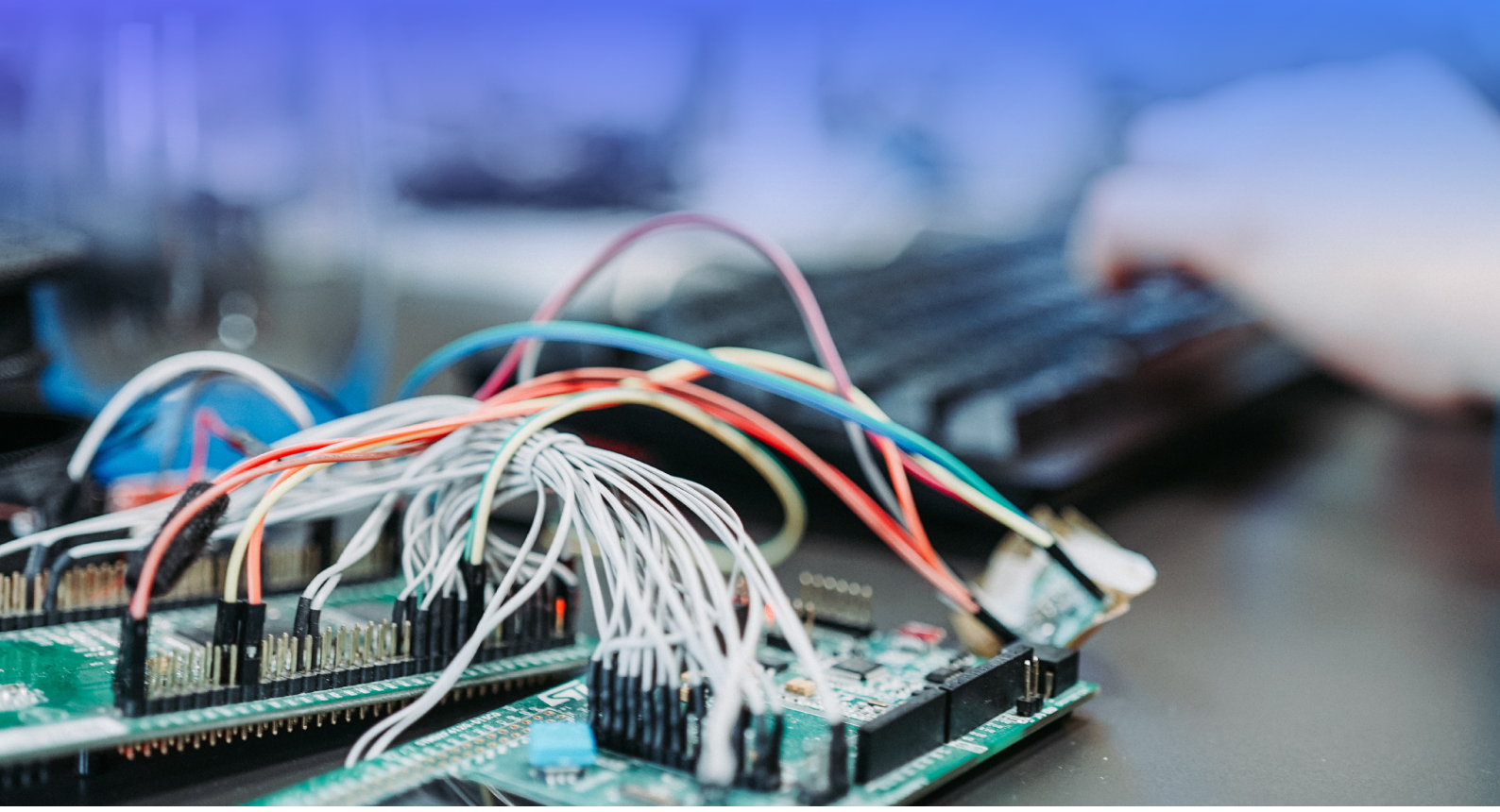
White Paper

SEALSQ
Newsletter PKI for IoT V1.0



SEAL SQ's accredited Root-of-Trust and Public Key Infrastructure combined with its tamper resistant secure elements including a preloaded digital certificate procure unpreceded security to any connected objects, be it an equipment on a factory floor, a smart meter or a remotely controlled device, such as a drone. This protects companies against ever increasing risk of cyberattacks, thus safeguarding their revenue, brand image and valuable assets.

Cyberattacks become increasingly efficient and rewarding for their perpetrators. Attacks such as Mirai and Stuxnet show that the need for protecting the device at factory floor becomes vital for any enterprise. While in the first example the malicious code was directly implemented in the connected device, in the second, the malicious code was able to control the device over an industrial network. This protection starts with an undisputed, unclonable identity, or birth certificate, issued and certified by a trusted party, from which a whole security foundation can be built in the device and in its communications.

Read More……

SEAL SQ's accredited Public Key Infrastructure Root-of-Trust combined with its tamper resistant secure elements including a preloaded digital certificate procure unpreceded security to any connected objects, be it an equipment on a factory floor, a smart meter or a remotely controlled device, such as a drone. This protects companies against ever increasing risk of cyberattacks, thus safeguarding their revenue, brand image and valuable assets.

