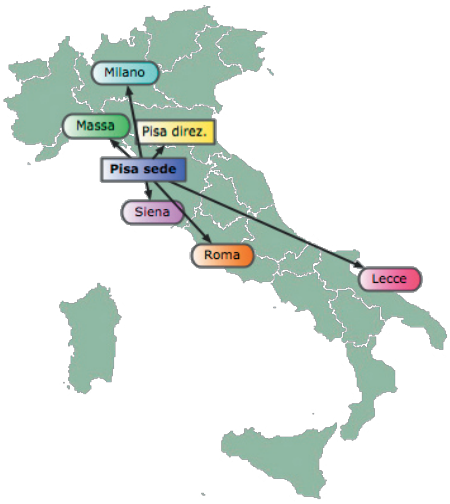
La gestione della privacy nell'accesso ai dati clinici tramite LDAP

R. Conte*, A. Ciregia*, L. Landucci**, D. Pierotti**
* Istituto di Fisiologia Clinica, Consiglio Nazionale delle Ricerche (IFC-CNR), Pisa
** Dipartimento di Medicina Interna - Università degli Studi di Pisa
raffaele.conte@ifc.cnr.it

Parole chiave: LDAP, autenticazione, autorizzazione, accesso ai dati, dati sensibili

Nell'Istituto di Fisiologia Clinica del CNR all'attività di ricerca è affiancata un'intensa attività assistenziale erogata tramite ricovero o prestazioni ambulatoriali. Negli ultimi anni il sistema informativo dell'Istituto è cresciuto rapidamente fino a coprire in maniera capillare l'intera struttura distribuita sulle diverse sedi del territorio nazionale. Allo stato attuale il sistema informatico d'Istituto fornisce servizi a quasi 600 utenti nelle proprie sedi di Pisa (presso l'area della Ricerca e gli uffici amministrativi distaccati), Massa (presso l'Ospedale Pasquinucci), Lecce, Milano, Siena e Roma. I servizi sono molteplici, da quelli ad uso generale come la posta elettronica, i siti WWW Internet ed Intranet ecc., a quelli più specifici per la gestione del Sistema Clinico Centrale (il cuore della Cartella Clinica Informatizzata) e dei sistemi "periferici" per la gestione autonoma delle diverse unità operative (Emodinamica, EcoCardiografia, Medicina Nucleare, Laboratori di Analisi ecc.). Il sistema informativo è quindi cresciuto nel tempo integrando i sottosistemi nati e sviluppati all'interno dei diversi reparti, ognuno con le proprie caratteristiche e peculiarità. I problemi relativi alla sicurezza dei dati si sono conseguentemente moltiplicati e sono stati affrontati mediante l'utilizzo di diverse tecnologie e da vari punti di vista (dall'uso delle VLAN o di sottoreti fisicamente separate tramite firewall, all'uso di crittografia per le comunicazioni ecc.). La robustezza del sistema però viene vanificata se le credenziali di accesso ai dati sono deboli o se una revoca dei diritti di accesso ai dati (ad esempio per un utente che chiude il proprio rapporto con l'Istituto) non si riflette sui meccanismi di autenticazione e autorizzazione implementati per lo specifico servizio. Nella realtà descritta ogni sistema ha inizialmente previsto meccanismi di autenticazione propri, di conseguenza gli utenti si sono ritrovati a dover utilizzare diverse credenziali d'accesso, per ognuno dei sistemi e/o servizi utilizzati. A questo si è aggiunta la necessità di dover garantire l'accesso ai dati sensibili ai soli utenti che ne avevano diritto e con le modalità loro consentite, in funzione della specifica figura professionale. Questo non solo per una questione di etica ma anche perché è richiesto dalla normativa vigente. L'articolo 3 del "Codice in materia di protezione dei dati personali" (Decreto Legislativo del 30/6/2003 n.196) definisce il "principio di necessità nel trattamento dei dati", obbligando gli amministratori di sistemi informatici a configurare gli stessi in modo da ridurre al minimo l'utilizzazione dei dati personali e con modalità che consentano di identificare l'interessato (al trattamento) solo



