Comune di Prato Provincia di Prato

Servizio di manutenzione e gestione di un sistema WI-FI provinciale e sua espansione

Specifiche tecniche-funzionali

1 Introduzione

Il presente Capitolato Tecnico disciplina gli aspetti tecnici della fornitura di un servizio di connessione wireless gratuita a Internet in standard WiFi 802.11 b/g/n sul territorio provinciale, che si propone di far convergere le infrastrutture di rete WiFi preesistenti realizzate dalla Provincia di Prato e dal Comune di Prato in una nuova architettura di rete WiFi che espone un unico SSID "**pratowifi**" e che unifica le modalità di autenticazione degli utenti registrati al sistema: le attuali e distinte banche dati degli utenti registrati ai sistemi, di proprietà di ciascun ente (Comune e Provincia di Prato), convergeranno in una unica banca dati determinata dalla fusione delle due, secondo le modalità indicate più avanti.

Il fornitore si impegna a erogare i seguenti servizi (già presenti in ciascuna distinta rete WiFi della Provincia di Prato e del Comune di Prato) nella nuova architettura di rete WiFi per un periodo di 36 mesi:

- servizi di attivazione ed esercizio dei sistemi per la gestione della rete;
- servizi di provisioning degli utenti;
- servizi di logging degli accessi e data retention a norma di legge per l'erogazione del servizio di navigazione Internet ai cittadini.

L'affidamento è comprensivo delle attività necessarie per l'avvio operativo del sistema in merito alla gestione del passaggio dai precedenti operatori, con caricamento dei dati dai sistemi precedentemente in uso a quelli oggetto della presente fornitura, l'assistenza e la manutenzione come meglio precisato in seguito.

Oggetto dell'appalto è la fornitura dei seguenti servizi di base obbligatori:

- la presa in carico e riconversione dei due sistemi esistenti in un'unica infrastruttura di rete secondo le specifiche di capitolato;
- l'eventuale riconfigurazione degli apparati;
- la gestione e manutenzione degli apparati;
- l'erogazione del servizio di Service desk nei confronti degli utenti del servizio WiFi;

e la fornitura dei seguenti servizi con attivazione opzionale:

- la fornitura di Access Point di tipo indoor e outdoor con un preziario standard;
- attività di installazione di Access Point.

L'estensione delle reti WiFi esistenti è il risultato di collaborazioni formalizzate dalla Provincia di Prato e dal Comune di Prato attraverso la stipulazione di apposite convenzioni con altre Pubbliche Amministrazioni del territorio; pertanto il fornitore si impegna erogare servizi di base obbligatori e servizi con attivazione opzionale anche ad altri soggetti sulla base della sottoscrizione di specifici contratti alle condizioni previste nell'ambito del presente appalto.

La ripartizione dei costi di gestione di norma avverrà:

- per quanto riguarda i canoni di manutenzione in base al numero di AP;
- per quanto riguarda le forniture in base al preziario presentato;
- in base a ulteriori criteri di ripartizione precisati nel presente capitolato.

2 Situazione attuale

Gli attuali sistemi in uso alla Provincia di Prato e al Comune di Prato si basano sul software TOC TOC di Sokom Srl.

Gli Access Point installati sono:

- n.145 di proprietà della Provincia di Prato, Camera di Commercio di Prato e dell'Ordine degli avvocati di Prato (modelli MikroTik RB951-2n e Abocom WAP 2102);
- n.30 di proprietà dell'Amministrazione Comunale di Prato,

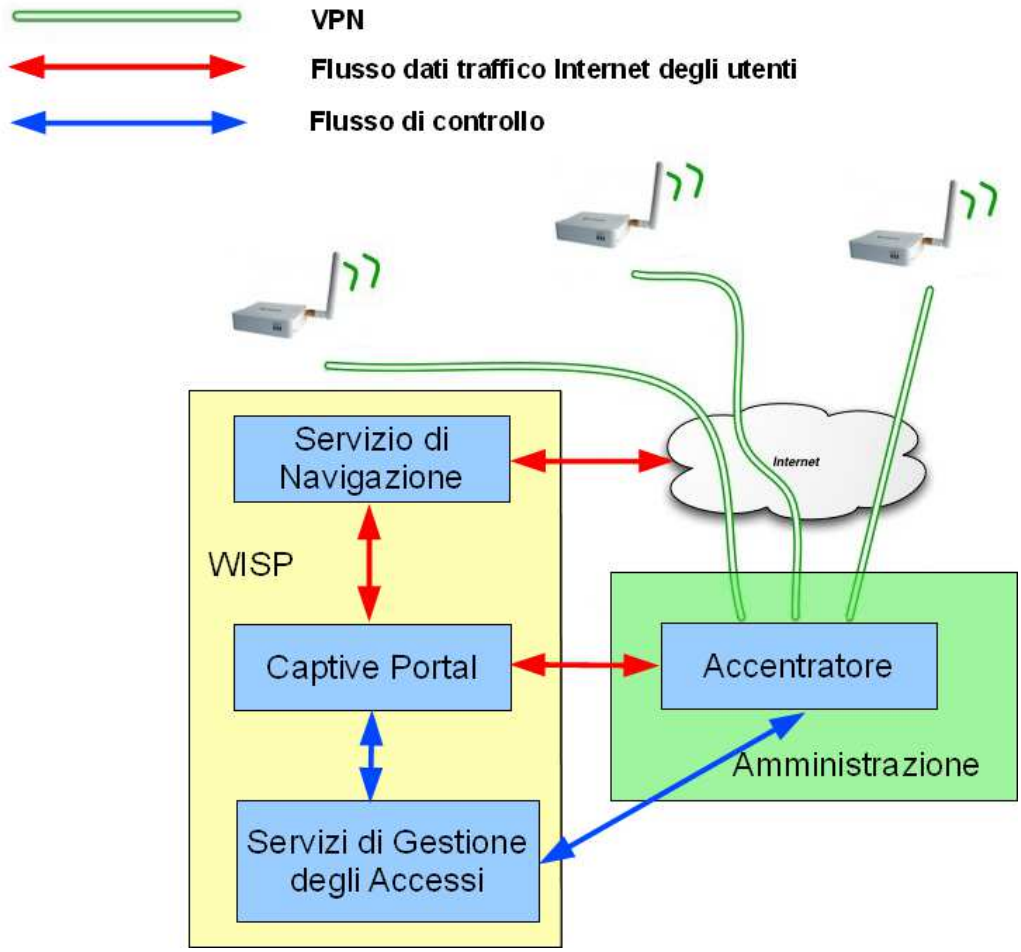
dislocati sul territorio provinciale.

Le informazioni di dettaglio riguardo al posizionamento degli apparati sono disponibili in rete ai seguenti indirizzi:

- http://mappahotspot.wifi.provincia.prato.it/ per la Provincia di Prato;
- http://wi-fi.comune.prato.it/htm/copertura.htm per il Comune di Prato.

Architettura attuale dell'infrastruttura della Provincia di Prato.

La rete WiFi della Provincia di Prato si compone di Access Point (AP) collegati a reti non dedicate, costituite da connessioni Internet preesistenti, come le reti interne dell'Amministrazione o semplici ADSL di terze parti (soggetti pubblici e privati che hanno aderito all'iniziativa e che hanno permesso l'installazione degli Access Point nei loro locali garantendo la fornitura a loro carico di alimentazione elettrica e connettività), che permettono di collegare ciascun AP attraverso una VPN



mediante OpenVpn al centro stella costituito dal "modulo Accentratore" collocato presso la Provincia di Prato.

