“Gestire” le identità per “gestire” la sicurezza dei dati

Raffaele Conte
Istituto di Fisiologia Clinica del CNR

Consortium GARR

Health Science Community
la medicina nelle arterie della rete GARR
Conferenza IRCCS
Roma, 12 Dic 2007:.
Aula Magna dell’Università di Roma 3

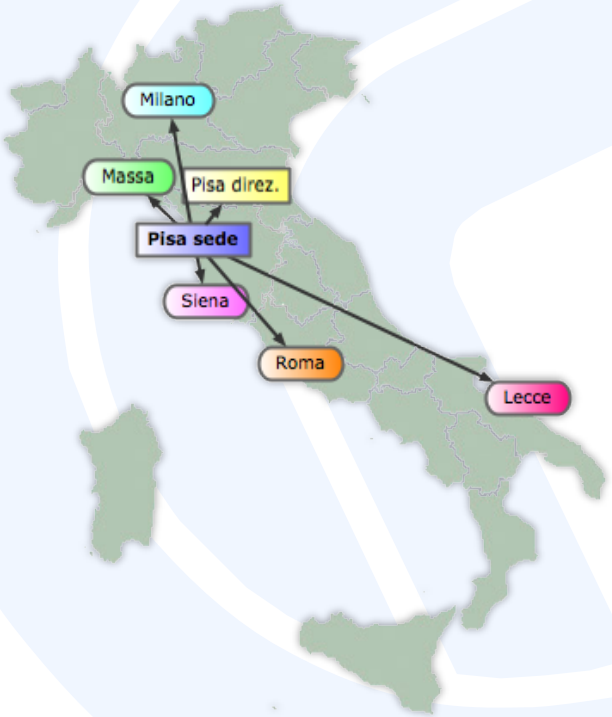
Obiettivo: la sicurezza dei dati

- Sicurezza: integrità, disponibilità, riservatezza
  - l'integrità dei dati può dipendere da:
    - l'integrità delle risorse (utenti)
      - la credibilità degli utenti
        - la gestione affidabile dei sistemi di autenticazione

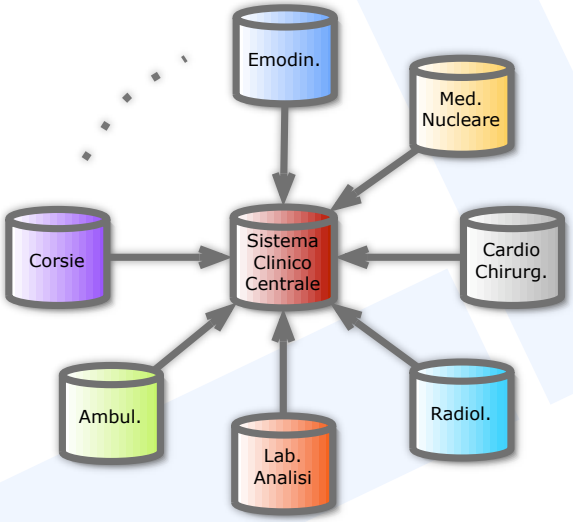
Obiettivo: la sicurezza dei dati

- Sicurezza: integrità, disponibilità, riservatezza
  - la riservatezza dei dati può dipendere da:
    - l'affidabilità delle informazioni sugli utenti
      - la gestione affidabile dei sistemi di autorizzazione

Un contesto sanitario: l'Istituto di Fisiologia Clinica



Organizzazione logica sistema clinico



Problematiche

- Inconsistenza dei dati relativi agli stessi utenti gestiti su più server
- Debolezza delle credenziali di accesso (molte)
- Condivisione delle credenziali
- Assunzione di responsabilità
- Accesso indifferenziato per tipologia di utenza (infermiere, medico, amministrativo, ecc.)
- Estrema volatilità del personale (laureandi, dottorandi, specializzandi, infermieri, ospiti ecc.)
- Normativa

Obblighi di legge

"Codice in materia di protezione dei dati personali" (D.L. 30/6/2003, n. 196)

Art. 3 (Principio di necessità nel trattamento dei dati)

1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Art. 34 (Trattamenti con strumenti elettronici)

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate [...] le seguenti misure minime:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

[...]

Obblighi di legge

D. L. 196/2003, ALLEGATO B - **DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA**

Sistema di autenticazione informatica

[...]

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

[...]

Obblighi di legge

D. L. 196/2003, ALLEGATO B - **DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA**

[...]