Sede e sezioni dell'IFC-CNR

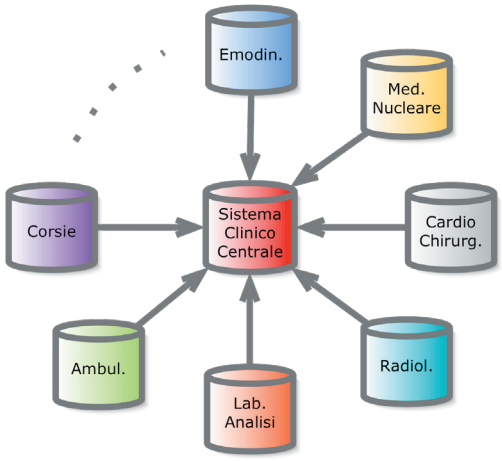


Fig. 2 Organizzazione logica del sistema clinico

in caso di necessità. L'articolo 34 dello stesso codice prevede, tra l'altro, esplicitamente l'uso di:

a) autenticazione informatica;

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

c) utilizzazione di un sistema di autorizzazione;

per l'accesso ai dati personali e/o sensibili.

Infine con l'allegato B della stessa legge vengono indicate quelle che sono le misure minime da implementare nei sistemi di autenticazione ed in quelli di autorizzazione.

Tutte le misure necessarie dovrebbero quindi essere implementate per ognuno dei sistemi di autenticazione con conseguente replicazione delle stesse azioni più volte.

A questo si aggiunge un altro problema: le informazioni relative agli utenti (nome, cognome, posizione, reparto di appartenenza ecc.) sono note all'"Ufficio del Personale", raramente agli amministratori di sistema. E questo deriva anche dall'alta volatilità del personale operante all'interno delle strutture. Infatti, oltre al personale dipendente (CNR, Università e Azienda Ospedaliera), all'interno della struttura operano diverse figure, presenti solo per periodi di tempo più o meno brevi, quali infermieri, tirocinanti, specializzandi, dottorandi, volontari ecc.

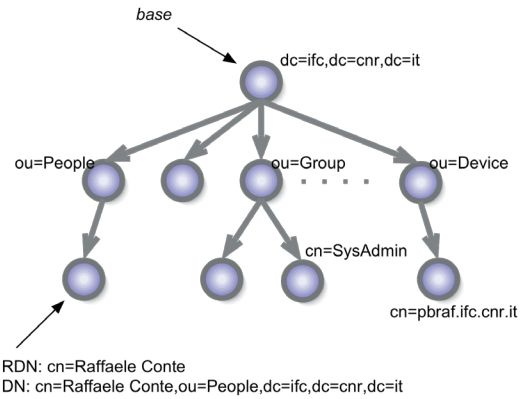


Fig. 3 Organizzazione gerarchica degli oggettti in LDAP

Le problematiche descritte sono state affrontate e risolte tramite l'utilizzo del protocollo LDAP (Lightweight Directory Access Protocol). LDAP è un protocollo di comunicazione per l'accesso ad un Directory Server, creato come semplificazione dell'OSI X.500. LDAP non è un DataBase ma utilizza un DataBase per rappresentare dati tramite oggetti con attributi, organizzati in una struttura gerarchica e con lo scopo di favorire le ricerche piuttosto che gli aggiornamenti. Oggetti e attributi vengono definiti formalmente tramite gli *Schema*. Il protocollo, nella versione 3, è descritto dettagliatamente nell'RFC 2251. Documenti successivi trattano altri aspetti legati al protocollo e vengono esplicitamente indicati nell'RFC 3377.

Nel protocollo LDAP l'organizzazione dei dati riflette quella di file e directory in un FileSystem o di hostname e domini sul Domain Name Service. Anche in questo caso è infatti possibile definire dei riferimenti a "collezioni di oggetti" esterne.