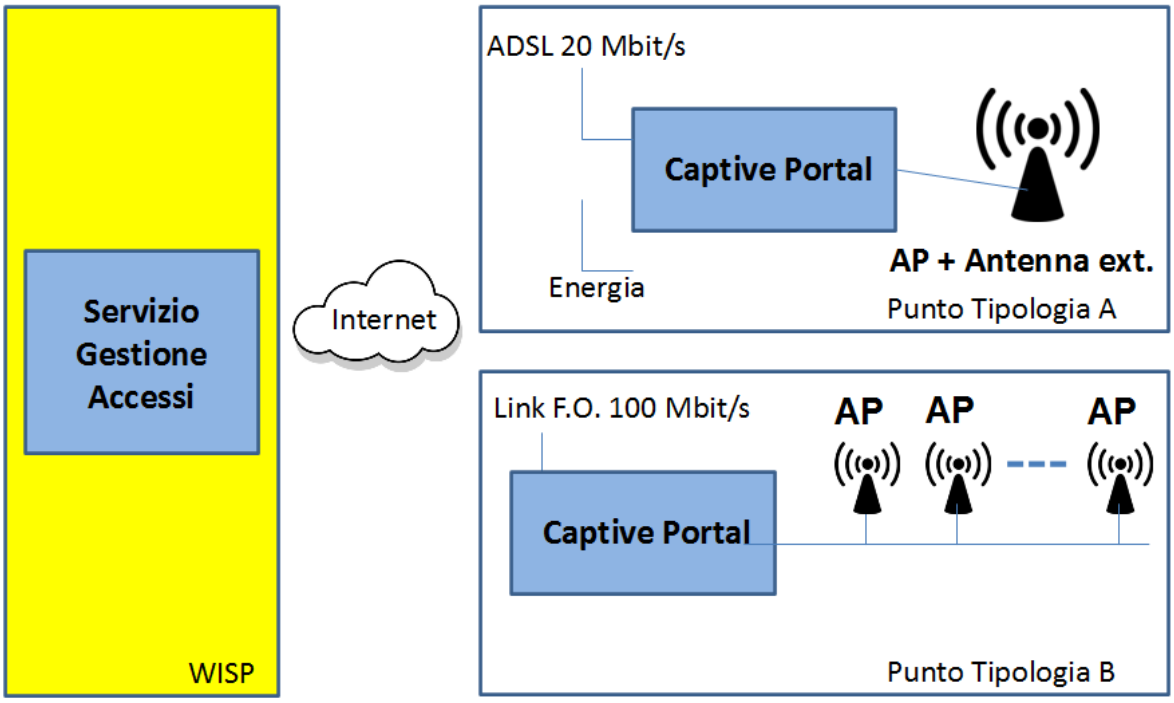
Le reti VPN garantiscono una autenticazione unica nei vari Access Point attraverso il captive portal centralizzato messo a disposizione dal fornitore che provvede a gestire la registrazione, autenticazione e navigazione degli utenti.

Il flusso di controllo e il flusso dati transitano esclusivamente su tali VPN; questa soluzione permette di assegnare indirizzi IP forniti dall'Operatore WISP e ad esso riconducibili indipendentemente dalla connessione di rete a cui ciascun AP è collegato.

Architettura attuale dell'infrastruttura del Comune di Prato.

La rete WiFi del Comune di Prato si compone di Access Point installati in piazze, strade e in genere nei luoghi di maggior interesse per la città che possono essere classificati secondo due tipologie:

- il tipo **A** identifica quegli Access Point (AP) della rete WiFi per i quali il fornitore eroga i seguenti servizi:
  - gestione del punto;
  - manutenzione di tutti i sistemi e apparati installati dal gestore della linea ADSL fino all'antenna esterna direttiva;
  - fornitura della connettività ADSL e dell'utenza elettrica per l'alimentazione dei sistemi e apparati.
- il tipo **B** identifica quegli Access Point (AP) della rete WiFi per i quali la manutenzione degli stessi, degli impianti e delle antenne è a carico del possessore dell'impianto mentre il fornitore è tenuto a erogare i seguenti servizi:
  - gestione del punto;
  - manutenzione di tutti i sistemi e apparati installati dal gestore della linea ADSL fino all'Access Point **escluso**;
  - fornitura del link a 100 Mbps simmetrico.



Gli Access Point del tipo **A** installati su palo e pressi luoghi pubblici aperti con captive portal locale, per i quali l'alimentazione elettrica e la connettività con ADSL 20 Mbps sono a carico del fornitore, sono i seguenti:

- Piazza Duomo (1 punto)
- Stazione Porta al Serraglio (1 punto)
- Piazza S. Agostino (1 punto)
- Piazza S. Domenico (1 punto)
- Piazza S. Marco (1 punto)
- Piazza Mercatale (3 punti)
- Piazza S. Maria delle Carceri (2 Punti)
- Parco Cascine di Tavola (2 punti)
- Parco di Galceti (3 punti)

Le due postazioni di tipo **B,** aventi ciascuna un proprio captive portale e un collegamento in fibra ottica a 100 Mbps, sono posizionate presso:

- Ospedale nuovo
- Comune di Prato

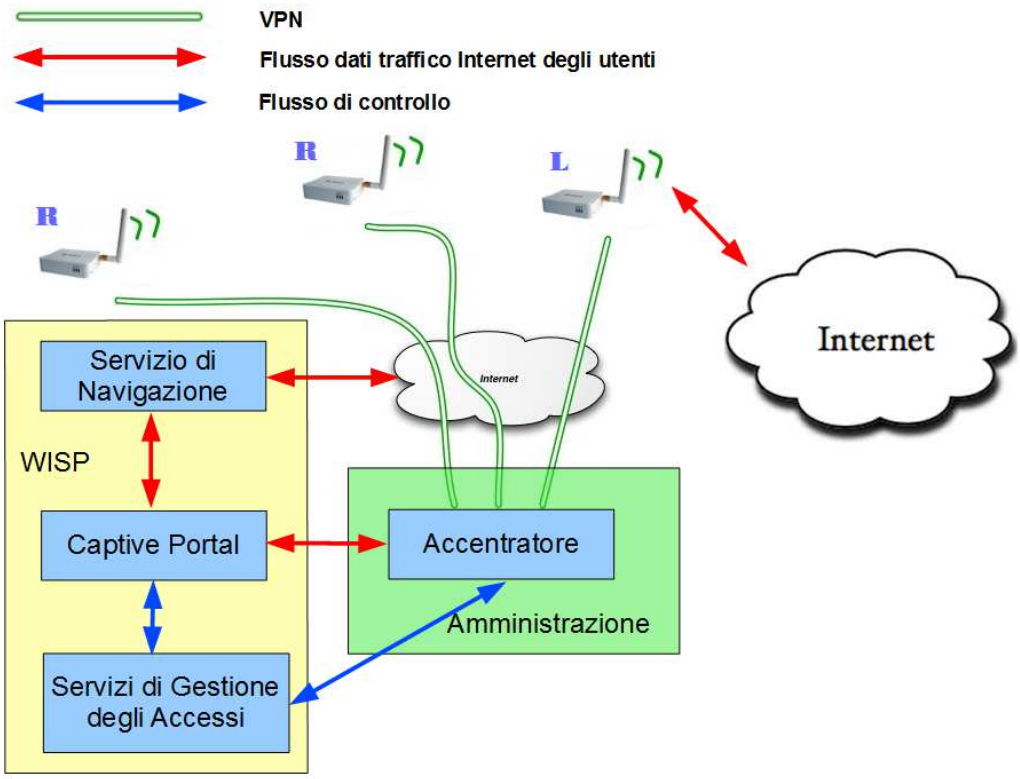
e attraverso di esse sono gestite in autonomia dalle Amministrazioni proprietarie gli accessi agli AP posizionati all'interno di esse.

La quantità delle singole tipologie di apparati (comprensive di marca e modello) saranno precisate prima della stipula del contratto.

3 Architettura e modalità di implementazione

3.1 Architettura del sistema

La soluzione offerta deve uniformare le due infrastrutture esistenti all'architettura sotto illustrata:



Nella figura sono evidenziati con le lettere **R** e **L** due modalità di funzionamento degli Access Point:

- il tipo **R** identifica quegli Access Point (AP) della rete WiFi (di norma collegati a reti non dedicate) che attivano una VPN mediante OpenVpn con il centro stella costituito dal "modulo Accentratore"; l'AP attraverso tale VPN utilizza il servizio centralizzato di autenticazione attraverso il captive portal centralizzato; anche il flusso dati di navigazione (servizi di navigazione) transita da tale VPN; pertanto l'indirizzo IP assegnato ai client connessi a tali AP viene stabilito dai sistemi centrali tramite VPN; questa configurazione garantisce il roaming dei clienti tra AP di tipo R;

  Caratteristiche tipo R:

  - Access Point connesso a reti non dedicate
  - VPN verso "modulo Accentratore" in cui transitano flussi dati e di controllo
  - Indirizzo IP assegnato da WISP
  - Captive portal centralizzato

- il tipo **L** identifica quegli Access Point (AP) della rete WiFi costituiti da Access Point che sono di norma collegati a reti dedicate e che instaurano una VPN mediante OpenVpn con il centro stella costituito dal "modulo Accentratore". L'AP impiega tale VPN per utilizzare il servizio centralizzato di autenticazione attraverso il captive portal che può essere sia centralizzato sia locale all'AP (oppure verso un URL specifico). Questo tipo di AP condivide il servizio di autenticazione con gli altri tipi di AP e il logging tramite specifica

VPN con il “modulo Accentratore”, ma il servizio di navigazione è gestito unicamente dal dispositivo stesso inpiegando la rete dedicata a cui è connesso e non quella del WISP tramite VPN come nel caso del tipo **R**; l'indirizzo IP sarà pertanto assegnato dalla rete a cui a è connesso e non dai sistemi centralizzati.

