Comune di Padova

Settore Servizi Informatici e Telematici

CAPITOLATO TECNICO

"Estensione copertura Wi-Fi cittadino 2018"

RDO n. XXX: GARA PER L'ESTENSIONE DI COPERTURA DEL Wi-Fi PUBBLICO DEL COMUNE DI PADOVA

Il Capo Settore SS. II. TT.

Ing. Alberto Corò

Sommario

1 PREMESSA

Il Comune di Padova intende estendere l'attuale copertura del Wi-Fi pubblico fornito gratuitamente ai cittadini dal Comune di Padova ed identificato come “PadovaWeb”.

Con questo progetto si intende coprire o migliorare la copertura delle zone di grande aggregazione, come le principali piazze del centro storico nonché zone di interesse turistico e culturale, come i musei comunali. Si intendono inoltre sostituire gli attuali apparati WiFi con tecnologia HP che ormai da diversi anni sono “end-of-life” e quindi obsoleti, infatti non si trovano più in commercio e non è più possibile stipulare contratti di manutenzione

Negli ultimi anni, il Comune di Padova ha coperto le sedi di maggior interesse pubblico, come il Centro Culturale San Gaetano, con apparati Wi-Fi di nuova tecnologia. Questa tecnologia è stata scelta in quanto si è visto sul campo che, rispetto ad altri competitor, hanno una migliore copertura, una notevole immunità alle interferenze con altri segnali radio Wi-Fi, specie nelle piazze e permettono una configurazione semplificata in fase di installazione (“zero configuration”).

Punto forte di questa tecnologia è la creazione di una “virtual cell” ovvero di un unico Access Point (AP) virtuale tra vari AP della stessa tecnologia distribuiti in una grande area, ad esempio un palazzo o una piazza. Questo permette un roaming praticamente istantaneo tra gli AP senza disconnessione per l'utente che si muove. Viene inoltre sempre garantito il migliore segnale WiFi agli utenti facendoli connettere in automatico all'AP più vicino ottimizzando la potenza trasmessa.

Tutto questo si traduce in un migliore servizio offerto ai cittadini.

Nel corso di questi ultimi anni il Comune di Padova ha investito molto, in termini di denaro e tempo, per implementare l'attuale architettura del WiFi cittadino.

2 OGGETTO DEL CAPITOLATO

Il presente capitolato contiene le specifiche tecniche relative alla fornitura degli apparati Wi-Fi necessari alla realizzazione dell'estensione della copertura del servizio Wi-Fi cittadino, compresa la sostituzione degli attuali apparati a tecnologia HP ormai obsoleti e non più manutenibili.

Sono compresi, oltre alla fornitura degli apparati, i servizi di consegna, la configurazione ed installazione del controller, i servizi di supporto all’avviamento, garanzia annuale, nonché il servizio di manutenzione sia sugli apparati oggetto della presente fornitura che sull’esistente.

Non è oggetto del presente appalto l'attività di installazione degli AP.

2.1 DEFINIZIONI ED ACRONIMI

Nel corpo del capitolato, ai termini di cui appresso, viene attribuito il significato riportato a fianco di ciascuno di essi:

- **AP:** Access Point, la porta radio Wi-Fi da installare.
- **Controller:** il dispositivo che sovraintende alla gestione e configurazione di tutti gli AP.

- **Capitolato Tecnico:** il presente documento.
- **Fornitura**: la vendita del sistema e di tutti i relativi servizi.
- **SS.II.TT.:** il Settore Servizi Informatici del Comune di Padova.
- **Amministrazione:** Comune di Padova.
- **Ditta:** la ditta aggiudicataria.

3 DESCRIZIONE DEL SISTEMA

3.1 CONTESTO ATTUALE

L'attuale sistema WiFi del centro storico è composto da:

- **1 controller Fortinet FortiWLC-200D** in grado di gestire fino a 200 AP.
- **71 AP Fortinet/Meru AP832e(i) da interno** installati presso varie sedi.

