Cineca OpenWiFi

Documentazione Tecnica
Novembre 2013

Cineca
Consorzio Interuniversitario
Sede Legale, Amministrativa e Operativa:
Via Magnanelli 6/3
40033 Casalecchio di Reno (BO)

Altre Sedi Operative:

Via R.Sanzio, 4
20090 Segrate (MI)
Tel.: 02-269951

Via dei Tizii, 6
00185 Roma
Tel.: 06-444861

A cura del Dipartimento Soluzioni e Servizi per l'Amministrazione Universitaria
Email: re.univ@cineca.it

Sommario

1. ACCESSO AL SERVIZIO DA PARTE DELL'UTENTE 5
1.1 COLLEGAMENTO AL SERVIZIO – AUTENTICAZIONE 5
MODALITÀ CAPTIVE PORTAL 5
MODALITÀ WPA/WPA2 802.1X 5
1.2 LIMITI DI ACCESSO 6
1.3 CREAZIONE DELL'UTENZA 6
1.4 RECUPERO PASSWORD DA PARTE DELL'UTENTE 8
RECUPERO PASSWORD VIA CHIAMATA TELEFONICA 8
RECUPERO PASSWORD VIA E-MAIL 8
1.5 FRONT-OFFICE PERSONALE DELL'UTENTE 8
2. COME FUNZIONA CINECA OPENWIFI 11
2.1 ARCHITETTURA DEL SISTEMA 12
2.2 *HOTSPOT* 13
2.3 CENTRO STELLA 14
2.4 CONNETTIVITÀ DEL CENTRO STELLA E DEGLI *HOTSPOT* 15
FIGURA 7 - COLLEGAMENTI DA E VERSO IL CENTRO STELLA 15
RACCOLTA DEL TRAFFICO DAGLI *HOTSPOT* VERSO IL CENTRO STELLA 15
CONNESSIONE DEL CENTRO STELLA A INTERNET 16
DISPONIBILITÀ DEL SERVIZIO 16
SICUREZZA DELLA SOLUZIONE 16
2.5 SISTEMA DI GESTIONE DEGLI ACCESS POINT 17
2.6 SISTEMA DI MONITORAGGIO 21
2.7 SISTEMA DI GESTIONE DEGLI ACCESSI 22
BACK-END DEL SISTEMA DI GESTIONE DEGLI ACCESSI 23
BACK-OFFICE DEL SISTEMA DI GESTIONE DEGLI ACCESSI 23
2.8 *FRONT-OFFICE* DEL SISTEMA DI GESTIONE DEGLI ACCESSI 26
2.9 REGISTRAZIONE UTENTI TRAMITE OPENWISP *USER MANAGEMENT SYSTEM* 26
REGISTRAZIONE ONLINE TRAMITE SIM/USIM 27
REGISTRAZIONE CON CARTA DI CREDITO 28
3. OPENWIFI E LE FEDERAZIONI 30
FREEITALIAWIFI 30
IDEM ED EDUROAM 30
4. RIFERIMENTI NORMATIVI 32

Questo documento contiene i dettagli tecnici del sistema Cineca OpenWiFi.
E' rivolto ai responsabili tecnici delle Amministrazioni interessate ad adottare la soluzione OpenWiFi. Per approfondimenti sul funzionamento tecnico di OpenWiFi scrivere allo staff tecnico all'indirizzo <openwifi@cineca.it>.

1. Accesso al servizio da parte dell'utente

1.1 Collegamento al servizio – Autenticazione

Il servizio Cineca OpenWiFi è fruibile da qualunque dispositivo dotato di un browser e di una scheda radio compatibile con lo standard IEEE 802.11 a/b/g/n a 2,4Ghz o 5Ghz: tipicamente laptop e smartphone.

Modalità Captive Portal

L'utente si deve connettere all'ESSID pubblicato da uno degli access point collegati al servizio (es. "<amministrazione>-wifi"). L'ESSID, non è protetto da alcun protocollo di sicurezza (es. WEP o WPA); tuttavia, il collegamento a qualsiasi risorsa di Internet è bloccato, ed il browser degli utenti viene ridiretto forzatamente ad una pagina del *captive portal* (i.e. captive page).
La *captive page* notifica al navigatore la necessità di procedere con l'autenticazione e, in caso questi non disponga di un'utenza valida, specifica le modalità per crearne autonomamente una (cf. "Creazione dell'utenza").
La navigazione e l'accesso alle risorse di Internet vengono abilitati non appena l'utente effettua con successo l'autenticazione. L'utente viene quindi reindirizzato alla pagina web cui si era riferito inizialmente.
E' comunque possibile configurare l'accesso a un insieme di contenuti Internet, veicolati attraverso un apposito ambiente navigabile senza autenticazione e in modo ristretto (i.e. "*walled garden*"), definito in fase di progettazione del servizio.
La *captive page* può inoltre essere personalizzata a seconda delle esigenze dell'Amministrazione (ad esempio, inserendo il logo dell'Amministrazione che offre il servizio).

Modalità WPA/WPA2 802.1x

In questa modalità l'autenticazione dell'utente è effettuata mediante il protocollo EAP che garantisce un elevato livello di sicurezza mediante meccanismi e protocolli crittografici.
In questa modalità ogni *access point* può annunciare due ESSID (ovvero reti Wi-Fi):

- uno protetto da WPA/WPA2, identificato, ad esempio, dal nome "<amministrazione>-wifi", che richiede l'inserimento di un nome utente e di una password per consentire la navigazione;
- uno non protetto, denominato ad esempio "<amministrazione>-registrazione" riservato alla registrazione (cfr. Creazione dell'utenza).

1.2 Limiti di accesso

Il sistema permette di configurare dei profili utente e dei limiti di accesso collegati, a livello di:

- tempo di accesso;
- quantità di dati scambiati;
- restrizione a determinati contenuti.

L'utente "standard" può usufruire del servizio ogni giorno per un tempo determinato, per default 1 ora, o trasferire una quantità predeterminata di traffico, per default di 300 Mbyte. L'utente viene disconnesso al verificarsi di una delle due condizioni. Tutti i "contatori" definiti per implementare le restrizioni sono automaticamente azzerati alla mezzanotte.
Se l'utente non effettua alcun tipo di traffico di rete per un periodo di tempo pari a 10 minuti, il *captive portal* forza il suo logout. L'utente dovrà effettuare nuovamente il login per scambiare nuovamente traffico.

Anche a seguito di autenticazione è possibile prevedere limitazioni in termini di siti accessibili. In caso di necessità da parte dell'Amministrazione di definire restrizioni, è possibile individuare la soluzione più opportuna in base alla tipologia e alla modalità delle restrizioni e valutando i costi dell'implementazione.

Tutte le politiche di autorizzazione, così come il numero di gruppi di utenze definite, sono personalizzabili. Ad esempio, è possibile configurare un "Power User", senza limiti di traffico e tempo di connessione. E' anche possibile dare un accesso privilegiato a particolari dispositivi, inserendoli in una lista di dispositivi autorizzati per i quali non è necessaria alcuna autenticazione. Ciò può consentire ad esempio l'uso della rete WiFi per la collezione periodica di informazioni raccolte da apparati sparsi per il territorio (es. traffico, inquinamento, webcam, etc.).

1.3 Creazione dell'utenza

La procedura di default per la creazione di un'utenza avviene tramite SIM/USIM. E' possibile configurare altre procedure per registrare un utente, descritte nella sezione "Sistema di gestione degli accessi": auto-registrazione tramite carta di credito, e registrazione tramite operatore con scansione della Carta di Identità.
Il sistema di registrazione via SIM/USIM, adeguato e personalizzato per le esigenze del progetto, viene utilizzato per l'autenticazione e l'identificazione degli utenti per i servizi al pubblico Wi-Fi conformemente alle esigenze

legislative attualmente in vigore. Il sistema assume che l'utente abbia un telefono mobile personale e che il possessore del telefono mobile sia stato a monte identificato al momento della vendita del servizio di telefonia mobile, come da prassi.

