

## 2° CONVEGNO IDEM

### GARR – The Italian Academic & Research Network

#### L'accesso alla rete wireless di UniFe e la sua integrazione con la federazione IDEM

*Autore:* Michele Lugli – Università di Ferrara

##### **Abstract**

Offrire connettività di rete a membri di altri Atenei è sempre più una necessità. Ciò deve avvenire in conformità con le vigenti norme inerenti la sicurezza informatica, il che pone in primo piano il tema dell'autenticazione. Questi due aspetti (autenticazione e accesso alla rete) costituiscono un argomento attualmente molto sentito.

Disporre di un sistema di autenticazione federato, quale IDEM, porta ben noti vantaggi e semplificazioni: uso di credenziali già esistenti, omogeneità e standardizzazione tra i membri della comunità, possibilità di implementare il single sign-on.

Un sistema molto semplice e ampiamente diffuso di accesso alla rete, nello specifico la rete wireless, è il cosiddetto "captive portal": è il meccanismo che intercetta la navigazione Web di un utente non ancora riconosciuto per ridirigerlo verso una pagina Web di autenticazione.

Il punto è quindi l'integrazione tra questi due sistemi. I prodotti captive portal più diffusi generalmente non hanno un supporto nativo per Shibboleth, l'architettura di autenticazione adottata dalla federazione IDEM.

L'Università di Ferrara ha valutato nel corso degli anni diversi sistemi di captive portal tra il panorama opensource, prestando attenzione alle prestazioni e alla scalabilità delle soluzioni esistenti. Per quanto concerne la federazione IDEM, ha poi valutato e implementato una possibile integrazione tra il sistema di captive portal attualmente in uso e Shibboleth, che avesse il minimo impatto con l'infrastruttura esistente e rispettasse nel contempo i requisiti imposti dalle normative, quali il monitoraggio degli accessi utente, il logging e il controllo del traffico di rete.

Il sistema di accesso alla rete wireless adottato dall'Università di Ferrara è gestito dal prodotto opensource "CoovaChilli": esso implementa una versatile architettura di captive portal/walled garden e fa uso del protocollo RADIUS per le funzioni di autorizzazione e accounting. La macchina che ospita questo sistema ha il completo controllo del traffico di rete wireless e, per la federazione IDEM, costituisce il Service Provider. L'integrazione tra i due sistemi fa sì che l'accesso alla risorsa web protetta dal Service Provider comporti l'accesso alla rete wireless di Ateneo.