3.2 CONTESTO FUTURO

Si vuole estendere l'attuale sistema del centro storico basato su tecnologia Fortinet/Meru e gli apparati oggetto di questa gara devono quindi integrarsi perfettamente ed essere quindi pienamente compatibili con gli attuali in possesso del Comune di Padova basati su tecnologia Fortinet/Meru. Le modalità di estensione sono le seguenti:

1. Nella sala server del SS.II.TT., assieme all'attuale **FortiWLC-200D**, si installerà un nuovo controller **tipo Fortinet FortiWLC-500D** per estendere la capienza dell'attuale portandola a 500 AP. Il nuovo controller dovrà inoltre essere in grado di gestire almeno 6000 client contemporaneamente. Questo nuovo controller dovrà sovraintendere a tutti gli AP oggetto di questa gara e ai Fortinet/Meru già installati.
2. Per minimizzare il caso di "single point of failure", l'attuale controller, il Fortinet **FortiWLC-200D**, fungerà da "fall back" ovvero da riserva nel caso il nuovo controller si guasti e/o sia in manutenzione programmata. Naturalmente questo potrà gestire solo 200 AP che verranno decisi da questa Amministrazione . Il "fall back" dovrà essere automatico e trasparente: in caso di guasto del nuovo controller, gli AP, inclusi gli attuali già installati, dovranno attestarsi sul **FortiWLC-200D** senza alcun intervento manuale. Analogamente, quando il nuovo controller ritornerà online, gli AP, inclusi gli attuali già installati, dovranno ritornare ad attestarsi sul nuovo controller senza alcun intervento manuale.
3. Nella sala server del SS.II.TT., assieme ai due controller ci sarà un'appliance hardware (non virtuale) **tipo FortiConnect**, che dovrà fungere da Identity Manager per tutti gli AP Fortinet/Meru installati e quelli oggetto di questa fornitura. Questa appliance dovrà inoltre integrarsi perfettamente con i su menzionati controller.
4. Sul territorio comunale, piazze, palazzi ed edifici, vi saranno svariati AP: quelli già installati basati su tecnologia Fortinet/Meru ed i nuovi perfettamente intercambiabili con gli attuali.

Tutti, nuovi e già installati, dovranno essere gestiti dal nuovo controller e dal precedente **FortiWLC-200D** senza necessità di alcuna patch software lato controller e/o lato AP.

Si intende estendere la copertura dei seguenti luoghi:

- Museo Eremitani e Cappella degli Scrovegni
- Palazzo Zuckermann
- Piazza Cavour con annesso museo
- Teatro Verdi
- Prato della Valle
- Completamento Piazze del centro

Su tutto il sistema così realizzato, l'attuale e l'estensione, si prevede un servizio di manutenzione.

4 SPECIFICHE DELLA FORNITURA

4.1 OGGETTO DELLA FORNITURA

I seguenti apparati e servizi sono oggetto delle fornitura. Verranno dettagliati più sotto.

Le forniture proposte dovranno avere avere caratteristiche analoghe o superiori a quelle sotto elencate:

Descrizione	**Quantità**
Access Point tipo Fortinet/Meru modello AP832e o superiore completi di antenna omnidirezionale	75
Access Point tipo Fortinet/Meru modello AP832i o superiore	10
Access Point tipo Fortinet/Meru modello AP122 o superiore	45
Access Point da esterno tipo Fortinet/Meru modello FAP-U422EV-E o superiore completi di antenna omnidirezionale	51
Wireless Controller tipo Fortinet/Meru FortiWLC-500D. Inclusa fornitura, installazione e configurazione. Inclusa la manutenzione per il primo anno e e servizio Help Desk	1
Appliance (apparato hardware, no Virtual Machine) tipo FortiConnect per autenticazione degli utenti WiFi con licenza per 10.000 utenti. Inclusa fornitura, installazione e configurazione. Inclusa la manutenzione per il primo anno e servizio Help Desk	1
Giornate di supporto all'avviamento	5

Tutte le componenti di fornitura sopra elencate sono da ritenersi come riferimento e le caratteristiche tecniche dei prodotti che saranno offerti dovranno avere caratteristiche analoghe o superiori. Nel caso di fornitura di prodotti analoghi, sarà cura dell'offerente presentare un quadro comparativo delle specifiche tecniche all'atto della stipula del contratto.