La procedura adottata è la seguente:

1. L'utente che per la prima volta usa il servizio si connette ad internet in modalità Wi-Fi ed aprendo una qualsiasi pagina in un browser riceve una pagina di benvenuto che invita alla registrazione. In questa pagina vengono richiesti i dati di identificazione dell'utente (nome, cognome, numero del telefono mobile, e-mail).
2. Viene assegnata in risposta all'utente una UserID (corrispondente al suo numero di cellulare). L'utente stesso avrà modo di scegliere una password che il sistema controllerà affinché la password rispetti dei requisiti minimi di robustezza.
3. L'ultimo passo richiesto all'utente è di fare una telefonata con il suo telefono mobile ad un numero di rete fissa (es. 0612345678) con identificatore di chiamata attivo (Caller ID), per verificare che il numero di cellulare sia effettivamente in suo possesso.
4. Il sistema intercetta la chiamata dal telefono e non risponde, la chiamata viene fatta cadere (non generando quindi alcun costo per l'utente). L'essenziale per il sistema è di individuare l'identificatore di chiamata (Caller ID); se è uguale a quello dichiarato dall'utente nella registrazione, il servizio viene sbloccato, altrimenti viene rifiutato.

Figura 1 - Registrazione tramite chiamata telefonica

E' da notare che questa procedura assicura che non ci siano costi di registrazione né per l'utente (la cui chiamata non viene terminata) né per

l'amministrazione (la quale non deve mandare SMS di conferma). L'amministrazione deve solo mantenere un numero limitato di linee telefoniche – quindi un costo fisso e non variabile – per assicurare il funzionamento della procedura.

1.4 Recupero password da parte dell'utente

Il sistema prevede due meccanismi volti a permettere il ripristino delle credenziali di accesso da parte degli utenti finali del servizio.

Recupero password via chiamata telefonica

Utilizzando gli stessi meccanismi della registrazione mediante chiamata da utenza telefonica mobile, l'accesso al form di modifica della password avviene effettuando una telefonata ad un numero di rete fissa. Come per una nuova registrazione, il sistema intercetta il Caller ID della chiamata e fa cadere la chiamata; nessun costo viene addebitato all'utente.

Recupero password via e-mail

Il *front-office* del sistema offerto consente l'accesso alla form di ripristino delle credenziali di accesso mediante invio di una e-mail contente un'URL univoca e auto-generata.

Figura 2 - Reimpostazione password via e-mail

1.5 Front-office personale dell'utente

Una volta registrati, gli utenti hanno la possibilità di accedere al front-office del proprio profilo e consultare lo storico delle navigazioni ed i dati personali inseriti in fase di registrazione.

L'utente è in grado di visualizzare i seguenti dati di consumo:

- traffico effettuato per giorno;
- minuti di traffico utilizzati per giorno;
- Byte utilizzati per sessione.

E' poi consentita agli utenti la modifica di tutti i dati memorizzati ad esclusione di quelli per loro natura immutabili oppure utilizzati per l'identificazione univoca (e a norma di legge). In particolare, non è possibile modificare i seguenti attributi:

- nome e cognome;
- nome utente (userid);
- numero di telefono cellulare (qualora utilizzato per l'identificazione - in questo caso il numero di telefono è l'unico elemento che consente l'identificazione certa del titolare. Nel caso l'utente cambi tale numero, dovrà ripetere la procedura di registrazione).

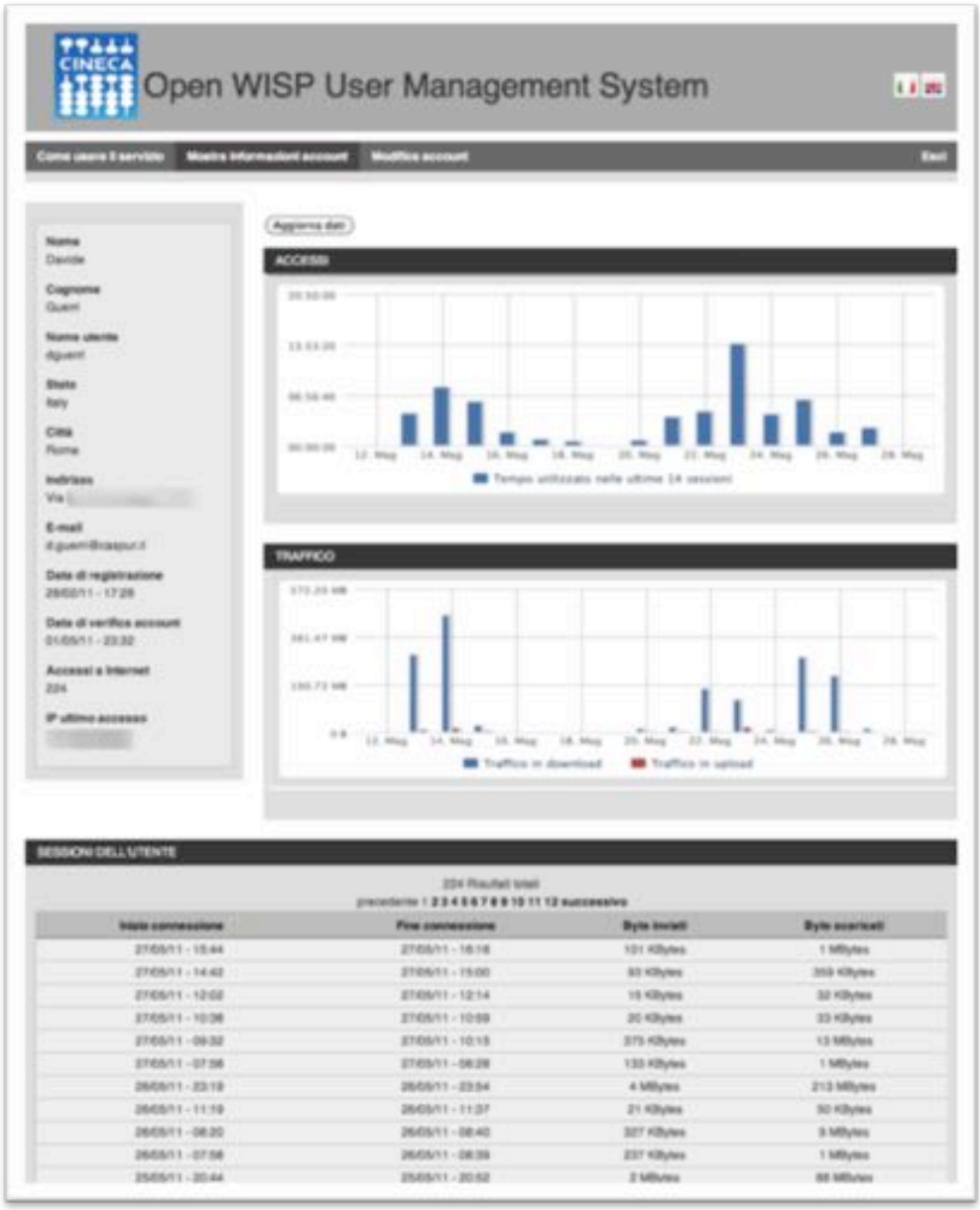

Figura 3 - Account dell'utente

L'utente può anche, in autonomia, disabilitare il proprio account. Trascorso un periodo di tempo personalizzabile (ma dipendente dagli obblighi

normativi in merito al tracciamento degli accessi al servizio pubblico), la relativa utenza sarà rimossa dal sistema. In qualunque momento, fino alla cancellazione definitiva dell'account, il servizio sarà riattivabile con la stessa modalità utilizzata in fase di registrazione.

