La gestione della Privacy nell'accesso ai dati clinici tramite LDAP

Raffaele.Conte@ifc.cnr.it

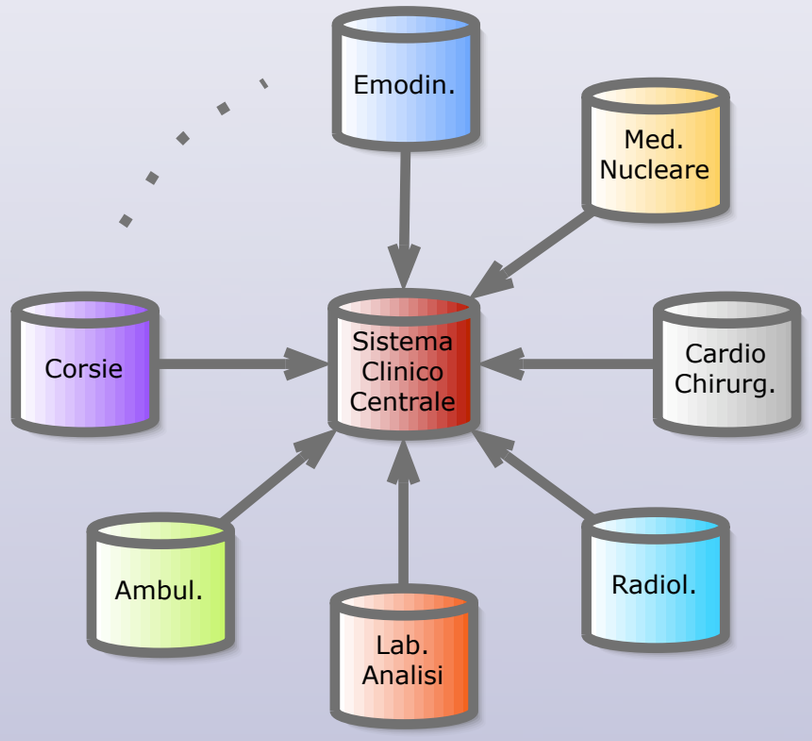
12 Maggio 2005

Istituto di Fisiologia Clinica

Il contesto: l'Istituto di Fisiologia Clinica 1/2

Sede e sezioni IFC

Organizzazione logica sistema clinico

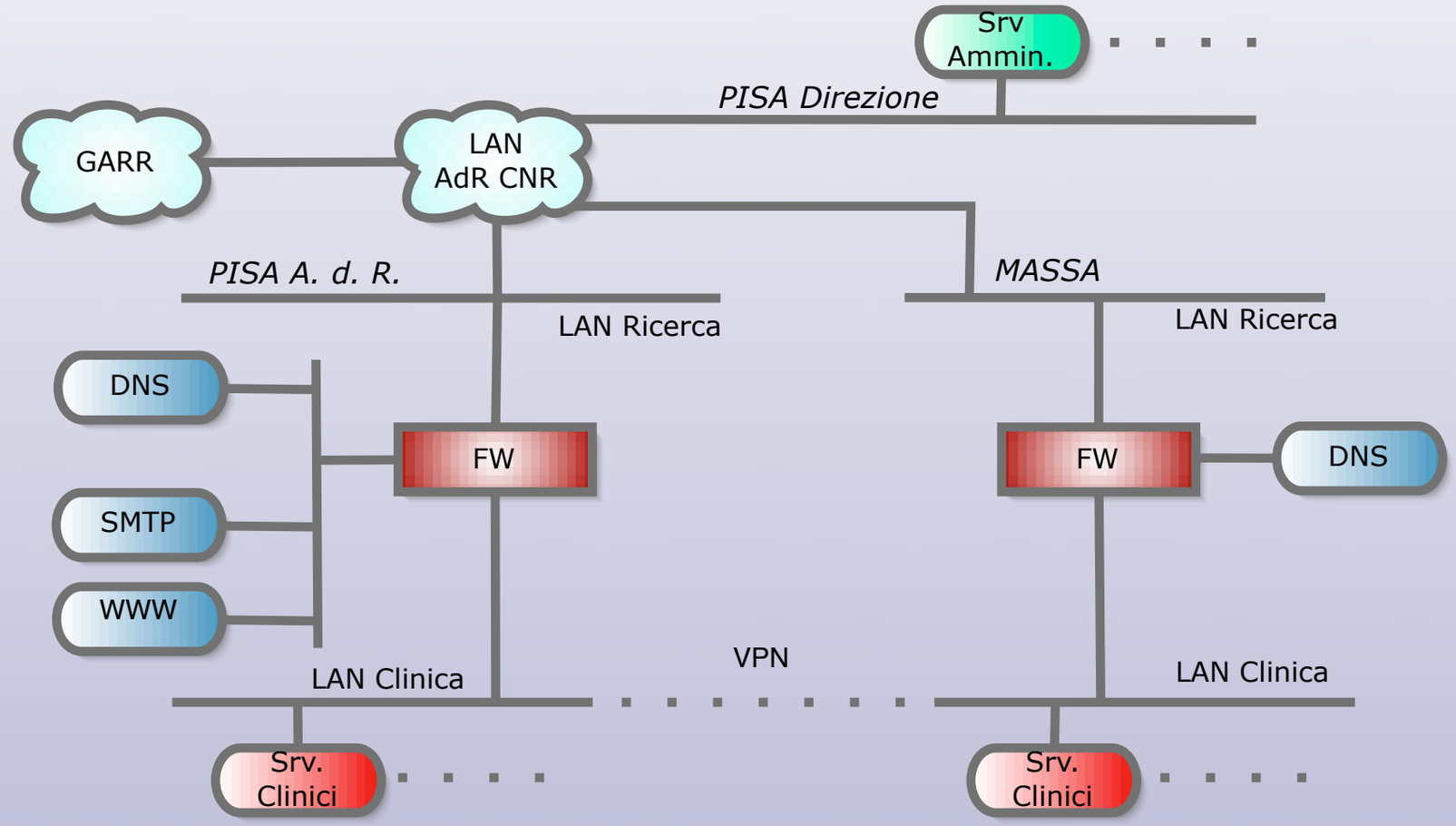


- Esistono diversi *trattamenti* dei dati ognuno con un proprio *Responsabile* che assegna gli *incarichi*

Il contesto: l'Istituto di Fisiologia Clinica 2/2

Scelte implementative: molti server per i diversi servizi...

...ma per gli stessi utenti!



Le informazioni sugli utenti verrebbero inserite più volte con conseguente rischio di inconsistenza!

Problematiche nell'accesso ai dati sensibili

- *Assunzione di responsabilità*
- *Debolezza credenziali di accesso*
- *Password di reparto!!!*
- *Gestione assegnazioni "incarico al trattamento dati"*
- *Accesso differenziato per tipologia di utenza (infermiere, medico, amministrativo, ecc.)*
- *Estrema volatilità del personale (laureandi, dottorandi, specializzandi, infermieri, ospiti ecc.)*

Gli obblighi di legge 1/2

- **“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;
 ...

Gli obblighi di legge 2/2

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.
[...]

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.

