Linee guida per l’erogazione del servizio pubblico wi-fi free

AGID

09 giu 2020

Indice

consultation

La consultazione pubblica relativa al presente documento è attiva dal **07 febbraio** al **08 marzo 2019**. Questo documento raccoglie il testo delle Linee guida Linee guida per l'erogazione del servizio pubblico wi-fi free, disponibile per la consultazione pubblica.

Negli ultimi anni si è assistito ad un processo evolutivo nell'ambito delle tecnologie di comunicazione in mobilità e/o senza fili che ha enormemente incrementato la diffusione di servizi sempre più sofisticati che hanno contribuito ad alimentare la necessità di connettività internet sempre disponibile. Tutto ciò è stato in larga parte favorito dalla disponibilità di dispositivi multicanale e dotati di adeguate risorse hardware nonché di piattaforme middleware modulari. La diffusione quindi di servizi e applicazioni ha concorso e concorre alla "Crescita Digitale" del Paese in questa era tecnologica «sempre» connessa, nella quale persone e cose sono in grado di comunicare e scambiare informazioni in tempo reale. La necessità di connessione permanente richiede evidentemente la disponibilità di accesso ad internet senza soluzione di continuità, pertanto il servizio di accesso ad Internet in mobilità, o wireless, viene a divenire esso stesso un servizio richiesto dagli utenti in particolare nei settori turistici, sanitari e della formazione. La Pubblica Amministrazione di conseguenza, in qualità di "facilitatore" all'accesso a questi servizi è chiamata a fornire nuovi servizi digitali, in modalità gratuita per gli utenti, e utilizzando le tecnologie Wi-Fi per la loro fruizione.

Fig. 1: Servizio WiFi free

CAPITOLO 1

Scenario

A seguito dell'emanazione del Regolamento Europeo N°1316/2013 per la promozione della connettività Internet e la sua estensione alle Comunità Locali (COM (2016)589)- nel seguito indicato anche come Regolamento -, il 2 dicembre 2016 il Consiglio Europeo ha adottato un orientamento generale su una proposta volta a promuovere connessioni internet gratuite nelle comunità locali mediante un programma finanziato dall'UE denominato «WiFi4EU».

La proposta mira a fornire Wi-Fi gratuito nei municipi, parchi pubblici e altri centri della vita pubblica. Uno degli obiettivi strategici della Commissione per il 2025 prevede che i siti dell'Unione in cui vengono erogati servizi pubblici, ad esempio le pubbliche amministrazioni, le biblioteche e gli ospedali, siano dotati di connessioni a internet fisse alla velocità del Gigabit al fine di poter erogare in maniera affidabile i servizi digitali.

Il Regolamento nasce nell'ambito della Strategia del *"Digital Single Market"* della DG Connect della Commissione Europea e ad esso vanno fatte riferire in ambito nazionale le previsioni dell'Art.8 bis del CAD. Tale articolo richiede che le PA forniscano il servizio di connettività Wi-Fi gratuito ai cittadini e turisti, utilizzando la banda internet disponibile sui propri collegamenti, senza impatto sui normali processi di lavoro.

In Italia, l'attuale scenario scenario di partenza per l'adozione di soluzioni per la realizzazione ed erogazione del servizio di Wi-Fi gratuito, presenta le seguenti caratteristiche:

- esistono già molte iniziative intraprese da parte di enti della PA;
- la cornice normativa relativamente alla sicurezza e alla privacy è in continua evoluzione e di recente emanazione;
- i requisiti normativi relativi alla gestione della sicurezza e della privacy sui dati degli utenti sono requisiti vincolanti per gli aspetti tecnologici.

Tutto ciò premesso, il presente documento intende definire le linee guida per l'erogazione del servizio WI-FI pubblico gratuito ai cittadini, da parte della Pubblica Amministrazione locale e centrale (PA) fornendo un quadro normativo e tecnologico entro il quale armonizzare le iniziative in essere con le strategie governative nazionali ed europee. L'Agenzia procederà all'aggiornamento nel tempo del documento al fine di mantenerlo allineato alle evoluzioni normative e tecnologiche del settore di riferimento.

Organizzazione del documento

Il presente documento è così strutturato:

- Cap.1 «Cosa è il Wi-Fi»: panoramica sugli standard comunemente usati, su una architettura tipica, sui criteri per garantire la sicurezza e prevenire potenziali attacchi cibernetici, le prestazioni obbligatorie in capo agli operatori di telecomunicazioni verso l'Autorità Giudiziaria e prescrizioni sulla Privacy;
- Cap.2 «Le maggiori esperienze della WI-FI pubblica nella PA»: descrive esperienze virtuose e soluzioni già adottate in ambito pubblico;
- Cap.3 «Criteri di implementazione del servizio per le PA «: tratta dei criteri tecnici implementativi del servizio per le Pubbliche Amministrazioni;
- Cap.4 «Possibili evoluzioni tecnologiche del servizio»: vengono descritti scenari di possibili evoluzioni tecnologiche e gestionali del servizio;
- Cap.5 «Federabilità dei servizi WI-FI «: descrive la possibilità di federare i servizi attraverso il progetto Wifi.Italia.it

1.1 Applicabilità e destinatari del documento

Come previsto dall'art.8-bis del d.lgs. 82 del 2005 e s.m.i. - Codice dell'Amministrazione Digitale -

"I soggetti dell'articolo 2, comma 2[1], favoriscono, in linea con gli obiettivi dell'Agenda digitale europea, la disponibilità di connettività alla rete Internet presso gli uffici pubblici e altri luoghi pubblici, in particolare nei settori scolastico, sanitario e di interesse turistico, anche prevedendo che la porzione di banda non utilizzata dagli stessi uffici sia messa a disposizione degli utenti nel rispetto degli standard di sicurezza fissati dall'AGID*".

Lo stesso art.8-bis al comma 2 prevede che

«I soggetti di cui all'articolo 2, comma 2, mettono a disposizione degli utenti connettività a banda larga per l'accesso alla rete Internet nei limiti della banda disponibile e con le modalità determinate dall'AGID».

In tale contesto normativo, il Piano Triennale per l'informatica nella Pubblica amministrazione triennio 2017-2020 (di seguito identificato anche come Piano Triennale) sottolinea l'importanza della connettività wifi pubblica nonché l'adeguamento delle infrastrutture facendo riferimento alla necessità di «*avviare i processi di adeguamento della propria connettività*», per fornire tra gli altri servizi digitali, quelli wireless necessari all'uso pubblico.

Nel seguito del presente documento verranno esposte le modalità attraverso le quali potrà essere resa disponibile la banda destinata al wireless gratuito da parte delle Pubbliche Amministrazioni. nonché i criteri di sicurezza da adottare in tale ambito.

[1] Le disposizioni del presente Codice si applicano a) alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione; b) ai gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse; c) alle società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b); 3. Le disposizioni del presente Codice e le relative Linee guida concernenti il documento informatico, le firme elettroniche e i servizi fiduciari di cui al Capo II, la riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, il domicilio digitale e le comunicazioni elettroniche di cui all'articolo 3-bis e al Capo IV, l'identità digitale di cui agli articoli 3-bis e 64 si applicano anche ai privati, ove non diversamente previsto.

CAPITOLO 2

Cosa è il Wi-Fi

Il Wi-Fi (Wireless Fidelity), detta anche rete wireless o rete Wi-Fi è una tecnologia che permette ai dispositivi di scambiarsi dati senza fili, utilizzando onde radio. Il WiFI, oggi, aggiornato e integrato da sviluppi e innovazioni, è diventato uno dei principali standard per la trasmissione dei dati in formato digitale ed è in continua diffusione e crescita.

Atto costitutivo di questa tecnologia può considerarsi la decisione della Federal Communications Commission (FCC) statunitense (l'ente regolatore del settore delle telecomunicazioni) di liberare alcune frequenze e renderle disponibili all'uso civile senza obbligo di licenza. Nel 1997 con la prima versione ufficiale del protocollo denominato «IEEE 802.11», sviluppato da una delle commissioni del Institute of Electrical and Electronic Engineers (IEEE), associazione internazionale di scienziati professionisti che si occupa di ricerche sulle nuove tecnologie, iniziò l'epoca delle trasmissioni wireless con una connessione che raggiungeva la velocità di 2 Mbit al secondo. Due anni più tardi, nel 1999, vedeva la luce il protocollo 802.11b, insieme con il nome «Wi-Fi» e il relativo logo e nasceva ufficialmente la tecnologia Wi-Fi. Da quel momento si è assistito al costante e continuo sviluppo di questa tecnologia e all'evoluzione degli standard anche per via della grande diffusione dei dispostivi mobili.