Tutte le componenti oggetto della forniture, tranne che per gli AP, si intendono complete di consegna, installazione e configurazione. Per gli AP si intende compresa la sola consegna in quanto l'installazione sarà a cura di questa Amministrazione. La consegna, l'installazione e la configurazione non vanno ad erodere in alcun modo le ore dedicate al "Supporto all'avviamento".

4.2 WIRELESS CONTROLLER

Numero 1 (**uno**) apparati tipo **Fortinet FortiWLC-500D** con capacità di gestire e configurare almeno **500 AP e 7500 utenti** contemporanei.

La fornitura include l'installazione e la configurazione. È inclusa anche la manutenzione per il primo anno dal collaudo il e servizio Help Desk

Questo Wireless Controller non dovrà richiedere alcuna licenza o altro onere da rinnovare a cura di questa Amministrazione per tutta la durata della sua vita, anche se non venisse rinnovato annualmente il contratto di manutenzione.

Le forniture proposte dovranno quindi avere avere caratteristiche analoghe o superiori a quelle sotto elencate:

HW Interfaces	
10/100/1000 Interfaces (Copper, RJ-45)	4
GE SFP Port	4
10 GE SFP+ Port	2
Console Port (RJ45, serial)	1
Capacity	
Maximum Access Points	500
Maximum Clients	7,500
Security	

Access Control	WEP, WPA-PSK, WPA-TKIP, WPA2-AES, 802.11i, 802.1X (EAP-TLS, EAP-TTLS, PEAP, LEAP, EAP-FAST, EAP-SIM, EAP-AKA, and EAP-MD5) Captive portal authentication against local database on the controller, RADIUS, and Active Directory RADIUS-assisted per-user and per-ESSID access control via MAC filtering
Policy	Per-user firewall with fine-grained policy management: admission control, packet prioritization, QoS flows, packet drop policy, bandwidth scaling, filter ID, network protocol, and source port filtering. System-configured or per-user, RADIUS-configured firewall policies
Management & Networking	
Zero Configuration	Access points automatically discover controllers and download configuration settings for zero-touch, plug-and-play deployment
System Management	Upgrades and management using System Director/Network Manager, support for SNMP, centralized WLAN security policies with multiple ESS profiles, VLAN-specific administrative/security policies
Intelligent RF Management	Coordination of access points with load balancing for predictable performance
VLAN Support	IEEE 802.1Q VLAN tagging, GRE Tunneling
QoS	WMM support, dynamic WMM rate adaptation, configurable QoS rules per user and application

Tutte le componenti di fornitura sopra elencate sono da ritenersi come riferimento e le caratteristiche tecniche dei prodotti che saranno offerti dovranno avere caratteristiche analoghe o superiori. Nel caso di fornitura di prodotti analoghi, sarà cura dell'offerente presentare un quadro comparativo delle specifiche tecniche all'atto della stipula del contratto .

Il controller dovrà già essere licenziato per almeno **500 AP e 7500** utenti contemporanei.

Il controller dovrà essere dotato del software necessario alla gestione e monitoraggio degli AP. Anche questo software non dovrà essere soggetto ad alcuna licenza da rinnovare.

Il nuovo controller dovrà gestire i precedenti AP con tecnologia Fortinet/Meru, già in possesso del Comune di Padova e i nuovi, oggetto di questa gara. Il controller dovrà quindi essere compatibile con essi garantendone la piena funzionalità.

L'Amministrazione non dovrà corrispondere alcuna licenza o altro onere alla Ditta o alla Ditta da cui sono stati acquistati i precedenti AP, per permetterne il pieno funzionamento.