Figura 4 - Modifica dell'account

2. Come funziona Cineca OpenWiFi

Il sistema Cineca OpenWiFi è basato su modalità *Plug&Play*: l'Amministrazione deve solo collegare gli Access Point (AP) forniti da Cineca alla rete ed alimentarli. Gli AP provvederanno immediatamente all'autoconfigurazione e saranno pronti all'uso. Prima della fornitura degli AP, Cineca avrà configurato il **Centro Stella** presso il proprio Data Center e personalizzato il portale di accesso degli utenti secondo le indicazioni dell'Amministrazione.

Gli Access Point, inoltre, non necessitano di connettività dedicata: possono essere installati su connessioni Internet preesistenti, come le reti interne dell'Amministrazione o semplici ADSL di terze parti. Questo rende facile e veloce la diffusione della rete WiFi dell'Amministrazione presso edifici pubblici (ospedali, scuole), ma anche locali commerciali (bar, ristoranti) e perfino abitazioni private. La sicurezza della soluzione è garantita dall'isolamento tramite VPN del traffico degli utenti da quello relativo alla connettività locale.

Per l'utente, l'architettura del sistema è trasparente: egli vede un ESSID unico annunciato su tutti gli *hotspot* della rete WiFi, si autentica sul portale (creando l'utenza se non ne possiede una) e naviga su Internet.

Figura 5 – Esempio di diffusione della rete WiFi

2.1 Architettura del sistema

Una volta siglato l'accordo tra Cineca e l'Amministrazione, Cineca provvede a:

- installare il numero desiderato di *hotspot* con il sistema operativo OpenWF (OpenWISP Firmware), sviluppato da Cineca;
- installare e personalizzare il Centro Stella secondo le specifiche richieste dall'Amministrazione. A seconda delle esigenze in termini di dimensionamento del servizio, il Centro Stella può essere installato su una macchina fisica o virtuale.

Gli *hotspot* vengono quindi inviati all'Amministrazione, che li può installare nei punti prescelti, con la sola condizione che vengano alimentati e collegati alla rete Internet (anche attraverso reti di terze parti, es. ADSL). A quel punto gli *hotspot* provvedono automaticamente all'autoconfigurazione e sono pronti all'uso entro qualche minuto. Nell'autoconfigurazione, gli *hotspot* scaricano dal Centro Stella le configurazioni specifiche per la rete dell'Amministrazione.

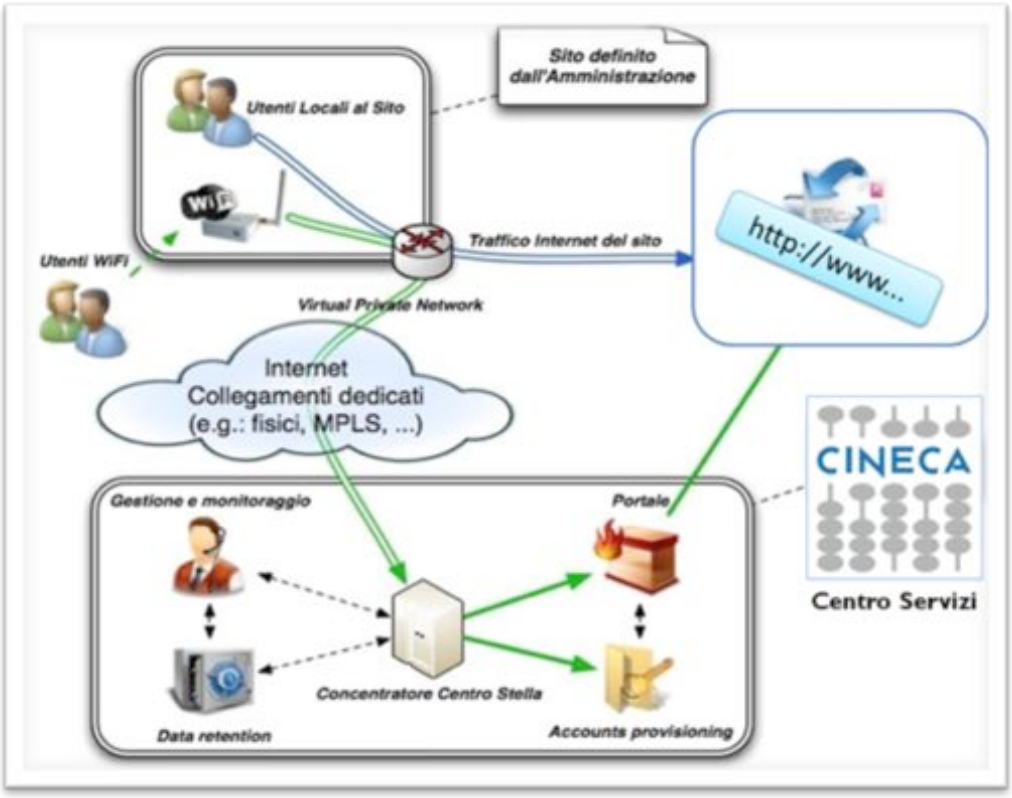

Figura 6 - Schema semplificato dell'architettura di OpenWiFi

Alla fine della configurazione, ogni Access Point serve l'ESSID per la rete WiFi dell'amministrazione, al quale possono collegarsi gli utenti. Inoltre l'Access Point mette in piedi una VPN con il centro stella; attraverso

questa VPN viene veicolato tutto il traffico dell'AP. In pratica dunque, il traffico di ogni utente attraversa la VPN verso il Centro Stella, e viene da questo inoltrato su Internet.

E' importante quindi sottolineare che il traffico utente non usa direttamente la connessione dell'AP (che potrebbe essere l'ADSL di una scuola o di un bar) per andare su Internet, ma viene incapsulato nella VPN. Questo significa che per il titolare della connessione a cui è collegato l'*hotspot*, il traffico della rete WiFi dell'Amministrazione è trasparente: ciò lo svincola dagli oneri d'identificazione e tracciamento degli accessi a norma di legge.

L'isolamento tramite VPN del traffico degli utenti da quello relativo alla connettività locale garantisce anche la sicurezza della soluzione.

2.2 *Hotspot*

Gli *hotspot* sono apparati di accesso wireless di alta qualità, installati con un sistema operativo open source denominato OpenWF. Questa è una customizzazione sviluppata da Cineca del sistema OpenWRT, distribuzione Linux dedicata principalmente a dispositivi wireless. OpenWRT è lo standard di fatto in un approccio non proprietario alla gestione di wireless access point: il sistema è in continua evoluzione ed è usato in ogni parte del mondo con un notevole numero di utilizzatori e sviluppatori.

La scelta di OpenWRT come base del sistema assicura un ampio grado di autonomia nel rapporto tra le componenti hardware/firmware e le componenti software utilizzate, al fine di evitare da un lato critiche dipendenze da specifici vendor di access point e dall'altro la massima flessibilità d'impiego dei prodotti.

Per produrre OpenWF, il team di sviluppo ha progettato e inserito in OpenWRT una serie di tool che permettono agli *hotspot* di essere pienamente integrati nell'architettura del sistema OpenWiFi. Gli access point sono in grado di autoconfigurarsi collegandosi al sistema centrale ed instaurare VPN con il Centro Stella.

Grazie alle molteplici periferiche di I/O, le mainboard degli access point possono essere dotate di diversi dispositivi quali ad esempio:

- sensori di temperatura esterna;
- modem per accesso 3G HSDPA;
- sensori di I/O;

- ulteriori unità radio per il collegamento a reti *hiperlan* o *mesh*;
- apparati di acquisizione video per videosorveglianza.

La tipologia di apparati consente inoltre la gestione di multipli ESSID con possibilità di concentrazione del traffico raccolto su VLAN differenti presso il centro servizi.

