PuntoSicuro

# ARTICOLO DI PUNTOSICURO

## Anno 19 - numero 4117 di mercoledì 08 novembre 2017

# Sistemi RFid: i limiti e le criticità per la privacy e la salute

***Una pubblicazione Inail si sofferma sull'uso della tecnologia RFId, per il riconoscimento a distanza, in applicazioni di sicurezza. I limiti del sistema, i pericoli per la privacy, la diffusione dei dati commerciali e i rischi per la salute.***

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

Roma, 8 Nov ? Il riconoscimento a distanza di un oggetto per mezzo di comunicazioni radio, attraverso **sistemi RFId** (Radio-Frequency Identification), è una tecnologia che ha avuto un rapido successo ed evoluzione: un trasponder (Tag) viene accoppiato all'oggetto che deve essere riconosciuto e un apposito lettore (Reader) può interrogare i Tag per ricavare le informazioni di interesse.

E questa tecnologia, presentata nel dettaglio nel documento *Inail " RFId (Radio-Frequency Identification) in applicazioni di sicurezza", può avere diverse applicazione anche in materia di salute e sicurezza nei luoghi di lavoro, come raccontato in* precedenti articoli *del nostro giornale.*

*Tuttavia questi* sistemi RFid*, per quanto utili ed evoluti, non sono esenti non solo da* ***criticità*** *ma anche da* ***pericoli per la privacy e la salute****.*

*Ed è lo stesso documento Inail a ricordare* alcuni aspetti critici nell'utilizzo della tecnologia RFid, almeno rispetto alle caratteristiche ideali del sistema.

Si indica che esistono, infatti, alcuni **problemi** "che costituiscono ancora un freno all'introduzione massiva degli RFId in taluni campi applicativi, anche se si spera che in un prossimo futuro potranno essere risolti con lo sviluppo tecnologico".

Viene presentato un breve **elenco**, non esaustivo, di tali problemi:

- "scarsa compatibilità 'worldwide' (non uniformità di frequenze e potenze operative in tutto il pianeta);

- difficoltà nell'allestimento dell'applicazione (mancanza di sistemi 'chiavi in mano', aspettative non realistiche indotte dagli integratori rispetto alle prestazioni effettive di Reader e Tag);

- mancata ripartizione dei costi sull'intera catena di distribuzione (produzione, trasporto, commercio);

- limiti fisici dei sistemi reali (scarsa distanza operativa, possibilità di fallimenti nelle operazioni di lettura, incompleta applicabilità su tutte le merci, bassa velocità di lettura-scrittura);

- scarsa flessibilità per la progettazione delle antenne con conseguenti limiti su forma, dimensioni e contenitori dei TAG;

- difficoltà ad ottenere fiducia dai consumatori (modesta sicurezza e protezione dei dati, impatto ambientale non trascurabile per alcuni tipi di Tag) e dalle aziende (alti costi del software applicativo, alto costo dei Tag, che viene percepito come il maggior fattore ostativo perché si somma al prezzo finale delle merci, limitata integrazione dei processi di 'tagging' in alcuni dei processi aziendali, immaturità tecnica dei sistemi 'middleware' che devono processare dati e istruzioni)".

Il documento affronta poi i **pericoli per la privacy**.

Si segnala, ad esempio, che il ciclo di vita dei Tag "supera spesso quello degli oggetti a cui il Tag è associato. I Tag passivi, in particolare, non necessitando di batterie, hanno aspettativa di vita teoricamente infinita, e continuano a funzionare anche quando la catena di distribuzione è giunta al termine". E questo significa che teoricamente è possibile "continuare ad interrogare gli oggetti a cui i Tag sono associati, anche se sono ormai da tempo in possesso di proprietari privati, traendo da ciò informazioni sulle abitudini di tali persone".

Il problema poi non è relativo solo ai Tag associati a singoli articoli di consumo, "che non hanno un'associazione diretta con i dati personali dei proprietari", ma può coinvolgere anche "altri oggetti abitualmente in possesso dei privati che invece possono consentire di risalire a dati personali (carte di pagamento o di accesso, passaporto elettronico, tessera sanitaria, chip biomedico, apparati elettronici, ticket, ecc.)".

In relazione a tale problematica, nel **settore della logistica**, "lo standard EPC-Gen2 prevede che i Tag contengano solamente un unico codice (ovvero un numero di serie), cosicché la lettura di un Tag (posizionato su di un oggetto a fini di inventario) sia identica (trattandosi di una soluzione a breve raggio) a quella di un codice a barre e quindi non contenga alcuna informazione utile sull'identità del possessore, mentre diverso è il discorso per i chip che contengono informazioni sensibili". In ogni caso aziende o organizzazioni di vario genere potrebbero comunque "ancora acquisire informazioni indebite sulla clientela, ad esempio potrebbero realizzare indagini di mercato sui consumi delle singole persone, acquisendo informazioni al momento del pagamento elettronico".