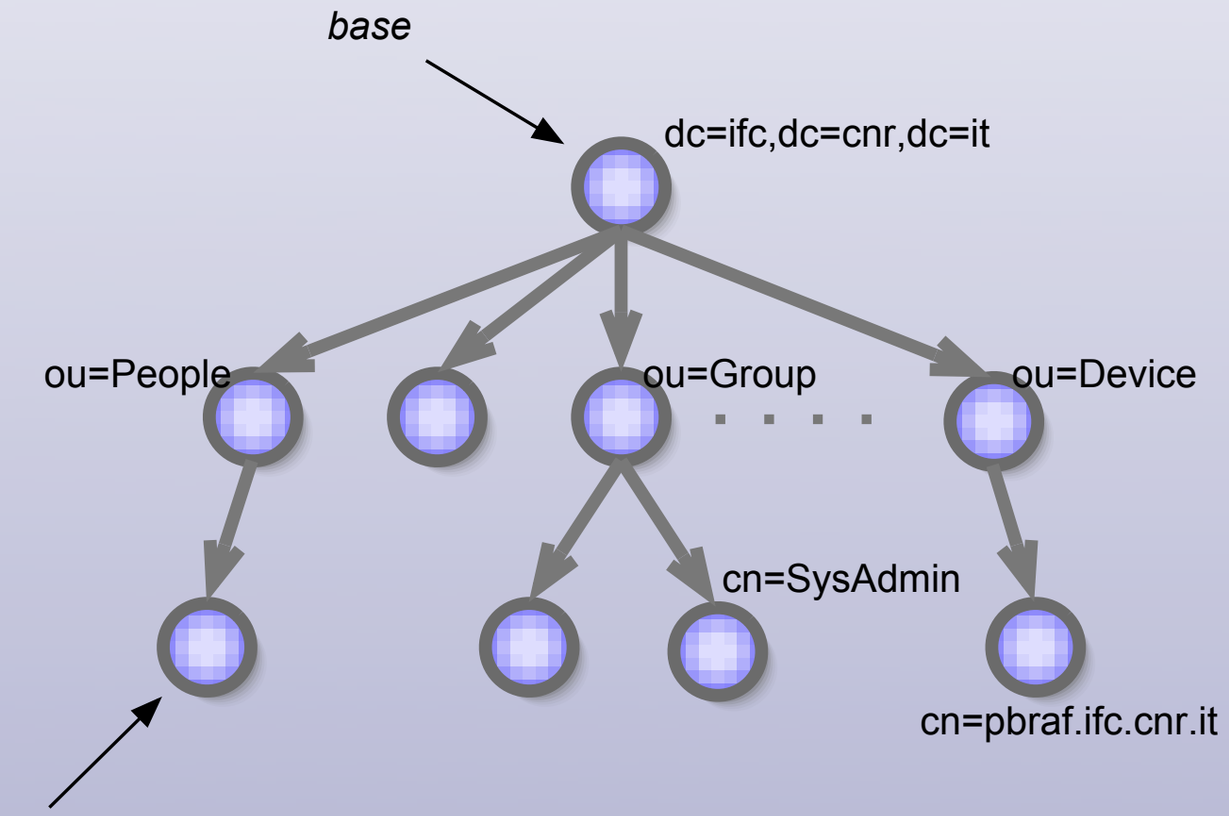
Cenni su LDAP 1/2

- *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)

Cenni su LDAP 2/2