Riassunto delle *feature* degli *hotspot*:

- irradiamento del segnale Wi-Fi a 2,4 Ghz e a 5 Ghz per uso diretto da parte dei terminali utente (802.11 a/b/g/n);
- gestibilità tramite piattaforma centralizzata;
- esposizione di una interfaccia web via Wi-Fi per la configurazione iniziale dell'apparato;
- gestione multipli ESSID tramite differenti VLAN;
- possibilità di instaurare VPN eventualmente contenenti VLAN;
- conformità con le normative europee;
- alimentazione elettrica tramite POE passivo;
- raggio di copertura del segnale radio Wi-Fi non inferiore ai 100 metri in campo aperto con antenna omnidirezionale;
- protezione degli accessi wireless tramite : WPA/WPA2, 802.1x;
- protezione da attacchi di tipo *denial of service* e *session hijacking*;
- aggiornamento delle configurazioni da remoto.

Tutti gli *hotspot* forniti sono garantiti per un periodo di 12 mesi.

2.3 Centro Stella

Tutti gli *hotspot* sono collegati al Centro Stella tramite VPN (oppure direttamente nel caso di reti dedicate esclusivamente al trasporto del traffico per il servizio WiFi). Il Centro Stella convoglia i flussi di traffico provenienti dagli apparati periferici verso Internet, garantendo il bilanciamento del traffico.

Il Centro Stella realizza le funzionalità di sicurezza di rete ed applica le politiche e limitazioni di accesso che vengono gestite dal captive portal e dal sistema di autenticazione.

Il Centro Stella ha le seguenti funzioni:

- raccogliere il traffico degli AP e instradarlo verso Internet;
- servire la pagina web del portale ("captive portal") della rete WiFi dell'Amministrazione, che contiene anche il front-end su cui i

fruitori del servizio possono consultare le informazioni relative alla loro utenza;
- autenticare gli utenti;
- far rispettare i limiti sull'uso del traffico;
- servire i sistemi di back-end
    - gestione degli utenti;
    - gestione degli access point;
    - monitoraggio degli access point.

Tutto il software utilizzato è rilasciato sotto licenze open source e non ha costi di sottoscrizione, manutenzione, aggiornamento ed estensione.

2.4 Connettività del Centro Stella e degli *hotspot*

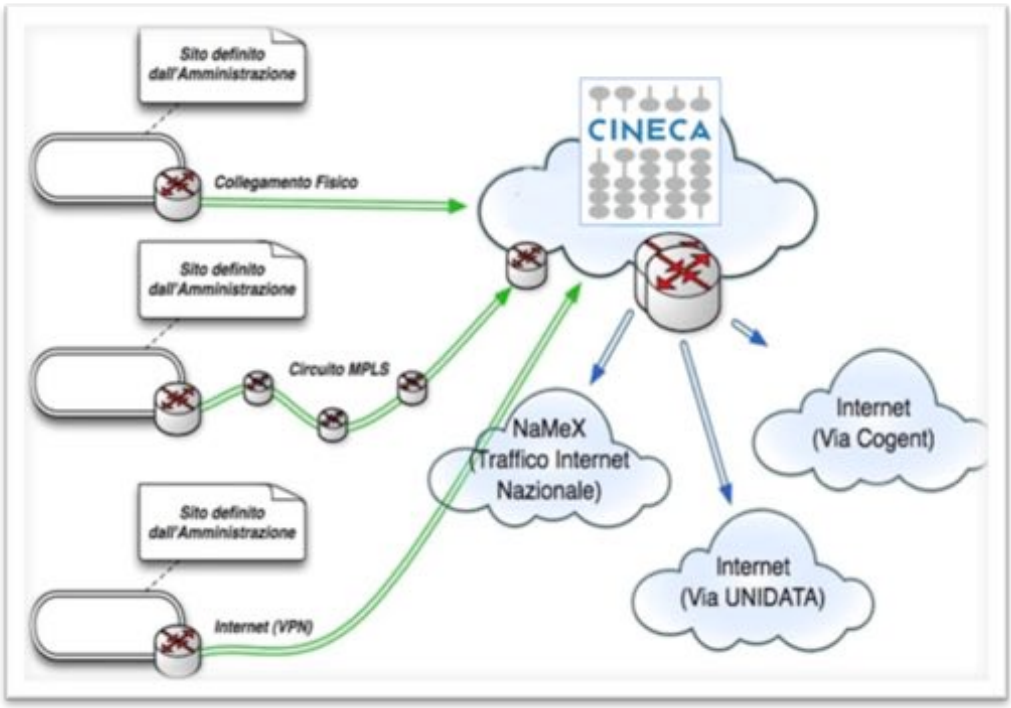

figura 7 - Collegamenti da e verso il Centro Stella

Raccolta del traffico dagli *hotspot* verso il Centro Stella

La raccolta del traffico degli *hotspot* può essere fatta tramite circuiti dedicati, oppure attraverso la rete Internet mediante canali cifrati sicuri. In particolare il traffico può essere raccolto nei seguenti modi:

- per mezzo di collegamenti diretti con gli apparati di accesso (es. kit di consegna per xDSL);

- mediante Virtual Private Networks (VPN) veicolate attraverso reti private o pubbliche preesistenti (es. Metropolitan Area Network o Regional Area Network);
- attraverso Virtual Private Networks (VPN), veicolate attraverso collegamenti ad Internet preesistenti di terze parti (ad esempio ADSL di scuole, ospedali, bar etc).

Connessione del Centro Stella a Internet

Il Centro Stella può essere installato presso Cineca oppure presso un altro data center selezionato dall'Amministrazione.
Nel caso di installazione presso Cineca, la connessione del Centro Stella a Internet è realizzata attraverso circuiti in grado di scalare a capacità multiple di 1 Gbit/s, garantendo un'elevata estendibilità. Nei locali di Cineca è presente il punto di interscambio NaMeX – al quale la rete Cineca è connessa – che ha fra i suoi associati i maggiori ISP italiani.
Il transito verso la "Big Internet" è invece garantito da collegamenti ridondati (attraverso Cogent Communication e Unidata) con una banda complessiva di 300 Mbps (scalabili a 2Gbps).

Disponibilità del servizio

Come detto, a seconda delle esigenze dell'Amministrazione e del dimensionamento desiderato della rete WiFi, il Centro Stella può essere installato su una macchina fisica o virtuale.

Il Centro Stella è dotato di un sistema di logging che invia i messaggi a un log collector; inoltre il Centro Stella è sotto backup, per cui lo stato della macchina può essere recuperato in caso di perdita dei dati.

Sicurezza della soluzione

I flussi di traffico provenienti dai client Wi-Fi vengono opportunamente instradati, al fine di non consentire la comunicazione tra utenti, mediante:

- un'opportuna configurazione del collettore delle VPN (vietando il bridging tra VPN e tramite firewalling layer 2);
- un'opportuna configurazione degli apparati periferici (*client isolation* sull'ESSID).

Tale accorgimento consente a ogni client la sola raggiungibilità dei gateway d'accesso (i.e.: captive portal/firewall) evitando la diffusione di malware e la saturazione delle risorse di rete dovuta, ad esempio, al file-sharing tra utenti anche non autenticati (la separazione dei client degli utenti finali è una contromisura estremamente efficace per potenziali DoS quali, ad

esempio, la presenza di server DHCP su apparati utente, o di attacchi informatici quali l'ARP poisoning).
Le *captive pages*, ove gli utenti forniscono le credenziali di accesso, sono consultabili esclusivamente per mezzo del protocollo HTTPS. Per l'intero periodo della fornitura, vengono installati e mantenuti i relativi certificati X509 firmati da una Certification Authority riconosciuta dai browser.

Si osservi che, laddove sono utilizzate le VPN per convogliare il traffico proveniente dagli apparati periferici, si fa uso di certificati X509, gestiti mediante una PKI privata localizzata all'interno del sistema di gestione, per autenticare entrambi gli endpoint dei tunnel. Questa funzionalità evita l'utilizzo di apparati "non autorizzati" e consente l'esclusione di *hotspot* "compromessi" (es. rubati o "manipolati") mediante revoca dei relativi certificati.

