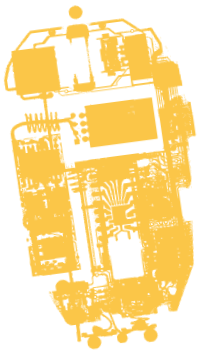
TECNOLOGIA TRASPARENTE



TOWER 2.0

ARCHITETTURA DI AUTENTICAZIONE PER RETI WIRELESS FEDERATE

Tower è un'architettura di autenticazione, con minimi requisiti hardware, nata dall'evoluzione di progetti opensource per gestire gli accessi utente ad una rete dati, tipicamente (ma non solo) wireless. Nata originariamente come Tower, basata su core NoCat, nella versione più recente si evolve in Tower 2.0 basato su piattaforma opensource Pfsense che offre:

- facilità di utilizzo da parte dell'utente che si autentica per accedere ai servizi di rete;
- supporto per il roaming "trasparente" tra enti e operatori federati con l'asset Transparent Roaming;
- una soluzione modulare e scalabile;
- elevato livello di sicurezza per le credenziali di accesso anche per gli utenti in roaming.

A COSA SERVE

Si tratta di una soluzione chiavi in mano che permette di:

- accedere a servizi di navigazione web e più in generale a servizi di rete attraverso un captive portal;
- controllare l'accesso alle reti wireless e wired per servizi pubblici e privati;
- avere una soluzione modulare e scalabile;
- supportare la nomadicità degli utenti tra reti e hot-spot diversi;
- gestire la piattaforma attraverso un'interfaccia grafica web based (GUI) di semplice utilizzo;
- autenticare gli utenti su piattaforme diverse, come ad esempio Shibboleth, X.509, ecc.
- utilizzare sistemi di registrazione automatica per gli utenti (via SMS).

LA NUOVA PIATTAFORMA TOWER 2.0

Nella nuova veste, la piattaforma Tower passa ad un core Pfsense, che consente una migliore attività di sviluppo delle funzionalità avanzate, la disponibilità di un'interfaccia di gestione web evoluta per la configurazione e il monitoring dello stato delle connessioni e del sistema.
L'architettura Tower si compone di un gateway basato su sistema operativo opensource PfSense integrato con le funzionalità di autenticazione federata proprie di Tower e di un sistema di autenticazione web-based svincolato da piattaforme HW specifiche, bensì implementabile per varie tipologie di sistemi di autenticazione: in particolare soluzioni Shibboleth e di autenticazione con certificati X.509.

In particolare Tower è ora completato dall'integrazione di:

- **Sistemi di autenticazione web-based Shibboleth**: abilita il servizio Tower all'autenticazione dell'utente su architettura Shibboleth.
- **Autenticazione con riconoscimento certificati X.509**: abilita il servizio Tower all'autenticazione dell'utente che si identifica attraverso l'uso del proprio certificato X.509.
- **SMS gateway zero-cost (lato provider)**: l'utente invia un messaggio di richiesta all'SMS gateway indicando la password scelta per l'account che viene creato automaticamente.
- **Ingegnerizzazione della gestione dei log**: l'architettura permette di gestire in modo ottimizzato i principali log prodotti dal sistema, creare punti di raccolta e selezione delle informazioni utili all'amministratore e garantire un backup completo dei file di log, interfacciabile ai sistemi di backup più diffusi.
- **Transparent roaming**: applicazione Android per l'accesso trasparente alla rete federata Tower che fa parte del catalogo degli asset di CSP.

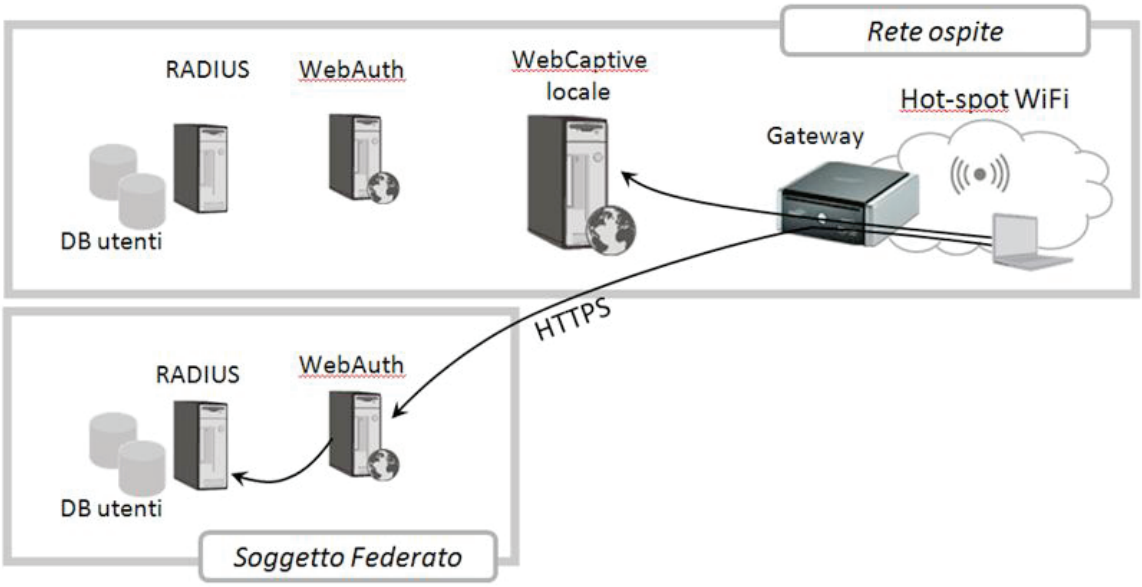
>>

ARCHITETTURA DEL SISTEMA E SICUREZZA

L'architettura Tower si compone di tre elementi software che possono integrarsi sulla stessa piattaforma hardware:

- un gateway che controlla l'accesso alla rete con router e firewall integrati dall'asset Mynos;
- un portale WebCaptive che identifica il dominio dell'utente attraverso lo username (re-direzione all'authentication web server di pertinenza);
- un portale WebAuth che verifica le credenziali degli utenti attraverso il sistema di autenticazione appropriato per il dominio: RADIUS, Shibboleth, X.509, ecc.

Nel caso di una rete federata condivisa da più soggetti, l'utente inserisce i dati sensibili come la password, direttamente sul portale WebAuth del proprio ente, avendo così garantita la massima riservatezza, grazie anche alla cifratura e autenticazione tramite protocollo SSL.
Inoltre, l'ente che offre la connettività alla rete è certo che l'utente sia abilitato poiché il sistema di autenticazione permette di "firmare" digitalmente la risposta autorizzativa. Per un'agevole integrazione con i backend di autenticazione più diffusi, il server WebAuth supporta il protocollo AAA RADIUS (tramite libreria PHP), in modo da ottimizzare l'uso di architetture di autenticazione/accounting già operative presso la rete dell'operatore.



CSP - innovazione nelle ICT
Via Nizza 150, 10126 Torino (Ingresso da Via Alassio, 11/c)
Tel. +39 011 48.15.111 Fax +39 011 48.15.001
www.csp.it - innovazione@csp.it