2.1 Gli standard del Wi-Fi

In questo paragrafo mostreremo le tappe fondamentali delle certificazioni dello IEEE che stabiliscono gli standard tecnologici sui quali i produttori realizzano i loro dispositivi Wi-Fi. Ad oggi gli standard Wi-Fi esistenti sono 9, anche se i più utilizzati sono 4.

Tabella 2.1: Tappe fondamentali implementazioni ordinate per velocità di trasmissione crescente WiFi

Certificazione	Velocità di trasmissione max	Frequenza di lavoro	Mezzo trasmissivo
802.11	Da 1 a 2 Mb/s	2.4 GHz	Infrarossi/onde radio
802.11b	11 Mb/s	2.4 GHz	Onde Radio
802.11a	54 Mb/s	5,4 GHz	Onde Radio
802.11g	54 Mb/s	2.4GHz	Onde Radio
802.11n	300 Mb/s	2.4GHz/5,4 GHz	Onde Radio
802.11ac	1300 Mb/s	5,4 GHz	Onde Radio
IEEE 802.11ad	6750 Mb/s	60 GHz	Onde Radio

Come possiamo notare in tabella, l'evoluzione tecnologica avvenuta a cavallo degli ultimi 20 anni, si focalizza sulla velocità di trasmissione, ma come vedremo ne prossimi paragrafi anche nei sistemi di sicurezza ed autenticazione.

Nel giugno 2003 venne rilasciata la certificazione 802.11g, che fa segnare un netto miglioramento nelle prestazioni (sia per la forza del segnale sia per i picchi di velocità raggiungibili) rispetto ai due predecessori. Lo standard 802.11g lavora sulla banda di frequenza da 2,4 GHz, copre aree di circa 100 metri e permette teoricamente la trasmissione di dati fino a 54Mbps (sebbene mediamente si attesti attorno ai 22-24 Mbps). Un ulteriore avanzamento delle prestazioni si è avuta con la certificazione 802.11n, rilasciata nel 2009. Questo nuovo standard si basa sull'utilizzo di diverse antenne MIMO (multiple-input, multiple-output) che lavorano sulle frequenze di 2,4 GHz e 5 GHz consentendo velocità che possono, in teoria, arrivare anche 600 Mbps. A questo è seguito lo standard 802.11ac, che ha portato le velocità di connessione a 1,3 Gbps (il doppio rispetto allo standard n, oltre 20 volte più veloce rispetto allo standard g) per via della differente divisione in sottobande della banda da 5 GHz e dall'impiego di differenti standard di comunicazione. Negli ultimi anni, la Wi-Fi Alliance ha studiato e definito altri tre standard che, sfruttando bande di comunicazioni differenti, ampliano lo spettro delle possibili applicazioni e utilizzi dello standard senza fili. L'IEEE 802.11ah sfrutta la banda da 1 gigahertz per connessioni più stabili e meno soggette al rumore; l'IEEE 802.11af, detto anche super Wi-Fi, lavora sulla banda di comunicazione riservata alle comunicazioni televisive per assicurare connessioni stabili e a grande velocità; l'IEEE 802.11ad (detto anche WiGig), infine, lavora sulla banda di frequenza dei 60 GHz e, pur coprendo distanze minori, può raggiungere la velocità di connessione di 7 gigabit ed è utilizzabile per le applicazioni "smart home" che richiedono una banda sempre più ampia e stabile.

2.2 Architettura di una rete Wi-Fi

Una rete Wi-Fi è composta da uno o più Access Point (AP) che possono essere adibiti a «sorgente» del segnale, e uno o più client che si connettono ad essa.

A sua volta le rete Wi-Fi è generalmente collegata alla rete fissa; l'Access Point può infatti essere considerato come il Gateway tra la rete senza fili e quella fissa. Il segnale wireless di un singolo access point solitamente copre un'area tra i 50 ed i 100 metri in base alla configurazione architettonica dell'area coperta, ma può essere esteso in diversi modi. Si può amplificare, ad esempio, attraverso il collegamento di differenti AP tramite cavo, oppure creando un «ponte» wireless con ripetitori di segnali. Ogni AP trasmette, ogni 100 ms, un pacchetto dati, chiamato *beacon*[2] contenente lo SSID (Service Set Identifier) che rappresenta l'identificativo della rete e altre informazioni, come il protocollo di sicurezza utilizzato. Il client (qualsiasi dispositivo dotato di scheda Wi-Fi o un ripetitore di segnale) può decidere di connettersi alla rete seguendo diverse logiche: ad esempio, può collegarsi alla rete con un SSID noto, ossia a una rete alla quale già ci si è connessi in precedenza, oppure a quella dal segnale più forte e che quindi garantisce le prestazioni migliori (modalità *always best connected*).

[2] Frame non cifrati

2.3 Accesso e autenticazione alla rete Wi-Fi

Ogni volta che un client accede ad una rete wireless, si avvia un processo di autenticazione che consiste in tre fasi: discovery della rete, autenticazione e associazione. Ognuna di queste tre fasi avviene con lo scambio di richieste e risposte tramite *beacons*. La fase di autenticazione è la parte più delicata dell'intero processo.

2.3.1 Discovery della rete

Questa fase permette ad un client di individuare la presenza della rete, cercando il segnale degli AP secondo determinate regole (segnale più forte, velocità maggiore, ecc.); la rete trovata può essere aperta o chiusa. Una rete wireless aperta si comporta in modo che gli AP inviino periodicamente degli opportuni frame non cifrati che contengono tutte le informazioni che servono ai client per collegarsi (SSID, velocità di trasmissione, ecc.). In una rete chiusa, invece, è compito dei client preoccuparsi di trovare gli AP tramite l'invio su varie frequenze di opportuni frame di richiesta, in attesa che un AP in ascolto risponda con un frame di risposta.

2.3.2 Autenticazione

Una volta completata la fase di discovery, un client deve autenticarsi presso l'AP con cui vuole comunicare. L'autenticazione è un processo che permette a due soggetti in comunicazione di scambiare delle credenziali, consentendo successivamente di verificare la validità delle stesse attraverso protocolli specifici che utilizzano metodi di cifratura.

2.3.3 Associazione

Se un client wireless è stato autenticato con successo, allora può chiedere di essere associato alla rete. In pratica il client sceglie un unico AP (generalmente secondo le strategie di discovery) che poi lo abilita a collegarsi. Con la fase di associazione si conclude il processo di autenticazione.

2.4 Sicurezza ed autenticazione

Un ruolo cruciale nel progettare una rete sicura è giocato dall'autenticazione delle parti in comunicazione, per garantire la confidenzialità dei dati in transito. Infatti per autenticazione si intende quel processo che permette di stabilire con certezza l'interlocutore. La confidenzialità invece, si riferisce alla garanzia che i dati in transito siano accessibili solo alle parti interessate, e per questo scopo si utilizza la crittografia. Un utente che voglia accedere ad un network deve possedere delle credenziali di accesso come ad esempio un account o un certificato digitale, deve ad ogni modo essere in grado di stabilire, in modo sicuro, che il Server oppure, per le reti WI-FI l'Access Point che chiede le credenziali appartenga effettivamente ad una rete legittima, in modo da non fornire le proprie informazioni ad un sistema non autorizzato.

Molteplici sono state le soluzioni adottate per garantire la sicurezza delle reti wireless che si sono evolute nel corso degli anni. I meccanismi inerenti la cifratura e l'autenticazione erano direttamente definiti dallo standard con il protocollo WEP (Wired-Equivalent-Privacy), che ha in seguito mostrato gravi falle di sicurezza. L'evoluzione di tale protocollo è il WPA (Wi-Fi Protected Access) nelle due versioni: WPA e WPA2. Notiamo che esistono due implementazioni di WPA2:

- WPA2-PSK (pre-shared key) o personal
- WPA2-Enterprise (o WPA2 802.1X).

La prima è destinata ad un uso personale e per piccole reti di ufficio, mentre la seconda è per uso aziendale e di più complessa configurazione. Per il corretto funzionamento del sistema di autenticazione WPA2-Enterprise[3] si rende necessario un server di autenticazione *«Radius»* (Remote Authentication Dial In User Service).

Nel caso di una wireless, è l'AP che è adibito alle funzioni di controllore di accesso. Il Radius, o un server/servizio di autenticazione che risponda agli standard definiti dalle RFC 2865 e 2866, permette di validare l'identità dell'utente, trasmessa dal controllore di accesso, e di rinviare a quest'ultimo i permessi associati in funzione delle informazioni di identificazione fornite. Inoltre, tale server permette di memorizzare e di rendere compatibili le informazioni riguardanti gli utenti per, ad esempio, mantenerle per renderle disponibili per attività giudiziaria (nel caso di un service provider ad esempio).