Altra caratteristica imprescindibile per questa fornitura è la modalità "**Rogue AP Detection**" ovvero la capacità di individuare falsi AP installati per uso fraudolento come ad esempio rubare numeri di carte di credito, password, ecc.

Questo nuovo controller verrà installato a cura della Ditta in sala server al SS.II.TT. assieme al già presente **FortiWLC-200D**.

La fornitura del controller deve comprendere tutti gli accessori meccanici per montaggio a RACK, alimentatore e cavetteria necessaria.

4.3 ACCESS POINT

Il progetto prevede l'acquisto di **181 AP perfettamente compatibili con il controller Fortinet FortiWLC-200D già installato, il nuovo controller tipo Fortinet FortiWLC-500D e l'Identity Manager oggetto di questa fornitura.**

La fornitura NON include l'installazione e la configurazione. Deve invece essere inclusa, per il primo anno dal collaudo e solo per gli AP oggetto di questa fornitura, la manutenzione 8x5 (8 ore per 5 giorni lavorativi) ed il servizio Help Desk. Questa si intende che nel caso di guasto di un AP di questa fornitura, la Ditta dovrà garantire il seguente servizio (c.d. swap):

- Consegna di un nuovo AP (stesso modello o superiore compatibile con il Wireless Controller e Identity Manager) presso la sede del Comune di Padova e ritiro contestuale, sempre presso la sede del Comune di Padova, del dispositivo guasto. Tutto questo senza alcun onere per l'Amministrazione.

Il servizio dovrà avere il seguente SLA:

- Ritiro dell'AP guasto e consegna di quello nuovo entro 24 ore lavorative.

Gli AP non dovranno richiedere alcuna licenza o altro onere da rinnovare a cura di questa Amministrazione per tutta la durata della loro vita.

Questi dovranno essere compatibili con il controller **FortiWLC-200D** già installato e il nuovo tipo **Fortinet FortiWLC-500D** senza l'uso di alcuna patch e/o programma o quant'altro, sia lato AP che lato controller.

Come detto, una delle principali caratteristiche degli AP attualmente installati presso questa Amministrazione è la "**virtual cell**" con tecnologia "**single channel**". Per assicurare piena compatibilità con il parco installato, gli AP di nuova fornitura dovranno funzionare con la medesima tecnologia.

Gli AP oggetto della fornitura dovranno integrarsi perfettamente con l'Identity Manager oggetto di questa fornitura e qui sotto specificato senza la necessità di alcun software non licenziato da Fortinet.

Come detto in precedenza, per imprescindibili esigenze di resilienza, deve essere possibile configurare negli AP più controller in modo che in caso il controller principale si guasti o si spenga per una manutenzione programmata, gli AP automaticamente e senza alcun intervento manuale passino al controller di "backup" e immediatamente essere operativi. Quando il controller principale ritornerà online, gli AP, inclusi gli attuali già installati, dovranno ritornare ad attestarsi su questo senza alcun intervento manuale ed essere immediatamente operativi.

Le forniture proposte dovranno avere avere caratteristiche analoghe o superiori a quelle dei modelli elencati al punto 4.1. Nel caso di fornitura di prodotti analoghi, sarà cura dell'offerente presentare un quadro comparativo delle specifiche tecniche all'atto della stipula del contratto.

Tutti gli Access Point oggetto della fornitura dovranno essere consegnati a carico della Ditta in un magazzino del SS.II.TT. che verrà indicato in fase di aggiudicazione.

4.4 IDENTITY MANAGER

Per fornire un maggiore controllo sugli accessi e permettere alle forze dell'ordine di identificare chi commette degli illeciti tramite il WiFi cittadino messo a disposizione del Comune di Padova, ci si intende dotare di un appliance (**apparato fisico, non Virtual Machine**) Identity Manager di formato 1U. Ovviamente questo deve essere perfettamente compatibile ed integrato con i due controller visti in precedenza e con gli AP (sia i nuovi che gli esistenti).

Questo dovrà essere licenziato per almeno 10.000 utenti contemporanei.

