Secure Authentication per applicazioni Smart Disposable

Il tema della cybersecurity non si esaurisce nell'ambito della progettazione di dispositivi medici attivi, o di software come dispositivo medico [1][2][3], ma occupa un ruolo centrale nella protezione dei consumatori di tecnologie medicali dai rischi posti dalla contraffazione.

Nell'ambito *healthcare*, la minaccia introdotta da dispositivi contraffatti ha una ricaduta rilevante sugli aspetti di *safety*, quindi è da tenere in considerazione durante l'intero ciclo di vita del dispositivo medico.

In particolare, in questo articolo si affronterà la protezione di Smart Disposables per l'identificazione di prodotti contraffatti attraverso tecniche di autenticazione, utilizzando Secure Elements e tag RFID di ultima generazione.

Il problema dei prodotti medicali contraffatti

Nel 2017, l'Organizzazione Mondiale della Sanità ha stimato che 1 medicinale su 10 nei passi a basso e medio reddito sia di qualità non standard o falsificato [4]: il dato fa scaturire considerazioni importanti riguardo la protezione da prodotti contraffatti, in quanto non solo rappresentano un serio rischio per la salute, ma hanno anche un notevole peso economico.

I sistemi di etichettatura dei prodotti si stanno evolvendo verso il formato digitale: se in passato le etichette erano esclusivamente cartacee, oggi si riscontra un maggiore utilizzo di etichette integrate nel prodotto, ad esempio utilizzando tag RFID. Questa evoluzione pone le basi per l'applicazione di standard di cybersecurity ai sistemi di etichettatura, proteggendo l'utilizzatore finale da prodotti contraffatti. L'autenticazione garantisce la sicurezza e la legittimità del dispositivo medico, oppure la sua efficacia nel caso in cui si stia etichettando farmaco.

Secure authentication: cosa si intende?

Per *Secure Authentication* si intende un processo di verifica dell'autenticità del dispositivo medico tramite tecniche crittografiche. Alla base di questi processi c'è l'utilizzo di componenti integrati capaci di accelerare gli algoritmi di crittografia, come ad esempio i Secure Elements [5]. Una possibile applicazione è quella in cui il Secure Element viene utilizzato per autenticare uno Smart Disposable, ovvero un dispositivo medico di consumo integrato con un sistema elettronico di riconoscimento.

Nonostante i *disposables* siano prodotti di consumo, rappresentano un target dal valore elevato e necessitano quindi di essere protetti dalla contraffazione. Tramite l'utilizzo di un circuito integrato in cui è presente un Secure Element, che mantiene al sicuro le chiavi crittografiche, al momento dell'utilizzo il *disposable* può essere riconosciuto come autentico. L'autenticazione può avvenire sia in maniera simmetrica che asimmetrica, attraverso la combinazione dell'utilizzo di chiavi private e pubbliche.

A differenza dell'utilizzo di un semplice Tag RFID, il Secure Element presenta dei vantaggi aggiuntivi:

Tag RFID	Secure Element
Assenza di memorie sicure	Storage sicuro dei segreti crittografici, come chiavi e certificati
Assenza di accelerazione crittografica	Accelerazione degli algoritmi di crittografia in hardware
Assenza di Secure Provisioning	Secure Provisioning di chiavi e certificati
Canale di comunicazione non sicuro: le operazioni di lettura e scrittura prevedono un trasferimento dei dati verso l'esterno	Gestione sicura dei dati: tutte le operazioni crittografiche sono effettuate all'interno del componente, evitando il trasferimento di dati sensibili all'esterno

Tabella 1: Differenze funzionali tra Tag RFID e Secure Element.

UCODE® RFID: Tag di ultima generazione con Crittografia

Esistono dispositivi RFID di ultima generazione, come gli UCODE® RAIN RFID [6], che uniscono la tecnologia di tagging RFID con il livello di sicurezza posto dal Secure Element. L'autenticazione di questi sistemi avviene attraverso la risoluzione di una challenge crittografica: un dispositivo autenticatore invia una sequenza di bytes al tag RFID, che li cifra utilizzando la sua chiave privata. In questo modo, i segreti crittografici non vengono esposti verso l'esterno e l'autenticità viene confermata tramite la verifica della risposta. Il limite ad oggi è l'utilizzo esclusivo di algoritmi simmetrici.

Conclusioni

In conclusione, esistono diverse tecnologie capaci di proteggere i dispositivi medici dalla contraffazione, che permettono di azzerare i rischi posti alla salute dai prodotti di qualità inferiore.

Fonti:

1. Cybersecurity per dispositivi medici: soluzioni hardware e software per sistemi embedded a prova di regolamento europeo - Teoresi Group
2. Cybersecurity nei dispositivi medici: cosa richiede il MDR 2017/745 - Teoresi Group
3. Security-by-Design in Medical Software (IEC 81001-5-1)
4. Substandard and falsified medical products
5. Disposable Authentication | Microchip Technology
6. UCODE® RAIN RFID | NXP Semiconductors

Keywords: Contraffazione, Smart Disposable, Secure Authentication, RFID Tag, Security-by-Design, Defense-in-Depth, Cybersecurity, Software as Medical Device, Health Software

Autore: Gaia Di Federico, Progettista Elettronico R&D