Market Segment: Medical Equipment

Health and Wellness Start with Trust

Medical equipment makers need to balance the safety and privacy of the patient, the cost and convenience for the medical provider, and the liability and risks for their own company. With so much at stake, security and privacy by design are a must.

Device connectivity has an increasing impact on the medical industry. Besides convenience for caretakers, this also leads to risks of cyber attacks, which was evident when the FDA recalled 500 thousand internet-connected pacemakers for fears over hacking. While more equipment is being connected to various networks, consumables like catheters and body sensors are also (wirelessly) connected to medical equipment. Clearly, medical equipment needs to be safe from cyber attacks, guarantee privacy of the patient, and keep costs, liability and risks for the device maker low. At the same time, the growing connectivity also allows new business models for equipment makers, like pay-per-use or monitoring the use of consumables. But none of this is possible without the trust that is critical in this market. So, what are the security risks medical equipment makers need to overcome?

Keywords: medical equipment, security, Root of Trust (RoT), cryptographic keys

Problem

- Connecting medical equipment to a network requires device authentication and encrypting data to protect communication and network
- Connecting and monitoring the use of consumables requires mutual authentication
- Medical equipment typically contains secret and valuable IP that needs to be protected from reverse-engineering and counterfeiting

Solution

- These problems have in common that they require cryptographic keys to guarantee trust
- Creating unclonable keys that cannot be altered or copied requires them to be rooted in hardware, creating a Root of Trust (RoT)
- SRAM PUFs are a flexible and low-cost way to create this secure RoT on any medical device

Results

- An unclonable, immutable, invisible and unique identity as a robust trust foundation for security and privacy by design
- Secure, authenticated data delivering end-to-end protection when connected with network
- Secure connections with consumables allowing rollout of new business models
- Protection of valuable IP on medical device

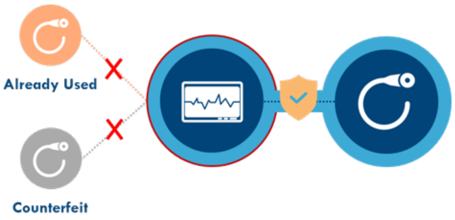
An SRAM PUF key is never stored and cannot be copied. It is immutable and invisible to attackers, creating an unparalleled anchor of trust.

Requirements for medical equipment are changing. Manufacturers need to balance the safety of patients with the increasing demands for connectivity, to increase convenience for care providers and add business opportunities for themselves. But to guarantee safe operation of a device, the connections with the network need to be secured, consumables need to be authenticated, and IP inside the device needs to be protected. How can equipment makers deal with all these new requirements?

Hardware-Based Root of Trust

Foundational for security of medical equipment are cryptographic keys that allow authentication to the network, encrypting data, authenticating consumables, and protecting valuable IP. This is needed to keep connected medical equipment safe, such as pacemakers, insulin pumps, and sensing equipment. Keys are derived from the secret identity of the device, which should be rooted in hardware. It must be impossible to read or alter this identity or to clone it to create counterfeit devices. So, how do an identity and keys get on a device, and how are they stored securely? Through Intrinsic ID's SRAM PUF technology. SRAM PUFs create unclonable, device-unique keys from tiny variations in silicon of the device's main chip. These keys are never stored and cannot be copied. They are immutable and invisible to attackers, creating an unparalleled Root of Trust. SRAM PUF keys are the foundation for many security solutions:

- Network connectivity: Authentication and encryption to protect communication & data
- IP protection: Signing and encrypting IP with device-unique SRAM PUF keys to prevent reverse-engineering & device counterfeiting
- Consumable connectivity: Authentication protocols to allow monitoring of consumables



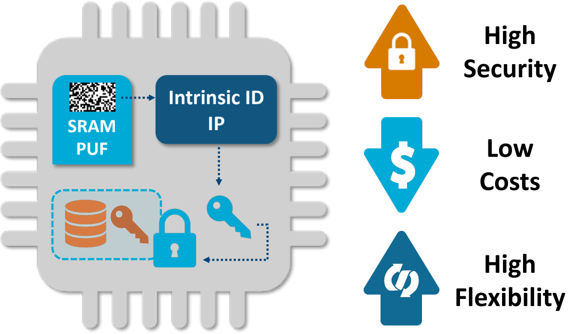
SRAM PUF Availability

Intrinsic ID provides its SRAM PUFs with the described security solutions integrated in the hardware of chips from several vendors, but also in software and as FPGA implementation for inclusion in device firmware. The solution has a very small footprint and a low cost.

Algorithms for both symmetric and public key cryptography are included, and compliant with NIST specifications. SRAM PUFs can be implemented on any typical microcontroller. For FPGAs without accessible SRAM, Intrinsic ID provides a solution that creates a PUF in the programmable fabric of the FPGA.

SRAM PUFs offer the best-in-class combination of high security, low cost and high flexibility:

- Security is high, as keys never leave the chip's security perimeter and are never stored
- Cost is low, because no additional security hardware or key programming is required
- Flexibility is high, because the software or firmware can be added to a device after manufacturing, which allows for retrofitting of security on existing medical devices



Bottom Line Benefits

- Trust: an unclonable, immutable and invisible identity for security and privacy by design
- Device authentication and data security
- Secure connections with consumables
- Protection of valuable IP on medical devices
- Flexible integration, including retrofitting

INTRINSIC ID

www.Intrinsic-ID.com | info@Intrinsic-ID.com