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

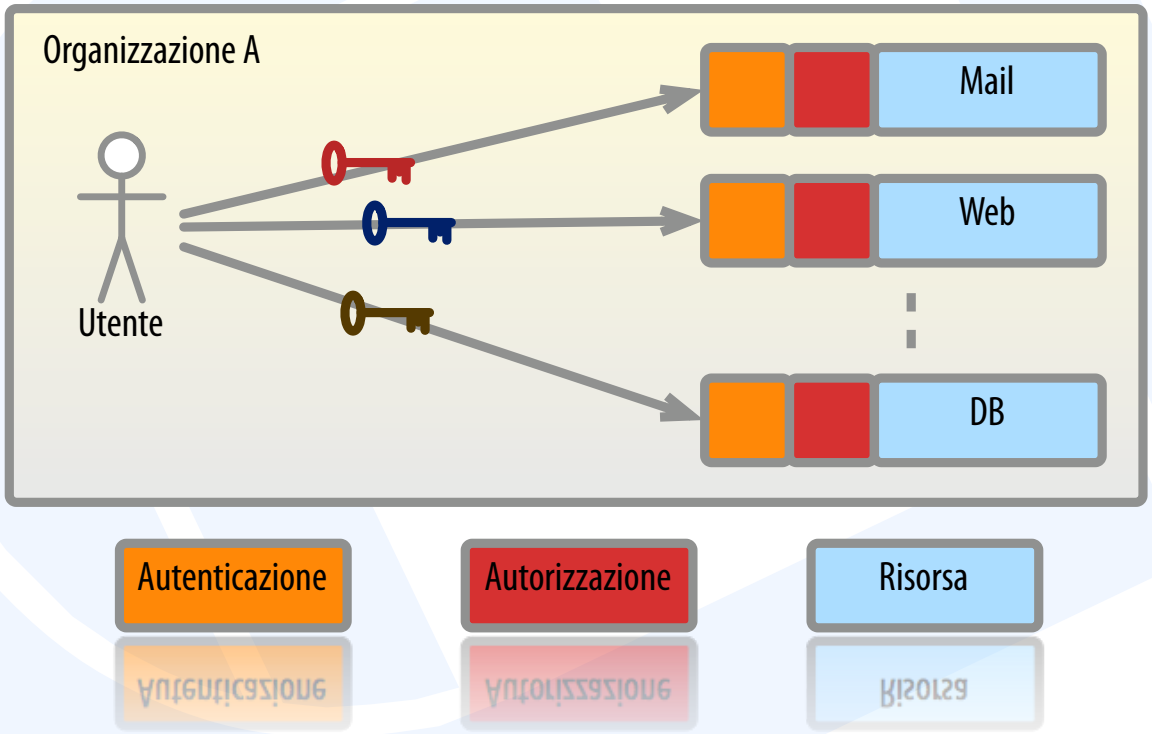
[...]

AAI

- Authentication and Authorization Infrastructure
  - Riduzione del numero di credenziali lato utente
  - Propedeutica per Single Sign-On
  - Eliminazione delle incoerenze relative ai dati dell'utente
  - Autorizzazione basata su attributi/ruoli (ABAC/RBAC)

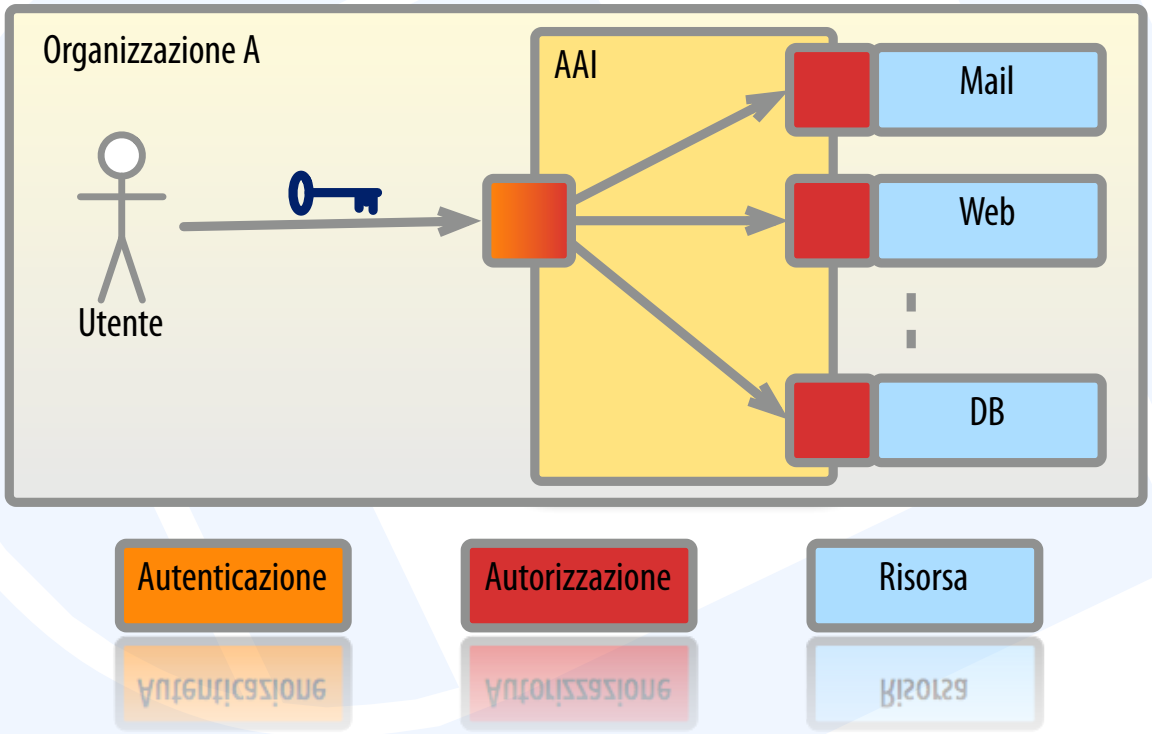
AAI

senza Infrastruttura di AA



AAI

con Infrastruttura di AA



LDAP: cosa...

