Abstract: "Gestire" le identità per "gestire" la sicurezza dei dati

Raffaele Conte (Istituto di Fisiologia Clinica del CNR)

In seguito all'evoluzione tecnologica degli ultimi anni, i sistemi informativi delle aziende sanitarie sono cresciuti rapidamente fino a coprire capillarmente le intere strutture organizzative. I problemi relativi alla sicurezza dei dati si sono conseguentemente moltiplicati anche in considerazione del fatto che in queste realtà la quasi totalità dell'informazione trattata rientra nella categoria dei cosiddetti "dati sensibili". Tali problemi possono e devono essere affrontati sotto vari punti di vista (fisico, logico, applicativo e procedurale) e con l'ausilio delle tecnologie che lo stato dell'arte offre (VLAN, firewall, crittografia ecc.). La robustezza del sistema potrebbe però essere 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'ente di appartenenza - non si riflette sui meccanismi di autenticazione e autorizzazione implementati per lo specifico servizio. Inoltre, spesso avviene che differenti servizi prevedano distinti meccanismi di autenticazione, di conseguenza gli utenti si ritrovano a dover utilizzare diverse credenziali d'accesso, per ognuno dei sistemi e/o servizi utilizzati. A questo si aggiunge la necessità di dover garantire l'accesso ai dati sensibili ai soli utenti che ne hanno diritto e con le modalità loro consentite, in funzione della specifica figura professionale, non solo per una questione etica ma anche perché richiesto dalla normativa vigente.

Tutte le misure necessarie dovrebbero quindi essere implementate per ognuno dei sistemi di autenticazione con conseguente replicazione delle stesse azioni più volte. Inoltre, le informazioni relative agli utenti (nome, cognome, posizione, reparto di appartenenza ecc.) sono note all'Ufficio del Personale, raramente agli amministratori di sistema, anche a causa dell'alta volatilità del personale operante all'interno di una struttura sanitaria dove solitamente operano diverse figure, quali infermieri, tirocinanti, specializzandi, dottorandi, volontari ecc., presenti solo per periodi di tempo più o meno brevi.

Le problematiche descritte possono essere affrontate e risolte andando a gestire i profili degli utenti, con l'implementazione di un *Identity Manager*, tramite l'utilizzo del protocollo LDAP (Lightweight Directory Access Protocol).

Gli stessi concetti applicabili in un contesto locale (intranet) possono essere riprodotti su più larga scala quando un servizio utilizzato dagli utenti di un'organizzazione viene offerto da un soggetto esterno all'organizzazione stessa.

In effetti la diffusione di servizi Web-based forniti anche a terzi pone il problema della gestione dell'accesso ai dati da parte di utenti poco noti o totalmente ignoti a chi offre il servizio. Il più delle volte, l'accesso ad un servizio richiede l'iscrizione da parte dell'utente al servizio stesso, mediante la sottomissione di un insieme di dati personali più o meno significativo. In questo modo i dati dell'utente verranno replicati su diversi sistemi con conseguenti problemi di privacy e di consistenza (i dati potrebbero subire variazioni senza che il gestore del servizio possa venirne a conoscenza).

In una simile situazione una possibile alternativa è quella di stabilire degli accordi formali fra le parti e costituire una *Federazione* di servizi infotelematici. La gestione delle identità diventa quindi essenziale e alla figura del *Service Provider* (SP) - il fornitore del servizio - si affianca quella dell'*Identity Provider* (IdP). L'IdP fornirà al SP garanzie riguardo l'identità dell'utente che voglia accedere ad un servizio fornito da quest'ultimo e le informazioni relative al suo profilo (ruolo, affiliazione ecc.) necessarie per stabilire se l'accesso al servizio può essere concesso e con quali modalità.

Da qualche tempo molte organizzazioni (in particolar modo quelle a fini di ricerca come Internet2 americana, SWITCH svizzera, RedIRIS spagnola ed altre) si stanno organizzando in federazioni per l'erogazione dei servizi infotelematici. Anche in Italia, nell'ambito del GARR, è in corso un progetto per la creazione di un sistema federato per la condivisione di servizi fra enti di ricerca ed università.