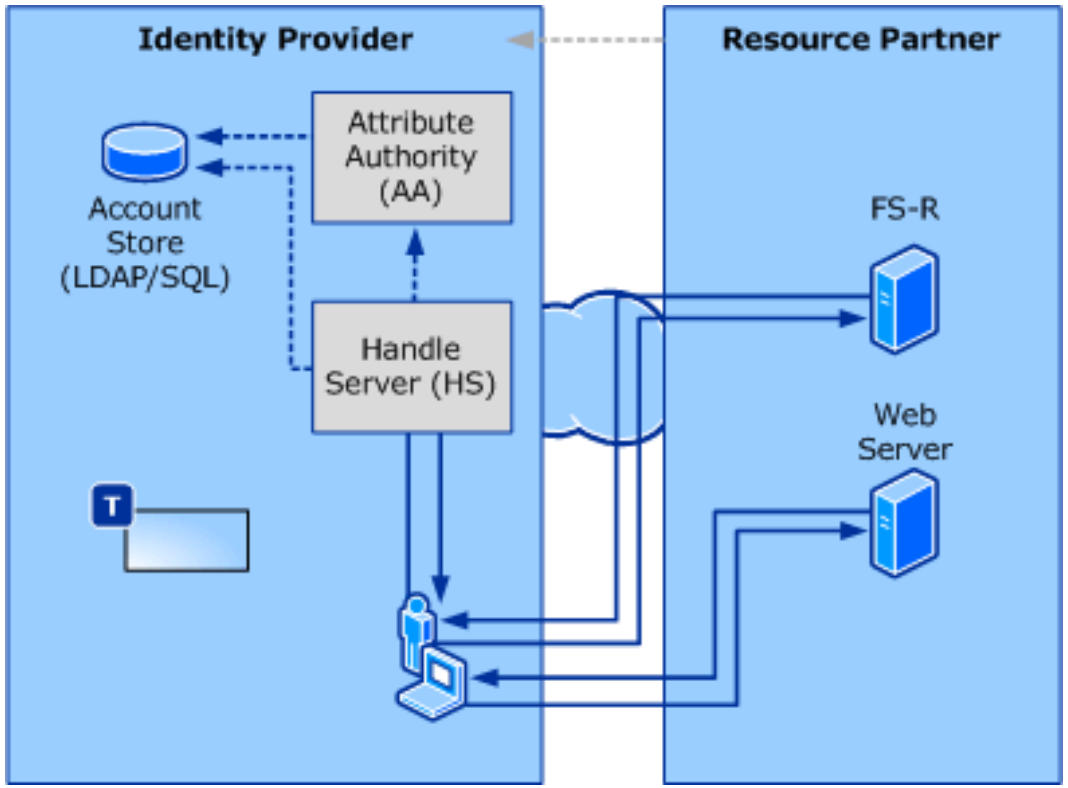
- Verso le applicazioni federate SAML (interne ed esterne)
  - Delega autenticazione a SSO-Polimi
  - Preleva gli attributi da OpenLDAP
  - Disponibile per SP interni Polimi
  - Disponibile per SP IDEM

Autenticazione e autorizzazione (con Shibboleth®)



Sviluppi futuri: Shibboleth e ADFS

- Integrazione ADFS (Active Directory Federation Server) e Shibboleth
  - Autenticare servizi ADFS tramite Shibboleth
    - Es.: MS Outlook webmail, Altiris Client Management, MS Sharepoint
  - Shibboleth IdP come Account Federation Server



Grazie!

Crediti

Le immagini sono tratte dalla collezione stock.xchng (http://www.sxc.hu/)