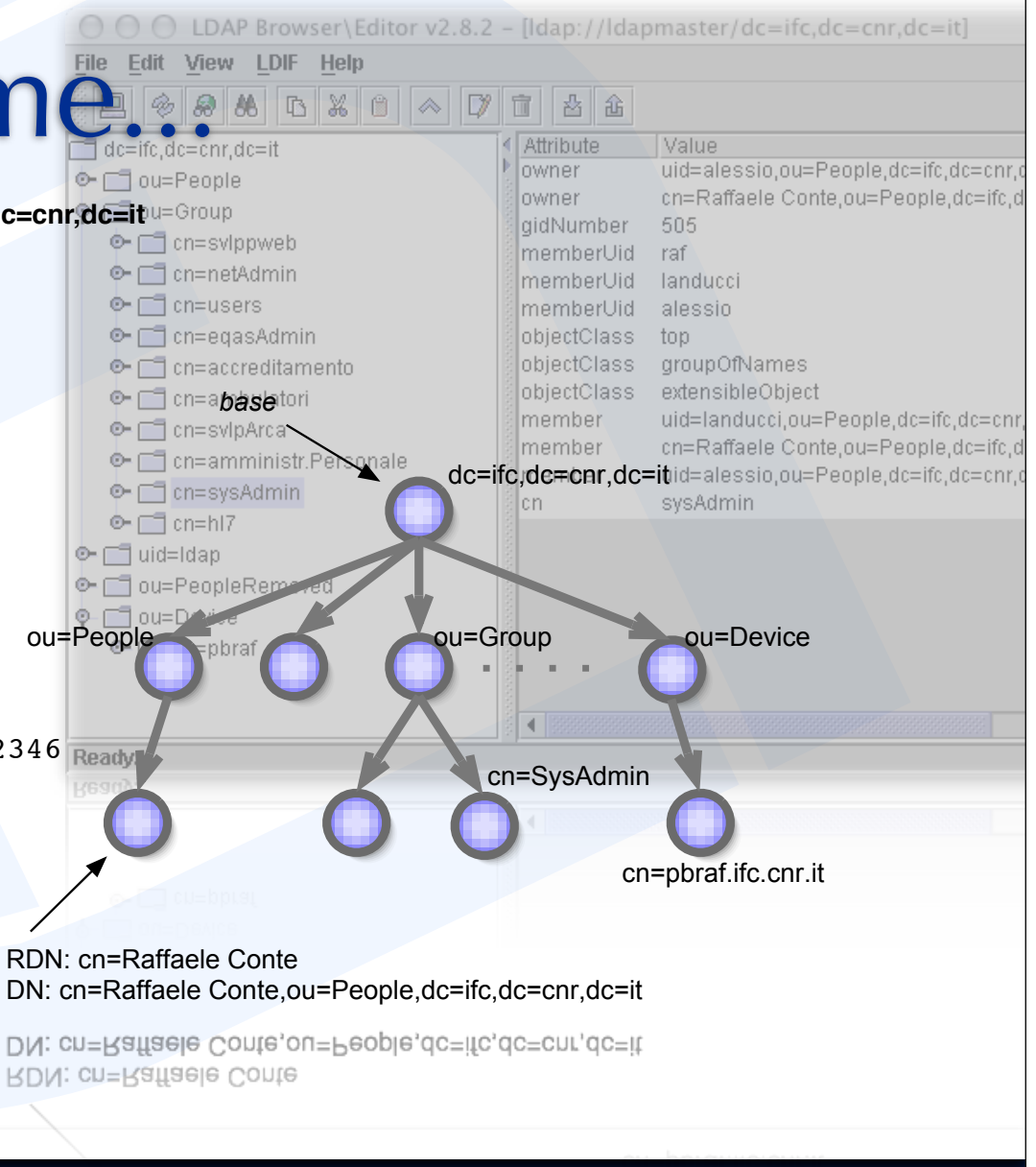
- Il Lightweight Directory Access Protocol deriva (come semplificazione) dall' X.500 OSI Directory Access Protocol
- Non è un DataBase ma utilizza un DataBase per organizzare e rappresentare dati:
  - tramite oggetti con attributi;
  - gerarchicamente ed in maniera da favorire le ricerche piuttosto che le modifiche.