Si individuano due tipologie di AP di tipo **L**:

Caratteristiche tipo L1:

- Access Point connesso a reti dedicate messe a disposizione dall'Ente
- VPN verso “modulo Accentratore” in cui transitano solo flussi di controllo
- Indirizzo IP assegnato dalla rete dell'Ente
- Captive portal centralizzato o locale all'AP o verso un URL specifico

Caratteristiche tipo L2:

- Access Point collegato alla rete dati ADSL messa a disposizione dal fornitore nell'ambito del presente contratto (servizio di connettività con almeno velocità di navigazione (download) 20 Mbps e di trasmissione (upload) 1 Mbps)
- VPN verso “modulo Accentratore” in cui transitano solo flussi di controllo
- Indirizzo IP assegnato dalla rete dell'Ente
- Captive portal centralizzato o locale all'AP o verso un URL specifico

Ogni Access Point di tipo **L2** dovrà essere dotato della propria interconnessione ad Internet, tramite linea xDSL con indirizzo IP fisso, avente banda minima di upload di 1 Mpbs e di download di 20 Mbps; sarà esclusivamente consentito l'utilizzo di connessioni WiFi (sia dedicate che condivise con quelle utilizzate dagli utenti del servizio) per l’interconnessione degli stessi Access Point sia tra di loro che a Internet solo per quelle locazioni degli Access Point dove gli operatori di telecomunicazioni avranno dichiarato di non poter fornire un accesso in tecnologia xDSL in un raggio inferiore a 100 metri.

In fase di realizzazione del servizio, a fronte di inaspettate problematiche nel posizionamento delle apparecchiature, l’Amministrazione richiedente l'installazione dello specifico AP potrà valutare se mettere a disposizione i propri edifici per ospitare le apparecchiature, le terminazioni di rete e/o di alimentazione.

Saranno apprezzate le soluzioni realizzate attraverso software Open Source. In questo caso il software in formato sorgente, le personalizzazioni, le installazioni ed ogni altra modifica farà parte della fornitura.

Il fornitore deve mettere a disposizione i servizi e le infrastrutture individuate in figura e contenute nel blocco denominato WISP e consistenti in:

- erogazione di servizi di attivazione;
- esercizio di sistemi software per la gestione della rete;
- servizio di provisioning degli utenti;
- servizio di logging degli accessi e data retention a norma di legge per l’erogazione del servizio ai cittadini;
- servizio di client isolation su wifi;
- servizio di captive portal e servizio di navigazione (**se previsto dal tipo di AP**);
- fornitura del “modulo Accentratore” (che rimarrà di proprietà della Provincia di Prato e che dovrà essere collocato presso la Provincia di Prato);
- collegamento telematico del “modulo Accentratore” con Internet in modo che possa ricevere tutte le connessioni VPN degli AP di tipo **R** e che funzioni da gateway per la navigazione

(l'indirizzo IP pubblico da cui l'utenza finale risulta navigare dagli AP di tipo **R** deve essere quello fornito dal WISP) con una banda minima di 100Mbps in download e 20 Mbps in upload.

Il sistema dovrà rimanere inserito nell'ambito del progetto **"Free ItaliaWiFi"**

La soluzione che dovrà essere fornita deve garantire le necessarie forme di “isolamento” dei client grazie alle quali agli utenti non sia possibile violare i computer altrui o quelli della struttura che offre il servizio, disporre di meccanismi “plug & play” che consentono agli utenti la connessione senza modifica delle impostazioni del proprio dispositivo; in virtù del sistema di autenticazione adottato la soluzione deve garantire la possibilità di risalire agli autori di specifici comportamenti sulla rete consentendo lo scaricamento della responsabilità su soggetti terzi rispetto al gestore.

In ogni caso il sistema deve essere in grado di memorizzare i dati di autenticazione e il MAC address del dispositivo utilizzato da ciascun utente per connettersi, con cui poter risalire univocamente a un particolare utente, potendo provare l’estraneità del gestore della rete ai comportamenti altrui.

È escluso qualsiasi altro utilizzo delle apparecchiature installate sul territorio da parte della società erogatrice del servizio. Le apparecchiature installate dovranno essere utilizzate solo ed esclusivamente per erogare il servizio in nome e per conto delle Amministrazioni Committenti.

Nelle piazze e nei luoghi oggetto del servizio sono presenti cartelli che segnalano la presenza del servizio WiFi recanti il logo identificativo del progetto. Gli oneri relativi all’installazione di nuovi cartelli e la manutenzione dei cartelli preesistenti e nuovi sono a carico della società fornitrice del servizio. I cartelli dovranno avere dimensioni di almeno 60cm x 40cm e dovranno essere almeno due per area.

3.2 Interazione con il “modulo Accentratore”

I servizi di autenticazione e di logging degli access devono essere erogati interfacciandosi con il nodo “modulo Accentratore” che realizza tutti i collegamenti VPN con gli Access Point di tipo **R** distribuiti sul territorio.

La rete è infatti strutturata in modo che tutti gli Access Point di tipo **R** instaurino una VPN con il centro stella costituito dal “modulo Accentratore” collocato presso la Provincia di Prato in modo da garantire una autenticazione unica nei vari Access Point attraverso il captive portal centralizzato messo a disposizione dal fornitore.

Il fornitore dovrà configurare ogni Access Point in modo che stabilisca la connessione VPN verso il “modulo Accentratore” tramite nome-host (vpn.pratowifi.it) invece che direttamente tramite indirizzo ip. Il “nome-host” vpn.pratowifi.it sarà infatti il nome assegnato al “modulo Accentratore” attraverso i DNS dell'Amministrazioni Committenti.

L'eventuale aggiornamento del firmware a bordo degli Access Point attualmente esistenti è una attività a carico del fornitore senza alcun ulteriore onere per l'Amministrazioni Committenti.

3.3 Limitazioni di utilizzo

Gli utenti che si autenticheranno tramite il captive portal potranno navigare liberamente sulla rete Internet fino al raggiungimento giornalmente di un limite temporale e/o di un limite di traffico effettuato.

I limiti di utilizzo saranno comunicati dalle Amministrazioni Committenti in sede di esercizio del contratto che potranno essere distinti per ciascun Captive Portal; saranno apprezzate soluzioni che permettono di ottnere limiti di utilizzo diversificati per ciascun Access Point.

Al raggiungimento di uno di questi limiti, la sessione scadrà e l’utente e fino alla fine della giornata non potrà usufruire ulteriormente dei servizi di navigazione una volta autenticato nuovamente sul Captive Portal.

L’Amministrazioni Committenti potranno liberamente modificare nel corso dello svolgimento del servizio i valori di tempo e di banda. Sarà apprezzata la possibilità di assegnare differenti valori di tempo e di traffico ai vari Access Point dislocati sul territorio.

Il sistema dovrà consentire la possibilità di limitare il numero di ri-connessioni giornaliere per ciascun utente.

Gli utenti potranno liberamente accedere alla rete, ma saranno implementate limitazioni sulle porte utilizzabili per la trasmissione dei dati. In particolare gli utenti che si autenticheranno tramite il captive portal potranno accedere a servizi pubblicati sulla rete Internet solo sulle porte relative al funzionamento dei protocolli FTP, SSH, DNS, HTTP e HTTPS.

