



Promemoria «WLAN»

Stato:

4 luglio 2018

Contenuto

1	Scopo del promemoria	2
2	Situazione iniziale	2
3	Panoramica dei tipi di punti di accesso WLAN	2
4	Guida per la determinazione di punti di accesso WLAN pubblici gestiti professionalmente	3
4.1	Che cosa è un punto di accesso WLAN?	3
4.2	Quando un punto di accesso WLAN è pubblico?	3
4.3	Che cosa significa «gestiti professionalmente»?	4
5	Identificazione	4
5.1	Chi è soggetto all'obbligo di identificazione degli utenti finali?	4
5.2	Che cosa si intende per «mezzi di identificazione adeguati»?	5
6	Esempi	5
6.1	Elenco esemplificativo di punti di accesso WLAN pubblici gestiti professionalmente	5
6.2	Elenco esemplificativo di punti di accesso WLAN senza obbligo di identificazione	6
7	Ricerca per zona di copertura dell'antenna e analisi della copertura di rete in caso di WLAN	6
7.1	Analisi della copertura di rete in caso di WLAN	6
7.2	Ricerca per zona di copertura dell'antenna in caso di WLAN	7

1 Scopo del promemoria

Il presente promemoria precisa, sulla base di esempi, l'espressione «punti di accesso WLAN pubblici gestiti in maniera professionale» ai sensi dell'articolo 19 capoverso 2 OSCPT¹ in relazione all'obbligo di identificazione degli utenti finali.

Descrive pure l'analisi della copertura di rete (art. 64 OSCPT) e la ricerca per zona di copertura dell'antenna (art. 66 OSCPT) in caso di WLAN.

2 Situazione iniziale

L'obbligo, di cui all'articolo 21 capoverso 1 lettera d LSCPT² per i fornitori di servizi di telecomunicazione (FST), di trasmettere al Servizio SCPT altri dati, stabiliti dal Consiglio federale, sui servizi di telecomunicazione, che permettono l'identificazione delle persone è specificato nell'articolo 19 capoverso 2 OSCPT per i punti di accesso WLAN pubblici gestiti in maniera professionale:

Art. 19 cpv. 2 OSCPT

«² I FST devono garantire l'identificazione con mezzi adeguati di tutti gli utenti finali dei punti di accesso WLAN pubblici gestiti in maniera professionale».

Per motivi di proporzionalità, con la revisione totale dell'OSCPT il Consiglio federale non introduce un obbligo generale di identificazione degli utenti finali dei punti di accesso WLAN pubblici, per evitare che ad esempio le economie domestiche e le piccole imprese che mettono a disposizione di terzi i loro WLAN siano tenuti a effettuare l'identificazione degli utenti finali. L'obbligo di identificazione è invece limitato ai punti di accesso WLAN pubblici «gestiti professionalmente» (vedasi n. 4.3).

3 Panoramica dei tipi di punti di accesso WLAN

Ai fini del presente promemoria sono rilevanti tre tipi di punti di accesso WLAN:

1. punti di accesso WLAN pubblici gestiti professionalmente
2. punti di accesso WLAN pubblici non gestiti professionalmente
3. punti di accesso WLAN non pubblici

¹ Ordinanza del 15 novembre 2017 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (**OSCPT**; RS **780.11**); entrata in vigore: 1° marzo 2018

² Legge federale del 18 marzo 2016 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (**LSCPT**; RS **780.1**); entrata in vigore: 1° marzo 2018

4 Guida per la determinazione di punti di accesso WLAN pubblici gestiti professionalmente

Per applicare l'articolo 19 capoverso 2 OSCPT devono essere adempiute cumulativamente le tre condizioni seguenti:

1. si tratta di un **punto di accesso WLAN**;
2. è **pubblico**;
3. è **gestito professionalmente**.

4.1 Che cosa è un punto di accesso WLAN?

- Si tratta di un punto di accesso, senza fili, a una rete pubblica di telecomunicazione (accesso alla rete) che può trovarsi in locali privati o pubblici.
- L'accesso alla rete avviene tramite una rete locale in radiofrequenza basata perlopiù su uno degli standard IEEE-802.11 (Wireless LAN, WLAN).

4.2 Quando un punto di accesso WLAN è pubblico?

Un punto di accesso WLAN è pubblico se l'accesso alla rete è per principio a disposizione di terzi. È irrilevante se l'accesso alla rete è protetto da password o no. I terzi sono altre persone fisiche o giuridiche.