RFC 2251 ed altri (specificati in RFC 3377)

LDAP: come...

dn: cn=Raffaele Conte,ou=People,dc=ifc,dc=cnr,dc=it

```
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Raffaele Conte
uid: raf
sn: Conte
givenName: Raffaele
userPassword:: xYzXyZxYzXyZ
shadowLastChange: 12136
departmentNumber: BIM
mail: raf@ifc.cnr.it
uidNumber: 501
telephoneNumber: +39 050 315 2346
loginShell: /bin/bash
gidNumber: 100
employeeNumber: 7658
gecos: Raffaele Conte, BIM
roomNumber: 79&A&T
l: Pisa
homeDirectory: /home/raf
shadowWarning: 7
```

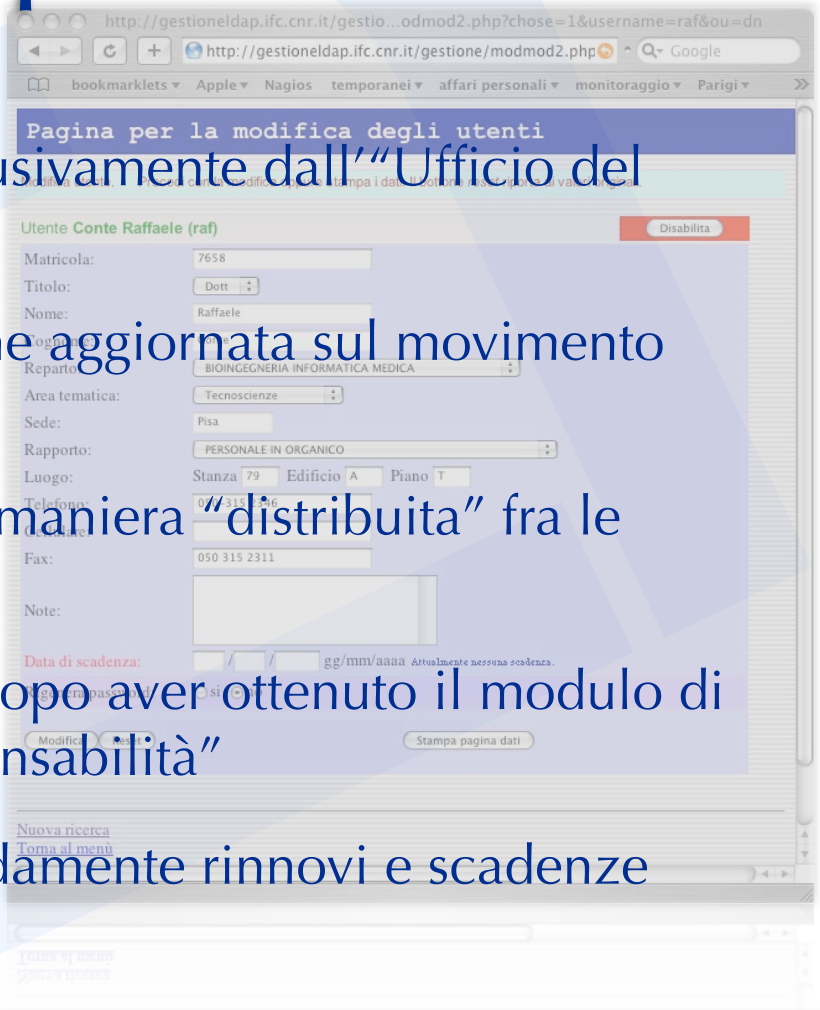


LDAP: perché...

- Standard (organizzazione dei dati)
- Cross-platform
- Ampiamente supportato
- Ottimizzato per le operazioni di ricerca e lettura
- Meccanismi di replica built-in
- Sofisticati sistemi controllo accessi (ACL)