Di seguito l'analisi del funzionamento di una rete resa sicura con lo standard 802.1x:

1. Il controllore di accesso, avendo ricevuto precedentemente una richiesta di connessione da parte dell'utente, invia una richiesta di identificazione;

2.L'utente risponde alla richiesta e invia una risposta al controllore di accesso, che la inoltra al server di autenticazione;

3.Il server di autenticazione invia la risposta di identificazione (metodo di identificazione) al controllore di accesso, che lo trasmette all'utente;

4. L'utente, la cui identità è corretta, viene accettato sulla rete o su una parte di rete, secondo i permessi;

5.Se l'identità dell'utente non si è potuta verificare, il server di autenticazione invia un rifiuto e il controllore di accesso rifiuterà l'accesso alla rete all'utente.

2.5 Sicurezza e prevenzione di potenziali attacchi

Garantire la sicurezza di un sistema informativo e, delle informazioni in esso contenute, si traduce nell'impedire a potenziali soggetti attaccanti l'accesso o l'uso non autorizzato di informazioni e risorse.

Al fine di mitigare gli attacchi, la perdita di dati e utilizzo improprio delle infrastrutture, si rende necessario impedire la contraffazione ovvero la capacità di creazione e invio di falsi messaggi creati con le credenziali di un utente autorizzato dal sistema.

Le tecniche intrusive di rete più comuni consistono nella:

- capacità di inserimento di apparati wireless non autorizzati;
- capacità di intercettazione passiva e monitoraggio del traffico di rete;
- capacità di disturbo del segnale (jamming);
- capacità di attacchi ai meccanismi di cifratura per via di debolezze riscontrate a livello protocollare per furto di dati;
- errori nella configurazione della rete wireless.

Le tecniche di intrusione succitate, implementate con diverse tecnologie ed in costante evoluzione, possono mettere a repentaglio la sicurezza delle informazioni e dei dati, per i quali l'organizzazione deve garantire:

- Integrità: dati non modificati durante la trasmissione;
- Segretezza e Riservatezza: cifratura dei dati in modo che non siano intercettabili;
- Controllo Accessi: controllo accessi alle risorse da e per il sistema;
- Disponibilità: un sistema deve essere disponibile almeno al 99,9% e solo per gli utenti accreditati;

[3] Questo tipo di gestione amministra correttamente non solo gli accessi ma anche i profili di servizio. L»802.1x si basa sul protocollo EAP (Extensible Authentication Protocol), definito dall»IETF, il cui ruolo è di trasportare delle informazioni di identificazione degli utenti. Il funzionamento del protocollo EAP è basato sull'utilizzo di un controllore di accesso, (l'authenticator), che stabilisce l'accesso alla rete per un utente (il supplicant).

- Autenticazione: verifica dell'identità dichiarata dall'utente.

Con riguardo all'autenticazione ci possiamo riferire all'identificazione certa degli utenti nella rete, degli host, delle applicazioni, dei servizi e delle risorse[4]

[4] Le tecnologie standard che permettono questo includono alcuni protocolli di autenticazione come RADIUS (Remote Authentication Dial-In Users Service), Kerberos. Inoltre nuove tecnologie che si fondano su Certificati Digitali, Smart Card e Token si stanno imponendo sempre più nelle soluzioni per la definizione e verifica dell'identità.

CAPITOLO 3

Framework normativo per la gestione del servizio Wi-Fi

Il rapido sviluppo dei servizi nel cosiddetto «spazio cibernetico», se da un lato presenta innumerevoli vantaggi, quali l'abbattimento delle frontiere geografiche, l'erogazione di nuovi tipi di servizi e lo scambio di conoscenza a livello globale, dall'altro è fonte di nuovi e complessi rischi.

Gli eventi avversi nel cyberspazio, l'evoluzione delle tecniche di hacking, la necessità di controllo delle reti e infrastrutture per via del fenomeno crescente del terrorismo, impone, contemporaneamente ai requisiti della sicurezza e della privacy, la necessità per Operatori di Telecomunicazioni di fornire all'attività giudiziaria i dati di traffico telematico o telefonico utili a risalire all'identità dell'utente.

Il Parlamento Europeo con la Direttiva (eu) 2016/1148 del 6 Luglio 2016, in coordinamento con Enisa[5] richiede agli operatori di collaborare allo sviluppo di misure, per raggiungere un elevato comune livello di sicurezza delle reti e dei sistemi informativi in Europa.

La normativa italiana a supporto del tema del presente documento appare ancora stratificata, scarsamente intellegibile e soprattutto poco diffusa.

Senza pretesa di esaustività nel trattare una tematica tanto complessa, con il presente contributo si intende fornire alcune indicazioni, per orientarsi nell'evoluzione della disciplina del free wi-fi nonché del regime di responsabilità, civile e penale, del gestore del servizio, n caso di uso non conforme della rete da parte dell" utenza.

Con riguardo all'ordinamento italiano, la normativa in materia di controllo, accesso e gestione del Wi-Fi libero va fatta risalire all'art. 7, D.L. 27 luglio 2005, n.144[20] (c.d. decreto Pisanu) convertito in L. 31 luglio 2005, n. 155, recante «misure urgenti per il contrasto del terrorismo internazionale».

Il decreto, adottato sull'onda delle preoccupazioni in materia di sicurezza a seguito degli attentati terroristici del 2005 a Londra, all'art. 7 poneva in capo ai gestori di punti di accesso ad internet alcuni obblighi di preventiva identificazione degli utenti.

Si trattava in sostanza di procedure che permettevano l'identificazione degli utenti, come la creazione manuale di account con associazione al numero di documento di identità dello *user* oppure la validazione degli utenti via SMS o tramite carta di credito. Successivamente con il c.d. decreto Milleproroghe (D.L. 29 dicembre 2010, n. 225[21], art. 2,

[5] European Union Agency for Network and Information Security.

[20] http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2005-07-27;144!vig=

[21] http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2010-12-29;225!vig=

comma 19, convertito con L. 26 febbraio 2011, n. 10[22]) sono stati abrogati il quarto e quinto comma dell'art. 7 del decreto Pisanu, che prevedevano gli obblighi di preventiva identificazione degli utenti.

Il suddetto orientamento è stato definitivamente confermato con l'adozione del c.d. decreto del «Fare» (D.L. 21 giugno 2013, n. 69[23], art. 10, convertito in L. 9 agosto 2013, n. 98[24]), il quale, sintetizzando quanto già definito dalle precedenti modifiche abrogative e colmando in parte il vuoto normativo che avevano lasciato, ha liberalizzato l'accesso alla rete internet tramite tecnologia Wi-Fi, escludendo qualsiasi obbligo di preventiva autenticazione da parte degli utilizzatori.

Sono tuttavia vigenti per gli operatori di Telecomunicazione obblighi di conservazione dei dati di traffico, che permettano l'identificazione dell'utente per 12 mesi e misure di sicurezza da applicare, secondo le prestazioni obbligatorie imposte dall'art.132 Dlgs 193/2003 modificato da Dlgs 109/2008 (Dlgs Frattini).

Di recente emanazione è infine il Dlgs Gentiloni in tema di applicazione delle normative europee sulla sicurezza che estende a 6 anni l'obbligo di conservazione dei dati di traffico che permettano l'identificazione dell'utente.

3.1 Prestazioni Obbligatorie per Operatori di Telecomunicazioni verso l'Autorità Giudiziaria e prescrizioni sulla Privacy

I requisiti per garantire la sicurezza sulle reti Wi-Fi si focalizzano principalmente, come si evince da quanto riportato fin qui, sul controllo dell'accesso in termini di verifica dell'identità utente, che viene autorizzato all'accesso sulla base di permessi e privilegi stabiliti dal provider.

Gli aspetti di verifica dell'identità o, in generale, la capacità di poter identificare l'utente attraverso le infrastrutture tecnologiche sono normati dal Codice delle Comunicazioni Elettroniche (c.c.e.).

Il suddetto codice all'art.96 introduce per la prima volta in Italia il concetto di «prestazioni obbligatorie» che operatori di telecomunicazioni devono garantire all'Autorità Giudiziaria.

Tale concetto è recepito direttamente dalla direttiva europea sulle autorizzazioni, facente parte del c.d. «Pacchetto Telecom».

Questo tema sembra avere meno dignità, se confrontato con altri come l'antifrode o la sicurezza informatica o la sicurezza cibernetica, ma al contrario, come questi gode di una naturale autonomia in termini di competenza, tantoché ci si potrebbe riferire alle «prestazioni obbligatorie» come disciplina autonoma.

