IDEM: affidabilità e riservatezza nella gestione delle identità per l'accesso a servizi remoti

Raffaele Conte
Istituto di Fisiologia Clinica del CNR

V Conference on Internet Document Delivery
and Inter-library cooperation

Gestione delle identità: affidabilità

- l'utente è effettivamente chi dice di essere
- le informazioni che lo riguardano (profilo)

sono:

- aggiornate
- "garantite"

Gestione delle identità: riservatezza

- per il fornitore: sui dati acceduti
- per l'utente: sulle informazioni personali fornite (dati, operazioni effettuate, preferenze ecc.)

Problematiche

- Inconsistenza dei dati, relativi a stessi utenti, gestiti su più server
- Debolezza delle credenziali di accesso
- Condivisione delle credenziali
- Assunzione di responsabilità
- Accesso indifferenziato per tipologia di utenza (studente, docente, amministrativo ecc.)
- Estrema volatilità del personale (laureandi, dottorandi, specializzandi, ospiti ecc.)
- Obblighi di legge

AA

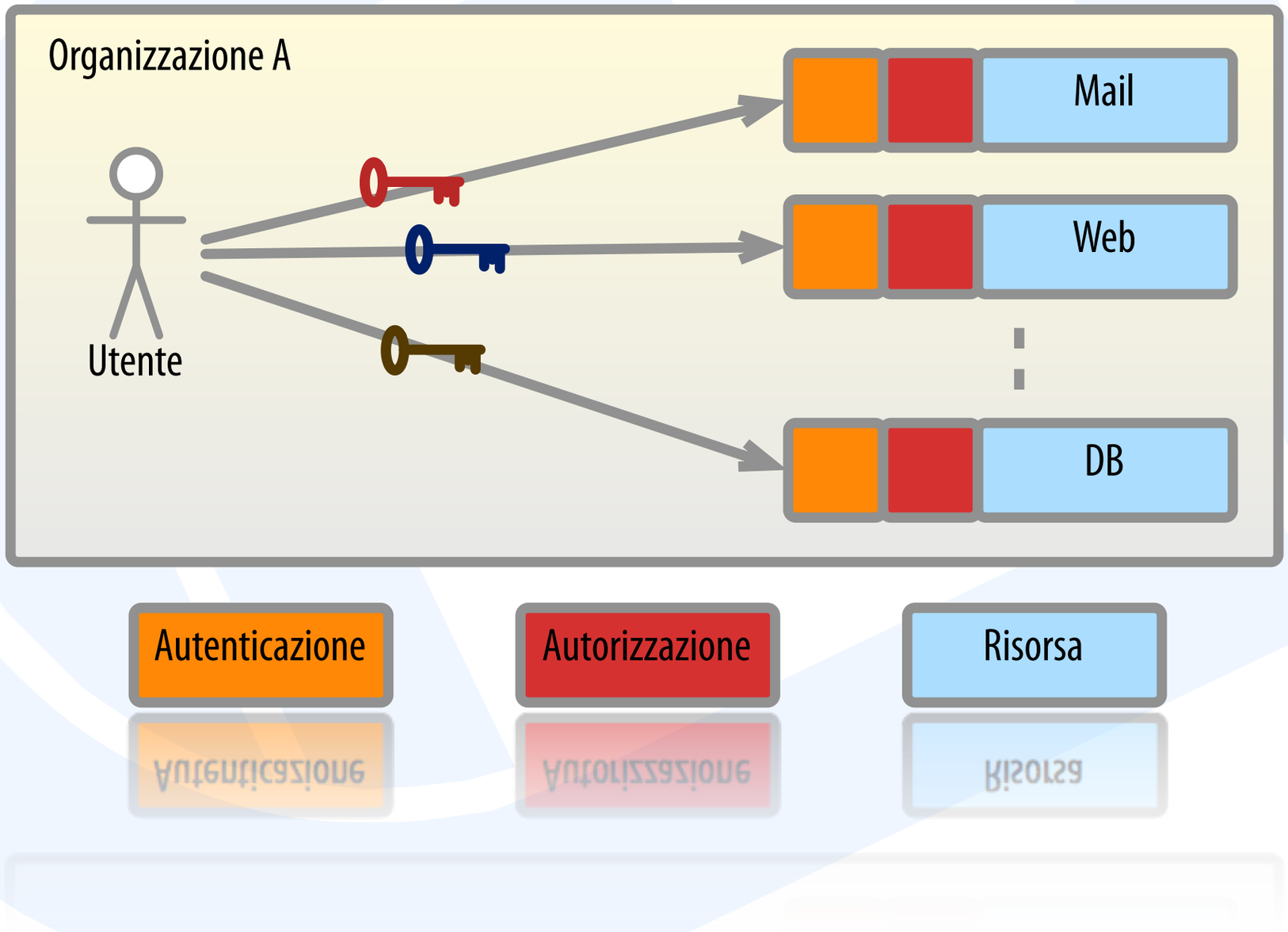
- Autenticazione: l'utente è effettivamente chi dichiara di essere?
- Autorizzazione: se sì, a quali dati e con quali modalità può accedere?