Esempi che illustrano il concetto di «pubblico» e «non pubblico»:

- punti di accesso WLAN pubblici: negli aeroporti, nelle stazioni, alle fermate dei mezzi pubblici, nei mezzi pubblici, nel settore alberghiero, nella gastronomia, nei negozi, nei centri commerciali, nelle strade e nelle piazze pubbliche
- punti di accesso WLAN non pubblici: se l'accesso alla rete è disponibile soltanto a persone non considerate terzi (p. es. collaboratori, membri dell'economia domestica)

Denominazioni usuali per i punti di accesso WLAN pubblici³:

WLAN Hotspot, Wi-Fi®⁴ Hotspot, Wi-Fi®, Public Wireless LAN (PWLAN).

³ Non sono compresi i servizi WLAN gestiti da FST e messi a disposizione unicamente dei clienti del FDA nel quadro di un'altra prestazione (p. es. abbonamento per cellulare, abbonamento banda larga), come Wi-Free di UPC o EAP-SIM di Swisscom (stato: febbraio 2018). Gli utenti di simili servizi WLAN gestiti da FST vengono identificati come clienti del FST.

⁴ Wi-Fi® (anche: WiFi) è un marchio registrato della Wi-Fi Alliance (www.wi-fi.org).

4.3 Che cosa significa «gestiti professionalmente»?

Il punto di accesso WLAN pubblico è «gestito professionalmente» se è gestito da una persona fisica o giuridica («specialista WLAN») che gestisce svariati punti di accesso WLAN pubblici in diverse ubicazioni (ossia non nella medesima ubicazione).

Fondandosi sull'articolo 2 OST⁵, il concetto di medesima ubicazione è definito come segue:

1. i punti di accesso WLAN pubblici si trovano all'interno dello stesso edificio; oppure
2. i punti di accesso WLAN pubblici si trovano nei limiti di un immobile, di due immobili contigui oppure di due immobili dirimpettai separati da una strada, un vicolo, una linea ferroviaria o un corso d'acqua.

Per «gestire» si intendono in particolare una o varie prestazioni seguenti per il punto di accesso WLAN pubblico:

- gestione della configurazione;
- manutenzione a distanza o manutenzione in loco;
- controllo dell'accesso, gestione delle autorizzazioni, conteggio (AAA, Authentication Authorization Accounting);
- controllo (monitoraggio) del funzionamento regolare;
- aggiornamenti software e firmware;
- gestione delle capacità (capacity management);
- servizio clienti, supporto clienti.

5 Identificazione

5.1 Chi è soggetto all'obbligo di identificazione degli utenti finali?

È soggetto all'obbligo di identificazione degli utenti finali il FST che gestisce o fa gestire il punto di accesso WLAN pubblico. È anche rilevante sotto quale nome è messo a disposizione l'accesso Internet, ossia chi si presenta come il fornitore dell'accesso WLAN pubblico nei confronti degli utenti finali. Il FST può trasmettere l'obbligo di identificazione a terzi (outsourcing). In questo caso le disposizioni dell'articolo 23 OSCPT (ricorso ad ausiliari) devono essere osservate.

⁵ Ordinanza del 9 marzo 2007 sui servizi di telecomunicazione (OST; RS 784.101.1)

5.2 Che cosa si intende per «mezzi di identificazione adeguati»?

Per mezzi di identificazione adeguati, si parla in questo caso anche di identificazione indiretta, si intendono le registrazioni implicite o semplificate mediante indicazioni affidabili (trusted) che consentono una sufficiente identificazione degli utenti finali.

Sono ipotizzabili i mezzi seguenti:

- codice di accesso via SMS sul cellulare e memorizzazione del MSISDN;
- identificazione mediante carta di credito e memorizzazione dei dati dell'autorizzazione;
- identificazione mediante indicazioni affidabili dei partner di roaming (p. es. WISPr, eduroam) e memorizzazione dei dati dell'autorizzazione;
- codice di accesso individuale per camera in albergo associato alla registrazione dell'ospite;
- identificazione mediante carta d'imbarco negli aeroporti e memorizzazione dei relativi dati (p. es. la scansione della carta d'imbarco genera un voucher [codice di accesso] per il WLAN);
- identificazione mediante la carta di un programma per frequent flyer che permette l'accesso alla lounge e memorizzazione dei dati dell'autorizzazione.