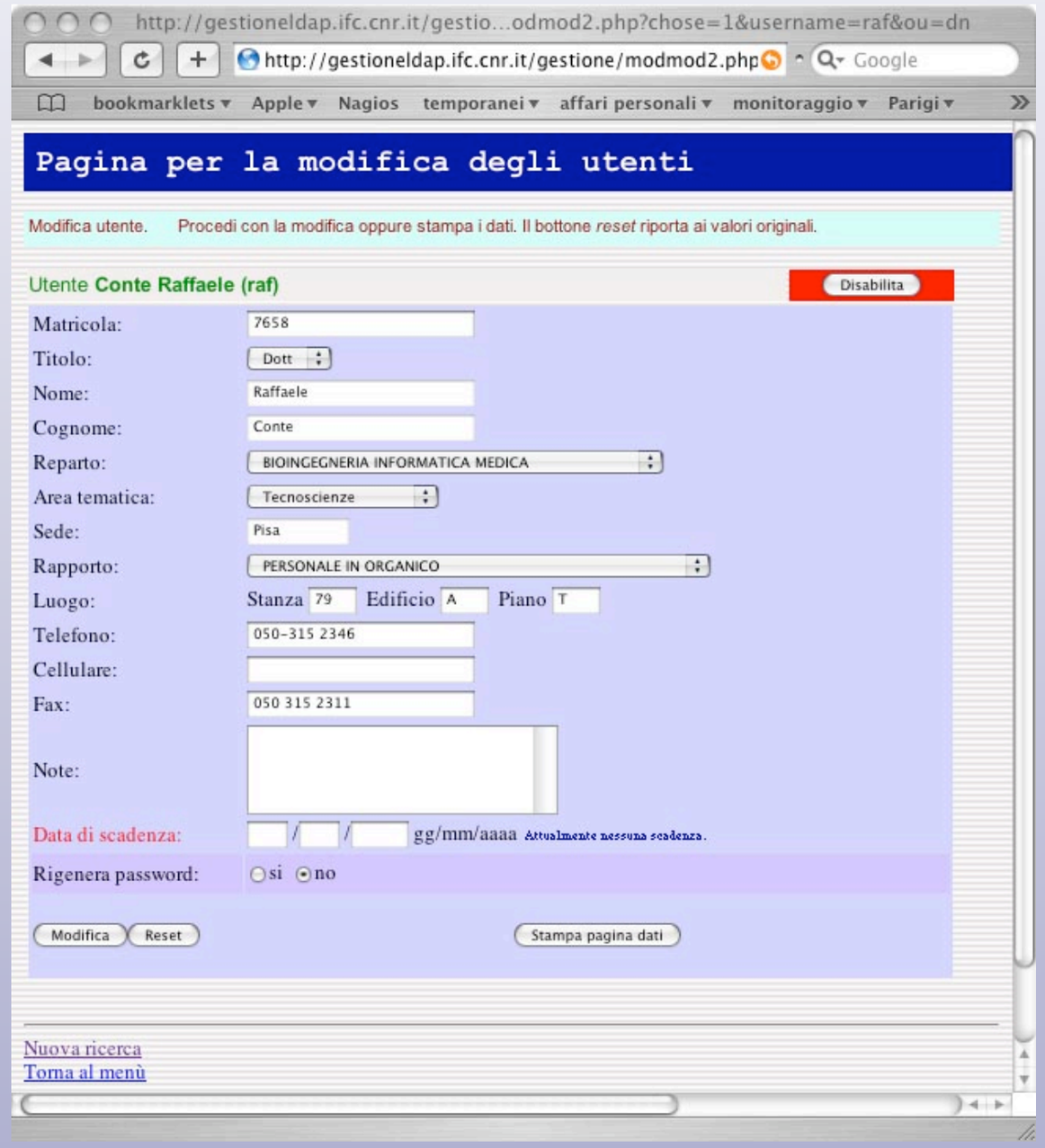
Gli oggetti sono organizzati in maniera simile ad un File System o al DNS con possibiltà di "riferimenti"