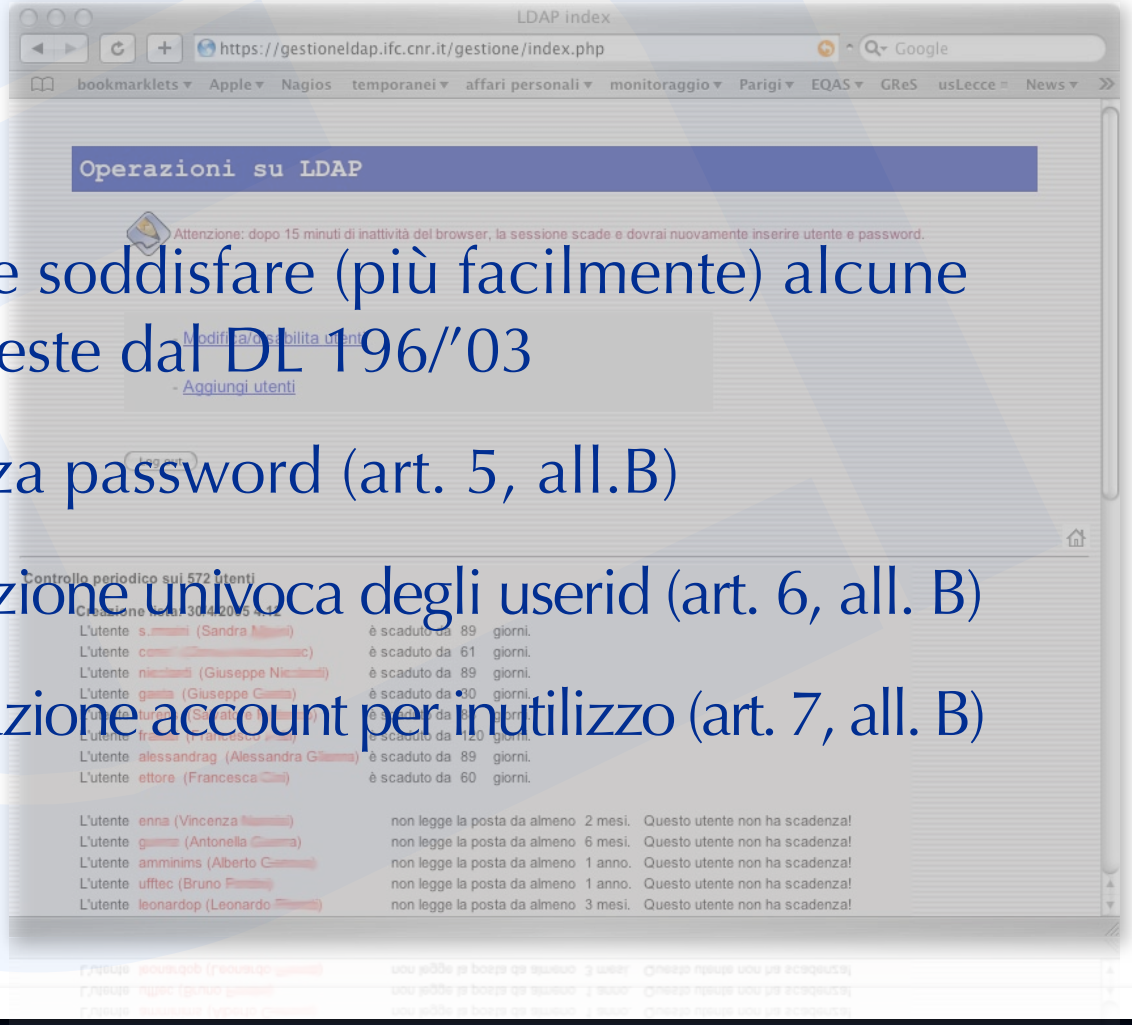
Gestione del profilo utente

- Il profilo è gestito esclusivamente dall'"Ufficio del personale"
  - conosce la situazione aggiornata sul movimento del personale
  - può gestire i dati in maniera "distribuita" fra le diverse sedi/sezioni
  - crea il profilo solo dopo aver ottenuto il modulo di "Assunzione di Responsabilità"
  - può gestire più rapidamente rinnovi e scadenze



Gestione del profilo utente

- È possibile soddisfare (più facilmente) alcune misure richieste dal DL 196/'03
  - scadenza password (art. 5, all.B)
  - assegnazione univoca degli userid (art. 6, all. B)
  - disabilitazione account per inutilizzo (art. 7, all. B)



Autorizzazione "implicita"

- Filtri:
  1. cerca l'utente con il profilo:

     ```
     username = <in input>
     reparto = BIM or ELDA
     ruolo = Tecnologo
     ```

  2. Se esiste: autentica con password <in input>

Alcune informazioni potrebbero essere disponibili solo dopo l'autenticazione

Autorizzazione "esplicita"