Whenever a device gets connected to a network to be remotely monitored and controlled, direct contact with this device is lost. Physical barriers, such as entry doors to get to the factory being gone and the device often being accessed through a Zero Trust Network such as the Internet , its functioning can be altered by unauthorized parties, resulting in a loss of assurance that data coming from it is actually authentic, unmodified, unspied and therefore trustworthy.

Hackers enjoy such weaknesses.

Connecting a device without the proper security is asking for trouble. The question is not if you'll be attacked, the question is when.

Protecting a connected device comes down to some basic rules:

• Authenticating the device at first connection and throughout operation, avoiding unwanted clones or phantom devices occupy resources and send fake data

• Securing the communication channel to ensure data is unaltered, authentic, unique, and confidential

• Preventing unauthorized firmware execution and updates

The foundation of digital security is digital identity. SEAL SQ, as a Swiss provider of WebTrust approved digital certificates and certified tamper resistant secure elements, offers globally trusted digital identities from the very moment of device manufacturing. Through its lifetime, this device can be identified, authenticated, authorized and thus trusted thanks to SEAL SQ's INeS completely integrated Certificate Management System

What is a digital Identity?

A digital identity is the digital equivalent of a passport or photo ID. It consists of a unique digital attribute stored in the device, recognized and certified by a trusted third party. This attribute is actually stored in a secure element, a tamper resistant microcontroller located in the device, holding a secret private key and a related public key cryptographically signed together with other information by this trusted Certificate Authority (CA).

Authenticating a device

The authentication of a device is done through industry-standard protocols, such as SSL/TLS. This protocol allows a backend server or IoT platform to check the validity of the digital identity. It checks the status of the device certificate and its origin. It also checks the signature the device generates on a given random challenge. If the digital identity passes verification, the device is considered authentic beyond doubt, as the information used in the device to generate the signature is protected by the tamper resistant secure element and thus cannot be spoofed or cloned.

Securing the communication

From the digital identity verification, based on the secret information used therein, session keys are derived to protect the communication channel. Communication can be encrypted, authenticated and its integrity protected. As the secure element handles this key derivation, here again, a solid trust can be vested in this secure communication channel.

Preventing unauthorized firmware execution and updates

A connected device is vulnerable to malicious firmware modifications through standard channels implemented for firmware updates. A simple login/password is not sufficient at all to protect any firmware modification. A simple digital signature based on a public/private key pair held by the editor of the new firmware neither, as clever hackers can circumvent software protection around the signature verification.

Here again, a secure element brings a real advantage for the protection of the editor's public key certificate and the validation of the signature of the new firmware.

Examples of applications

These types of protection have been successfully applied to applications such as:

• Smart metering: SEAL SQ's FIPS 140-2 Level 3 certified VaultIC420 secure element has helped the equipment manufacturer to comply with national regulations with regards to the supply of gas or electricity meters.

• Professional drones: SEAL SQ's VaultIC405 secure element has brought security in both drone and remote control, as well as in data transmission between both and when sending video footage to the ground.

• Asset tracking Bluetooth Low Energy beacons: SEAL SQ's VaultIC series of secure elements have brought authenticity and security to the data transmitted by the beacon to a backend service

Key features of VaultIC4xx secure elements

• FIPS 140-2 Level 3 or NIST CAVP certification

• Tamper-resistant secure hardware (Common Criteria EAL5+ certified product family) including:

- Protection against side channel attacks
- Monitoring of environmental parameters
- Protected memory

• Rich cryptographic toolbox powered by a large choice of algorithms (DES/3DES, AES 128/192/256, MAC, RSA up to 4096 bits, DSA up to 2048 bits, ECC up to 576 bits)

• Unilateral authentication (host authenticates VaultIC) and mutual authentication (host and VaultIC authenticate each other)

• Certified Random Number Generator

• On-chip key pair generation or digital identity generation and injection by SEAL SQ's VaultiTrust™ service

• Choice of interfaces: I2C, SPI, USB, GPIO

• Various memory sizes managed by file system

• 2.7-5.5V power supply

• Extended temperature range (-40°C to +105°C)

• QFN44, QFN20, SOIC8 or custom package

Key features of INeS

• Complete Certificate Management System for the needs of IoT. From certificate creation to lifecycle management, INeS solution is agile, scalable, economical and easy to use.

• Management of objects with their device types and their digital certificates, in particular for TLS authentication and digital signature applications

• Advanced Web GUI (Graphic User Interface) with multi-tenant capabilities where multiple independent instances of one or multiple applications operate in a shared environment

• Simple management of settings for certificate and device profiles

• Versatile REST APIs that allow easy integration with the business applications of the customer for device registration, certificate issuing, renewal and revocation. The REST API is available as an Open API for easy backend implementation for communications like HTTPS and MQTTS.

• Available as a service from SEAL SQ's secure datacenter or installed on premises

• Managed through customized web interfaces, allowing full deployment for users using standard web browsers (Chrome, etc.)

• Certificate enrolment by the device through standard protocols