

Allegato 1

Documento Unico di Specifiche Tecnico-Funzionali per fornitura, posa, installazione, configurazione della nuova rete wireless ospedaliera e relativa formazione all'uso della stessa

Introduzione

La rete Wi-Fi attuale di ISMETT utilizza lo standard 802.11b. ISMETT intende dotarsi di nuovi dispositivi in grado di costituire il nucleo di una rete di nuova generazione più performante, scalabile e sicura ma funzionalmente coerente con la rete esistente al fine di mantenere la continuità del servizio.

Una rete Wi-Fi così migliorata in grado di attuare una separazione fra i servizi che sono veicolati e la rete stessa, consentirebbe l'adozione di nuovi servizi ad uso interno quali, ad esempio, il tracciamento di apparati medicali e il supporto di apparati IOT

I nuovi dispositivi Wi-Fi che costituiranno la rete debbono essere dotati dello standard 802.11ac, i dispositivi di networking debbono essere in grado di gestire sezioni della rete al fine di garantire una migliore scalabilità, minori punti di controllo e stabilità più elevata.

La fornitura deve comprendere una soluzione integrata in grado di gestire e monitorare, attraverso un'unica interfaccia i dispositivi della rete presenti nella nuova infrastruttura wireless (i.e. access point, wireless controller e dispositivi di networking, dispositivi di localizzazione).

Si richiede inoltre, una piattaforma in grado di effettuare servizi di localizzazione avanzati in grado di utilizzare le informazioni sulla posizione e la presenza di dispositivi provenienti dall'infrastruttura wireless. Questa elaborazione deve essere fornita fuori banda affinché la rete non subisca rallentamenti e non venga ostacolata la scalabilità.

La soluzione completa dovrà quindi essere composta dalle seguenti macro-componenti:

- A. Infrastruttura di rete wireless borderless;
- B. Software di gestione;
- C. Soluzione di localizzazione dispositivi.

Gli apparati oggetto di offerta e fornitura possono essere anche non perfettamente corrispondenti a quanto di seguito descritto a condizione che vengano rispettati i requisiti minimi richiesti per ciascuna tipologia e che siano equivalenti sotto il profilo prestazionale.

Requisito essenziale è che l'intera fornitura provenga dallo stesso produttore al fine di semplificare le operazioni di gestione e di minimizzare il rischio di incompatibilità fra produttori differenti.

Per tutti i prodotti è richiesto un servizio di assistenza NBD (next business day) della durata di 12 mesi dal collaudo, con intervento entro il giorno lavorativo successivo.

Inoltre, è richiesto il servizio di posa, installazione e configurazione degli apparati e formazione del personale.

1.1 Infrastruttura di rete wireless borderless;

L'infrastruttura wireless sarà costituita da (access point) coordinati centralmente da una coppia di controller (Wireless LAN Controller) in alta affidabilità, per la gestione fisica e logica, e dal software di definizione delle Policy per quel che riguarda la sicurezza di accesso unificata e senza fili.

Tale infrastruttura dovrà supportare gli ultimi standard tecnici e qualitativi, dovrà consentire il monitoraggio e generare gli alert relativi ad usi impropri della rete stessa (Rogue Access Points), dovrà essere abilitante nella fornitura di servizio di Guest Access, e dovrà gestire ed ottimizzare l'utilizzo dell'etere attraverso sistemi quali ClientLink e Clean Air, sistemi cioè che sono in grado di supportare grossi carichi della rete senza ridurne le performance anche in presenza di altri apparati radio che generano interferenze.

1.1.1 Access Point

In particolare sono richiesti 100 AP. In ogni caso i requisiti minimi che gli AP devono rispettare sono:

- conformità alla normativa 802.11ac wave 2 con supporto di 2x2 multi user MIMO e 2 spatial stream
- disponibilità di funzione Radio Resource Management (in collaborazione con il Controllore): capacità di gestire la copertura complessiva in modo dinamico, gestendo automaticamente i canali e le potenze di trasmissione di tutti gli AP, mitigando eventuali fault di AP.
- Funzionalità di beamforming su tutti i protocolli 802.11g/a/n/ac indipendentemente dal client, per il miglioramento delle prestazioni in trasmissione. La tecnologia beamforming implementata deve essere standard per il protocollo 802.11ac
- Capacità di analisi dello spettro e individuazione delle interferenze effettuato dal singolo Access Point, con individuazione della sorgente, localizzazione e modifica ai parametri trasmissivi per l'ottimizzazione delle performance, senza impatto sulle prestazioni.
 - Doppia radio a bordo con impiego flessibile della seconda radio. L'AP deve potere funzionare con una radio nella banda di frequenza a 2,4 GHz e l'altra a 5 GHz o con entrambe le radio nella banda di frequenza 5 GHz
 - Integrated Bluetooth low energy 4.1 radio
 - Disponibilità di due interfacce 10/100/1000BASE-T autosensing (RJ-45)
 - Supporto di vari metodi di autenticazione tra cui WPA2™ – Enterprise, Personal con i seguenti tipi di EAP :
 - EAP-TLS
 - EAP-TTLS/MSCHAPv2
 - PEAPv0/EAP-MSCHAPv2
 - PEAPv1/EAP-GTC
 - EAP-SIM
 - EAP-FAST