Questo Identity Manager non sarà sottoposto ad alcuna licenza o altro onere da rinnovare a cura di questa Amministrazione per tutta la durata della loro vita, anche se non venisse rinnovato annualmente il contratto di manutenzione.

Le caratteristiche dovranno essere le stesse o superiori a quelle dell'appliance Fortinet **FortiConnect**:

Supports up to 10,000 active users

Client Platforms Supported

Android 2.1 and greater

Apple iOS 7.0 and greater

Apple Mac OSX 10.7 and greater

Windows 10, Windows 7, Vista, XP SP3

Linux Ubuntu

Authenitication

Active Directory

LDAP

RADIUS / RadSec

Kerberos

Facebook

Twitter

Google Apps

SQL Database

rotocols Supported

802.1X PEAP-GTC

PEAP-MSCHAPv2

PEAP-TTLS WPA

WPA-PSK WPA2

WPA2-PSK

Supported Browsers

IE 7.0 and higher

Safari

Chrome

Firefox

Le caratteristiche tecniche dei prodotti che saranno offerti dovranno avere caratteristiche analoghe o superiori. Nel caso di fornitura di prodotti analoghi, sarà cura dell'offerente presentare un quadro comparativo delle specifiche tecniche all'atto della stipula del contratto.

4.4.1 Identity Manager formato "server"

Questa Amministrazione, in alternativa al dispositivo di cui al punto 4.4 (IDENTITY MANAGER), può prendere in considerazione la fornitura di un server in formato **1U** con installata al suo interno l'Identity Manager.

L'IM, installato all'interno del server, **deve avere tutte le caratteristiche del FortiConnect su elencate**.

Il tutto, hardware, sistema operativo e software, dovrà essere manutenuto e licenziato a cura della Ditta, ovvero questa Amministrazione considererà il tutto come un'appliance hardware e non dovrà pagare nulla alla Ditta o terzi in futuro se non il contratto di manutenzione annuale che comunque si riserva di stipulare.

Anche in questo caso **l'Identity Manager non dovrà richiedere alcuna licenza o altro onere da rinnovare a cura di questa Amministrazione per tutta la durata della sua vita, anche se non venisse rinnovato annualmente il contratto di manutenzione**. Quindi nel caso il contratto di manutenzione non fosse sottoscritto o non rinnovato in futuro, l'Identity Manager continuerà ad operare senza alcuna limitazione e l'Amministrazione non dovrà essere tenuta o costretta a pagare nulla a nessuno (ad esempio licenze per l'applicazione di Identity Manager, sistema operativo, software di virtualizzazione, ecc.).

Nel caso la ditta offra questa soluzione di tipo server, questo deve avere le seguenti caratteristiche minime e di marca preferibilmente Dell:

- Alimentazione ridondante (due alimentatori)

- Storage 2 TB in Raid 1

- 4 core

- RAM 32 Gbyte

Questa appliance (apparato hardware, no Virtual Machine) varrà installata e configurata a cura della Ditta in sala server al SS.II.TT.

La fornitura include la manutenzione specificata al punto 4.5 (MANUTENZIONE) per il primo anno.

4.5 MANUTENZIONE

La ditta dovrà garantire i servizi di manutenzione sotto specificati, sugli apparati e per i periodi di seguito specificati:

A) - durante il periodo di garanzia della durata di un anno a decorrere dal collaudo di cui al punto 5.4, su tutti gli apparati oggetto della fornitura in argomento;

B) - per la durata di un anno alla scadenza del periodo di garanzia su tutti gli apparati oggetto della fornitura in argomento;

C) - per la durata di due anni a decorrere dalla data di collaudo di cui al punto 5.4 su tutti gli apparati dell'attuale sistema descritti al punto 3.1 (CONTESTO ATTUALE)(1 controller e 71 AP).

4.5.1 Manutenzione hardware e software dei due Wireless Controller, dell'Identity Manager e supporto help desk primo livello

Manutenzione **8x5 (8 ore per 5 giorni lavorativi) con sostituzione "on site"** della macchina guasta con una nuova entro **24 ore lavorative**. Tale supporto darà diritto a tutti gli aggiornamenti (major/minor releases e patch) gratuiti del software, sia del controller che degli AP.