Il c.c.e. prevede la *«Possibilità per le autorità nazionali competenti di effettuare legalmente intercettazioni delle comunicazioni in conformità della direttiva 97/66/CE e della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati»*.

Le «prestazioni obbligatorie» costituiscono parte integrante delle stesse comunicazioni e, anche, la Comunità europea le inserisce tra le condizioni necessarie per la concessione dell'autorizzazione agli operatori.

Non è quindi perfettamente corretto esaminare il tema in questione esclusivamente dal punto di vista della «security» o della «cyber security», riferendosi a requisiti fondamentali come «segretezza», «riservatezza «e» integrità».

Il riferimento quindi è l'art. 96 del c.c.e., modificato dalla legge n. 228 del 24 dicembre 2012 (legge di Stabilità del 2012), il quale afferma al comma 2 che *«Le prestazioni relative alle richieste di intercettazioni sono individuate in un apposito repertorio nel quale vengono stabiliti le modalità ed i tempi di effettuazione delle prestazioni stesse, gli obblighi specifici, nonché il ristoro dei costi sostenuti»*. Possiamo elencare di seguito quelle che nella pratica si intendono come «prestazioni obbligatorie per l'Autorità Giudiziaria:

[22] http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2011-02-26;10!vig=
[23] http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2013-06-21;69!vig=
[24] http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2013-08-09;98!vig=

1. **la fornitura di informazioni anagrafiche dell'utenza intestataria del contratto**, in termini di informazioni che l'operatore ha registrato per l'attivazione del servizio, eventualmente comprendendo le informazioni di fatturazione, con l'indicazione della data in cui si è risolto il contratto;
2. **l'intercettazione delle comunicazioni**, mediante fornitura dei contenuti e dei metadati ad essi associati, intesa come intercettazione delle comunicazioni sia a livello di accesso, cioè indipendentemente dai servizi usufruiti dall'utenza come appunto la telefonia o la connessione dati, sia a livello di servizio come ad esempio del solo servizio email;
3. **il tracciamento delle comunicazioni**, inteso come fornitura dei soli metadati che accompagnano i contenuti delle comunicazioni intercettate;
4. **la localizzazione dell'utenza**, valida solo per la telefonia mobile, che si suddivide in localizzazione standard associata alla comunicazione e localizzazione di precisione che prescinde dalle comunicazioni dell'utente;
5. **l'identificazione dell'utenza**, intesa come il risalire all'identificativo tecnico che è stato utilizzato dall'utenza, valido sia per le connessioni dati per le quali dall'IP si vuole risalire al numero di telefono oppure all'hot spot che ha fornito l'accesso, sia per lo stalking telefonico (in questo caso si ricorre all'override);
6. **la sospensione o la limitazione dei servizi**, come ad esempio nel caso delle email in cui si inibisce temporaneamente l'accesso;
7. **la documentazione integrale del traffico storico**, con la fornitura delle informazioni prescritte dal dlgs n. 109 del 30 maggio 2008(7);
8. **il sequestro dei contenuti**, intesi come contenuti a disposizione dell'operatore e tecnicamente sequestrabili come ad esempio le email in precedenza inviate/ricevute e conservate dall'utente sul server email oppure i messaggi in segreteria telefonica.

L'inadempienza dell'operatore totale o parziale, configura fattispecie di reato, comporta sanzioni economiche, nei casi più gravi, la sospensione o ritiro licenza.

Contestualmente alle prestazioni obbligatorie esistono, le prescrizioni del Garante per la Privacy del 17 gennaio 2008 G.U. n. 30 del 5 febbraio 2008, in materia di sicurezza dei dati del traffico telefonico e telematico che richiedono:

- adozione di specifici sistemi di autenticazione basata su tecniche di *«strong authentication»*;
- conservazione dei dati di traffico per accertamento e repressione reati utilizzando sistemi informatici fisicamente distinti da quelli utilizzati;
- di rendere i dati di traffico immediatamente non disponibili allo scadere dei termini previsti dalle disposizioni vigenti;
- controllo delle attività svolte sui dati di traffico da ciascun incaricato del trattamento;
- attività almeno annuale di controllo interno all'organizzazione;
- proteggere i dati di traffico con tecniche crittografiche.

L'obbligo di identificazione dell'utente è quindi posto in capo all'operatore di telecomunicazioni e solleva il *«provider»* del servizio Wi-Fi, dalla responsabilità di dover rispondere sui vincoli dell'identificazione utente.

Il *«provider»* del Servizio è in ogni caso responsabile della gestione della sicurezza della propria rete, e di seguito fissiamo alcuni punti:

- secondo le normative sulla privacy in vigore sia a livello nazionale che europeo, con particolare riferimento al Regolamento Ue 2016/679, il cosiddetto GDPR, chi effettui trattamento di dati personali di utenti deve avvalersi di misure tecnicamente in grado di assicurare la protezione di suddetti dati, rendendoli sicuri da intrusioni esterne o interne alla rete
- rendere disponibile agli utenti la connettività Internet implica responsabilità secondo il Codice Civile e secondo i principi della responsabilità oggettiva, dei danni causati da eventuali attività non lecite commesse da parte degli

utenti, a meno di non aver messo in pratica tutte le misure necessarie a controllare il servizio e a impedire che gli atti illeciti potessero essere commessi

- è tuttavia necessario dotarsi di sistemi di gestione della connettività e dell'autenticazione che permettano all'operatore di poter tracciare il traffico telematico degli utenti per poter rispondere ai suddetti obblighi.

Per i fornitori di accesso ad Internet tramite Wi-Fi, è opportuno e consigliabile pertanto dotarsi di adeguati sistemi di sicurezza informatica e di identificazione dell'utente,

Gli utenti della rete Wi-Fi aperta al pubblico, in buona sostanza, non devono poter agire in regime di anonimato una possibile azione correttiva quindi **consiste nell'imposizione di un obbligo di previa identificazione per ottenere l'accesso**;

Concludendo, nonostante l'attuale orientamento della giurisprudenza della Suprema Corte di Cassazione e della Corte di Giustizia Europea, il *«trend»* del free Wi-Fi e del regime di irresponsabilità dei gestori di «*hotspot»* non può darsi per scontato. Il dilagare del fenomeno terroristico, infatti, ha già condotto a dibattiti circa l'opportunità di bloccare le reti Wi-Fi pubbliche in caso di emergenza in molti Paesi europei. Resta quindi da verificare fin dove l'esigenza di controllo di Internet e di prevenzione dei reati commessi tramite il web si spingerà[6].

3.2 Identità digitale e Accesso alle infrastrutture

La «Dichiarazione dei diritti in internet»[7] definisce il diritto all'identità digitale per ciascuna persona all'art.9, dove si afferma la possibilità, per gli utenti di esistenza di molteplici identità digitali.

Per la verifica o nuova assegnazione delle identità digitali i *Service Provider* si servono degli *Identity Provider,* i quali hanno il compito di verificare l'identità dell'utente attraverso determinati processi di riconoscimento e conseguentemente creano l'identità digitale certificata.

In Italia è stato implementato da AgID il servizio SPID, ovvero il Sistema Pubblico per la gestione dell'Identità Digitale[8], introdotto per migliorare la fruibilità dei servizi erogati in rete da parte delle pubbliche amministrazioni, ai sensi dell'art. 64 CAD[9].

Nei sistemi Wi-Fi, una volta verificata l'identità digitale di un utente in forma diretta o indiretta, ad esempio attraverso la SIM, la carta di credito oppure l'accesso con SPID, ecc.., verrà creata l'utenza e le opportune credenziali o certificati per l'accesso a internet. Di seguito all'identificazione in rete verrà assegnato al *device* un indirizzo IPv4 di rete privata, a causa della scarsità di IPv4 pubblici. La soluzione a questo problema potrebbe consistere nell'adozione di IPv6, ma attualmente, i servizi erogati dai Provider e dalle PA non sono abilitati a tale protocollo sebbene le reti degli operatori lo siano. Si rende necessario quindi supplire all'esaurimento degli indirizzi e alla difficoltà di utilizzo di IPv6, implementando meccanismi di mascheramento tra indirizzi privati e pubblici[10].

[6] Fonte Altalex, 24 febbraio 2017, Articolo di Giulia Tebaldi.

[7] Documento elaborato dalla Commissione per i diritti e i doveri relativi ad Internet a seguito della consultazione pubblica, delle audizioni svolte e della riunione della stessa Commissione del 14 luglio 2015.

[8] La definizione di Identità Digitale data da SPID è la «rappresentazione informatica della corrispondenza biunivoca tra un utente ed i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale».