In Istituto è stato creato un sistema, composto da un server *master* e due server *slave*, accessibile mediante protocollo http con pagine costruite *ad hoc*, mediante le quali è possibile gestire i profili di accesso ed i parametri per l'autenticazione degli utenti. È importante notare che il sistema gestisce le credenziali di autenticazione ed i soli profili degli utenti, mentre non tratta le autorizzazioni di accesso ai servizi, che vengono gestite localmente al servizio stesso. Anche in questa fase però LDAP offre un contributo notevole perché la decisione sulla

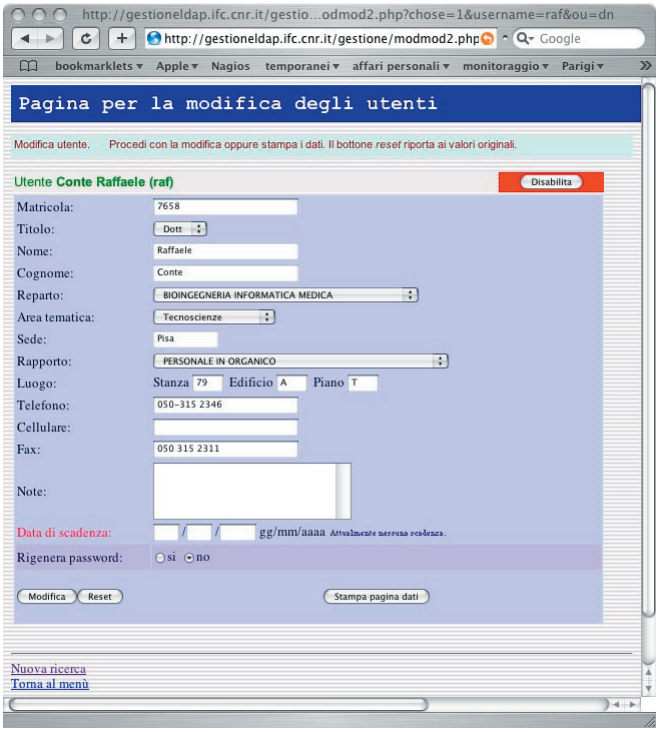


Fig. 4 Pannello per la creazione del profilo utente

concessione o meno dell'autorizzazione per l'accesso al servizio, deriva anche da parametri ricavati dal profilo dell'utente memorizzato sul server LDAP o dall'appartenenza o meno ad un gruppo predefinito.

La procedura per la concessione dei diritti di accesso ai servizi, allo stato attuale, si compone di due fasi. Nella prima si costruisce il profilo dell'utente: l'utente presenta presso l'ufficio del personale, unitamente alla documentazione che formalizza il suo rapporto con l'Istituto (sia esso temporaneo o a tempo indeterminato), una richiesta di accesso ai servizi informatici ed un modulo di assunzione di responsabilità (in alternativa sottoscrive una rinuncia esplicita all'accesso al sistema informatico d'Istituto).