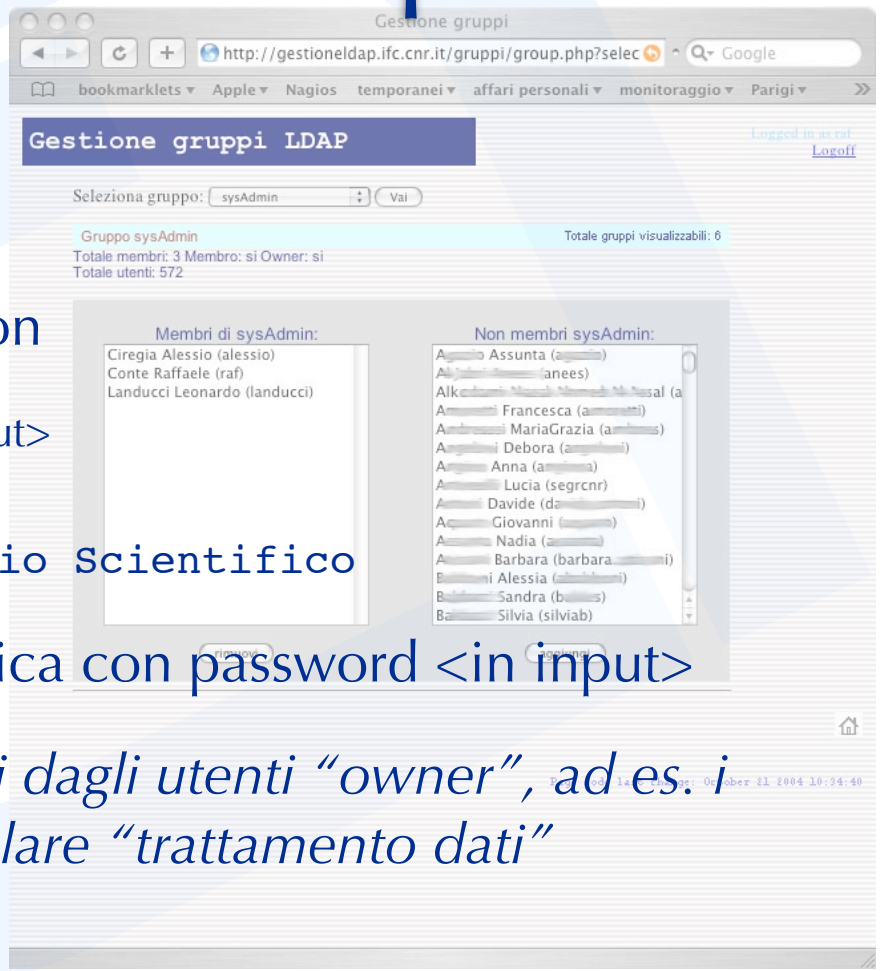
- Gruppi:
  1. cerca l'utente con

     username = <in input>

     and

     `gruppo = Consiglio Scientifico`

  2. Se esiste: autentica con password <in input>



I gruppi vengono gestiti dagli utenti "owner", ad es. i responsabili del particolare "trattamento dati"

Estensioni

- autorizzazioni per ruolo/orario
- indirizzario utenti
- autenticazione in rete 802.1X (gw radius-ldap)
- Single Sign-On (in associazione con Kerberos)
- ...

Pro e Contro

- Vantaggi
  - creazione/modifica dei profili utente gestita da chi possiede le informazioni sugli utenti (Ufficio del Personale) senza intermediari
  - informazioni sugli utenti centralizzate ma automaticamente replicate
  - personale tecnico cura gli aspetti tecnologici piuttosto che amministrativi
  - immediata propagazione della “revoca di tutti diritti” (disabilit. utente)
  - gestione delle autorizzazioni effettuata da responsabile del servizio o particolare trattamento dati

Pro e Contro

- Svantaggi
  - tutte le comunicazioni richiedono kerberos o cifratura
  - i servizi devono essere “fidati”
  - carpita la password di un utente si può accedere a tutti servizi per i quali è autorizzato *(discutibile!!!)*

Il sistema LDAP è molto critico: un problema su esso compromette l’accesso a tutti i servizi che lo utilizzano!!

Importante configurare le repliche opportunamente!!!

...e se l'utente è esterno all'organizzazione che offre il servizio?

Problematiche

Oltre a quelle precedenti, sempre valide

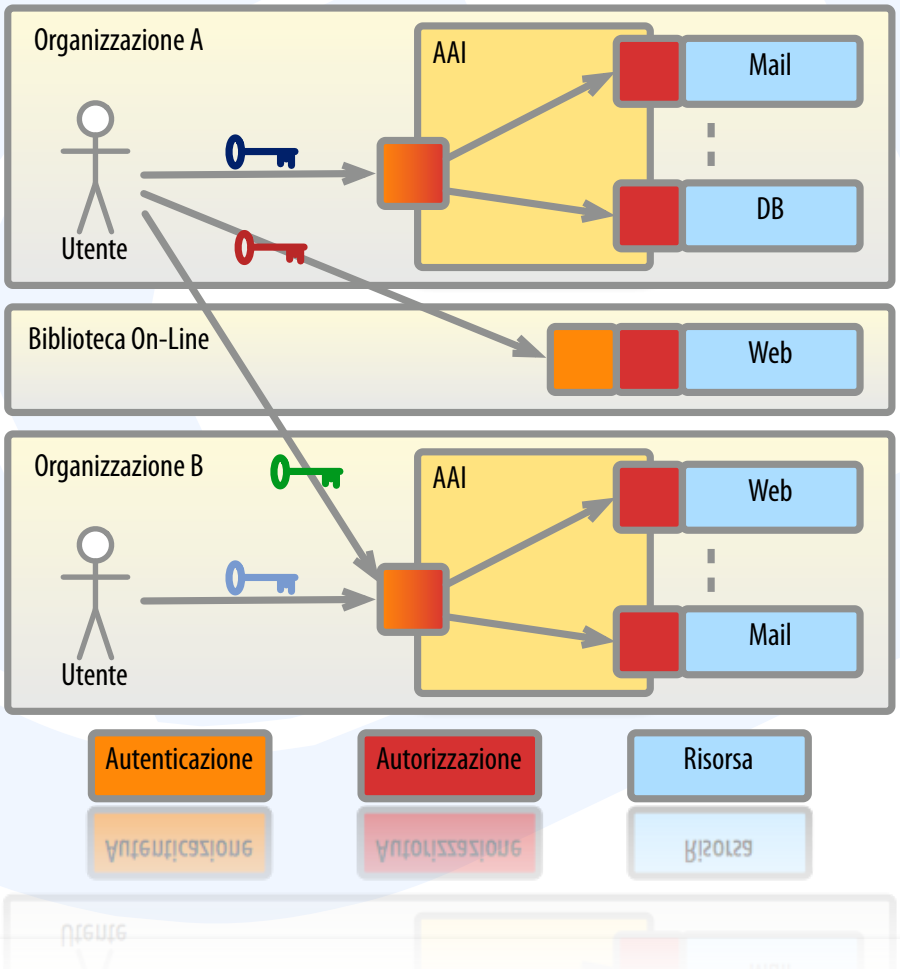
- per l'utente:
  - nessun controllo sulle regole di riservatezza relative alle informazioni fornite
  - uso di password diverse per servizi diversi (per evitare l'uso inappropriato delle stesse su altri servizi)
- per il fornitore del servizio
  - scarse informazioni sull'utente
  - possibilità di variazione dei dati a sua insaputa