L’Amministrazioni Committenti potranno liberamente modificare nel corso dello svolgimento del servizio quali ulteriori protocolli ammettere tramite gli Access Point.

3.4 Interconnessione con altre sorgenti di autenticazione

L’Amministrazioni Committenti hanno intenzione di integrare il sistema di accesso WiFi con altri sistemi di accesso aventi le medesime caratteristiche di sicurezza. È quindi necessario che il sistema proposto possa interagire con detti sistemi almeno tramite il protocollo RADIUS sia accettando credenziali remote, che offrendo il proprio database agli altri enti ed aziende autorizzate dalle Amministrazioni Committenti. Nel canone di manutenzione annuale dovrà essere ricompreso il costo per l’integrazione del sistema fornito con un massimo di 5 sistemi RADIUS che saranno indicati dalle Amministrazioni Committenti.

3.5 Captive portal

Il sistema deve consentire che ciascun Access Point possa offrire una pagina splash configurabile (grafica e link dipendenti) e diversa in base all’Access Point in cui l'utente si autentica.

Il sistema deve inoltre assicurare la disponibilità di un Walled garden (elenco di siti visitabili senza previa autenticazione) specificato sia mediante classi di IP che mediante URL.

E’ permesso alla società fornitrice del servizio di inserire, in posizione marginale e con una dimensione massima di 234 x 60 pixels (half banner) un riferimento commerciale del tipo: “servizio realizzato da…… “ includente il proprio logo e motto.

Il captive portal dovrà prevedere un sistema di CMS (Content Management System) in modo che il portale possa essere personalizzato velocemente sia dal personale dell’Amministrazioni Committenti che dal personale della società operante il servizio, dietro richiesta dell’Amministrazioni Committenti.

Il captive portal dovrà fornire indicazioni relativamente alla procedura di registrazione.

3.6 Collegamento telematico con il modulo “Accentratore”

Il fornitore deve fornire un collegamento telematico adeguatamente dimensionato in termini di banda tra il “modulo Accentratore” e Internet, attraverso cui transita tutto il traffico dell'architettura di rete WiFi per gli Access Point di tipo **R,** in modo da garantire che non costituisca un “collo di bottiglia” per la connettività del sistema nel suo complesso.

Tale banda dovrà essere almeno di 100Mbps in download e 20 Mbps in upload.

3.7 Navigazione Internet e Policy

In seguito all'autenticazione dell'utente questo potrà navigare senza alcuna restrizione di siti secondo le policy stabilite e configurabili sulla base sei seguenti parametri:

- Volume dati per connessione
- Tempo di connessione
- Numero di connessioni in un dato tempo

- Numero massimo di dispositivi per utente contemporanei

Il sistema deve poter consentire policy differenziate per singolo AP o gruppo di AP.

3.8 Modalità di ampliamento del sistema

Sulla base del modello organizzativo basato sulla stipulazione di apposite convenzioni che governa la rete WiFi federata, il fornitore dovrà prevedere la gestione di Access Point secondo queste due modalità:

- di proprietà di terzi da configurare e/o gestire nella rete;
- di proprietà (acquisti nell'ambito della presente fornitura o già esistenti) delle Amministrazioni Committenti.

Il sistema non deve avere alcuna limitazione riguardo al numero di utenti registrati al sistema.

Ciascun Access Point di nuova fornitura nell'ambito del presente appalto deve garantire almeno un numero minimo di 100 connessioni contemporanee.

Nell'ambito del contratto il fornitore si rende disponibile a fornire, secondo un listino definito in fase di offerta, gli Access Point del modello adeguato a essere impiegati nell'infrastruttura in modo che ciascuna amministrazione aderente al progetto possa acquisire gli apparati per estendere la copertura della rete WiFi secondo le proprie necessità.

4 Licenze e diritti di proprietà

Sono di proprietà esclusiva della Provincia di Prato:

- gli Access Point già in possesso e quelli acquisiti nell'ambito del presente appalto;
- l'hardware dedicato al nodo accentratore;
- il codice sorgente dei captive portal locali degli Access Point di proprietà di tipo **L**.

Sono di proprietà esclusiva del Comune di Prato:

- gli Access Point già in possesso e quelli acquisiti nell'ambito del presente appalto;
- il codice sorgente dei captive portal locali degli Access Point di proprietà di tipo **L**.

Sono di proprietà esclusiva del singolo soggetto aderente al contratto:

- gli Access Point già in possesso e quelli acquisiti nell'ambito del presente appalto;
- il codice sorgente dei captive portal locali degli Access Point di proprietà di tipo **L**.

Sono di proprietà condivisa della Provincia di Prato e del Comune di Prato:

- il codice sorgente dei captive portal remoti usati dagli Access Point di tipo **R** e di quelli di tipo **L** configurati per l'impiego di captive portal remoti;
- il data base degli utenti registrati.

Con riferimento al database degli utenti contenente tra l’altro le informazioni di accesso e di navigazione che verrà costituito nel corso dell’esercizio del servizio, si precisa altresì che:

- i proprietari ne sono titolari ai sensi della vigente normativa sulla Privacy;
- la società fornitrice del servizio sarà responsabile esterno del trattamento dei dati per tutto il periodo del contratto.

Il fornitore del servizio permetterà ai tecnici delle due Amministrazioni Committenti l’accesso diretto in lettura al database così costituito tramite comandi SQL.

Al fine di consentire la trasferibilità tecnologica della soluzione realizzata verso altri sistemi il precedente fornitore è obbligato a fornire tali dati, secondo un tracciato record da concordare per il suo utilizzo in altri sistemi, nonché la documentazione di progetto necessaria.

A conclusione del contratto, il fornitore è obbligato a fornire tali dati, secondo un tracciato record da concordare per il suo utilizzo in altri sistemi, nonché la documentazione di progetto necessaria al fine di consentire la trasferibilità tecnologica della soluzione realizzata verso altri sistemi.

5 Servizio di registrazione utenti al sistema

La procedura di registrazione degli utenti al servizio si compone principalmente di due fasi:

- Inserimento dei dati personali
- Verifica dei dati personali

5.1 Inserimento dati personali

Durante la prima fase è necessario inserire i propri dati anagrafici:

- compilazione di un form con i dati essenziali dell'utente:
  - nome
  - cognome
  - data di nascita
  - indirizzo (Via - CAP - Città - Stato)
  - e-mail
  - numero telefonico del cellulare italiano (che costituirà il nome utente per l'accesso al servizio)

5.2 Flessibilità profilazione utenti

Occorre prevedere anche la possibilità di profilare l'utente attraverso l'eventuale iscrizione a newsletter in email e/o SMS da aggiungere nel pannello di registrazione rispetto all'insieme minimale dei dati per l'iscrizione.

Questa flessibilità nell'adattamento del form di registrazione deve consentire la personalizzazione dello stesso sulla base di parametri come l'Amministrazione associata a ciascun Access Point in modo da permettere così di personalizzare i parametri opzionali richiesti sulla base di specifiche esigenze locali (per esempio iscrizione a un servizio di newsletter specifico per una sola amministrazione).

5.3 Assegnazione password e verifica

Una volta completata l'autenticazione il sistema deve provvedere ad assegnare la password via SMS al numero indicato in fase di registrazione; al primo collegamento si deve presentare la maschera per la conferma della password inviata via SMS o per la sua modifica (si deve poter confermare quella assegnata senza cambiarla).

5.4 Pannello gestione utenza

Il portale di autenticazione mette a disposizione un pannello utente, accessibile inserendo il nome utente e la password scelti, che consente l'accesso a una sezione privata dove consultare le proprie statistiche di utilizzo e i propri dati personali.

Tale pannello permette inoltre di disabilitare il proprio account, che potrà essere riabilitato ripetendo la procedura di verifica dei propri dati personali.

Nel caso di password dimenticata, il portale di autenticazione mette a disposizione un apposito pannello tramite cui accedere alla funzione di recupero che può avvenire tramite e-mail o telefono cellulare.

5.5 Accesso utenti non aventi cellulare italiano

Per consentire l'accesso anche a utenti non in possesso di cellulare italiano il fornitore si rende disponibile a mettere a disposizione un insieme di account utente pre-attivati per turisti o avventori.

Il fornitore si impegna a stabilire il periodo di validità (1 giorno o 1 settimana per esempio) da assegnare a tali account che si attiveranno al primo utilizzo.

