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

Raffaele Conte - Maggio 2008
Istituto di Fisiologia Clinica del CNR

In seguito all'evoluzione tecnologica degli ultimi anni, i sistemi informativi delle organizzazioni sono cresciuti rapidamente fino a coprire capillarmente le intere strutture. I problemi relativi alla sicurezza dei dati si sono conseguentemente moltiplicati con la necessità di essere affrontati da vari punti di vista (fisico, logico, applicativo e procedurale) e con l'ausilio delle tecnologie che lo stato dell'arte può offrire. Nonostante ciò la robustezza del sistema può 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. Tali situazioni sono tanto più frequenti quanto più sono numerosi i servizi con autonomi sistemi di autenticazione.
Le problematiche descritte possono essere affrontate e risolte tramite l'implementazione di un *Identity Manager,* se limitate ad un contesto locale (intranet), ma gli stessi problemi si possono riproporre su più larga scala quando un servizio utilizzato dagli utenti di un'organizzazione viene offerto da un soggetto esterno all'organizzazione stessa. Infatti la diffusione di servizi Web-based forniti anche a terzi amplifica il problema della gestione dell'accesso ai dati da parte di utenti poco noti o totalmente ignoti a chi offre il servizio. Come spesso accade, l'accesso ad un servizio richiede la preventiva 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 più classica figura del *Service Provider* (SP) - il fornitore del servizio - si affianca quella dell'*Identity Provider* (IdP).
Da qualche tempo molte organizzazioni (in particolar modo quelle a fini di ricerca come Internet2 americana, SWITCH svizzera, RedIRIS spagnola ed altre) si sono organizzate in federazioni per l'erogazione dei servizi infotelematici. Anche in Italia, con il patrocinio del GARR, è in corso un progetto (IDEM) con lo scopo di creare un sistema federato per la condivisione di servizi fra enti di ricerca e università.