[9] D.lgs. 7 marzo 2005, n.82, come modificato dall'art. 17-ter del decreto legge n. 69 del 2013.

[10] Comunemente questa tecnica appena descritta è chiamata Network Address Resolution.

CAPITOLO 4

Le Maggiori esperienze della WI-FI pubblica nella PA

Analizzeremo in questo capitolo alcuni esempi di soluzione per l'implementazione del Wi-Fi pubblico nella PA muovendo da esperienze realizzate nelle città di Roma e Milano che, come molte altre PA locali hanno dato impulso al Wi-Fi pubblico. Per quanto riguarda la PA centrale è possibile invece evidenziare l" esempio virtuoso costituito dal protocollo di Intesa siglato da MISE, MIBACT e Agenzia per l'Italia Digitale[11]

4.1 La soluzione di Roma Capitale

Roma Capitale[12], mediante il progetto Digit Roma permette ai cittadini e a tutti coloro che si trovano occasionalmente in città (per lavoro, per turismo. . .) di avere accesso alla connessione gratuita ad internet, attraverso una rete di hotspot WiFi.

La registrazione avviene recandosi presso uno dei punti di accesso con il proprio dispositivo mobile (notebook, smartphone o tablet) dotato di un'interfaccia Wi-Fi, e consiste, connettendosi all'SSID DIGIT-Roma e tramite *«captive portal»*, nel fornire nome, cognome, e-mail e numero di telefono mobile. Nell'ambito della procedura di registrazione l'utente è richiesto di effettuare una chiamata gratuita al numero indicato, per convalidare la registrazione. Una volta chiusa la chiamata, il sistema invia una mail con username e password alla casella email indicata nella procedura di registrazione.

Dal momento dell'identificazione è necessario effettuare il primo accesso entro le successive 24 ore, altrimenti la registrazione viene annullata e occorrerà ripetere l'operazione.

Una volta effettuata la registrazione, sarà possibile fruire di 4 ore di connessione gratuita al giorno, conteggiate sulla base dell'effettivo tempo di navigazione nell'arco delle 24 ore.

Negli ultimi mesi a Roma Capitale è stata attivata anche la procedura di autenticazione tramite SPID ovvero il sistema pubblico di identificazione.

La soluzione basata su SPID svincola evidentemente il soggetto erogatore da tutti gli oneri derivanti dalla necessità di registrazione/identificazione e conseguente generazione delle credenziali.

Tale soluzione non è tuttavia utilizzabile qualora il soggetto richiedente sia uno straniero.

[11] http://www.agid.gov.it/notizie/2016/07/26/spid-accordo-mise-mibact-accesso-unico-Wi-Fi-pubblico
[12] http://www.digitromawifi.it/it/faq.html

4.2 La soluzione del comune di Milano

Nelle zone di copertura ciascun utente ha a disposizione, per la navigazione, un servizio di accesso ad internet illimitato 24 ore su 24, 7 giorni su 7 ad alta velocità.

La registrazione avviene, una volta rilevata la rete wireless tramite SSID, direttamente sul dispositivo attraverso la pagina di benvenuto dove dovranno essere fornite le informazioni richieste tra le quali obbligatoriamente andrà inserito il numero di cellulare di un gestore telefonico italiano o straniero sul quale verrà inviato un SMS gratuito con il codice di accesso. L'accesso alla rete OpenWifiMilano[13] avviene connettendosi al link ricevuto via SMS che conterrà anche il codice di accesso che potrà essere utilizzato anche con altri sistemi (tablet, PC portatili, etc.). Il suddetto codice è valido permanentemente.

Come possiamo notare sia a Milano che Roma la registrazione può avvenire attraverso la SIM del dispositivo mobile. Questa procedura di identificazione è indiretta in quanto, per vedersi assegnare una scheda SIM da un gestore telefonico, necessariamente occorre essere stati identificati.

4.3 Il Progetto Wifi.Italia.it

In questo quadro tecnologico, con l'obiettivo di fornire un sistema di accesso semplificato e unico per i cittadini italiani e i turisti, nonché favorire razionalizzazioni di spesa e riuso dei sistemi tecnologici adottati dalle Amministrazioni Pubbliche è nato il progetto wifi.italia.it (www.wifi.italia.it[25]).

Il sistema wifi.italia.it, la cui architettura prende spunto da un progetto di integrazione delle reti Wi-Fi nato nelle università europee e ormai esteso in tutto il mondo chiamato Eduroam[14], è basato completamente su standard aperti ed è in preparazione il rilascio di tutto il SW in licenza Open Source, in collaborazione con developers.it promosso dalla Presidenza del Consiglio.

A seguito del Protocollo di Intesa sottoscritto da AgID, MiSE e MiBACT «Per la diffusione di piattaforme digitali al servizio del turista nel territorio italiano» che prevede diverse iniziative volte a favorire la digitalizzazione dei servizi in ambito turistico e culturale, il MISE ha provveduto, attraverso Infratel Italia SpA, allo sviluppo di una APP per dispositivi mobili, con la quale gli utenti possono accedere in maniera automatica e semplice a tutte le reti Wi-Fi federate al progetto. L'APP multipiattaforma, una volta scaricata e installata, richiede all'utente la registrazione (da febbraio 2018 è attiva anche la registrazione con credenziali SPID) che si conclude con la creazione sul dispositivo di credenziali di accesso utilizzate, in maniera completamente trasparente all'utente, nella richiesta di autorizzazione alla rete. L'utente, una volta autorizzato, può usufruire del servizio gratuito di connettività Internet fornito dalle sedi della PA. La banda dedicata al servizio, così come le soglie sul numero massimo di utenti o di allocazione temporale per utente, secondo la logica federata, sono quelle definite dalla rete che sta fornendo il servizio di accesso ad internet in quel momento. La soluzione resa disponibile allo stato consente l'esclusivo accesso per il tramite di dispositivi mobili (smartphone e tablet). In futuro sarà disponibile anche una soluzione per p.c.

L'idea di funzionamento del sistema si basa, pertanto, sulla disponibilità per gli utenti, di una APP che riconosce e interagisce con un SSID unico «wifi.italia.it».

Non appena un utente entra nell'area di copertura di un Access Point appartenente alla rete integrata, l'APP procede, in maniera del tutto trasparente, all'autenticazione e accede alla rete. Una notifica avverte l'utente che l'operazione è andata a buon fine. Quindi l'utente non deve selezionare alcuna rete e non deve passare per alcun Captive Portal, infatti l'accesso avviene in automatico.

Le reti Wi-Fi delle pubbliche amministrazioni, per diventare parte del sistema, devono quindi configurare i loro Access Point con un nuovo SSID, senza necessariamente dismettere gli altri servizi e/o SSID, impostato con autenticazione 802.1x verso un Authentication Server Radius remoto gestito da Infratel Italia.

[13] http://www.openwifimilano.it/

[25] http://www.wifi.italia.it

[14] Eduroam (Education Roaming) è il servizio che permette agli utenti in mobilità presso altre organizzazioni di accedere in modo semplice e sicuro alla rete wireless usando le stesse credenziali fornite dalla propria organizzazione.

Secondo questa architettura, la APP e il sistema wifi.italia.it gestiscono oltre alla prima (e unica) registrazione dell'utente, l'autenticazione dello stesso sulla rete. Una volta che l'utente viene autenticato con la APP la navigazione è totalmente gestita dalla rete che lo sta «ospitando «in quel momento.

Conseguentemente il sistema wifi.italia.it raccoglie e gestisce i dati di registrazione degli utenti e di quelli relativi alle loro autenticazioni sulle reti federate, anonimizzandoli e solo per i fini dell'esecuzione del servizio. Mentre i dati di navigazione, con il riferimento all'utente codificato e interpretabile solo da wifi.italia.it, ma non dalla rete, sono invece, raccolti e gestiti esclusivamente dalle reti federate secondo le modalità proprie di ciascuna rete

L'adesione al sistema permetterà alle amministrazioni di dismettere i sistemi di autenticazione e gestione delle identità degli utenti, allo stato attivi, per utilizzare l'accesso all'SSID *«wifi.italia.it»*.

L'adozione di tale soluzione da parte della PA, consentirebbe loro di eliminare i costi per la gestione di tali sistemi, nonché il carico, ed i relativi costi, in termine di gestione dei dati degli utenti, ai fini della legislazione sulla sicurezza dei dati personali.

CAPITOLO 5

Criteri di implementazione del servizio per le PA

5.1 Organizzazione e ruoli del Servizio

Nel *framework* organizzativo del servizio WI-FI possiamo individuare 3 ruoli:

- Service Provider: l'organizzazione o Ente che coordina e gestisce il servizio;
- Resource Provider: operatori che gestiscono l'infrastruttura di rete e la connettività internet e che permettono agli utenti di accedere a internet;
- User: l'utente finale del servizio.