Il fornitore deve inoltre mettere a disposizione un portale per l'associazione dell'identità agli account pre-configurati anche se il loro utilizzo può avvenire senza vincolo di associazione di identità.

5.6 Service desk

Il fornitore deve garantire la disponibilità di un servizio di supporto (in seguito **Service desk**) in modo da gestire eventuali difficoltà di accesso da parte degli utenti al servizio di navigazione: il servizio accessibile tramite chiamate ad un Call Center fornirà assistenza alla clientela per la procedura di registrazione, accesso, ed eventualmente il servizio di reset della password.

Il Call Center dovrà essere operativo almeno dal Lunedì al Venerdì, dalle ore 9:00 alle ore 19:00. Sarà apprezzata ogni estensione alle fasce orarie minime sopra indicate.

Il Call Center dovrà garantire un livello di accessibilità del servizio superiore al 90% (rapporto, nel mese considerato, tra il numero di unità di tempo in cui almeno una delle linee è libera e il numero complessivo di unità di tempo di apertura del Call Center con presenza di operatori, moltiplicato per 100).

Il tempo medio di attesa dovrà essere inferiore a 240 secondi (media aritmetica dei tempi di attesa telefonica delle chiamate dei cittadini). Il livello di servizio dovrà essere superiore al 80% (rapporto, nel mese considerato, tra il numero di chiamate telefoniche dei cittadini che hanno effettivamente parlato con un operatore e il numero di chiamate dei cittadini che hanno richiesto di parlare con un operatore).

A richiesta dell'Amministrazioni appaltanti, la società fornitrice del servizio dovrà presentare la statistica delle chiamate ricevute e dimostrare il rispetto dei valori richiesti.

La risposta sarà fornita tramite operatori professionali addestrati, in modo da garantire una uniformità di risposta nell'arco di tutta la durata dell'esercizio, sia nell'accoglienza della risposta che nella risoluzione delle seguenti problematiche:

- difficoltà di registrazione e di logon;
- difficoltà di navigazione;
- reset delle password di accesso;
- assistenza all'uso del portale per la gestione dei dati personali.

Per le operazioni di cambio password, gli operatori agiranno tramite profili personalizzati dell'interfaccia di back-office del sistema di autenticazione. Su richiesta di un utente (previa identificazione) sarà eseguito il reset della password che verrà comunicata all'utente stesso tramite SMS o email alle credenziali fornite in fase di registrazione. Gli operatori non saranno a conoscenza della password, ne potranno modificare i dati degli utenti in alcun modo.

Eventuali difficoltà di navigazione saranno valutate dall'operatore ed eventualmente gestite con un intervento di manutenzione, mirato ad effettuare una verifica degli apparati e del servizio.

6 Listino servizi

La fornitura comprende un insieme di servizi di base obbligatori e di servizi opzionali attivabili su richiesta sulla base di un listino di prezzi quotato in fase di offerta economica.

I servizi di base obbligatori riguardano:

- Fornitura del “modulo Accentratore”
- Canone generale del servizio che comprende infrastrutture centrali e il Service desk
- Costo collegamento tra “modulo Accentratore” e WISP
- Costo gestione e manutenzione AP indoor (da interno) di tipo **R** o **L**
- Costo gestione e manutenzione AP outdoor (da esterno) di tipo **R** o **L** inclusivo dei canoni per energia elettrica e collegamento Internet

I servizi opzionali riguardano:

- installazione esterna di AP su struttura muraria esistente;
- installazione esterna di AP su palo stradale esistente;
- installazione esterna di AP su palo stradale di nuova installazione;
- installazione interna di AP su struttura muraria esistente;
- fornitura di AP come da specifiche di seguito riportate.

Ciascun Access Point dovrà poter offrire fino ad un minimo di cinque SSID, uno identificato per il pubblico con l’accesso tramite Captive Portal, uno riservato per gli operatori dell’Amministrazioni Committenti con sicurezza WPA2 ed accesso libero senza Captive Portal o limitazioni. Gli altri SSID saranno riservati per usi futuri dell’Amministrazioni Committenti.
Sarà apprezzata la possibilità di assegnare differenti priorità al traffico dei vari SSID. Sarà apprezzata la capacità degli Access Point di operare in “Client Isolation” o “AP Isolation”, ovvero impedendo la comunicazione diretta tra differenti stazioni registrate sul medesimo Access Point.

6.1 Specifiche tecniche minime Access Point da interno

- supporto agli standard 802.11 b/g/n/h
- alimentazione Power over Ethernet o alimentazione 220vac con apposito alimentatore compreso
- supporto multi-SSID (almeno 5)
- operatività in "Client Isolation" o "AP Isolation"
- controllo remoto, sia tramite un'applicazione specifica sia tramite telnet, sia terminale SSH
- controllo tramite Console seriale
- controlla della larghezza di banda disponibile e in base al tipo di traffico (http, ftp, pop3, etc)
- firewall interno per esecuzione di NAT, MASQUERADE
- gestione code e firewall mark fino a livello 7, attraverso l'individuazione del fingerprint dei singoli pacchetti
- supporto Vlan e Vlan routing
- supporto DHCP
- software e firmware aggiornabili da remoto
- protocolli di routing dinamico
- implementazione VPN IPSEC, PPTP, LZTP, OpenVPN
- supporto criptazione radio tramite protocollo AES a 256 bit
- gestione code del traffico e supporto QoS e QoS avanzato
- supporto scripting per operazioni pianificate
- supporto SNMP per il monitoraggio remoto e strumenti di controllo della rete
- gestione utenti e profili

6.2 Specifiche tecniche minime Access Point da esterno modello mono-radio e antenna detached

- protezione IP65 o NEMA 4 (protezione completa contro la polvere e getti d’acqua da ogni direzione)
- supporto agli standard 802.11 b/g/n/h
- range temperatura di esercizio da -18 °C a + 46 °C
- alimentazione Power over Ethernet
- supporto multi-SSID (almeno 5)
- operatività in "Client Isolation" o "AP Isolation"
- controllo remoto, sia tramite un'applicazione specifica sia tramite telnet, sia terminale SSH
- controllo tramite Console seriale
- controllo della larghezza di banda disponibile e in base al tipo di traffico (http, ftp, pop3, etc)
- firewall interno per esecuzione di NAT, MASQUERADE
- gestione code e firewall mark fino a livello 7, attraverso l'individuazione del fingerprint dei singoli pacchetti
- supporto Vlan e Vlan routing
- supporto DHCP
- software e firmware aggiornabili da remoto
- protocolli di routing dinamico
- implementazione VPN IPSEC, PPTP, LZTP, OpenVPN
- supporto criptazione radio tramite protocollo AES a 256 bit
- gestione code del traffico e supporto QoS e QoS avanzato
- supporto scripting per operazioni pianificate
- supporto SNMP per il monitoraggio remoto e strumenti di controllo della rete
- gestione utenti e profili

6.3 Specifiche tecniche minime Access Point da esterno modello dual-radio e antenna detached

- protezione IP65 o NEMA 4 (protezione completa contro la polvere e getti d’acqua da ogni direzione)
- supporto agli standard 802.11 b/g/n/h
- range temperatura di esercizio da -18 °C a + 46 °C
- alimentazione Power over Ethernet
- supporto multi-SSID (almeno 5)
- operatività in "Client Isolation" o "AP Isolation"
- controllo remoto, sia tramite un'applicazione specifica sia tramite telnet, sia terminale SSH
- controllo tramite Console seriale
- controllare della larghezza di banda disponibile e di intervenire a seconda del tipo di traffico (http, ftp, pop3, etc)
- firewall interno per esecuzione di NAT, MASQUERADE
- gestione code e firewall mark fino a livello 7, attraverso l'individuazione del fingerprint dei singoli pacchetti
- supporto Vlan e Vlan routing
- supporto DHCP
- software e firmware aggiornabili da remoto
- protocolli di routing dinamico
- implementazione VPN IPSEC, PPTP, LZTP, OpenVPN
- supporto criptazione radio tramite protocollo AES a 256 bit
- gestione code del traffico e supporto QoS e QoS avanzato
- supporto scripting per operazioni pianificate