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:: e1NIQX12ZzI...
shadowLastChange: 12136
departmentNumber: ELDA
mail: raf@ifc.cnr.it
uidNumber: 501
telephoneNumber: 050-315 2346
loginShell: /bin/bash
gidNumber: 100
employeeNumber: 7658
gecos: Raffaele Conte, ELDA
roomNumber: 79&A&T
l: Pisa
homeDirectory: /home/raf
shadowWarning: 7

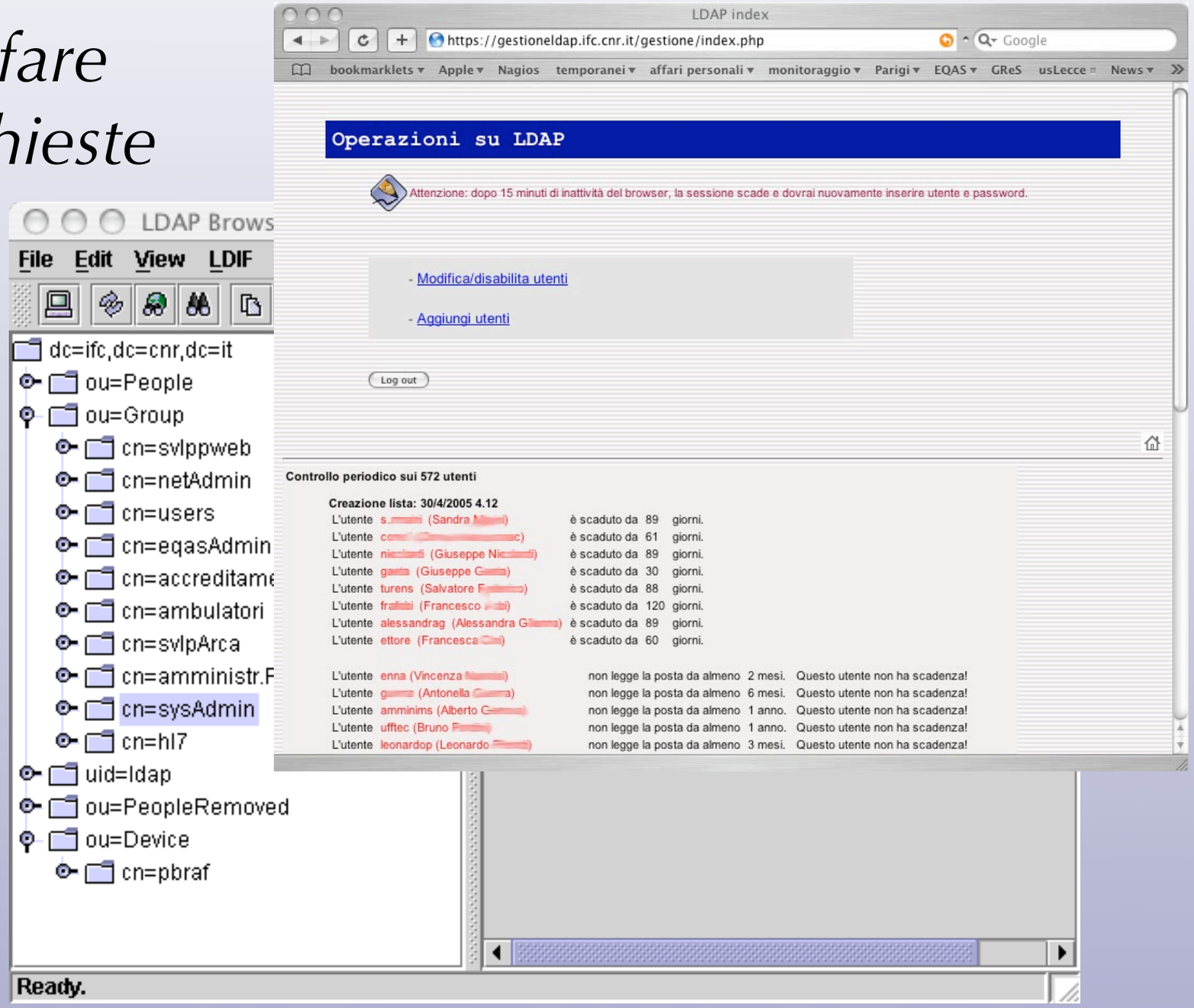
Centralizzazione del profilo utente 1/2

- *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*



Centralizzazione del profilo utente 2/2