Andiamo ad analizzare in dettaglio i suddetti ruoli

5.1.1 Il Service Provider

Il Service Provider è il fornitore (organizzativo) del Servizio ed è rappresentato dall'Ente responsabile della progettazione, della gestione e delle evoluzioni del servizio stesso. Il Service Provider gestisce le policy di accesso per la connessione al servizio e per la generazione delle credenziali, necessarie agli utenti, per poter accedere alla rete. Nel presente documento il Service Provider è rappresentato dall'Amministrazione che eroga il servizio.

5.1.2 Resource provider

Il Resource Provider fornisce l'infrastruttura di rete e la connettività per l'utente che sia stato identificato secondo le modalità stabilite.

Il Resource Provider coincide con l'operatore che fornisce, attraverso la propria infrastruttura, l'accesso a Internet.

5.1.3 User

È l'utente finale del servizio, cittadino e/o turista, che accede al servizio WI-FI per l'accesso ai servizi digitali.

5.2 Architettura del servizio per le Reti della PA

Questo paragrafo intende fornire una panoramica delle possibili architetture per le Pubbliche Amministrazioni che debbano erogare il servizio WI-FI, senza entrare in dettagli tecnologici specifici. Ciò che si propone questo paragrafo è fornire indicazioni in merito ai requisiti funzionali necessari a realizzare il servizio, che possano essere implementati nei diversi modelli di gestione IT dagli Enti interessati.

Da quanto riportato nei paragrafi precedenti, si sottolinea l'obbligatorietà di identificazione in modalità diretta o indiretta dell'utente, da parte di almeno uno dei provider infrastrutturali, al fine di poter rispondere ai dettami normativi in materia di tracciabilità dell'utente.

5.2.1 Identificazione

Oggi esistono molteplici installazioni del servizio Wi-Fi ad opera di enti della PA centrale e locale.

Nelle suddette implementazioni troviamo specifiche modalità di registrazione e autenticazione come ad esempio il *«captive portal»*[16], passando da soluzioni semplici, come la ricezione delle credenziali via SMS, a più elaborate, prevedendo la compilazione di moduli on-line.

Per quanto riguarda l'identificazione dei turisti, visti gli oneri di identificazione posti in capo agli albergatori, si ritiene opportuno investigare in merito alla possibilità di interoperare con le strutture alberghiere al fine di poter assegnare credenziali per l'utilizzo della Wi-Fi gratuita per il periodo di permanenza in Italia.

Da quanto espresso nel presente documento, si ribadisce comunque la necessità di identificazione dell'utente, attraverso meccanismi diretti o indiretti, che consentano agli operatori di ottemperare alle prestazioni obbligatorie nei confronti dell'autorità giudiziaria.

L'architettura del servizio prevede che l'utente finale ovvero il cittadino, o il turista, si colleghi all'hotspot del servizio Wi-Fi pubblico dell'Amministrazione, e venga autorizzato all'accesso.

Le credenziali generate all'atto dell'iscrizione al servizio vengono riutilizzate in tutte le connessioni successive dell'utente finale[17].

5.2.2 Configurazione della rete interna

Le Amministrazioni devono garantire l'accesso WI-FI gratuito agli utenti attraverso Access Point o Hot Spot installati presso le proprie sedi fornendo connettività internet.

Al fine di realizzare tale servizio si rende necessario che sulle reti delle Amministrazioni siano configurate regole di segregazione del traffico e sicurezza.

In particolare le Amministrazioni dovranno realizzare, sulla propria rete interna, un'infrastruttura dedicata al servizio Wi-Fi, secondo una delle seguenti modalità:

- rete fisica separata e dedicata al servizio;
- una rete virtuale di livello 2 della pila ISO/OSI;
- rete virtuale di livello 3 della pila ISO/OSI (MPLS).

Le ultime due opzioni prevedono la configurazione di Virtual LAN (VLAN), per poter segregare il traffico, che con opportune politiche di routing, verrà trasportato alla prima uscita disponibile su Internet.

[16] Il «captive portal» è una pagina web, mostrata agli utenti di una rete di telecomunicazioni, per effettuare la connessione ad Internet.

[17] Al primo accesso l'utente si collega ai server (Radius o Network Access Server) che devono verificare l'identità, e associare le credenziali all'utente. La condizione vincolante all'autorizzazione all'accesso è che l'identità dell'utente sia verificabile: di fatti è possibile utilizzare modalità indirette come la registrazione al servizio attraverso la SIM del cellulare o numero di carta di credito (in particolare per gli stranieri) e/o il servizio SPID per gli utenti italiani. Il numero dei dispositivi associabili all'utenza dipende dai vincoli posti dal Service Provider.

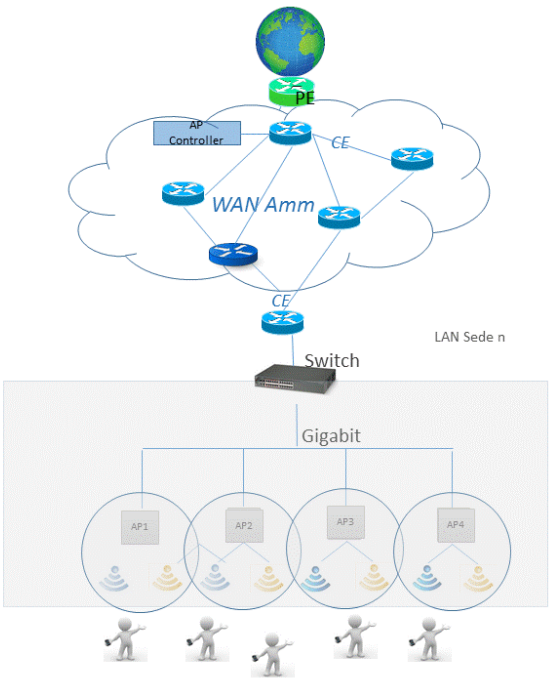

Fig. 5.1: Architettura rete PA

La rete interna deve consentire la configurazione descritta avendo le seguenti caratteristiche minime:

- Cablaggio di categoria minima UTP CAT-4 (è necessaria la categoria 5E o 6 per il supporto dello standard 802.11ac Wave2);
- Apparati di tipo ethernet switched;
- Subnet di indirizzi IP, dedicata al servizio.

Sarà necessario, inoltre, implementare i seguenti protocolli e servizi:

- DHCP (Dynamic Host Configuration Protocol), protocollo usato per assegnare gli indirizzi IP agli utenti;
- DNS (Domain Name Service), servizio di directory, utilizzato per la risoluzione di nomi di Host in indirizzi IP;
- Smart Switch per il supporto di più istanze del protocollo Spanning Tree, di LAN virtuali (VLANs) secondo lo standard 802.1Q, mirroring delle porte
- supporto della QoS (Quality of Service).

Sulla rete dedicata al servizio, fisica o virtuale, saranno attestati gli Access Point dell" area, i firewall dedicati e il collegamento (logico o fisico) verso il router di frontiera della sede.

5.2.3 Rete Geografica

In generale, il traffico Wi-Fi trasportato dagli access point delle sedi remote, attraverso la suddetta rete interna dedicata, avrà un accesso Internet attraverso il router di frontiera dell'Amministrazione.

Nel caso l'Amministrazione abbia una sola sede, il router di frontiera consegnerà il traffico alla rete dell'operatore, che a sua volta lo trasporterà con le opportune classificazioni.

Per le Amministrazioni con più sedi, collegate con una intranet geografica, il traffico locale è trasportato fino al router di frontiera, attraversando tutta l'infrastruttura geografica (intranet) e consegnato all'operatore dal router di frontiera.

Il collegamento geografico tra il router di frontiera dell'Amministrazione, il router dell'operatore e il canale dedicato al traffico del servizio Wi-Fi, può essere realizzato attraverso più modalità:

- Link comune con classificazione del traffico Wi-Fi Less Than Best Effort per non sovraccaricare o deteriorare il traffico di normale funzionamento dell'amministrazione in linea con l'art.8 bis del CAD;
- Link fisico dedicato al servizio con uscita su Internet;
- Link virtuale (es. MPLS) dedicato al servizio.

In ciascuno dei suddetti casi devono essere previste opportune misure di sicurezza che insistono sul traffico Wi-Fi, meglio se collocate prima della consegna del traffico all'operatore.