AAI federata

- Autenticazione locale, presso l'organizzazione di appartenenza
- Accesso a servizi remoti, di altre organizzazioni senza ulteriori autenticazioni

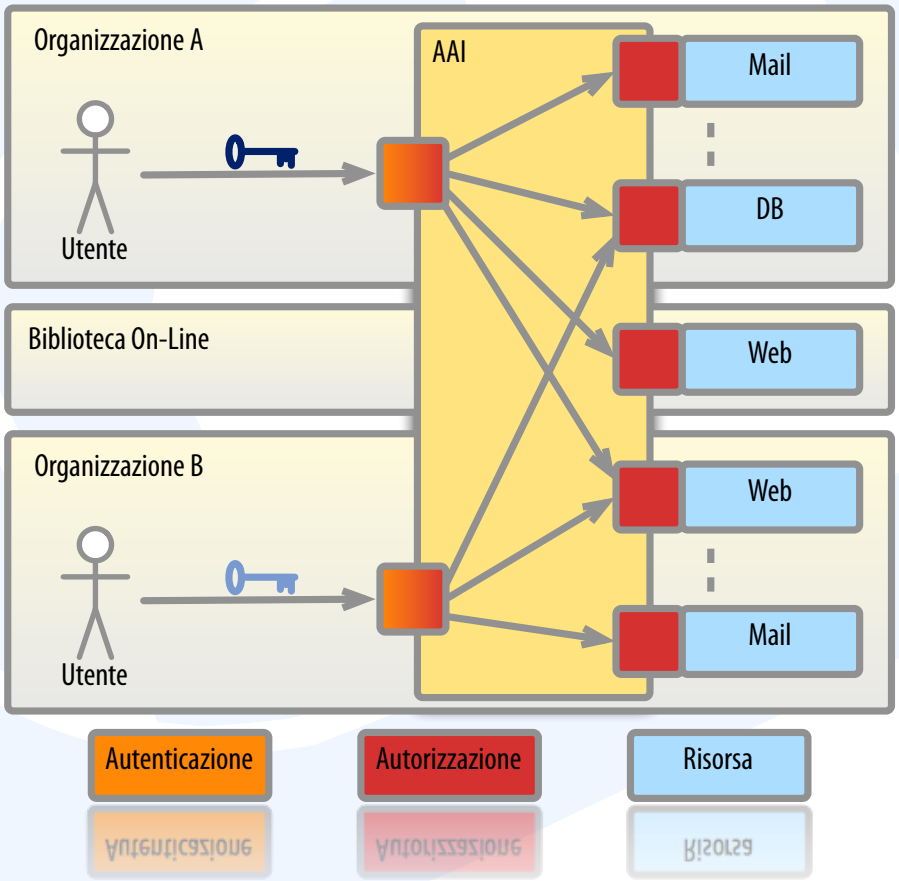
AAI federata

senza AAI Federata



AAI federata

con AAI Federata



SAML

- *Security Assertion Markup Language*
  - framework XML-based
  - sviluppato da OASIS
  - standard per lo scambio fra organizzazioni di informazioni relative all'identità e all'accreditamento di un utente presso la propria organizzazione