1.1.2 Wireless Lan Controller

I WLC proposti, dovranno fornire un ampio set di opzioni di instradamento dei servizi e delle applicazioni, un'interfaccia Web che permetta all'amministratore della rete di definire profili multipli

per gli utenti, che comprendano la priorità del traffico, l'utilizzo della banda, l'accesso guest e le politiche di sicurezza. Queste politiche sono flessibili e possono essere applicate per utente, gruppo o applicazione

Sono richiesti due controllori (WLC) in configurazione alta affidabilità con licenze per gestire almeno 100 Access point, dovranno essere in grado di gestire ciascuno almeno 20.000 client e di controllare ciascuno almeno 1500 access point.

I dispositivi dovranno essere dotati inoltre di alimentazione ridondata, dovranno essere compliant al nuovo standard 802.11ac ed essere dotati ciascuno di 2 x 10 Gigabit porte di uplink (SFP+) per garantire alte performance fino a 20 Gbps di throughput del traffico wireless.

In caso di guasto di un controllore il passaggio di client e AP dal controllore attivo a quello in ridondanza calda deve avvenire in tempi inferiori al secondo per non interrompere le applicazioni in corso.

Il controllore deve inoltre rispettare i seguenti requisiti minimi:

- Supporto standard IEEE 802.11a/b/g/n/ac.
- Supporto multi SSID, VLAN to SSID mapping (protocollo IEEE 802.1Q);
- Supporto AP Group
- Supporto WLAN to VLAN mapping & WLAN to AP Group assignment;
- Il Controller deve consentire di indirizzare il traffico utente in locale (Local Forwarding) o verso un punto centralizzato (Centralized Forwarding). La scelta deve essere possibile per singola WLAN;
- Supporto client roaming: nell'ipotesi di controller multipli si richiede il supporto del roaming intra-controller;
- Supporto configurazione Mesh
- Supporto di funzioni di Wireless Intrusion Detection (WIDS) con possibilità di rilevare Rogue AP
- Supporto di tecniche di Wireless QoS (classificazione e packet marking)
- Supporto dei principali standard di riferimento per la sicurezza e la cifratura:
 - Wi-Fi Protected Access (WPA)
 - IEEE 802.11i (WPA2)
 - Wired Equivalent Privacy (WEP) and Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC): RC4 40, 104 and 128 bits (both static and shared keys)
 - Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
- Supporto dei principali metodi di autenticazione:
 - IEEE 802.1x, database locale; server esterni AAA: Active Directory, RADIUS, LDAP;
 - RFC 3579 RADIUS Support for EAP
 - RFC 3748 Extensible Authentication Protocol (EAP)
 - Web-based authentication
 - MAC Address authentication
 - Captive Portal: locale e/o esterno.

Il software richiesto deve assicurare e semplificare la gestione della rete wireless e wired oggetto della presente proposizione (i.e. endpoint, apparati attivi e passivi).

Il sistema di gestione deve essere quindi in grado di consentire funzioni di monitoring centralizzato, provisioning, configurazione e controllo. Deve assicurare inoltre meccanismi di Context-aware security gestendo la sicurezza dell'accesso alla rete ed ai servizi in base al contesto in cui si opera (client, device, policy), identificare in maniera granulare qualsiasi dispositivo che richiede l'accesso all'infrastruttura, indipendentemente dalla modalità, dal luogo o dalla tipologia; controllare il collegamento di ogni dispositivo direttamente dal primo punto di accesso in modo da eliminare alla fonte possibili rischi di infezione o di intrusione non autorizzata; definire dei controlli automatici basati sulla tipologia dell'utente (User Profiling).

La piattaforma dovrà essere interamente virtualizzata, installata quindi su macchine virtuali fornite da questa amministrazione basate su Microsoft Hyper-V, e dovrà essere garantita l'affidabilità, la robustezza e la disponibilità dei servizi.

Tale piattaforma dovrà avere un licensing di durata illimitata e modulare, potranno essere acquistati blocchi di licenze in funzione del numero di endpoint client e device (apparati dell'infrastruttura).