5.2.4 Misure minime di sicurezza

L'Amministrazione deve garantire opportune misure di sicurezza per la gestione del traffico Wi-Fi. Si elencano di seguito le funzionalità minime richieste:

- Firewalling, per il controllo e la protezione a livello perimetrale della rete;
- Antivirus, per la protezione a livello centrale, per evitare compromissioni da malware provenienti dai dispositivi mobili;
- Data Loss Prevention, per la protezione dei dati e per evitare perdite di informazioni aziendali;
- Policy di web-filtering, per l'utilizzo dei soli protocolli sicuri[18], per l'accesso al servizio e la limitazione ai soli siti web e servizi consentiti.

5.2.5 Access Point - AP

Al fine di garantire un segnale wireless stabile, è fondamentale progettare il posizionamento degli AP, in modo tale che non si verifichino interferenze e si massimizzi la copertura, e parallelamente, minimizzare le sovrapposizioni. Gli AP gestiti sono controllati e configurati centralmente, da un apparato controller, in grado di ottimizzare la rete come mostrato di seguito a titolo esemplificativo, mediante:

- Gestione dell'utilizzo degli Access Point;
- Separazione corretta dellla rete di accesso dalla rete di trasporto;
- Collegamento di tutti gli access point alla LAN (rete di trasporto) esclusivamente in modalità cablata.

Gli AP devono garantire funzionalità di gestione dei client, del routing e della banda disponibile, al fine di instradare correttamente il traffico WI-FI, e in generale devono avere le seguenti caratteristiche:

- essere conformi agli standard IEEE 802.11a, 802.11b, 802.11g, 802.11n. Quest'ultimo standard deve essere supportato sia nella banda 2.4 GHz che 5 GHz.
- essere alimentabili anche in modalità Power-overEthernet (PoE) in accordo allo standard IEEE 802.3af, senza perdita significativa di prestazioni.
- devono supportare il meccanismo del «VLAN tagging» secondo lo standard 802.1q e devono poter essere gestiti su di una «tagged VLAN».
- essere aggiornati automaticamente col software appropriato via rete e senza necessità di interventi in campo, a partire dal Centro di Controllo.
- essere di tipo Dual Radio (Band Unlocked) / Dual Band, in grado di offrire accesso ai client sia nella banda 2,4 GHz che 5 GHz, oppure di offrire in banda 5 GHz connettività di tipo Mesh per connettere gli Access Point non

[18] Transport Layer Security (TLS) è una tecnologia che la connessione ad una rete sia sicura

cablati (detti Mesh Access Point o MAP) agli Access Point cablati alla rete wired (detti Root Access Point o RAP).

- devono supportare canali da 20MHz e 40MHz.
- devono supportare almeno 8 SSID (Service Set Identifiers); per ogni SSID dovrà essere possibile definire delle policy specifiche per la sicurezza e l'autenticazione.
- devono supportare anche il protocollo di autenticazione 802.1x su server Radius remoto
- devono supportare la funzionalità di «client isolation».

5.2.6 Centro di controllo

Gli Access Point possono essere gestiti attraverso il centro di controllo, che dovrà consentire, la configurazione e la gestione della rete Wi-Fi, da un unico punto centralizzato interno o esterno all'Amministrazione.

5.2.7 Sicurezza del Sistema

La sicurezza del sistema deve essere garantita attraverso l'applicazione di policy che prevedano sia tecniche di web – filtering per poter limitare l'accesso a siti consentiti che l'utilizzo di protocolli sicuri per l'accesso ai servizi come HTTPS.

Ad ogni modo il responsabile del servizio Wi-Fi dovrà concordare con il responsabile dei servizi di sicurezza, delle sessioni almeno annuali di **vulnerability assessment** dell'intera infrastruttura.

5.3 Requisiti del servizio per le Amministrazioni collegate su SPC

L'accesso al servizio WI-FI verso i cittadini sarà reso disponibile attraverso l'infrastruttura SPC di connettività della quale sono dotate le Amministrazioni.

Le risorse di banda disponibili al servizio WI-FI, non devono in alcun modo degradare il funzionamento dei processi digitali della Pubblica Amministrazione.

Durante lo svolgimento del normale orario di lavoro di ciascun Ufficio e sede di Ente pubblico coinvolto, il servizio dovrà usufruire della sola capacità di banda Internet non utilizzata per i normali processi aziendali e comunque, nell'orario di chiusura non dovrà interferire con i servizi digitali erogati in regime di continuità ovvero H24.

La Banda non utilizzata, che potrebbe essere assegnata al servizio Wi-Fi, potrà essere determinata attraverso una attività di monitoraggio in *real-time,* da effettuarsi a cura dell'Amministrazione per il tramite di opportuni strumenti per l'analisi della rete.

Il Capitolato di gara Consip, per la Connettività, ha definito Classi di Servizio e Ambiti atti all" identificazione e separazione dei traffici pregiati e diretti o verso Internet, Intranet e Infranet.

La figura di seguito riporta un'ipotesi di architettura con l'ambito Wi-Fi aggiuntivo realizzato attraverso una nuova VRF[19] sugli apparati degli operatori.

Per quanto riguarda l'implementazione del servizio sulla rete interna o sulla rete geografica, l'Amministrazione deve erogare il servizio Wi-Fi, realizzando una delle opzioni menzionate ai paragrafi precedenti.

[19] È una tecnica di routing per la segregazione virtuale delle risorse di rete

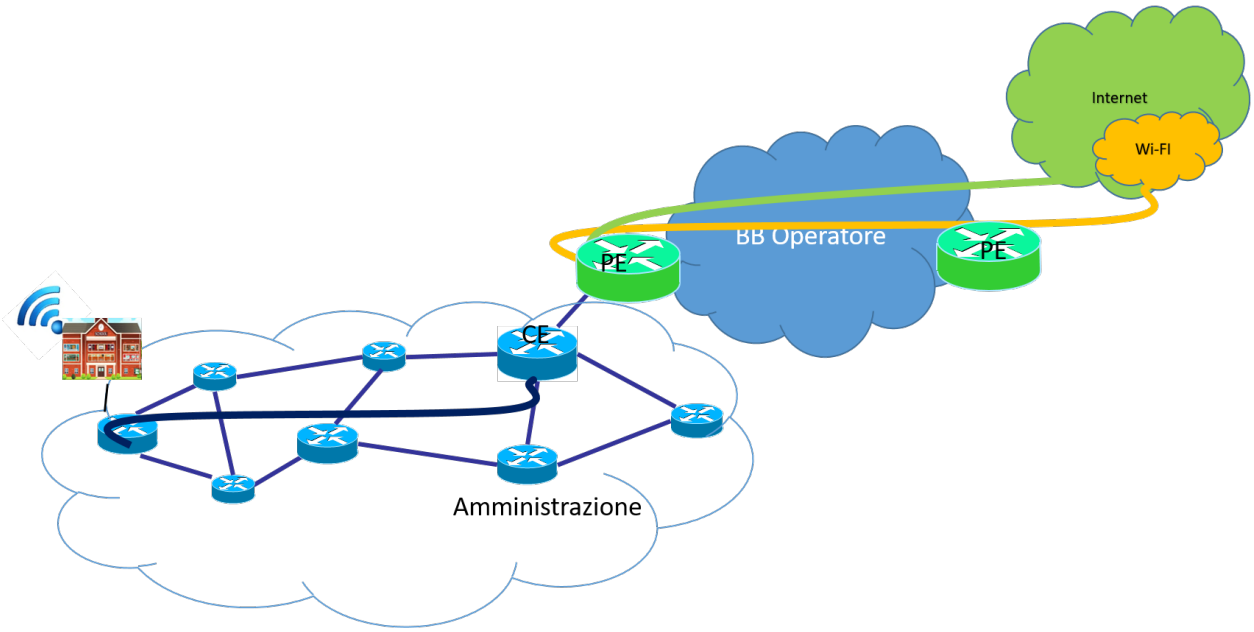

Fig. 5.2: Definizione Ambito WiFi SPC

5.4 Utilizzo di spazio di indirizzamento IPv6

Nel caso l'Amministrazione volesse utilizzare uno spazio di indirizzamento IPv6 da assegnare al servizio WI-FI, è consigliato l'utilizzo dello spazio privato, al fine di evitare eventuali problemi di DDoS tra utenti dello stesso hot spot.