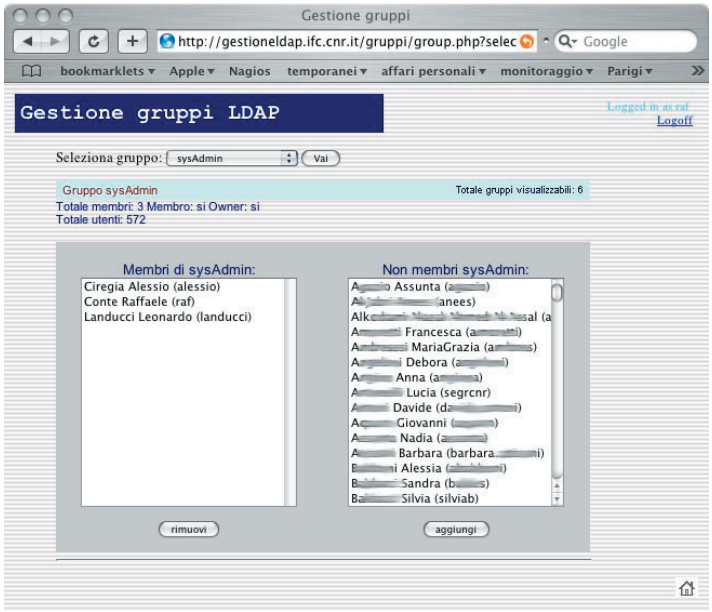


Fig. 5 Pannello per la gestione dei gruppi

Successivamente, il personale dell'ufficio, inserisce nel server LDAP i dati dell'utente, fra cui il tipo di rapporto con l'Istituto, la figura professionale ed il reparto di appartenenza, consegnando all'utente stesso un modulo con la propria password ed i parametri per la configurazione del servizio di posta elettronica. L'utente viene inoltre iscritto automaticamente ad una mailing list d'Istituto utilizzata per eventuali comunicazioni.

La seconda fase, l'autorizzazione all'accesso ai servizi, viene gestita dagli stessi responsabili dei servizi. L'autorizzazione può essere concessa in maniera implicita (automatica) o in maniera esplicita. La prima modalità può essere utilizzata, ad esempio, per consentire l'accesso in sola lettura a tutti i membri di un reparto. Per fare ciò è sufficiente configurare il servizio in modo che interroghi il server LDAP, allo scopo di recuperare il profilo dell'utente e consentire l'autenticazione, solo sulla base di particolari parametri (nell'esempio, il reparto di appartenenza) utilizzando il meccanismo dei filtri sulle interrogazioni.

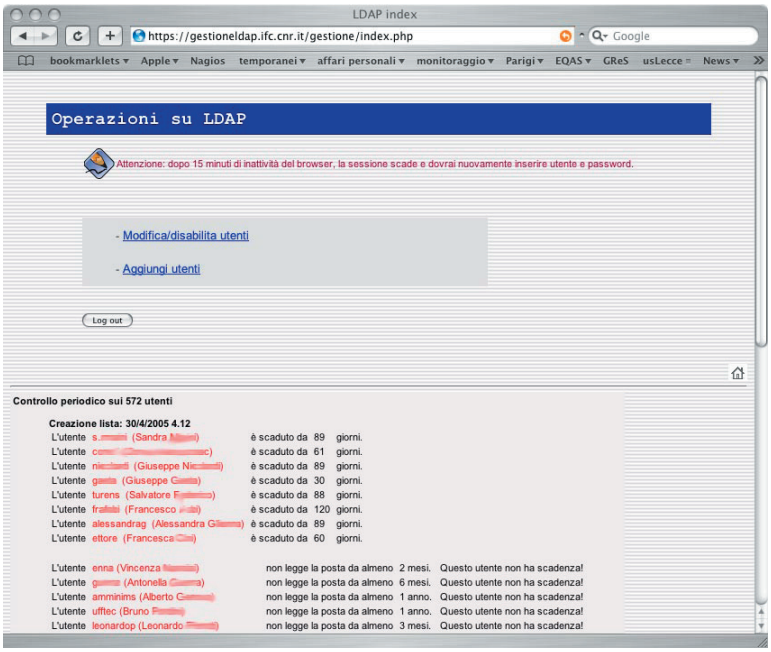


Fig. 6 Evidenza degli account scaduti o non più utilizzati

Nel caso in cui si voglia concedere l'autorizzazione in maniera esplicita ci si avvale dell'uso dei gruppi. In questo caso il servizio interroga il server LDAP per verificare l'appartenenza dell'utente allo specifico gruppo e consentirne l'autenticazione. Il protocollo prevede fra i vari schema, diversi tipi di gruppo. Allo stato attuale sono stati utilizzati i *groupOfNames*, poiché questi prevedono l'attributo *owner* (il proprietario del gruppo), estesi con attributi dei *posixGroup* necessari ai FileSystem dei sistemi UNIX. È possibile quindi creare appositamente un gruppo per l'autorizzazione ad uno specifico servizio definendo come owner il responsabile del servizio stesso. Questi ha la possibilità di includere o escludere utenti già presenti nel server, precedentemente inseriti dall'ufficio personale. In questo modo i diritti di accesso