In particolare, per l'infrastruttura WiFi il Sistema di Gestione e Monitoraggio dovrà:

- prendere in carico tutti i componenti della piattaforma WiFi regolandone il corretto funzionamento e consentendo facilità di monitoraggio, risoluzione dei problemi, logging e reporting.
- gestire la configurazione e le modifiche di tutti gli AP e tutti i Controller proposti.
- permettere agli operatori di aggiornare il firmware degli apparati
- permettere la consultazione via GUI, tramite accesso con Username e Password, dello stato dell'infrastruttura e dei suoi componenti.
- collezionare dati relativi all'utilizzo del sistema (es. traffico in/out, numero di macaddress per AP, etc.).
- includere strumenti grafici di pianificazione per il corretto dimensionamento dell'infrastruttura wireless per il supporto del traffico dati, voce e di applicazioni di localizzazione
- includere strumenti di troubleshooting per un'analisi step-by-step dei problemi e di errori di configurazione dei client wireless (es. problemi di autenticazione 802.1x)
- includere strumenti di gestione di problematiche di sicurezza wireless, con possibile integrazione con sistemi di Wireless IPS (Intrusion Prevention System)

1.3 Soluzione di localizzazione dispositivi

E' richiesta una piattaforma di localizzazione in grado di individuare la posizione di un dispositivo WiFi sulle mappe grafiche. Oltre alla posizione in tempo reale si richiede la memorizzazione di dati storici.

Gli oggetti da localizzare sono i dispositivi WiFi di uso comune ma anche tag RFID attivi. A questo proposito si richiede la fornitura di 20 tag attivi da impiegarsi per localizzare sia oggetti, come ad esempio strumenti medicali, che persone.

Il sistema deve operare sia sui dispositivi associati che su quelli non associati alla rete WiFi.

E' inoltre richiesto che il sistema consenta la presentazione di dati statistici riassuntivi su presenza di client WiFi in determinate zone nelle varie ore del giorno o nei giorni della settimana.

1.4 Posa, installazione e configurazione apparati

Gli Access Point necessitano di essere correttamente posizionati, al fine di garantire adeguati livelli di segnale evitando zone d'ombra e garantendo uniformità di copertura radio.

I punti di posizionamento degli AP, verranno determinati tramite il Survey della struttura da effettuare con la super visione di ISMETT.

Entro 7 giorni solari dall'ordine definitivo il fornitore deve fare il sopralluogo per determinare il posizionamento degli Access Point.

La fornitura comprende la posa e l'installazione materiale degli AP, nonché la fornitura e installazione di tutti gli accessori necessari (ad esempio fissaggi a parete e/o a soffitto, patch di collegamento al punto di rete, predisposto in prossimità, entro una distanza massima di 100mt) alla realizzazione e configurazione a regola d'arte del sistema

L'impresa aggiudicataria dovrà presentare un piano di installazione e formazione entro 7 giorni dall'aggiudicazione.

ISMETT dovrà approvare i piani di cui sopra entro 7 giorni dalla presentazione.

Fornitura, installazione di tutti gli apparati, configurazione del sistema a perfetta regola d'arte e collaudo positivo del medesimo sistema dovranno avvenire entro 45 giorni solari dall'approvazione del piano di installazione da parte di ISMETT.

5

1.5 Formazione

L'installazione e la messa in esercizio dell'intero sistema, dovrà includere un piano di formazione del personale dell'Istituto, che preveda i due livelli: gestione operativa del servizio, configurazione e gestione generale del sistema wireless.

La formazione dovrà essere articolata in sessioni che prevedano sia gli aspetti teorici che esercitazioni pratiche, dovrà essere effettuata presso la sede indicata dall'Istituto e dovrà comprendere un minimo di 16 ore di formazione, da erogare in moduli di 4 ore.

La formazione dovrà essere erogata da docenti in possesso di adeguata certificazione del Produttore Hardware.

La formazione dovrà essere erogata ed ultimata entro 30 giorni dal collaudo definitivo del sistema.

La fornitura di che trattasi è finanziata a mezzo del progetto: **“Potenziamento Infrastruttura di Ricerca GMP Facility, Laboratori di Ricerca e Servizi Diagnostici e Terapeutici dell'Istituto**

Mediterraneo per i Trapianti e le Terapie ad Alta Specializzazione (IRCCS-ISMETT)”. Il CUP di progetto è G76G17000130007.

La documentazione contabile della fornitura (ordine, fattura, pagamento) conterrà altresì la seguente dicitura:

“PO FESR 2014/2020. Azione 1.5.1 – Sostegno alle infrastrutture di ricerca considerate strategiche per i sistemi regionali ai fini dell’attuazione della S3” – nota del 13 gennaio 2017, prot. n. 1705 del Dipartimento Regionale delle Attività Produttive Servizio 5 – Assessorato Attività Produttive della Regione Siciliana. CUP G76G17000130007”.