AA... I

- Un'infrastruttura di Autenticazione e Autorizzazione:
  - riduce il numero di credenziali lato utente
  - è propedeutica per Single Sign-On
  - elimina le incoerenze relative ai dati dell'utente
  - consente l'autorizzazione basata su attributi/ruoli (ABAC/RBAC)

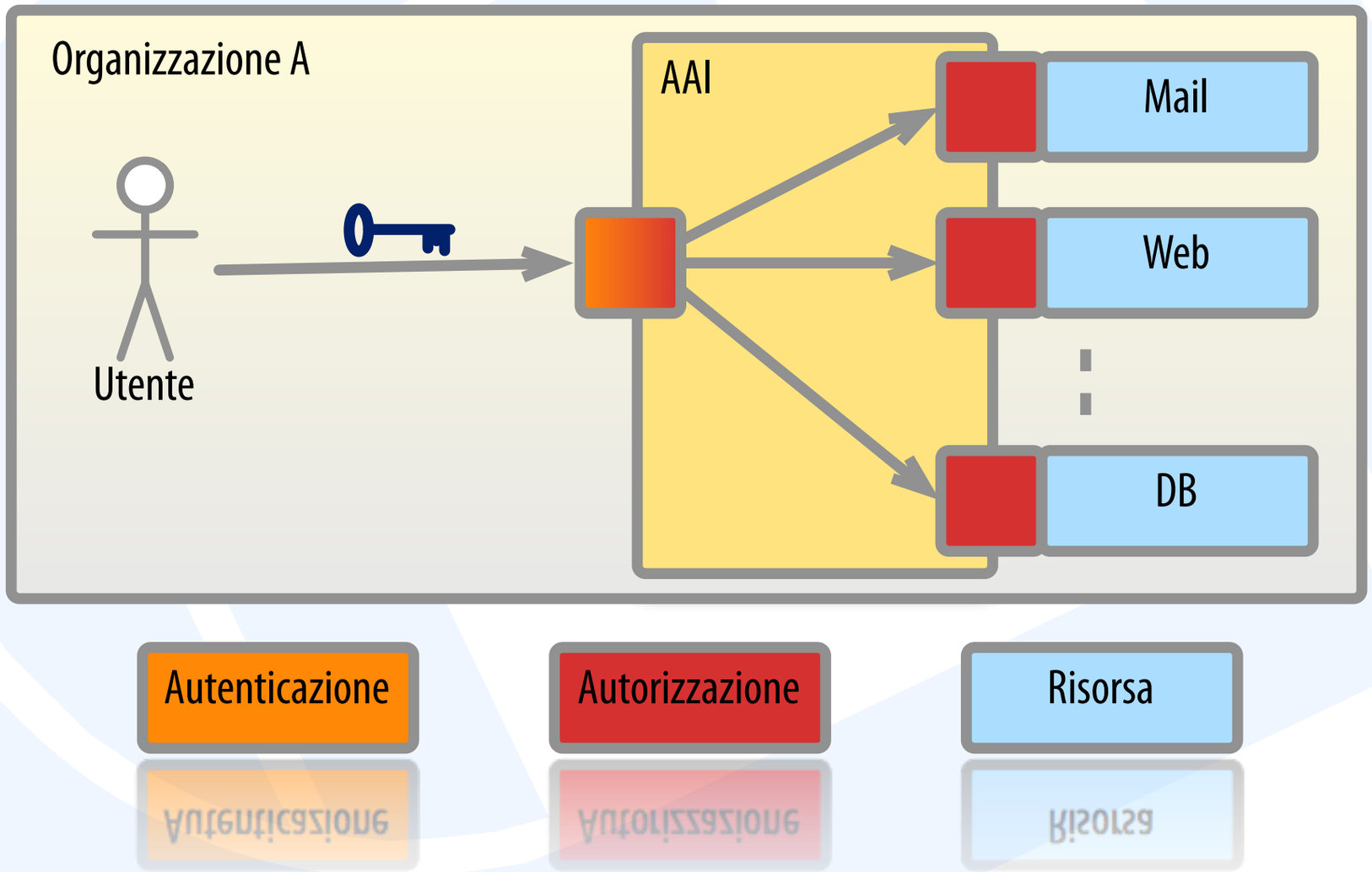
AAI

senza *Infrastruttura di AA*



AAI

con *Infrastruttura di AA*



LDAP: cosa...

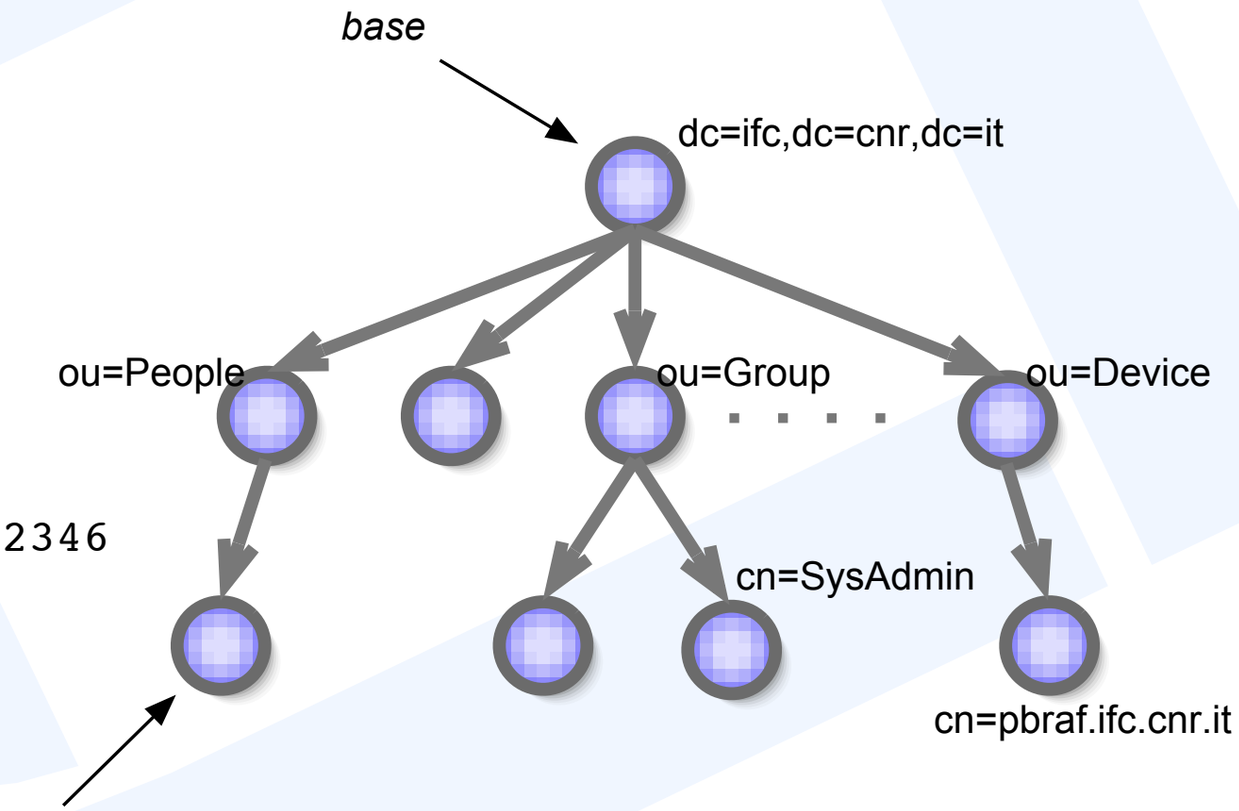
- Il Lightweight Directory Access Protocol deriva (come semplificazione) dall' X.500 OSI Directory Access Protocol
- Non è un DataBase ma utilizza un DataBase per organizzare e rappresentare dati:
  - tramite oggetti (entry) con attributi;
  - gerarchicamente ed in maniera da favorire le ricerche piuttosto 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 (l'organizzazione dei dati)
- Cross-platform
- Ampiamente supportato
- Ottimizzato per le operazioni di ricerca e lettura
- Meccanismi di replica built-in
- Sofisticati meccanismi controllo accessi (ACL)