- supporto SNMP per il monitoraggio remoto e strumenti di controllo della rete
- gestione utenti e profili

6.4 Specifiche tecniche antenna settoriale doppia polarizzazione per AP da esterno

- Antenna radio 2.4GHZ-MIMO
- polarizzazione verticale e orizzontale
- guadagno non inferiore a 12 dBi
- larghezza fascio verticale non inferiore a 15° a -3 dBi
- larghezza fascio orizzontale non inferiore a 110° a -3 dBi

6.5 Specifiche tecniche antenna omnidirezionale doppia polarizzazione per AP da esterno

- Antenna radio 2.4GHZ-MIMO 360°
- polarizzazione verticale e orizzontale
- guadagno medio non inferiore a 2 dBi
- Half Power Beamwidth (HPBW) orizzontale 360°
- Half Power Beamwidth (HPBW) verticale non inferiore a 30°

7 Infrastruttura hardware e telematica

Il sistema offerto dovrà essere in grado di gestire tutti gli Access Point installati prevedendo **un limite superiore di almeno 512 Access Point installati per ogni Captive Portal**: al fornitore saranno messi a disposizione tali ulteriori apparati (il cui approvvigionamento e montaggio sono a cura dell'Amministrazioni Committenti o accedendo al listino di servizio) su cui dovrà intervenire esclusivamente per la loro messa a punto (configurazione del firmware e definizione delle impostazioni di rete necessarie) per predisporli all'inserimento nel nuovo sistema.

Il sistema di registrazione non dovrà porre **limiti al numero di utenti registrati** sul sistema.

Il fornitore si impegna a monitorare con continuità le prestazioni del sistema, mettendo contestualmente a disposizione del personale tecnico dell'Ente una opportuno cruscotto (come meglio dettagliato successivamente) per l'interrogazione statistica sulle prestazioni del sistema, nel rispetto della vigente normativa in materia di privacy.

8 Riferimenti normativi

Il fornitore dovrà essere in possesso dell'autorizzazione generale per le reti e i servizi di comunicazione elettronica, così come previsto dall'Art. 25 del D.Lgs. 259/03 denominato "Codice delle Comunicazioni Elettroniche" e ai sensi del D.M. 28/5/2003 (Condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso Radio-LAN alle reti ed ai servizi di telecomunicazioni) - (elenco reperibile al seguente indirizzo: http://www.sviluppoeconomico.gov.it/index.php/it/comunicazioni/internet/internet);

Il fornitore dovrà essere iscritto nel registro degli operatori di comunicazione di cui all'articolo 1 della L. 249 del 31 luglio 1997, meglio disciplinato dalla DELIBERA N. 666/08/CONS dell'Autorità per le Garanzie nelle Comunicazioni (Allegato A, articolo 2) (elenco reperibile presso http://www.elencopubblico.roc.agcom.it/roc-epo/index.html).

In sede di indizione di gara non è ravvisato per l'appalto in question interferenza di cui all'art. 26 comma 1 lettera b e comma 3 del D.lgs 81/2008 e pertanto non è stato elaborato alcun Documento Unico di Valutazione dei Rischi di Interferenza (DUVRI). L'Amministrazioni Committenti si riserva anche sulla base degli elaborati tecnici che l'aggiudicatario produrrà per il rispetto delle prescrizioni del capitolato, e qual'ora se ne presenti la necessità, di elaborare un DUVRI specifico in relazione ai rischi di interferenza che via via si individueranno.

Oltre al rispetto della normativa nazionale in termini di irradiazione elettromagnetica e di fornitura di servizi di connettività al pubblico, dovranno essere rispettate anche le normative regionali e locali. Per le installazioni nel **territorio comunale di Prato**, si richiama a tal proposito il regolamento comunale per la progettazione e la gestione degli impianti di telecomunicazione (http://www.comune.prato.it/servizicomunali/norme/?act=i&fid=1380&id=20120214112440293) e in particolare:

- il comma 3 dell'art. 2 del Capo I che prevede che "I soggetti […] debbano presentare […] la migliore soluzione tecnica, praticabile al momento della richiesta, che riduca al livello più basso possibile i campi elettromagnetici";
- il comma 1 dell'art. 10 del Capo IV che prevede che l'installazione di nuovi impianti e le modifiche di quelli esistenti siano sottoposte ad autorizzazione comunale secondo il procedimento di rilascio dell'autorizzazione riportato nel successivo articolo 11 del regolamento.

A tal proposito si rende noto che alla data del presente bando, per il wireless non è stato ancora approvato da parte del Comune di Prato alcun "Piano Particolareggiato di Localizzazione" come previsto dall'art. 4, come invece è stato fatto per la telefonia mobile.

Al fine di verificare il rispetto della regolamentazione comunale in materia, la società aggiudicataria dovrà fornire entro 15 giorni dall'aggiudicazione, la documentazione necessaria per tale verifica, come previsto dal citato regolamento. La mancata presentazione della documentazione o la mancanza dei requisiti richiesti dal regolamento, comporterà l'annullamento dell'aggiudicazione ed il ricorso al fornitore successivo in graduatoria.

9 Oggetto della fornitura

È richiesta la fornitura di un servizio di connessione wireless gratuita ad Internet in standard WiFi 802.11 b/g/n sul territorio provinciale, che si propone di far convergere le infrastrutture di reti preesistenti realizzate dalla Provincia di Prato e dal Comune di Prato in una nuova architettura di rete WiFi che espone un unico SSID "**pratowifi**" che unifica le modalità di autenticazione degli utenti registrati al sistema: le attuali e distinte banche dati degli utenti registrati ai sistemi, di proprietà di ciascun ente (Comune e Provincia di Prato), convergeranno in una unica banca dati determinata dalla fusione delle due.

Il fornitore si impegna a erogare i seguenti servizi per un periodo di 36 mesi:

- servizi di attivazione ed esercizio dei sistemi per la gestione della rete;
- servizi di provisioning degli utenti;
- servizi di logging degli accessi e data retention a norma di legge per l'erogazione del servizio di navigazione Internet ai cittadini.

Nella fornitura sono compresi senza alcun ulteriore onere a carico dell'Amministrazioni Committenti:

- le attività necessarie per consentire la trasferibilità tecnologica della soluzione realizzata dal precedente fornitore, concordando con esso le modalità attuative, verso la nuova soluzione oggetto della fornitura e unificazione delle banche dati degli utenti registrati ai precedenti distinti sistemi;
- le attività necessarie per consentire la trasferibilità tecnologica della soluzione realizzata alla conclusione del periodo contrattuale verso altri sistemi concordando le modalità attuative con i nuovi soggetti aggiudicatari;
- l'erogazione dei servizi di base e opzionali descritti nel dettaglio in precedenza;
- fornitura tramite i server del fornitore di un servizio di DNS ai cittadini che si autenticheranno tramite il captive portal;
- la messa a disposizione di un'area riservata accessibile via Web con autenticazione tramite utente e password per l'estrazione di informazioni statistiche sul sistema, nel rispetto della vigente normativa in materia di privacy;
- sarà apprezzata la possibilità che ogni Access Point fornisca statistiche relativamente all'uso della banda tramite SNMP e la capacità di ogni Access Point (o di un sistema centrale, ma con indicazioni suddivise per Access Point) di fornire, tramite SNMP, informazioni sul numero dei client connessi;
- tramite l'area riservata accessibile via Web dovrà essere fornito un cruscotto da cui poter ottenere a titolo esemplificativo, sia in valore numerico sia espresso in forma grafico tramite istogrammi o altre forme di rappresentazione le seguenti informazioni:
  - numero di utenti registrati al sistema, in uno specifico intervallo temporale;
  - occupazione della banda complessiva di utilizzo di Internet e numero di accessi complessivi, in uno specifico intervallo temporale;
  - statistica di utilizzo di ciascun Access Point (censito all'interno del sistema e identificabile attraverso i propri dati informativi e mediante la loro localizzazione geografica) in termini di banda utilizzata e numero di utenti collegati, in uno specifico intervallo temporale;
- un servizio di monitoraggio del sistema che vigili sui seguenti aspetti:
  - utilizzo della banda a livello centrale al fine di individuare inadeguatezze della banda trasmissiva;