- *È possibile soddisfare 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:

- ldapsearch -s one -LLL -x -b "ou=People,dc=ifc,dc=cnr,dc=it" "(&(uid=raf)(ou=ELDA))"

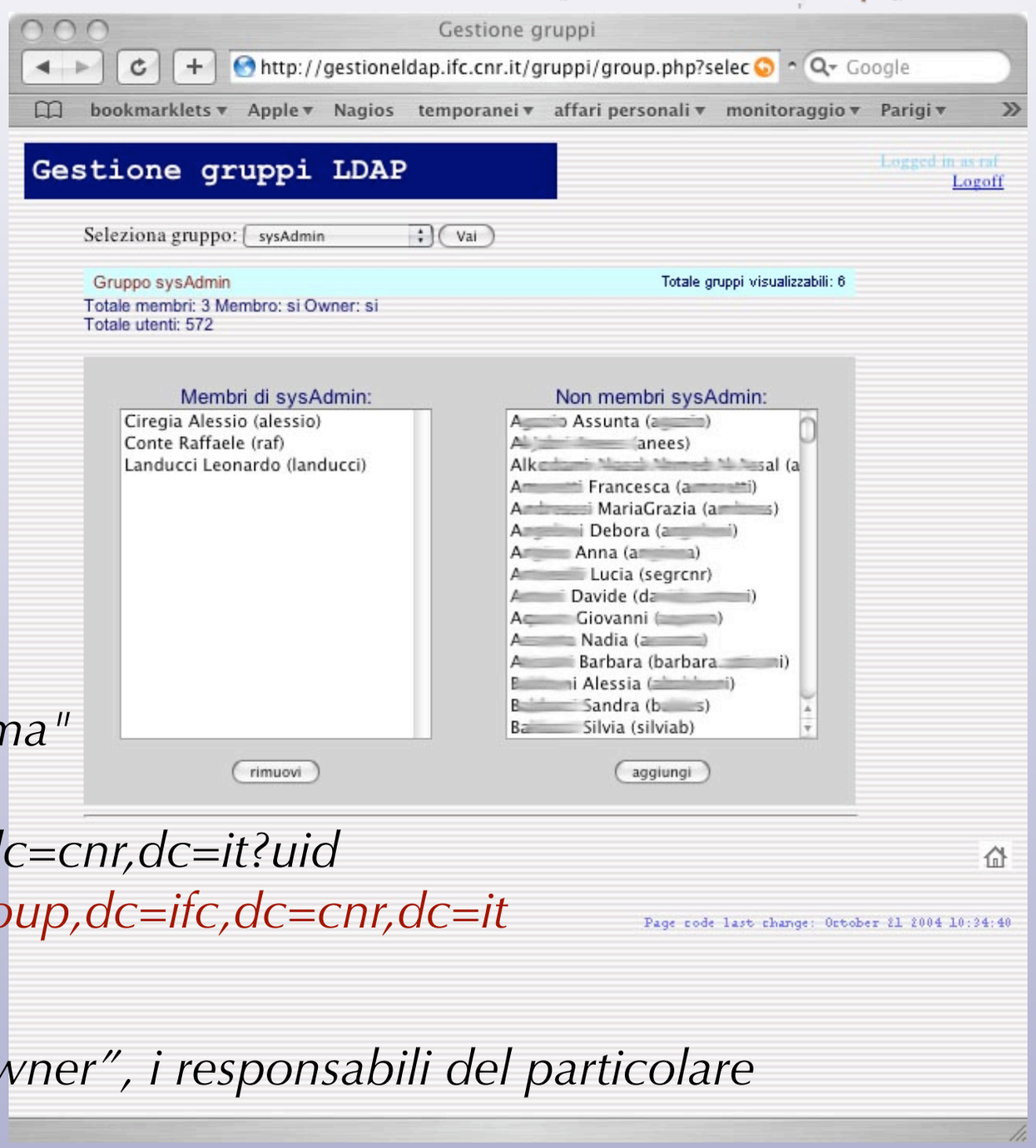
- *esempio in mod_auth_ldap (per Apache):*

```
<Directory /usr/share/doc>
    AllowOverride None
    Options Indexes FollowSymLinks
      Order allow,deny
      Allow from ifc.cnr.it
      AuthName "Documentazione sistema"
      AuthType basic
      AuthLDAPURL ldaps://ldap/ou=People,dc=ifc,dc=cnr,dc=it?uid?sub?(ou=ELDA)
      require valid-user
</Directory>
```