Gestione del profilo utente

- Il profilo può essere 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
  - può creare il profilo solo dopo aver ottenuto dall'utente l'"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>

È l’ufficio del personale che, inserendo correttamente il profilo dell’utente, autorizza implicitamente l’accesso ad un servizio (sulla base delle policy definite dal ServiceProvider)

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. il responsabile di un particolare servizio

Estensioni

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

Pro...

- 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

...e contro?

- necessaria cifratura delle comunicazioni o strong authentication (kerberos, certificati ecc.)
- 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

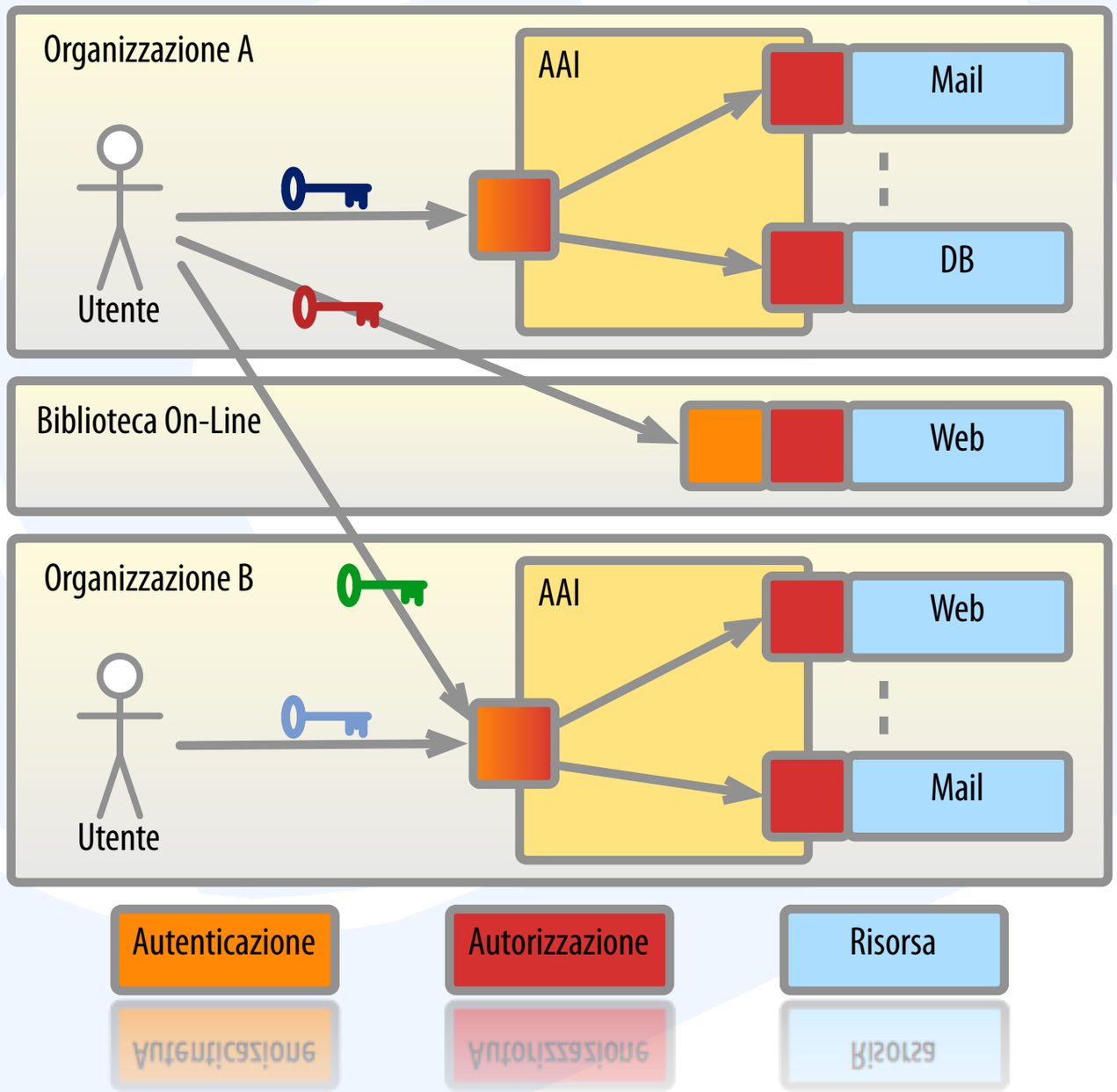
- per l'utente:
  - nessun controllo sulle regole di riservatezza relative alle informazioni fornite
  - uso di password diverse per servizi diversi (per evitare l'uso inappropriato delle stesse su altri servizi)
- per il fornitore del servizio
  - scarse informazioni sull'utente
  - possibilità di variazione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

AAI federata

- Una **federazione** è un insieme di organizzazioni d'accordo su regole comuni
- Autenticazione locale, presso l'organizzazione di appartenenza
- Accesso a servizi remoti (di altre organizzazioni) senza ulteriori autenticazioni