2.5 Sistema di gestione degli Access Point

Il sistema di gestione degli Access Point è ***OpenWISP manager***, sviluppato da Cineca e rilasciato con licenza open source (GPL-v3). Lo stesso sistema è utilizzato nell'ambito del progetto Provinciawifi della Provincia di Roma e del wifi pubblico di altre 14 Pubbliche Amministrazioni.
OpenWISP manager è realizzato mediante il framework open source Ruby on Rails versione 2.3.5, disponibile per Windows e Unix (tra cui Linux e Mac OS X). Ciò assicura la portabilità su più piattaforme e sistemi operativi.

Figura 8 - Configurazione hotspot tramite template

Le funzionalità del sistema sono le seguenti:

- graphic User Interface web-based con Ajax
- configurazione centralizzata e basata su template degli *hotspot* in termini di canali Radio utilizzati (802.11a-b-g-n);
    - ESSID annunciati e relativa tipologia di accesso alla rete (Open, WEP, WPA-PSK, WPA2-PSK, 802.1x con RADIUS);
    - VLAN definite;
    - bridging interno (ESSID – VLAN – Interfacce Ethernet)
    - VPN implementate;
    - Traffic Shaping con configurazione della banda garantita per interfaccia ethernet, ESSID, VLAN e VPN;
- sistema di controllo degli accessi basato su ruoli
- aggiornamento della configurazione degli apparati periferici automatica mediante interfaccia web
- inserimento e modifica dei dati di profilo relativi a ogni *hotspot* quali ad esempio
    - informazioni generali (nominativo "user-friendly" e note);
    - ubicazione dell'*hotspot* sia in formato testuale che in formato grafico. La georeferenziazione (i.e.: selezione delle coordinate GPS per latitudine e longitudine) degli *hotspot* può avvenire sia inserendo l'indirizzo del sito sia mediante interfaccia "punta e clicca";

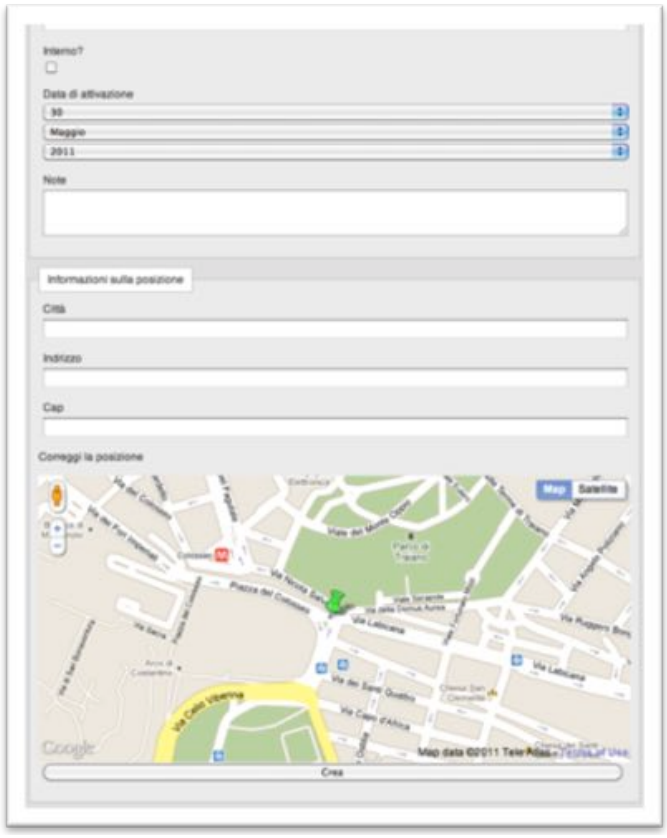

Figura 9 - Creazione Access Point - Ajax GUI con geolocalizzazione

- gestione traffic shaping (banda massima utilizzabile e banda minima garantita per ESSID e per VLAN) per template e per hotspot;
- possibilità di definire script personalizzati (eseguiti periodicamente o su base temporale per template o singolo *hotspot*) utilizzabili, ad esempio, per lo spegnimento delle schede radio in particolari orari o giorni.

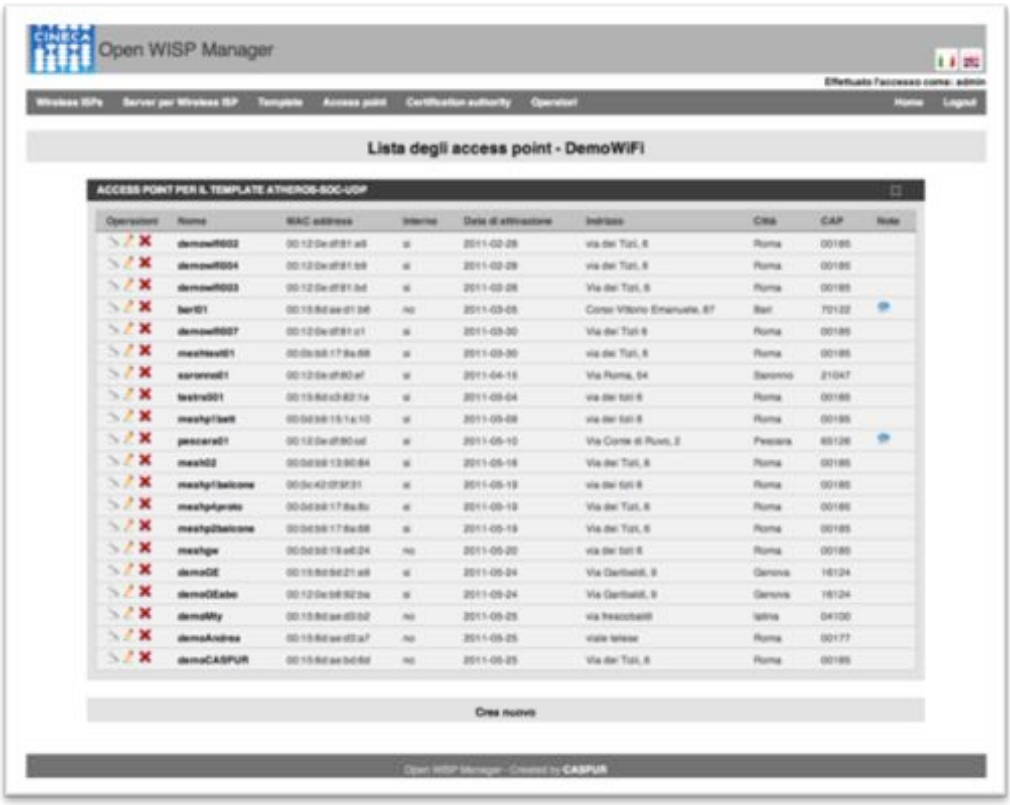

Figura 10 - Inventario access point

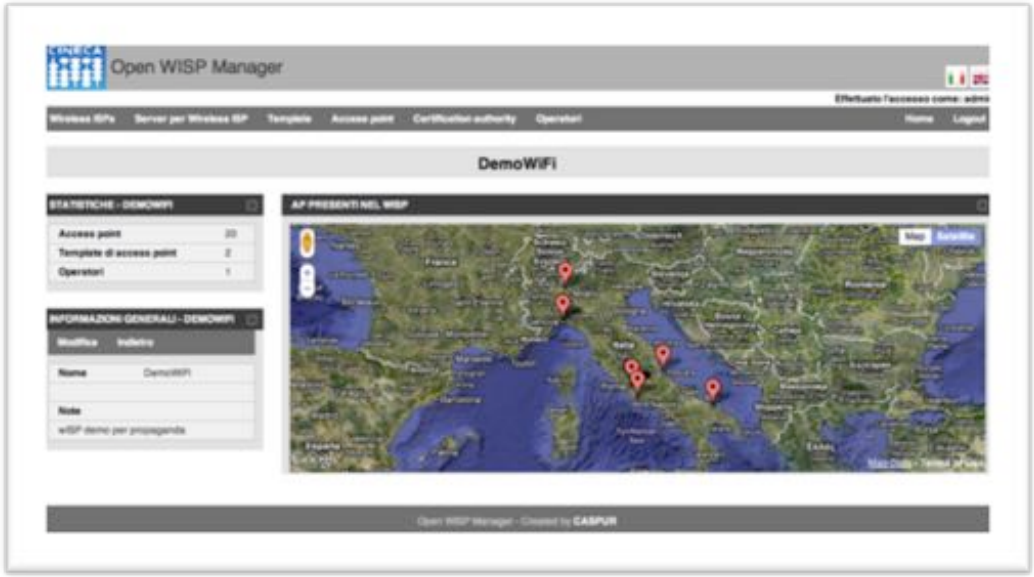

Figura 11 - Riassunto hotspot con geolocalizzazione

Ferma restando la possibilità di gestire le funzioni principali degli *hotspot* mediante interfaccia web, il sistema offerto prevede la possibilità di amministrare tutte le funzioni di ogni singolo apparato (compreso lo spegnimento e il riavvio) da consolle.