Autorizzazione *"esplicita"*

- Gruppi:
- *esempio (mod_authl_dap):*

```
<Directory /usr/share/doc>
    AllowOverride None
    Options Indexes FollowSymLinks
      Order allow,deny
      Allow from ifc.cnr.it
      AuthName "Documentazione sistema"
      AuthType basic
      AuthLDAPURL ldap://ldap/dc=ifc,dc=cnr,dc=it?uid
      require group cn=sysAdmin,ou=Group,dc=ifc,dc=cnr,dc=it
</Directory>
```



- *I gruppi vengono gestiti dagli utenti "owner", i responsabili del particolare "trattamento dati"*

Conclusioni

- *vantaggi*
  - *creazione e modifica dei profili utente gestita da chi possiede le informazioni sugli utenti (Ufficio del Personale) senza intermediari*
  - *immediata propagazione della "revoca di tutti diritti" (disabilit. utente)*
  - *gestione delle autorizzazioni effettuata dal responsabile del servizio o del particolare trattamento dati*
  - *il personale tecnico cura gli aspetti tecnologici piuttosto che amministrativi*
  - *le informazioni sugli utenti sono centralizzate ma automaticamente replicate*
- *svantaggi*
  - *tutti i servizi che richiedono autenticazione ed usano LDAP devono essere kerberizzati o offerti tramite SSL (TLS)*
  - *carpita la password di un utente si può accedere a tutti servizi per i quali è autorizzato (discutibile!!!)*

Estensioni dell'uso di LDAP

- *Ulteriori utilizzi*
  - *autorizzazioni per ruolo/orario*
  - *indirizzario utenti*
  - *DNS e conseguente autorizzazione utenti/macchine centralizzata su LDAP*
  - *autenticazione in rete 802.1X (gw radius-ldap)*
  - *Single Sign-On in associazione con Kerberos*
  - ...

Riferimenti

- RFC 2251, RFC 3377
- Carter G, *"LDAP System Administration"* , O'Reilly, 2003;
- Tuttle S, A Ehlenberger, R Gorthi, et al. *"Understanding LDAP - Design and Implementation"*, IBM RedBooks, 2004;
- http://www.openldap.org;
- Pinheiro Malère LE, *"LDAP Linux HOWTO", http://en.tldp.org/HOWTO/LDAP-HOWTO*;
- Williams AT, *“LDAP and OpenLDAP (on Linux Platform)”, ftp://kalamazoolinux.org/pub/pdf/ldapv3.pdf*
- Paternò G, *“Single Sign-On con Kerberos e LDAP”, http://gpaterno.free.fr/publications/SingleSignon/index.html*