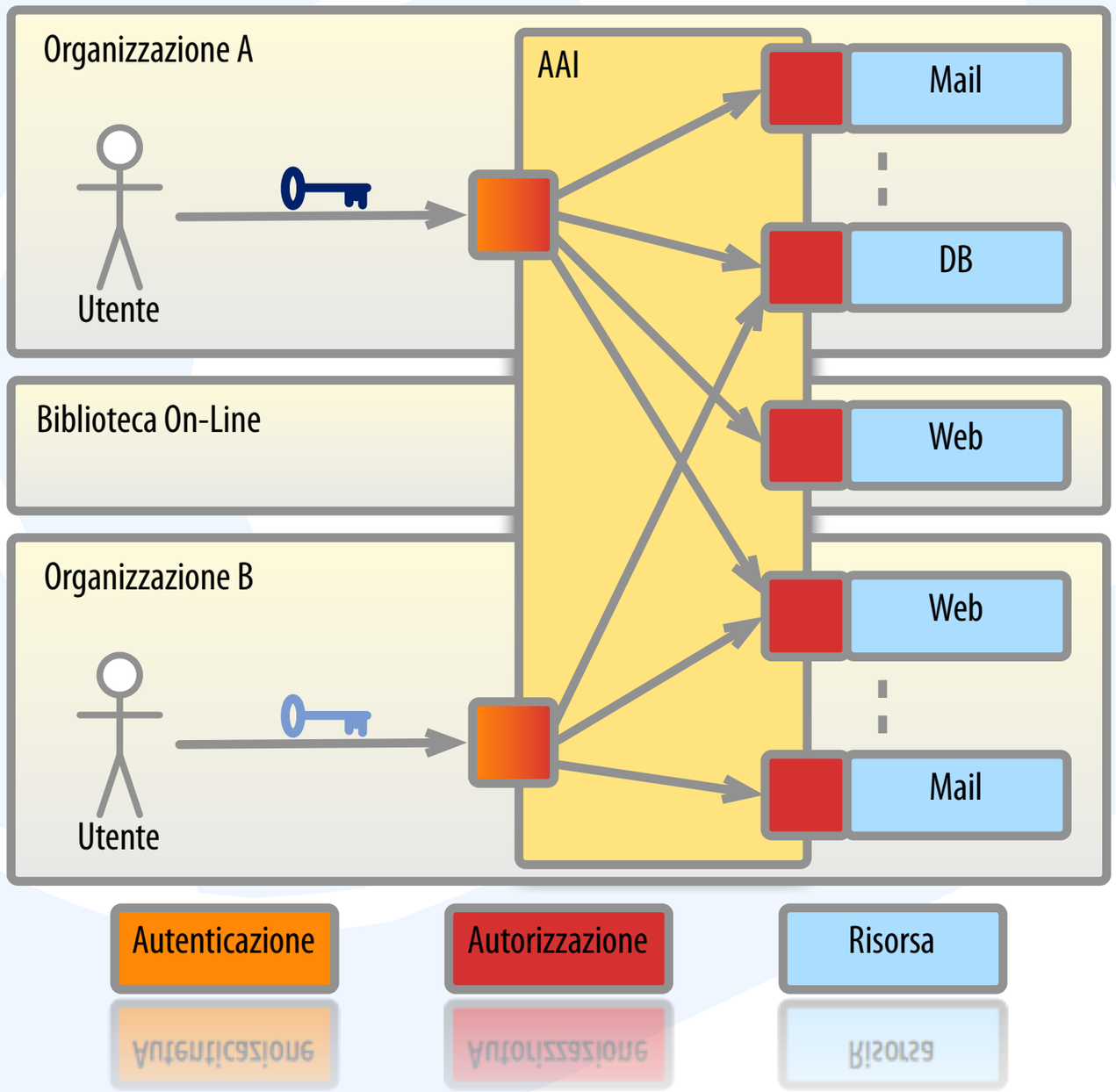
AAI federata

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

** Organization for Advancement of Structured Information Sciences*

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

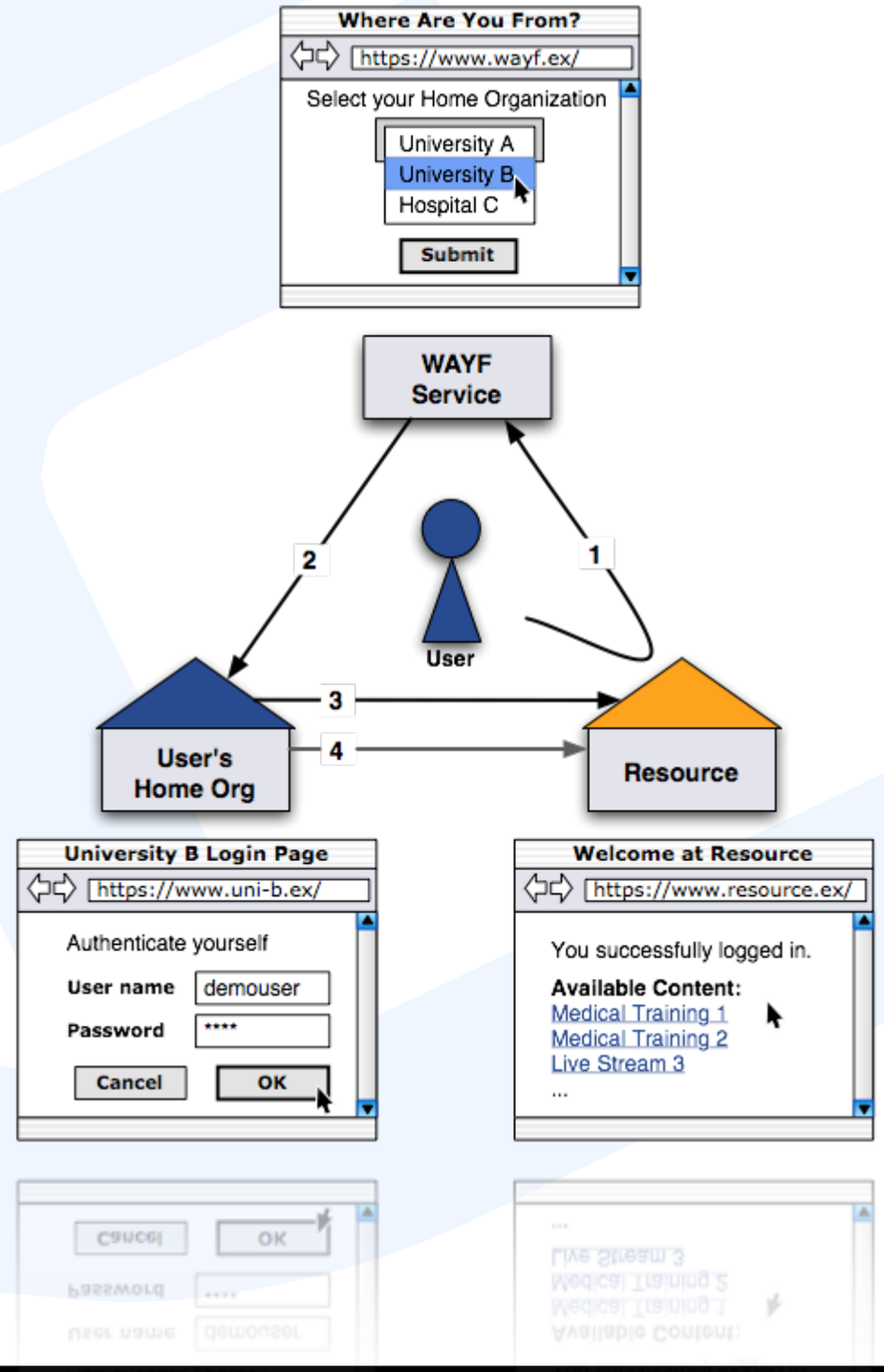
- Implementazione di SAML
- Progetto ufficiale di Internet2
- Rilasciato con Apache Software License

Shibboleth

Shibboleth.

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

AA con Shibboleth



Vantaggi AAI federata

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

Vantaggi AAI federata

- Per l'organizzazione:
  - controllo sul processo di autenticazione e autorizzazione
  - autorizzazione concessa in base al ruolo (RBAC)
  - risparmio sui costi (sottoscrizione riviste elettroniche, implem. nuovi servizi

Vantaggi AAI federata

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

Come sperimentare un'AAI federata?

Come sperimentare un'AAI federata?

- Aderendo ad IDEM
- progetto pilota patrocinato dal GARR
- durata: tutto il 2008

IDEM: servizi iniziali

- NILDE
- Science Direct (*Elsevier*)
- Servizio di videoconferenza GARR
- Altri eventuali (*Thomson Corp., Cambridge Scientific Abstract* ecc.)

IDEM: il supporto
(tramite GARR)

- Infrastruttura IT centrale
  - WAYF server
  - mappa federazione (metadati)
  - Certification Authority
- Service Provider di Test
- Supporto tecnico per gli IdP e gli SP
- IdP per eventuali “homeless”

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 (con rilascio attributi in base alle specifiche stabilite)
  - 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

- Tutti coloro che hanno contribuito a definire il Progetto IDEM
- Il comitato di gestione del Progetto
- per l'invito:
  - Silvana Mangiaracina
  - Roberto Cecchini, *responsabile del progetto*

Grazie!