Supporto **telefonico** di primo livello da parte della Ditta per richieste/problematiche relative ai controller, all'Identity Manager e agli AP, come ad esempio: guasti, indagini per malfunzionamenti o anomalie (troubleshooting) con risoluzione del problema o temporaneo "workaround", richieste di cambi di configurazione (anche di rete, ad es. cambio VLAN), ecc..

La Ditta dovrà garantire una presa in carico del problema entro **4 ore solari** dalla chiamata e dovrà fornire all'Amministrazione le previsione dei tempi di ripristino.

L'unica interfaccia per l'Amministrazione sarà la Ditta che si farà carico di risolvere il problema e in nessun caso dovrà venir chiesto a questa Amministrazione di interfacciarsi con il costruttore.

Nel caso di problematiche non risolvibili direttamente dalla Ditta (ad esempio un bug), questa si dovrà far carico di contattare il costruttore aprendo i relativi ticket e monitorarne con attenzione e solerzia l'evoluzione fino alla completa risoluzione del problema.

La manutenzione in oggetto dovrà essere "on site" se non gestibile via VPN.

4.5.2 Manutenzione AP

Questa voce vale solo per l'offerta di manutenzione successiva al primo anno.

In caso di guasto di un AP (inclusi i 71 già in possesso di questa Amministrazione) la ditta dovrà garantire il seguente servizio (c.d. swap):

- Consegna di un nuovo AP (stesso modello o superiore compatibile con il Wireless Controller e Identity Manager) presso la sede del Comune di Padova e ritiro contestuale, sempre presso la sede del Comune di Padova, del dispositivo guasto. Tutto questo senza alcun onere per l'Amministrazione.

Il servizio dovrà avere il seguente SLA:

- Ritiro dell'AP guasto e consegna di quello nuovo **entro 24 ore lavorative**.

4.5.3 Condizioni generali di supporto

Sia per il Wireless Controller che per l'Identity Manager la ditta deve garantire il pieno ripristino del funzionamento delle apparecchiature.

I servizi di manutenzione e supporto dovranno in ogni caso soddisfare le seguenti condizioni:

- Gli eventuali pezzi di ricambio dovranno essere quelli originariamente previsti dai costruttori; scostamenti da questa regola dovranno essere negoziati di volta in volta con questa Amministrazione.
- Qualora la Ditta non ritenesse conveniente procedere ad una riparazione potrà, previo gradimento esplicito di questa Amministrazione, sostituire definitivamente l’apparecchiatura guasta con altra di prestazioni e funzionalità equivalenti o superiori
- Nel caso di sostituzione è previsto il ripristino degli eventuali dati esistenti (ad esempio configurazione degli AP e impostazioni di rete) al momento del guasto a carico della Ditta.

5 ATTIVITÀ

5.1 POC (Proof of Concept)

Questa Amministrazione richiederà alla ditta di effettuare, entro 10 giorni lavorativi dalla stipula, un POC per dimostrare la validità tecnica e la perfetta funzionalità della soluzione proposta; il POC dovrà essere effettuato a cura e spese della ditta.

Il POC consisterà nell'installazione presso la sala macchina del SS.II.TT. del nuovo controller, dell'Identity Manager e di tre AP di nuova fornitura. Dovrà essere dimostrata la perfetta integrazione, come detto senza l'installazione sugli apparati esistenti di software o hardware non licenziato da Fortinet, con il controller **FortiWLC-200D** e gli AP esistenti in tecnologia Fortinet/Meru. Un pool di tecnici di questa Amministrazione valuterà il pieno successo del POC. Solo a valle di questo POC verrà accettata la fornitura.

Se il POC avrà esito positivo, questa attività verrà considerata come parte dell'installazione e configurazione del nuovo controller e dell'Identity Manager. Qualora gli apparati utilizzati per il POC siano materiale usato, ad esempio provenienti da fiere o laboratori, questi andranno sostituiti da apparati nuovi e riconfigurati.