al servizio possono essere concessi o revocati dagli stessi responsabili del servizio o del trattamento dati (quindi anche da personale non tecnico).
Le interrogazioni effettuate sul server LDAP possono tener conto anche di una eventuale data di scadenza, per quegli utenti che hanno un rapporto a tempo determinato con l'Istituto; così facendo la revoca dei diritti avviene automaticamente alla scadenza del contratto di lavoro.
Nel momento in cui un utente con contratto a tempo determinato dovesse rinnovare il proprio rapporto di lavoro con l'Istituto, sarà ancora una volta l'ufficio del personale a rinnovare conseguentemente l'account. Al contrario, nel caso di interruzione del rapporto prima della scadenza naturale, l'ufficio disabiliterà l'utente sul server, revocandogli così i diritti di accesso a tutti i servizi. È importante sottolineare che gli utenti creati sul sistema non vengono mai eliminati ma soltanto disabilitati (con conseguente revoca di tutti i diritti), questo perché il D.L. 196/03 richiede esplicitamente che *"il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi" (art.6, all.B)*. Per tenere traccia quindi degli identificativi utente creati sul sistema è stato definito un sottoalbero (ou = PeopleDisabled) nel quale vengono "trasferiti" i profili degli utenti disabilitati. L'accesso a questo sottoalbero è impedito a tutti (amministratori esclusi), in modo da negare sicuramente un'eventuale richiesta di autenticazione. È possibile utilizzare un attributo per indicare la scadenza dell'account, ma si deve evidenziare che resta a carico dell'amministratore del sistema (che utilizza LDAP) considerare il valore di questo attributo in fase di autenticazione.
Ancora, la normativa richiede che *"le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, [...]" (art.7, all.B)* e *"la parola chiave [...] è modificata [...] 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" (art.5 all.B)*. Per soddisfare tale richiesta sono stati utilizzati gli attributi dell'oggetto *shadowAccount* (in particolare *shadowExpire* e *shadowAccount*), conforme allo standard *Posix*. Gli attributi deve essere quindi considerati in funzione dei dati trattati sull'archivio che necessita di autenticazione (il periodo di scadenza potrebbe essere diverso). Tramite l'ausilio di script specifici è possibile disabilitare l'accesso al servizio obbligando l'utente a modificare la propria password.
Grazie all'estrema flessibilità dell'Access Control List di OpenLDAP (utilizzato per implementare il sistema), l'accesso ai dati è consentito anche ai singoli utenti che possono accedere in sola lettura ad un sottoinsieme di questi ed anche in scrittura ad una parte dei propri dati (password, numero telefonico, localizzazione del proprio studio). I dati pubblicamente accessibili possono essere consultati sia tramite pagine, sul sito Internet d'Istituto, create appositamente, che tramite altre applicazioni installate sui PC degli utenti (programmi per la gestione degli indirizzi, per la posta elettronica ecc.).
Oltre ai vantaggi precedentemente descritti il sistema si presta ad essere utilizzato in qualsiasi altro contesto che richieda autenticazione, ad esempio per l'accesso ad una rete (tramite protocollo 802.1X) su cui sono trattati dati sensibili o al contrario per accedere ad Internet da una rete chiusa (tramite un ProxyWeb). Il sistema potrà inoltre essere esteso in modo da gestire diversi e più robusti meccanismi di autenticazione, quali ad esempio Kerberos o meccanismi che fanno uso di chiavi pubbliche.

Bibliografia

- Carter G, "LDAP System Administration" , O'Reilly, 2003;
- Tuttle S, Ehlenberger A, Gorthi R, et al. "Understanding LDAP - Design and Implementation", IBM RedBooks, 2004;
- Tuttle S, Godbole K, McCarthy G, "Using LDAP for Directory Integration", IBM RedBooks, 2004;

- http://www.openldap.org;
- Pinheiro Malère L E, “LDAP Linux HOWTO”, http://en.tldp.org/HOWTO/LDAP-HOWTO;
- Williams A T, “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