Per gli access point che utilizzano le VPN, questa funzionalità è garantita anche nel caso in cui gli AP siano posizionati dietro un firewall o un meccanismo di NAT, mediante inoltro della VLAN di amministrazione all'interno di ogni tunnel.

Poiché Cineca è ideatore, sviluppatore e manutentore del software open source OpenWISP Manager, è possibile realizzare qualunque tipologia di personalizzazione, anche in funzione dell'evoluzione del progetto, secondo le esigenze dell'Amministrazione.

2.6 Sistema di monitoraggio

Il sistema di monitoraggio consente, mediante un'interfaccia web, l'analisi e la visualizzazione dello stato di tutti i dispositivi monitorati.
In particolare sono disponibili, anche per l'accesso da parte di incaricati dell'Amministazione, le seguenti informazioni:

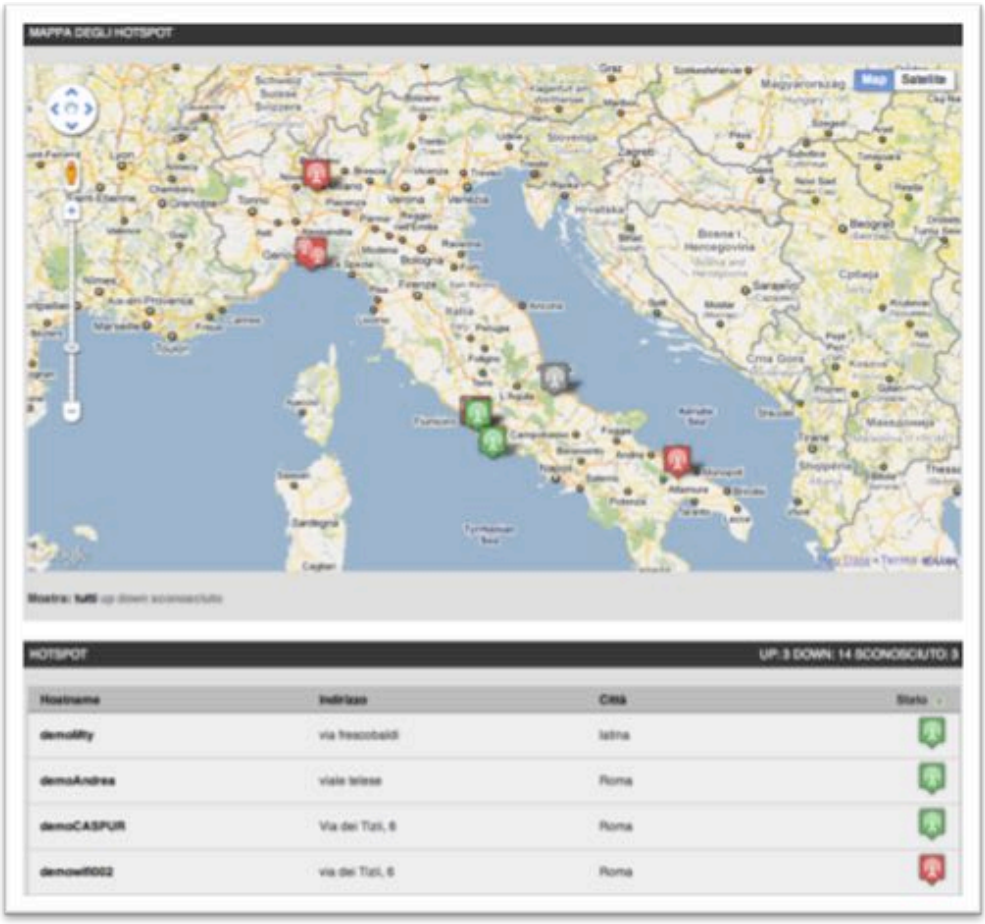

Figura 12- Mappa di monitoraggio Access Point

- numero di apparati monitorati;
- numero di apparati che presentano un'allerta;
- riassunto del profilo degli *hotspot* (situazione e posizione geografica);
- storico della raggiungibilità degli apparati nell'ultimo mese di attività mediante grafici.

Il sistema di monitoraggio fornisce uno strumento di visualizzazione degli *hotspot* localizzati su una mappa interattiva web-based (basata sul servizio Google Maps) dalla quale è possibile l'immediata visualizzazione dello stato di funzionamento degli *hotspot* mediante indicatori simbolici (i.e.: icone di stato) e consentire il collegamento alle informazioni di dettaglio presenti all'interno del sistema stesso.

Figura 13 - Dettaglio configurazione Access Point

2.7 Sistema di gestione degli accessi

Il sistema di gestione degli accessi è OpenWISP User Management System, un'evoluzione del sistema utilizzato nell'ambito del progetto Provinciawifi della Provincia di Roma. Tale sistema, sviluppato da Cineca, è rilasciato con licenza open source (GPL-v3).

L'OpenWISP User Management System è realizzato mediante il framework Ruby on Rails, utilizzando un database MySQL come back-end. Una delle finalità principali del sistema in oggetto è quella di impostare opportunamente la configurazione del server RADIUS, che costituirà l'authentication server utilizzato dal captive portal.

Il sistema di gestione degli accessi è costituito da tre parti:

- *Back-end* del sistema;
- *Back-office* del sistema per l'accesso e la gestione da parte degli operatori;
- *Front-office* del sistema per l'accesso e la gestione da parte degli utenti.

Back-end del sistema di gestione degli accessi

Il back-end del server RADIUS, ovvero il database degli utenti registrati, è implementato mediante un DBMS MySQL opportunamente configurato.
Sul back-end dell'authentication server sono preconfigurati due gruppi di utenze con differenti politiche di limitazione dell'accesso basate su contatori di tempo e/o traffico trasmesso/ricevuto dall'utente in un periodo di tempo definito, già menzionate in precedenza nella sezione relativa ai limiti di accesso da parte dell'utente:

Standard User

Utente "standard": può usufruire del servizio per un tempo determinato, per default 1 ora (attributo RADIUS Max-Daily-Session) o trasferire un massimo predeterminato, per default di 300 Mbyte, di traffico al giorno (attributo RADIUS Max-Daily-Session-Traffic). Questa tipologia di utente viene automaticamente disconnessa al verificarsi di una delle due condizioni. Tutti i "contatori" definiti per implementare le restrizioni sono automaticamente azzerati alla mezzanotte.

Power User

Utente privilegiato, non ha limiti di traffico e tempo di connessione.

Tutte le politiche di autorizzazione, analogamente al numero di gruppi di utenze definite, sono personalizzabili.
Se l'utente non effettua alcun tipo di traffico di rete per un periodo di tempo pari a 10 minuti (configurabile, agendo sull'attributo RADIUS Idle-Timeout), il captive portal forza il suo logout.