Nel caso il POC avesse esito negativo il contratto verrà risolto di diritto e la Ditta nulla potrà pretendere da questa Amministrazione.

In tal caso la Ditta dovrà riprendersi, a propria cura e spese, gli apparati e nulla le sarà dovuto.

5.2 CONSEGNA

Solo nell'ipotesi di esito positivo del POC, la consegna del materiale dovrà essere effettuata a carico della Ditta entro **30 (trenta)** giorni continuativi dalla data dell'ordine.

In ogni caso, il completamento della fornitura, intendendosi per tale l'erogazione di tutte le attività qui previste per le fasi dell'installazione, del supporto all'avviamento e collaudo, deve avvenire entro e non oltre **45 (quarantacinque)** giorni continuativi decorrenti dalla data dell'ordine.

Il materiale dovrà essere così consegnato (previ contatti con i riferimenti che verranno segnalati nella RDO):

- Wireless Controller e Identity Manager al terzo piano del SS.II.TT. in sala macchine

- AP magazzino di questa Amministrazione.

5.3 INSTALLAZIONE E CONFIGURAZIONE

Qualora non tutte le attività siano state completate con il POC (vedi paragrafo 5.1), la Ditta dovrà provvedere:

- All'installazione del nuovo Wireless Controller e Identity Manager presso il rack indicato da questa Amministrazione e situato in sala server del SS.II.TT.
- Alla configurazione del nuovo Wireless Controller e Identity Manager. Questi dovranno lavorare in sincronia tra loro e con gli attuali AP installati. Verrà fatto il setup dei seguenti profili di autenticazione per l'Identity Manager (di seguito IM) e Wireless Controller (di seguito (WC):

    - Completa identificazione degli utenti tramite protocollo Radius secondo le modalità indicate da questa Amministrazione. Il tutto dovrà essere gestito dall'IM, quindi senza alcun server Radius esterno. Dovrà essere configurata anche la schermata di login.
    - Semplice Captive Portal con il logo del Comune di Padova, le condizioni di servizio del WiFi pubblico e un “bottone” di OK per accettazione e continuare con la navigazione.
    - Come il punto precedente ma con una schermata particolare di esempio dedicata ad un evento e solo per certi AP.
    - Autenticazione, con schermata di login, con username/password predefiniti
    - Nessuna autenticazione
    - Social Login tramite Facebook, Google, ecc.
- Configurazione del “fall back” nei due WC (vecchio e nuovo).
- Al collegamento delle varie componenti del sistema in rete, secondo le specifiche indicate dall'Amministrazione.
- Al collegamento e alle relative prove di funzionamento/performance, in accordo con l'Amministrazione, dei sistemi oggetto della fornitura.
- Al tuning del sistema.
- Alla personalizzazione del sistema, qualora fosse necessaria e tecnicamente fattibile.
- Per le attività sopra descritte la Ditta dovrà dedicare una risorsa di adeguate conoscenze e competenze.

Durante lo svolgimento delle suddette attività la ditta potrà contare sulla collaborazione dei tecnici del Comune.

5.3.1 Attività a carico del Comune di Padova

- Fornire almeno un contatto tecnico con appropriati diritti di accesso ai sistemi.
- Fornire eventuali *maintenance windows* nel caso fossero richieste dalla Ditta.
- Assicurare che siano soddisfatte tutte le richieste ambientali e operative prima dell’implementazione.
- Fornire l’accesso ai sistemi tramite rete VPN alla rete aziendale per eseguire le attività durante il normale orario di lavoro, o in un determinato intervallo temporale concordato con la Ditta.
- Fornire il supporto tecnico al personale messo in campo dalla Ditta.
- Dirimere in modo chiaro e trasparente con la Ditta eventuali problematiche relative a questioni di connettività, prestazioni e configurazione della rete.

- Verificare che i locali di lavoro siano adeguati per svolgere le attività.
- La stesura e la disponibilità delle connessioni elettriche e di rete ove necessario.