6 Esempi

6.1 Elenco esemplificativo di punti di accesso WLAN pubblici gestiti professionalmente

Per i seguenti esempi di punti di accesso WLAN pubblici gestiti professionalmente sussiste l'obbligo di identificazione degli utenti finali tramite mezzi adeguati.

Esempio	Caratteristica	Chi è soggetto all'obbligo di identificazione?
FDA Public WLAN	gestito dal FST	FST
WLAN alle stazioni, alle fermate dei mezzi pubblici o nei mezzi pubblici	gestito professionalmente	FST che mette a disposizione il WLAN
WLAN pubblico nella gastronomia o nel settore alberghiero	gestito professionalmente	FST che mette a disposizione il WLAN
WLAN pubblico in musei, biblioteche, sale eventi	gestito professionalmente	FST che mette a disposizione il WLAN
WLAN pubblico nelle città e nei Comuni	gestito professionalmente	FST che mette a disposizione il WLAN

6.2 Elenco esemplificativo di punti di accesso WLAN senza obbligo di identificazione

Per i seguenti esempi di punti di accesso WLAN non sussiste alcun obbligo di identificazione degli utenti finali.

In alcuni degli esempi seguenti, la caratteristica del punto di accesso WLAN determina se sussiste una gestione professionale e quindi un obbligo di identificazione.

Esempio	Caratteristica	Chi è soggetto all'obbligo di identificazione?
WLAN ospiti in imprese	non gestito professionalmente	nessuno
WLAN privato «aperto»	non gestito professionalmente	nessuno
WLAN ospiti privato	non gestito professionalmente	nessuno
WLAN pubblico non gestito professionalmente nella gastronomia e nel settore alberghiero	non gestito professionalmente	nessuno
WLAN pubblico non gestito professionalmente in musei, biblioteche, sale eventi	non gestito professionalmente	nessuno
WLAN pubblico non gestito professionalmente in un campeggio	non gestito professionalmente	nessuno

7 Ricerca per zona di copertura dell'antenna e analisi della copertura di rete in caso di WLAN

7.1 Analisi della copertura di rete in caso di WLAN

Secondo l'articolo 64 OSCPT, l'analisi della copertura di rete in vista di una ricerca per zona di copertura dell'antenna ai sensi dell'articolo 66 può ora essere ordinata anche per punti di accesso WLAN pubblici. Ciò ha tuttavia senso soltanto se il FST che gestisce questi punti di accesso WLAN pubblici può anche effettuare la rispettiva ricerca per zona di copertura dell'antenna. Contrariamente alla già nota analisi della copertura di rete per celle radio, che può essere allestita anche come mappa di copertura, per i punti di accesso WLAN pubblici non occorre allestire alcuna mappa di copertura. Si tratta invece di identificare i punti di accesso WLAN pubblici che più probabilmente coprono l'ubicazione designata (coordinate geografiche o indirizzo postale), se del caso tenendo conto di ulteriori indicazioni (p. es. orario, giorno della settimana, ubicazione all'interno o all'esterno di un edificio, piano, parte dell'edificio). L'autorità che dispone la sorveglianza comunica queste informazioni al Servizio SCPT, che le trasmette poi al FST con il mandato di sorveglianza.

L'obiettivo è identificare i punti di accesso WLAN pubblici che entrano in linea di conto per una ricerca per zona di copertura dell'antenna, poiché potrebbero aver consentito l'accesso alla rete nell'ubicazione in questione, eventualmente considerando le ulteriori indicazioni.

7.2 Ricerca per zona di copertura dell'antenna in caso di WLAN

L'articolo 66 OSCPT permette ora la ricerca per zona di copertura dell'antenna anche per i punti di accesso WLAN pubblici. Alla stregua della già nota ricerca per zona di copertura dell'antenna per celle radio, si tratta di una sorveglianza retroattiva, che concerne in primo luogo i FST soggetti a pieni obblighi di sorveglianza. Dato che i FST con obblighi di sorveglianza ridotti non sono tenuti a conservare i metadati, forniscono soltanto i dati eventualmente disponibili. L'identificativo da sorvegliare è l'identificativo univoco (p. es. BSSID o le indicazioni relative all'ubicazione secondo i termini designati dai FST) del punto di accesso WLAN pubblico. Il mandato di sorveglianza indica inoltre al FST il periodo di tempo per la sorveglianza retroattiva.