    - grado di utilizzo di ciascun Access Point finalizzato anche a individuare eventuali inadeguatezze della banda trasmissiva per gli Access Point;
    - malfunzionamenti dei sistemi centrali, per garantire la continuità del servizio a fronte di guasti hardware o difetti software;
    - malfunzionamenti dei sistemi periferici (Access Point) da segnalare ai referenti tecnici dell'Amministrazioni Committenti;
- dichiarazione periodica degli access point installati al Ministero delle Comunicazioni (autorizzazioni per reti a pubblico accesso), come da vigente normativa;
- redazione e presentazione, agli enti locali di riferimento, delle D.I.A. inerenti le autorizzazioni per l'eventuale installazione di Access Point da esterno;
- connettività Internet secondo l'architettura di rete descritta in precedenza e secondo i parametri di qualità minima indicati;
- captive portal con grafica personalizzata su modello fornito dalle Amministrazioni Committenti;
- sistema di registrazione/gestione utenti;
- sistema di federazione con proxy RADIUS al servizio FreeItaliaWifi;
- supporto di consulenza all'Amministrazioni Committenti nella progettazione di nuovi servizi avanzati da fruire attraverso l'infrastruttura wireless;
- servizio di estrazione di report statistici anonimi sull'uso della rete e dei suoi utenti;
- trasmissione di comunicazioni di servizio via mail e/o sms agli utenti;
- possibilità di fruire di alcuni servizi e portali scelti dall'Amministrazioni Committenti senza la registrazione e/o l'autenticazione al sistema (Walled garden).

10 Descrizione della fornitura

La fornitura è articolata nelle tre seguenti fasi:

- Installazione dei sistemi centrali;
- Migrazione e avvicendamento nella gestione del servizio con modifica della configurazione della connessione VPN di ogni Access Point da ip a nome-host (come specificato al paragrafo **Interazione con il "modulo Accentratore")**
- Collaudo

La sequenza temporale è descritta dalla seguente rappresentazione di GANTT:

T1	T2	T3
Installazione dei sistemi centrali	**Migrazione e avvicendamento nella gestione del servizio**	**Collaudo**

dove:

T1: Data inizio lavori;

T2: Data completamento dell'installazione dei sistemi e inizio della fase di Migrazione;

T3: Data di "Pronti al collaudo".

La durata delle tre fasi deve essere tassativamente inferiore a 2 (due) mesi, limite massimo per l'attivazione del sistema; il superamento di tale durata comporterà l'applicazione delle penali previste per compensare il prolungamento del contratto del procedente fornitore al fine di garantire la continuità del servizio.

10.1 Installazione dei sistemi centrali

La fase di installazione dei sistemi centrali è articolata nelle seguenti distinte attività:

- Analisi delle specifiche funzionali, implementazione/personalizzazione delle stesse;
- Recupero dati dai precedenti gestori;
- Installazione e configurazione dei sistemi centrali e ripopolamento con i dati recuperati dalle precedenti gestioni.

Tutte le attività di questa fase devono essere completate entro **il periodo indicato** in sede di offerta a partire dalla data di inizio lavori (o stipula del contratto).

I certificati SSL wildcard (cioè per l'intero dominio *.pratowifi.it) per i servizi erogati dal sistema attraverso i protocolli HTTPS saranno messi a disposizione dalle Amministrazioni Committenti.

La data di inizio lavori, e quindi l'inizio della consegna ed installazione della fornitura, decorre dalla data di comunicazione formale "inizio lavori" effettuata dal Responsabile del contratto alla Ditta aggiudicataria.

Il Responsabile del Fornitore notifica per iscritto al Responsabile del contratto, attraverso specifico verbale, la data di completamento di questa fase.

10.2 Migrazione e avvicendamento nella gestione del servizio

Parte integrante della fornitura è il caricamento della Base Informativa dei precedenti sistemi WiFi.

Le precedenti basi dati della Provincia di Prato e del Comune di Prato devono convergere in una sola; pertanto si potranno verificare le seguenti situazioni:

- scenario A: una persona fisica con un unico account nel sistema della Provincia di Prato

- scenario B: una persona fisica con un unico account nel sistema del Comune di Prato
- scenario C: una persona fisica con un account in entrambi i sistemi (Comune di Prato e Provincia di Prato)

La procedura di integrazione delle banche dati dovrà procedere pertanto all'unione dei due insieme dei dati procedendo così:

- scenario A: trasferimento delle credenziali utente/password nel nuovo sistema senza alcuna ulteriore azione
- scenario B: trasferimento delle credenziali utente/password nel nuovo sistema senza alcuna ulteriore azione
- scenario C: trasferimento delle credenziali utente/password relative all'account nel sistema della Provincia di Prato e comunicazione al soggetto della dismissione dell'altra coppia di credenziali a partire dalla data di entrata in funzione del sistema

Tale attività si realizza sotto la diretta responsabilità della Ditta aggiudicataria, che dovrà concordare con il precedente fornitore le modalità attuative per il trasferimento dei dati relativi alle configurazioni dei sistemi centrali di base per la gestione della rete, di provisioning degli utenti, di logging degli accessi e data retention a norma di legge.

La Ditta dovrà elaborare un piano di migrazione degli Access Point dal precedente sistema all'attuale in modo da ridurre al minimo i tempi di inutilizzabilità di tali apparati, che dovranno comunque essere inferiori ai tempi massimi stabiliti in 48 ore per singolo Access Point.

L’avviamento consiste nella graduale messa a regime del sistema nel rispetto dei tempi massimi complessivi e nei limiti dei tempi di attivazione massimi stabiliti per ciascun Access Point; questa ultima durata stabilisce il tempo massimo entro cui il singolo apparato può non essere on-line e quindi erogare servizio di connettività.

In considerazione della complessità del sistema, il piano di migrazione avverrà con gradualità, al fine di ridurre i disagi e verificare la corretta esecuzione dell'attività di trasferimento dal precedente sistema, secondo le seguenti fasi:

- attivazione dei sistemi centrali e recupero dei dati di registrazione degli utenti pregressi;
- attivazione di n.2 Access Point per ciascuna tipologia (**R** e **L**) per verificare il funzionamento del sistema di registrazione, autenticazione, monitoraggio ed erogazione dei servizi di navigazione;
- verifica e collaudo parziale dei sistemi attivati;
- attivazione di tutti gli altri Access Point con collaudo finale.

La Ditta offerente deve corredare la propria offerta con un Piano di Avvio in cui dovranno essere dettagliate e specificate le singole fasi di attivazione del sistema con i relativi tempi, tenendo presente i tempi massimi definiti dal bando.

Il Piano di Avvio sarà vincolante ed il suo rispetto da parte della Ditta rileverà ai fini della regolarità della prestazione a carico della medesima.

La data di “Fine Avviamento” del Sistema deve risultare da specifico verbale.

Il verbale deve essere firmato dal Responsabile del Fornitore.

Il Responsabile del Fornitore notifica per iscritto al Responsabile del contratto, attraverso lo specifico verbale predetto, la data di “Fine Avviamento” del Sistema.

Il Responsabile del contratto potrà integrare il verbale di “Fine Avviamento” del Sistema con proprie dichiarazioni, sottoscrivendo il verbale citato.

10.3 Collaudo

Il collaudo costituisce la fase finalizzata all'accertamento che:

- i sistemi centrali di registrazione, autorizzazione all'accesso ai servizi e monitoraggio siano in grado di svolgere le funzioni richieste e che presentino le caratteristiche tecniche dichiarate dalla Ditta aggiudicataria sulla scorta della documentazione fornita;
- il sistema nel suo complesso sia in grado di assicurare prestazioni regolari in condizioni normali di funzionamento;

In occasione del collaudo si dovrà almeno:

- verificare l'effettiva copertura delle aree elencate con l'utilizzo di un dispositivo portatile;
- verificare l'effettivo posizionamento della cartellonistica;
- effettuare l'attivazione di almeno due utenze verificando l'effettivo funzionamento delle politiche di accesso concordate;
- verificare in almeno tre punti perimetrali di ogni area oggetto di copertura la presenza effettiva, tramite il collegamento di un comune PC portatile, del 50% della banda nominale offerta dalle linee ADSL utilizzate, tramite il collegamento con un servizio su Internet pubblico oppure reso disponibile dalla società aggiudicataria.