Gli indirizzi privati o locali, analoghi a quelli IPv4, possono essere usati solo all'interno di ogni rete (o Site) e non vengono instradati all'esterno. Iniziano con i 9 bit: 1111 1110 1 (da FE8x::/9 a FEFx::/9) e sono anche detti «unregistered» o «nonroutable». Sono divisi in due categorie:

- i Link-local Addresses, che vengono sempre bloccati dai Router, e sono quindi locali solo ad un segmento di rete (switched LAN) o ad una subnet. Vengono usati per la «automatic address configuration», per le funzioni ND-Neighbor Discovery (es. Router discovery) e per l'ARP. Hanno come decimo bit uno «0», per cui cominciano con FE8x, FE9x, FEAx e FEBx;
- i Site-local Addresses, che possono essere instradati dai Router di una organizzazione solo all'interno della rete privata (Site), quindi tra le sue subnet, ma non verso Internet; iniziano con FECx, FEDx, FEEx ed FEFx, avendo come decimo bit un «1».

5.5 Sistema di monitoraggio centralizzato del funzionamento dei punti Wi-Fi

Ai fini del monitoraggio della rete Wi-Fi si suggerisce l'adozione da parte delle PPAA di un sistema di monitoraggio centralizzato che renda disponibili almeno le seguenti informazioni:

- Banda utilizzata;
- numero di apparati monitorati;
- numero di apparati in allarme per anomalie;
- informazioni sull" AP (situazione e posizione geografica);

- statistiche di funzionamento degli AP.

Il sistema di monitoraggio fornirà uno strumento di visualizzazione degli AP, dal quale sarà possibile l'immediata visualizzazione dello stato di funzionamento degli stessi. Consentirà inoltre il collegamento alle informazioni di dettaglio presenti all'interno del sistema stesso.

CAPITOLO 6

Possibili evoluzioni tecnologiche del servizio

La necessità di avere una rete wireless è stimolata dal modello di IT bimodale che, diventando diffuso, impone al reparto IT di soddisfare le aspettative del management, determinato a rendere impiegati e addetti più produttivi e mobili, attraverso una connettività più agile e flessibile e parallelamente ottenere una riduzione dei costi di gestione dell'IT.

Come già richiamato nel documento, l'architettura WiFi normalmente prevede l'utilizzo di controller (Controller Managed Wi-Fi), ossia apparati fisici (o virtuali) *on premise,* in grado di amministrare gli access point (AP) di cui si compone la rete Wi-Fi. Alla luce di diverse considerazioni economiche e tecniche, è possibile pensare ad una possibile migrazione del controller fisico in un'infrastruttura cloud, interna o esterna all'Amministrazione. Tale soluzione consentirebbe di amministrare l'infrastruttura e la sicurezza dell'intera rete Wi-Fi attraverso un singolo cruscotto di controllo. L'infrastruttura cloud consentirebbe di attivare nuovi Access Point, a livello geografico, senza necessità di supporto tecnico, in virtù della capacità di auto-configurarsi attraverso il cloud stesso.

CAPITOLO 7

Federabilità dei servizi WI-FI

Tecnologicamente le infrastrutture Wi-Fi già esistenti e, quelle da realizzare, possono essere federate.

La federabilità delle infrastrutture consiste principalmente nella condivisione di policy organizzative e tecniche che permettano di poter usufruire del servizio Wi-Fi in aree diverse da quelle nelle quali ci si è registrati al servizio stesso.

Le modalità tecnologiche di realizzazione delle federazioni sono diverse, ad esempio:

- si possono utilizzare le stesse credenziali su reti afferenti a diversi Service Provider, che propaghino reciprocamente le credenziali e gli SSID delle infrastrutture federate;
- l'accesso utente con la stessa password su due reti identificate da diversi SSID; in tale scenario le Amministrazioni dovranno sincronizzare i database degli utenti.

Federare le risorse, e in particolare il servizio Wi-Fi, porta vantaggi dal punto di vista della resilienza, in quanto la distribuzione geografica delle infrastrutture finisce per accrescere la possibilità di accesso alla rete. La federazione è uno dei punti basilari per lo sviluppo del servizio Wi-Fi pubblico, relizzando globalmente una maggiore disponibilità di servizi.

CAPITOLO 8

Conclusioni

Il cammino della Pubblica Amministrazione verso la trasformazione digitale e la sempre crescente offerta di servizi in modalità cosiddetta *«smart»* verso il cittadino, devono essere necessariamente supportati da una struttura che ne consenta la piena fruizione in mobilità. In tale ambito la Pubblica Amministrazione può recitare un ruolo cruciale teso a facilitare l'accesso da parte di cittadini a questi ed altri servizi disponibili sulla rete internet.

La facilità di implementazione ed erogazione del servizio Wi-FI è la chiave per permetterne la diffusione e l'utilizzo anche in aree con un marcato *digital-divide*. Le iniziative di PA locali sul territorio nazionale sono molteplici.

I servizi di accesso a Internet attraverso Wi-Fi gratuito rappresentano quindi il volano per lo sviluppo di nuovi servizi digitali, dei settori turistico, sanitario e di formazione che maggiormente beneficiano della possibilità di utilizzo delle nuove tecnologie.

Il Progetto wifi.italia.it sperimenta la realizzazione di una rete federata in tutto il Paese, offrendo notevoli spunti per una corretta implementazione e gestione del servizio

AgID nella programmazione del Piano Triennale 2017-2019 si è proposta quale obiettivo la crescita della diffusione della connettività Wi-Fi negli Uffici della Pubblica Amministrazione accessibili al pubblico. Il presente documento, la cui prima versione è stata prevista dal piano triennale 2017-2019, sarà aggiornato annualmente in modo da tenere conto di tutte le evoluzioni tecnologiche e normative che si presenteranno man mano nel tempo.

CAPITOLO 9

Riferimenti e Fonti

1. Codice delle comunicazioni elettroniche
2. Piano Triennale[26]
3. Regolamento Europeo Privacy n°679/2016 c.d. GDPR
4. CCM[27]
5. Regolamento Europeo No 1316/2013
6. CAD: decreto legislativo 7 marzo 2005. n. 82 e s.m.i. recante «Codice dell'amministrazione digitale»
7. Sicurezza e giustizia[28]
8. Eur Lex[29]
9. Altalex, 24 febbraio 2017, Articolo di Giulia Tebaldi
10. Info open wifi Milano[30]
11. Comunie di Roma[31]

[26] https://pianotriennale-ict.italia.it/piano/
[27] https://it.ccm.net/contents/102-802-1x-eap
[28] https://www.sicurezzaegiustizia.com/le-prestazioni-obbligatorie-per-lautorita-giudiziaria-come-disciplina-di-studio/
[29] http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32013R1316
[30] https://info.openwifimilano.it/IlServizio.aspx
[31] https://www.comune.roma.it/pcr/it/digit_roma.page

CAPITOLO 10

Glossario

10.1 A

AP Access Point, apparato di accesso per reti senza filo. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

10.2 B

Bluethooth Standard industrial per trasmissione dati a corto raggio

10.3 C

CAD Codice dell'Amministrazione Digitale

Captive Portal Il CP è una pagina web di registrazione che viene mostrata agli utenti di una rete di telecomunicazioni, dopo che essi abbiamo effettuato una richiesta HTTP

10.4 D

DG Directorate General

10.5 E

EAP Extensible Authentication Protocol

10.6 F

FCC Federal Communications Commission

10.7 G

GDPR General Data Protection Regulation

10.8 H

HOST Un host è un computer oppure dispositivo mobile connesso in rete

10.9 I

IEEE Electrical and Electronic Engineers

ISO/OSI Pila È un modello di rete per le interconnessione riservata ai calcolatori, realizzato a livelli, in cui ogni livello fornisce servizi a quello successivo, in tutto è composto da sette livelli

IT Information Technology

10.10 K

Kerberos Protocollo di rete atto all'autenticazione su rete informatica basato su crittografia simmetrica

10.11 L

LTE Long Term Evolution

10.12 M

MIMO Multiple Input Multiple Output

MPLS Multiprotocol Label Switching

10.13 N

NAS Network Attached Storage, ovvero apparati di memoria con interfaccia di rete

NAT Network Address Resolution

10.14 O

OLO Other Licenced Operator

10.15 P

PSK Pre-Shared Key , Chiave segreta condivisa

10.16 R

Radius Remote Authentication Dial In User Service

10.17 S

SIM Subscriber Identity Module, modulo relativo all'identità dell'abbonato

SMS Short Message Service ossia servizio di messaggi brevi attraverso la rete cellulare

10.18 U

UMTS Universal Mobile Telecommunications System

10.19 V

VRF Virtual Route Forward

10.20 W

WEP Wired Equivalent Privacy, protocollo utilizzato per rendere sicure le trasmissioni WI-FI

Wi-Fi Wireless Fidelity è una tecnologia per le reti locali senza fili, basata sulla famiglia degli standard 802.11

WPA Wi-Fi Protected Access

WPA2 WI-FI protected Access, esiste anche la versione 2, protocollo utilizzato per rendere sicure le trasmissioni WI-FI

Indice