Nel documento si indica poi che un altro problema relativo alla privacy è relativo al **tracking dell'individuo** per mezzo di sistemi RFId. E anche in questo caso il problema "assume maggiore rilevanza in presenza di Tag che contengano a bordo informazioni personali che potrebbero essere soggetti a letture non autorizzate per finalità diverse da quelle originarie".

Tuttavia, continua il documento, questo problema è, "allo stato attuale della tecnologia RFId, alquanto sopravvalutato risultando più teorico che pratico. Infatti, una limitazione proviene direttamente dalla piccola estensione delle zone di copertura dei Reader degli RFId".

Si indica che distanze di lettura "dipendono fortemente dalle condizioni ambientali e dalle tecnologie utilizzate. In pratica le normative e i dispositivi attuali prevedono le seguenti portate operative:

- per i Tag passivi da 125 a 134.2 kHz, la distanza di lettura varia da quasi a contatto a circa 1 m;

- per i Tag a 13,56 MHz, la distanza di lettura varia da quasi a contatto a circa 1 m;

- per i Tag UHF passivi usati per la logistica (da 860 a 960 MHz), la distanza tipica prevista dalla normativa varia da 1 a 10 metri".

E i Tag UHF, quelli con la maggiore portata, subiscono poi una limitazione della portata "in presenza di acqua e, poiché il corpo umano è composto al 70% da acqua, l'ipotesi di utilizzarli (in forma cutanea) per il controllo degli spostamenti di una persona

(pedinamento), anche se non impossibile, è poco efficace".

Dunque in relazione alla portata limitata della comunicazione wireless dei Tag, per il tracking sarebbe necessario "un numero enorme di lettori sparsi su un territorio con lievitazione dei costi relativi". E si sottolinea anche che il tracking visivo "assicura la copertura di distanze maggiori con migliore accuratezza, e che le forze dell'ordine, se incaricate dall'autorità giudiziaria, possono accedere ben più facilmente ai dati degli operatori di telefonia mobile per seguire gli spostamenti di persone ricercate o soggette ad indagine".

Una problematica diversa è quella poi del **tracciamento degli spostamenti del personale di un'azienda**, all'interno dell'azienda stessa, per mezzo delle tessere RFId di riconoscimento ed accesso.

In questo caso anche Tag passivi da 125 a 134.2 kHz o da 13,56 MHz "potrebbero essere utilizzati. Posizionando i Reader in corrispondenza delle porte delle stanze è possibile un grossolano posizionamento del personale (presenza o assenza all'interno della stanza)". E l'effettiva realizzabilità di tali sistemi di tracciamento "è legata agli accordi sindacali e all'accettazione da parte del personale interessato".

Il documento si sofferma poi sul **pericolo di diffusione di informazioni commerciali**, con particolare riferimento a quelli relativi all'etichettatura elettronica.

Si indica che poiché i "***product code***" sono ormai "molto diffusi in ambito commerciale come identificatori di prodotti (catene produttive e gestione di magazzino), la violazione della segretezza della comunicazione wireless di risposta dei Tag (e la vendita al mercato nero dei dati relativi ai prodotti) costituisce un rischio per l'attività produttiva e commerciale delle aziende, con danni economici potenzialmente rilevanti e un possibile guadagno per le aziende competitrici".

In conclusione il documento riporta anche alcuni riferimenti agli eventuali **rischi per la salute**.

Il documento segnala che l'Agenzia IARC (International Agency for Research on Cancer) ha classificato i campi elettromagnetici a radiofrequenza come 'possibilmente cancerogeni per gli esseri umani (Gruppo 2B)', una categoria generalmente usata quando '*un'associazione causale è considerate credibile, ma la casualità, il pregiudizio o l'incertezza, non possono essere esclusi con ragionevole confidenza*'.

E dunque è necessario "evitare esposizioni indebite per durata e potenza di esseri umani ai campi elettromagnetici" ed esistono limiti opportuni "che dipendono dalla frequenza e devono essere verificati di caso in caso a seconda dell'applicazione specifica".

In questo senso, segnala infine il documento Inail, analizzando opportunamente i vari parametri necessari al funzionamento del sistema (frequenza, ampiezza/potenza, durata) è possibile che "la maggior parte delle attuali applicazioni RFId siano realizzabili senza problemi per la salute, soprattutto se i dispositivi hanno una sufficiente distanza dal corpo".

RTM

***Scarica il documento da cui è tratto l'articolo:***

Dipartimento innovazioni tecnologiche e sicurezza degli impianti, prodotti e insediamenti antropici dell'Inail, " RFId (Radio-Frequency Identification) in applicazioni di sicurezza", a cura di Giovanni Luca Amicucci e Fabio Fiamingo, versione 2016, pubblicazione gennaio 2017 (formato PDF, 2.26 MB).

Vai all'area riservata agli abbonati dedicata a " RFId in applicazioni di sicurezza".

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

**www.puntosicuro.it**