Per la specificità dei dati trattati, il collaudo non potrà verificare la correttezza dell'operazione di recupero dei dati pregressi: la Ditta aggiudicataria si impegna pertanto a intervenire a correggere tutti i malfunzionamenti che si dovessero manifestare, offrendo un canale di comunicazione specifico agli utenti del sistema già registrati.

10.4 Modalità di esecuzione del Collaudo

Il collaudo del sistema sarà avviato entro 20 giorni lavorativi dalla data di notifica scritta da parte del Responsabile del Fornitore, del verbale di "Fine Avviamento".

Il processo di collaudo consiste nella verifica della rispondenza funzionale del sistema alle prescrizioni del Capitolato Tecnico e del Progetto-Offerta della Ditta aggiudicataria.

Il collaudo è svolto da una Commissione di Collaudo composta da personale individuato dalla Provincia di Prato e dal Comune di Prato, qualificato per le verifiche di natura tecnico-informatica e per la verifica delle funzionalità e delle operatività del sistema.

Il collaudo verifica che il sistema sia conforme in riferimento ai requisiti funzionali descritti nel Capitolato Tecnico e nel Progetto-Offerta della Ditta, anche sulla scorta di tutte le prove funzionali e diagnostiche stabilite nella documentazione prodotta dalla Ditta.

I risultati del collaudo sono documentati in uno specifico verbale, firmato dai componenti la commissione di collaudo. Il Rappresentante della Ditta aggiudicataria potrà integrare il verbale suddetto con proprie dichiarazioni, sottoscrivendo il verbale citato.

Qualora in fase di collaudo risultassero vizi, difetti o discordanze tra i prodotti consegnati e quanto previsto dal contratto o dall'offerta tecnica delle ditte aggiudicatarie, la Commissione di Collaudo richiederà per iscritto alla Ditta aggiudicataria di effettuare i rifacimenti e le modifiche necessari per eliminare i vizi, i difetti e le discordanze riscontrate.

In caso di collaudo negativo, la Ditta aggiudicataria ha l'obbligo di rimuovere tutte le anomalie delle forniture rispetto alla non rispondenza alle specifiche ed a malfunzionamenti, nel termine di 10 giorni solari, consecutivi ed ininterrotti, a decorrere dalla data del verbale di collaudo che ha accertato le irregolarità.

Qualora l'esito del collaudo risulti negativo non si considererà conclusa la fase di installazione della rete e non saranno sospesi i termini da cui far decorrere le eventuali penali relative alla messa in esercizio della rete.

L’avvenuta eliminazione di carenze o difetti deve risultare dal nuovo certificato di collaudo redatto dalla Commissione di Collaudo. Le operazioni di collaudo sono ripetute alle stesse condizioni e modalità, con eventuali oneri a carico della Ditta aggiudicataria, entro 15 (quindici) giorni solari dal precedente collaudo e tale ritardo non sospenderà il pagamento delle relative penali se dovute.

I risultati del collaudo devono risultare da specifico verbale, composto da documenti firmati dalla Commissione di Collaudo.

Il collaudo positivo non esonera la Ditta aggiudicataria per eventuali difetti ed imperfezioni che non fossero emersi all’atto del collaudo ma venissero in seguito accertati.

Resta in ogni caso ferma la facoltà da parte delle Amministrazioni Committenti, qualora i vizi o carenze eventualmente riscontrati non siano facilmente eliminabili, di rifiutare in tutto o in parte la fornitura a danno della Ditta aggiudicataria, ferma restando l’applicazione delle penali.

Il pagamento della fornitura sarà effettuato:

- il servizio di manutenzione con canone anticipato con cadenza mensile/bimestrale a scelta del fornitore;
- i corrispettivi relativi alle forniture al termine del collaudo di ciascuna.

Il pagamento del servizio sarà effettuato dietro la presentazione di fattura che saranno liquidate sulla base delle procedure in uso presso gli enti committenti.

11 Servizi di supporto alla fornitura

Durante il periodo di erogazione del servizio di accesso ad Internet, tutti i seguenti sistemi e dispositivi dovranno essere mantenuti in perfetto funzionamento ed efficienza secondo i livelli di servizio successivamente riportati:

- i sistemi centrali;
- il “modulo Accentratore”;
- gli AP indoor (da interno) di tipo R o L;
- gli AP outdoor (da esterno) di tipo R o L inclusivi dei servizi di alimentazione elettrica e connettività Internet.

Per gli apparati Access Point che si rende necessario sostituire, indipendentemente dal fatto che siano preesistenti o forniti nell'ambito del contratto, la Ditta è tenuta a fornire il servizio di eventuale riconfigurazione rispetto a quella base di fabbrica al fine di renderli utilizzabili all'interno del sistema.

Tutti gli apparati devono essere ripristinati a spese dell'affidatario in caso di danni causati da qualsiasi evento compreso gli atti vandalici. Questo comprende anche la cartellonistica installata.

L’attività di manutenzione dei sistemi centrali deve comprendere:

- gli interventi tecnici necessari per eliminare i difetti riscontrati durante l’utilizzo dei sistemi o per l’installazione di eventuali nuove release del software di base;
- gli interventi tecnici necessari per adeguare i programmi applicativi alla evoluzione della normativa;
- l’addestramento del personale tecnico dell'Amministrazioni Committenti all’utilizzo delle funzioni modificate/aggiunte a seguito di interventi di manutenzione e consegna della relativa documentazione.

Per la manutenzione correttiva questo servizio deve almeno prevedere:

- la raccolta delle segnalazioni relative a malfunzionamenti applicativi;
- la presa in carico del problema che deve essere garantita entro il **tempo massimo di due ore** dal ricevimento della segnalazione;
- la risoluzione dei malfunzionamenti;
- la produzione della reportistica tecnica.

Il sistema di accesso Wireless ad Internet offerto dovrà essere operativo 24 ore al giorno per 7 giorni la settimana. Eventuali interruzioni del servizio per manutenzioni straordinarie dovranno essere comunicate almeno 48 ore prima.

L’inoperatività programmata non potrà riguardare più del 25% degli apparati contemporaneamente ed essere pubblicizzata anche mediante opportune pagine sul captive portal.

La Ditta si impegna a risolvere i malfunzionamenti sulla propria piattaforma nei tempi e modi specificati di seguito.

Per quanto riguarda la tempestività nella risoluzione dei problemi si precisa che i tempi di intervento si calcolano a partire dalla ricezione della richiesta da parte del servizio di manutenzione se la ricezione stessa è avvenuta durante un giorno lavorativo negli orari delle Amministrazioni Committenti, mentre la ricezione viene fatta coincidere con le ore 8:00 del primo giorno lavorativo seguente a quello di ricezione della segnalazione, nel caso in cui il messaggio abbia raggiunto il servizio di manutenzione al di fuori dell’orario sopra indicato.

Il tempo di risoluzione dei problemi è calcolato come il tempo intercorrente tra i momento della ricezione della richiesta di intervento da parte del servizio di manutenzione della Ditta aggiudicataria ed il momento della ricezione da parte della Provincia della comunicazione di avvenuta risoluzione del malfunzionamento o della avvenuta soddisfazione della richiesta. Il problema è da considerarsi risolto anche se il malfunzionamento è provvisoriamente risolto con interventi manuali o automatici di immediata attivazione, purché venga contemporaneamente attivato l'intervento di risoluzione definitiva del problema.

Il ripristino delle funzionalità del sistema deve essere garantito secondo i seguenti livelli di servizio:

- Ripristino dell'operatività di un Access Point non funzionante a seguito di guasto di un componente del sistema – 72 ore
- Modifica del limite temporale e di traffico per singolo Access Point – 72 ore (se offerto)
- Modifica del limite temporale e di traffico per tutti gli Access Point – 72 ore
- Modifica dei protocolli da permettere o filtrare sugli Access Point – 72 ore
- Modifica del contenuto del captive portal per singolo Access Point – 72 ore (se offerto)
- Modifica della lista dei siti web liberamente accessibili da ogni singolo Access Point – 72 ore
- Modifica del contenuto del captive portal per tutti gli Access Point – 72 ore
- Integrazione di un sistema di autenticazione esterna tramite RADIUS – 7 gg
- Modifica dei requisiti di identificazione e registrazione degli utenti – 15 gg