Secure Authentication for Smart Disposable Applications

The scope of cybersecurity does not end with the design of active medical devices, or software as a medical device [1][2][3], but plays a central role in protecting medical technology consumers from the risks posed by counterfeiting.

In the healthcare sector, the threat introduced by counterfeit devices has a significant impact on safety aspects, so it must be taken into account throughout the entire life cycle of the medical device.

In particular, this article will address the protection of Smart Disposables for the identification of counterfeit products through authentication techniques, using Secure Elements and the latest-generation RFID tags.

The problem of counterfeit medical products

In 2017, the World Health Organization estimated that 1 in 10 medicines in low- and middle-income markets are of non-standard quality or falsified [4]: this number raises important considerations regarding protection from counterfeit products, as they not only represent a serious health risk, but also have a significant economic weight.

Product labeling systems are evolving towards the digital format: while in the past labels were exclusively paper based, today there is an increased use of embedded labels, for example using RFID tags. This evolution lays the foundation for the application of cybersecurity standards to labeling systems, protecting the end user from counterfeit products. Authentication ensures the safety and legitimacy of the medical device, or its effectiveness in the case of pharmaceutical labeling.

Secure authentication: what does it mean?

Secure Authentication refers to the process of verifying the authenticity of the medical device using cryptographic techniques. The use of built-in components, such as Secure Elements, is at the heart of these processes, in order to accelerate encryption algorithms [5]. One possible application is where the Secure Element is used to authenticate Smart Disposables, i.e. a consumer medical device integrated with an electronic authentication system.

Although disposables are consumer products, they represent a high-value target and therefore need to be protected from counterfeiting. Using an integrated circuit containing the Secure Element,

which keeps the cryptographic keys safe, at the time of use the disposable can be recognized as authentic. Authentication can take place both symmetrically and asymmetrically, through the combination of the use of private and public keys.

Unlike using a simple RFID Tag, the Secure Element has additional advantages:

RFID Tags	Secure Element
No secure memory	Secure storage of cryptographic secrets, such as keys and certificates
No cryptographic acceleration	Acceleration of cryptographic algorithms in hardware
Absence of Secure Provisioning	Secure Provisioning of Keys and Certificates
Non-secure communication channel: read and write operations involve data transfer to the outside	Secure data management: all cryptographic operations are carried out within the component, avoiding the transfer of sensitive data outside

Table 1: Functional differences between RFID Tag and Secure Element.

UCODE® RFID: Latest generation tag with Encryption

There are state-of-the-art RFID devices, such as the UCODE® RAIN RFID [6], which combine RFID tagging technology with the level of security set by the Secure Element. The authentication of these systems takes place through the resolution of a cryptographic challenge: an authenticating device sends a sequence of bytes to the RFID tag, which encrypts them using its private key. In this way, cryptographic secrets are not exposed to the outside world and authenticity is confirmed by verifying the response. The limit to date is the exclusive use of symmetric algorithms.

Conclusion

In conclusion, there are several technologies capable of protecting medical devices from counterfeiting, which make it possible to eliminate the health risks posed by inferior products.

Sources:

1. Cybersecurity for medical devices: hardware and software solutions for embedded systems in compliance with European regulations - Teoresi Group
2. Cybersecurity in medical devices: what MDR 2017/745 requires - 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: Counterfeiting, Smart Disposable, Secure Authentication, RFID Tag, Security-by-Design, Defense-in-Depth, Cybersecurity, Software as Medical Device, Health Software

Author: Gaia Di Federico, R&D Electronic Engineer