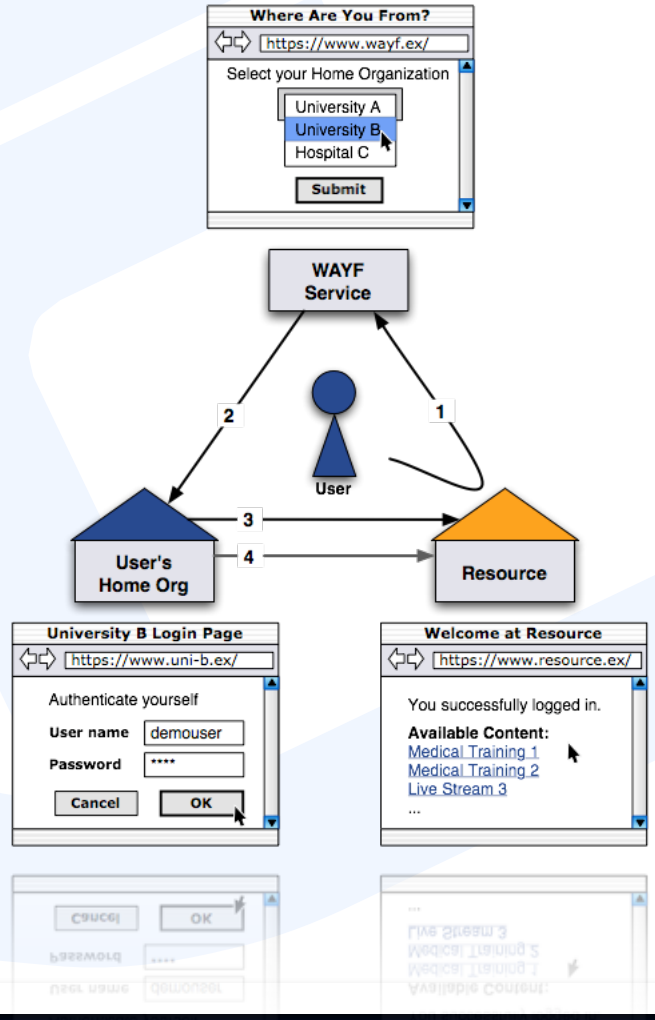
SAML

- Sviluppato per rendere sicuri i servizi web-based
- Consente Web-SSO
- Oltre al *"tradizionale"* Service Provider (SP) introduce i concetti di:
  - Identity Provider (IdP)
  - Metadati: "coordinate" dei partecipanti

Shibboleth

- Implementazione di SAML
- Progetto ufficiale di Internet2
- Rilasciato con Apache Software License

Il processo di AA federata



© 2006 SWITCH

Vantaggi AAI federata

- Per l'utente finale
  - utilizzo di credenziali uniche
  - controllo sulle informazioni diffuse
  - rilascio dati personali solo se necessario

Vantaggi AAI federata

- Per l'organizzazione:
  - controllo sul processo di autenticazione e autorizzazione
  - autorizzazione concessa in base al ruolo (RBAC)

Vantaggi AAI federata

- Per il fornitore del servizio:
  - riduzione oneri gestione credenziali
  - utilizzo di informazioni aggiornate e affidabili

Possibili applicazioni in ambiente sanitario

- Accesso ad utilità del SSR
- Servizio centralizzato di deposito beni digitali (archiviazione CC elettroniche)
- Mobilità professionisti sanitari
- Mobilità pazienti

Come sperimentare un'AAI?

- Aderendo ad IDEM

- progetto pilota patrocinato dal GARR
- durata: tutto il 2008

Consortium GARR

IDEM: servizi iniziali

- NILDE (Network Inter-Library Document Exchange)
- Videoconferenza GARR (dal 4/'08)
- Altri eventuali (Thomson Corp., Elsevier ecc.)

IDEM: il supporto GARR

- Infrastruttura IT centrale
  - WAYF server
  - elenco certificati CA
  - mappa federazione (metadati)
- Supporto tecnico per gli IdP e gli SP
- GARR-CA e SCS
- GARR-CERT

IDEM: requisiti

- Per i fornitori di servizi:
  - adeguamento agli standard tecnici indicati (SP Shibboleth)
  - riservatezza verso terzi
  - implementazione conforme alle specifiche di GARR-AAI

IDEM: requisiti

- Per i fruitori dei servizi:
  - realizzazione IdP Shibboleth
  - mantenimento log
  - disponibilità a fornire informazioni sul sistema di accreditamento e gestione utenti

IDEM: risultati attesi

- Rafforzamento sistemi di AA
- Promozione di sistemi di riconoscimento basati su utente/profilo
- Riduzione della diffusione di informazioni personali
- Riconoscimento reciproco delle organizzazioni GARR
- Promozione nuovi servizi anche da partecipanti
- Possibilità di estensione e/o confederazioni

Riferimenti

- LDAP: RFC 2251,3377 ecc.
- Carter G, "LDAP System Administration" , O'Reilly, 2003;
- http://www.openldap.org;
- http://www.oasis-open.org
- http://shibboleth.internet2.edu/
- http://www.idem.garr.it

Ringraziamenti

- IFC - CNR
- Tutti coloro che hanno contribuito a definire il Progetto IDEM
- Il GARR

Grazie!