Back-office del sistema di gestione degli accessi

Il back-office dell'OpenWISP User Management System può venire **usato dagli operatori** per effettuare una serie di operazioni di gestione delle utenze. È possibile personalizzare il sistema, ad esempio creando i seguenti profili operatore:

- Operatore addetto alla registrazione

- Possibilità di registrare nuove utenze allegando una scansione del documento di identità;
- Possibilità di effettuare ricerche tra gli utenti su base nome, cognome e documento di identità;
- Visualizzazione dei seguenti dettagli:
- stato utente (attivo/non attivo)
- data e ora di registrazione
- data e ora di attivazione
- data e ora di ultimo accesso

Figura 6 – Back-office: modifica utenze

- Operatore di help-desk
  - Possibilità di effettuare ricerche tra gli utenti su base dati di profilo
  - Visualizzazione dei seguenti dettagli:
    - dettagli profilo
    - data e ora di registrazione
    - modalità di registrazione
    - data e ora dell'attivazione
    - log degli accessi
    - dati di consumo

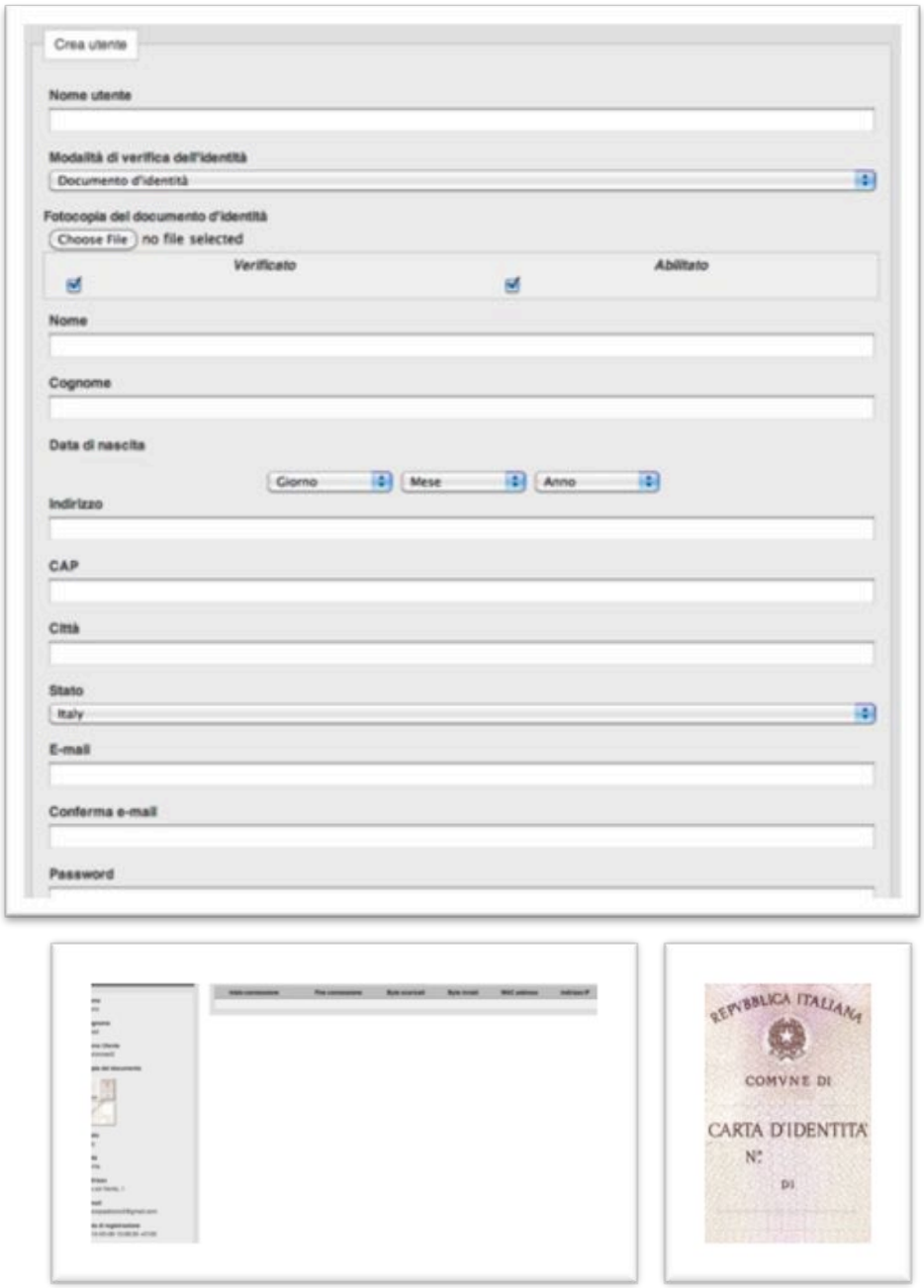

Figura 7 – Back-office: creazione utenza con upload documento d'identità

- Amministratore delle utenze
    - Possibilità di visualizzare, in forma aggregata, il numero di utenti registrati, il numero di utenti attivati, il numero di utenti collegati, con relative serie storiche;
    - Possibilità di effettuare ricerche utente su base dati di profilo
    - Visualizzazione dei seguenti dettagli:
        - dettagli profilo
        - data e ora di registrazione
        - attivazione
        - log degli accessi
        - dati di consumo

- Procedura di modifica dei dati dell'utente, con possibilita di modifica del gruppo d'utenza.

Per accedere al back-office dell'OpenWISP User Management System gli operatori possono richiamare una URL specifica e autenticarsi opportunamente.

2.8 *Front-office* del sistema di gestione degli accessi

Sulle *captive pages*, verso cui sono ridiretti i browser di tutti gli utenti, qualora non siano ancora autenticati, è fornito un link al sistema di front-office per la gestione degli accessi. Il front-office dell'OpenWISP User Management System costituisce l'interfaccia con la quale **gli utenti finali** del servizio possono svolgere tutte le attività di registrazione, auto-assistenza e auto-gestione, tra cui recupero password, consultazione delle informazioni personali e dei dati di navigazione.
Il sistema di front-office per la gestione è anche disponibile in versione mobile, con la rilevazione automatica della tipologia del dispositivo.

Figura 8 - Auto-gestione utenza: istruzioni e accesso

Figura 9 - Auto-gestione utenze: interfaccia mobile

2.9 Registrazione utenti tramite OpenWISP *User Management System*

In conformità alla normativa vigente in merito alla fornitura di servizi pubblici di connettività Internet, la registrazione autonoma degli utenti si avvale principalmente dell'identificazione tramite SIM/USIM di un operatore di telefonia italiano. In alternativa, è possibile implementare un meccanismo di identificazione mediante carta di credito.

Come descritto nella sezione "Back-office", è possibile inoltre creare nuove utenze mediante l'identificazione "de-visu" effettuata da personale incaricato.
Indipendentemente dal tipo di auto-registrazione, sarà chiesto agli utenti di specificare i seguenti dati personali:

- nome e cognome;
- numero di telefono cellulare (solo nel caso di identificazione via SIM/USIM);
- Indirizzo e-mail;
- userid e password per l'accesso al servizio.

Il sistema prevede la possibilità di disabilitare le utenze, in modo autonomo o decorso un periodo di tempo configurabile dall'ultimo utilizzo. Per abilitare nuovamente un'utenza sarà necessario ripetere la procedura di attivazione.
Le auto-registrazioni effettuate con SIM/USIM, quelle effettuate con carta di credito e le registrazioni effettuate de-visu sono conformi alla normativa vigente.

Registrazione online tramite SIM/USIM

Questo tipo di registrazione, lo stesso utilizzato per il WISP Provinciawifi, richiede che l'utente dimostri il possesso di un'utenza di telefonia mobile di un operatore italiano. L'utenza sarà abilitata solo in seguito alla verifica del numero di telefono specificato.