5.4 COLLAUDO

Come specificato nel precedente punto 5.2 (CONSEGNA), il superamento del collaudo deve avvenire entro il limite massimo di **45 (trentacinque)** giorni continuativi decorrenti dalla data dell'ordine.

Il collaudo sarà considerato positivamente superato qualora tutti i risultati siano conformi ai criteri di superamento qui sotto specificati e verrà fornita la **documentazione di tutti i prodotti in formato pdf**.

Al termine del collaudo con esito positivo, verrà redatto apposito verbale sottoscritto anche dalla Ditta, che ne riceverà copia.

In caso di esito negativo del collaudo, la Ditta dovrà provvedere a correggere le anomalie riscontrate e ad effettuare nuovamente il collaudo entro **8 (otto) giorni solari** dalla data del verbale di collaudo negativo.

Nel caso in cui anche il secondo collaudo risultasse negativo, l'Amministrazione, valutata la natura e l'entità delle anomalie riscontrate, potrà risolvere il Contratto, fatto salvo il diritto al risarcimento di tutti i danni diretti ed indiretti comunque subiti dall'Amministrazione.

5.4.1 **Criteri per il superamento del Collaudo**

- Il nuovo Wireless Controller (WC) e Identity Manager (IM) dovranno essere correttamente installati e funzionanti nel rack indicato dall'Amministrazione.
- Il nuovo WC dovrà essere in grado di gestire/configurare tutti gli AP già in possesso di questa Amministrazione e già installati sul territorio. La funzionalità di questi AP dovrà essere piena: non dovrà esserci alcuna riduzione di funzionalità e prestazioni rispetto il funzionamento con il precedente controller.
- Verrà inoltre eseguita una prova con alcuni nuovi AP, oggetto di questa fornitura, che verranno installati, a cura di questa Amministrazione, in uno o più siti, anche in sostituzione dei presenti. Questi nuovi AP si dovranno configurare automaticamente e funzionare perfettamente una volta connessi alla rete, come per i precedenti ("zero configuration") sia nel nuovo che nel precedente WC.
- Il "fall back" dal nuovo al precedente WC è perfettamente funzionante su 3 AP di test
- Tutti i profile di autenticazione indicati in 5.3 (INSTALLAZIONE E CONFIGURAZIONE) sono perfettamente funzionanti.

La fornitura e i relativi servizi di cui ai precedenti paragrafi, saranno sottoposti a collaudo dall'Amministrazione al fine di verificare la conformità di detti servizi con le specifiche di cui al presente Capitolato Tecnico.

Il Fornitore e l'Amministrazione potranno concordare eventuali modifiche.

5.5 SUPPORTO ALL'AVVIAMENTO

Le seguenti attività dovranno essere svolte in giornate lavorative on-site di 8 ore ciascuna.

Numero 5 (cinque) giornate così distribuite:

- 3 (tre) giornate per il supporto all'avviamento e "training on job" dell'Identity Manager

- 2 (due) giornate per il supporto all'avviamento e "training on job" del nuovo Wireless Controller incluso la gestione del "fall back" tra i due Controller, come specificato precedentemente.

Per le attività sopra descritte dovrà essere dedicata una risorsa di adeguate conoscenze e competenze.

5.6 REQUISITI DI CONFORMITÀ

Dovranno essere rispettate tutte le disposizioni attualmente vigenti, incluse quelle dettate dall'ARPAV, in termini di sicurezza, emissioni elettromagnetiche/immunità in particolare per il Wi-Fi in ambito pubblico. A titolo di esempio non esaustivo:

Sicurezza: EN 60950, CE, CSA 60950, UL 60950, CB IEC60950-1 (tutte le varianti nazionali), EN60825-1, IRAM, BUS, BSMI, SONCAP;

Emissioni/Immunità: FCC Parte 15 Classe A, ICES-03, CE, KCC, VCCI, AS/NZS CISPR 22, EN55022, EN55024, EN61000-3-2, EN61000-3-3, BSMI