Figura 11 - OpenWISP User Management System – Front-office - Registrazione nuova utenza via telefono cellulare operatore Italiano

Nel dettaglio, il sistema di attivazione degli account richiede che l'utente effettui una chiamata dal numero inserito in fase di registrazione verso un numero di rete fissa (decade 0) associato ad un'utenza Voice over IP (VoIP). Un sistema automatico acquisisce il Caller-id del chiamante e, nel caso in cui esso sia associato a un'utenza non ancora attivata, provvede ad abilitare quest'ultima alla fruizione del servizio. La chiamata viene quindi chiusa senza costi per il chiamante. Il risultato del processo viene notificato all'utente mediante un'apposita pagina web e mediante posta elettronica.

Qualora l'utente non effettui la chiamata entro un periodo di tempo T (configurabile) dalla registrazione, il sistema provvede alla rimozione dei dati inseriti da quest'ultimo.
Il sistema ha inoltre le seguenti funzionalità:

- inibizione della registrazione di più account su uno stesso numero di cellulare;
- verifica dell'appartenenza del numero di cellulare alla classe di numerazione italiana;
- configurazione, modifica e aggiunta di classi di numerazione differente, anche internazionale.

Si osservi che il sistema di registrazione online mediante SIM/USIM prevede l'utilizzo di un numero di telefono relativo a un servizio di telefonia VoIP basato su SIP. Tale servizio è gestito da Cineca e viene dimensionato a seconda del numero di utenti previsti dall'Amministrazione.

Registrazione con carta di credito

Al fine di consentire la registrazione di utenti privi di un numero di telefonia mobile rilasciato da un operatore italiano, il sistema può essere integrato con il servizio Gestpay offerto da Banca Sella. Ciò consente di ottenere un'identificazione sicura dell'utente verificando la titolarità della carta di credito. La procedura di inserimento dei dati deve essere completata entro 10 minuti.
Questa modalità di registrazione prevede, successivamente all'inserimento dei dati della carta di credito, il redirect del browser sul sistema di registrazione all'interno del profilo utente.
L'utente non ha alcun costo per usufruire del servizio.

Figura 10 Maschera di inserimento dei dati della carta di credito

Si osservi che la conformità alla vigente normativa è assicurata dalla memorizzazione dell'identificativo della transazione, che costituirà l'unico metodo per risalire con certezza all'identità dell'utente.

Con il sistema d'identificazione mediante carta di credito, gli estremi utilizzati per le disposizioni di pagamento non sono mai gestiti dalle applicazioni del WISP. Come risultato si svincola l'Amministrazione dagli oneri connessi al trattamento di tali dati.

3. Openwifi e le Federazioni

FreeitaliaWiFi

La soluzione Cineca è predisposta per l'integrazione della rete WiFi dell'Amministrazione in FreeItaliaWiFi, federazione di reti WiFi delle amministrazioni pubbliche. FreeItaliaWiFi è stata fondata da Provincia di Roma, Comune di Venezia e Regione Sardegna, ed ha ricevuto l'adesione di numerose altre Amministrazioni locali.

Gli utenti delle reti WiFi di un'Amministrazione aderente a FreeItaliaWifi hanno la possibilità di autenticarsi con le stesse credenziali presso le reti WiFi delle altre Amministrazioni aderenti. Questo permette ai cittadini di spostarsi per l'Italia senza dover creare nuove utenze su tutte le reti WiFi delle Amministrazioni locali in cui si recano.

IDEM ed eduroam

Grazie ad un accordo di collaborazione con GARR, la soluzione CINECA, è predisposta per annunciare le reti *IDEM* ed *eduroam* su tutti gli access poimt.
Le **Università** e gli **Enti di ricerca** (definiti anche Identity Provider) ai quali appartengono gli utenti che utilizzano queste due reti sono le **sorgenti autoritative**.

IDEM è la Federazione di Autenticazione e Autorizzazione delle organizzazioni che appartengono alla rete GARR.
In questo caso il servizio di autenticazine offerto da CINECA è in modalità Captive Portal.
Per accedere alla rete, i docenti, i ricercatori e gli studenti, si collegheranno all'ESSID *idem*. Al primo tentativo di richiesta di una pagina web verranno rediretti sul Captive Portal CINECA (service provider registrato nella Federazione IDEM).

Scegliendo l'autenticazione federata verranno rediretti sul servizio *WAYF* (Where Are You From) di GARR dove potranno selezionare l' Identity Provider. A questo punto l'utente verrà rediretto sulla pagina di autenticazione dell'Identity Provider dove immetterà le credenziali precedentemente fornitegli. Concluso il processo di autenticazione, l'utente può proseguire la navigazione Internet. L'attributo richiesto per

poter accedere al servizio è *edupersonPrincipalName.*

eduroam è il servizio che offre, su scala mondiale, un accesso wireless sicuro alla rete ed è un marchio registrato di TERENA.
In questo caso il servizio di autenticazione offerto da CINECA è in modalità WPA2/802.1x.
Per accedere alla rete, i docenti, i ricercatori e gli studenti si collegheranno all'ESSID *eduroam.*
Previa configurazione del proprio dispositivo di accesso alla rete (la configurazione è indicata dall'ente di appartenenza), gli utenti potranno autenticarsi alla rete attraverso il proxy radius CINECA (Service Provider registrato nella Federazione Eduroam) utilizzando lo standard 802.1x.

Tipicamente i collegamenti tra gli access point ed i Service Provider eduroam ed idem sfruttano connessioni VPN *layer 2.*

4. Riferimenti normativi

- Delibera AGCOM 26 novembre 2008 666/08/CONS Regolamento per l'organizzazione e la tenuta del registro degli operatori di comunicazione;
- Decreto Ministeriale (Gasparri) 28 Maggio 2003 Condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso Radio-LAN alle reti e ai servizi di telecomunicazioni;
- Decreto Ministeriale (Landolfi) 4 ottobre 2005, Condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso radio LAN alla rete e ai servizi di telecomunicazioni;
- Decreto Legislativo 30 giugno 2003 n. 196 Codice in materia di protezione dei dati personali, e s.m.i.;
- Decreto Legislativo 1 agosto 2003 n. 259/2003 Codice delle comunicazioni elettroniche, e s.m.i.;
- Decreto Legislativo 30 maggio 2008 n. 109, "Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE";
- Legge 31 luglio 2005, n. 155, Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale, e s.m.i.;
- Con riferimento alle modalità di accesso Wi-Fi in ambito pubblico e alle misure relative all'identificazione dell'utente si specifica che, con nota del 27 novembre 2007, il Ministero dell'interno – dipartimento della pubblica sicurezza ha ritenuto che per soddisfare i requisiti della norma vigente (decreto legislativo n. 144/05 convertito con modificazioni con legge n. 155/05) sia sufficiente l'utilizzo di una SIM/USIM, quale mezzo per attivare le procedure necessarie a ottenere le credenziali di accesso alla rete, in quanto consente l'identificazione seppur indiretta dell'utente. Il Ministero ha

ulteriormente precisato che è comunque necessario che la messaggeria sia veicolata attraverso una carta SIM/USIM rilasciata all'utente nel rispetto delle disposizioni, relative all'identificazione dell'utente, stabilite dall'art. 55 del decreto Legislativo n. 259/03, con conseguente esclusione delle SIM/USIM rilasciate da Paesi stranieri.

- Decreto Legislativo 29 giugno 2010, n.128 - "Modifiche ed integrazioni al decreto legislativo 3 aprile 2006, n. 152, recante norme in materia ambientale, a norma dell'articolo 12 della legge 18 giugno 2009, n. 69" - pubblicato nella *Gazzetta Ufficiale* n. 186 dell'11 agosto 2010 - Suppl. Ordinario n. 184.
- Decreto legislativo 9 agosto 2013, n. 98 - "Conversione, con modificazioni, del decreto-legge 21 giugno 2013, n. 69. Disposizioni urgenti per il rilancio dell'economia"