White Paper

Seal SQ
BatterySEAL solution

How to protect your brand and your battery driven application from the risks arising from the use of campatible batteries in original devices ? use SEAL SQ's VaultIC 183/186 solutions

SEAL SQ's revolutionary battery authentication solution provides an innovative method to protect brands and their customers from the risks arising from the use of compatible batteries in original devices: a brand's reputation, liability and revenue are secured, while customers' safety and assets are preserved.

Batteries are well settled to be the preferred method for powering devices. As the market for replacement batteries grows, so does the number of compatible offers. Fake batteries hurt the corporate bottom line beyond just the loss of profits, they can also destroy brand reputation by delivering poor performance or even cause personal damage to the end users. Manufacturers need to limit or even disable the use of these non-original equipment in their devices. But how to identify non-original batteries beyond doubt?

BatterySEAL is the solution designed by SEAL SQ. It consists of a digital identity generated and injected into a tamper resistant secure element, a set of software libraries to reduce integration efforts and a customization service if required, all with government grade security level.

Read More……

SEAL SQ's revolutionary battery authentication solution provides an innovative method to protect brands and their customers from the risks arising from the use of compatible batteries in original devices: a brand's reputation, liability and revenue are secured, while customers' safety and assets are preserved.

Batteries are well settled to be the preferred method for powering devices. We'll find them in many equipment, including power tools, medical devices and electric vehicles. The advantages are obvious, but come with a flow of drawbacks that can easily ruin brand's reputation: the aftermarket of batteries is huge and hundreds of companies are now proposing compatible batteries of questionable quality. Their performance decreases with their price. More importantly, low quality batteries can be dangerous: they can explode and damage devices, or even injure people.

Apart from that, compatible batteries jeopardize the original manufacturer's revenue.

To cope with these issues, SEAL SQ proposes its highly secure BatterySEAL solution, to uniquely identify and authenticate original batteries. It consists of a tamper resistant secure element, a digital identity securely generated and injected, a set of software libraries to reduce integration efforts, and a customization service if required. SEAL SQ aims at the highest standards of security and is certified Common Criteria and FIPS.

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 battery

Authenticating a battery consists of checking if its certificate is correctly signed by the trusted CA and if its secret private key corresponds to the corresponding known public key contained in the certificate.

Obviously, this secret private key shall remain secret. Knowing this secret would allow hackers to produce clones of the original device – like printing an undetectable fake passport.

Therefore, the digital identity is stored in a tamper resistant chip, SEAL SQ's VaultIC186 or VaultIC183, to be protected against all sorts of physical and logical attacks. The digital identity itself is generated by the globally trusted CA, the OISTE Foundation

operated by SEAL SQ, and injected in SEAL SQ's government grade secure production environment, with our VaultITrust service. The authentication itself is performed by the host microcontroller of the device powered by the battery. SEAL SQ provides software libraries to help develop the microcontroller firmware.

Key Features of BatterySEAL

BatterySEAL consists of

- Tamper resistant secure microcontroller with embedded firmware: VaultIC186 or VaultIC183
- Generation of digital identities and certificates and injection of these into VaultIC186/VaultIC183 in SEAL SQ's Common Criteria security certified production facility
- Development of host microcontroller specific secure cryptographic library (WISeDeveloper service)
- Example C-Source code of authentication process and communication protocol to be integrated into the host microcontroller firmware to reduce integration efforts

Key Features of VaultIC186/VaultIC183

- Unilateral authentication (host authenticates VaultIC) and mutual authentication (host and VaultIC authenticate each other)
- On-chip host certificate validation for flexible host authentication
- On-chip key pair generation
- Elliptic Curve digital signature (GF2n) B-163 to B-283
- 528-byte read/write user file system with configurable access control
- Four 32-bit counters, secured by Elliptic Curve Cryptography and protected against power loss by anti-tearing mechanism

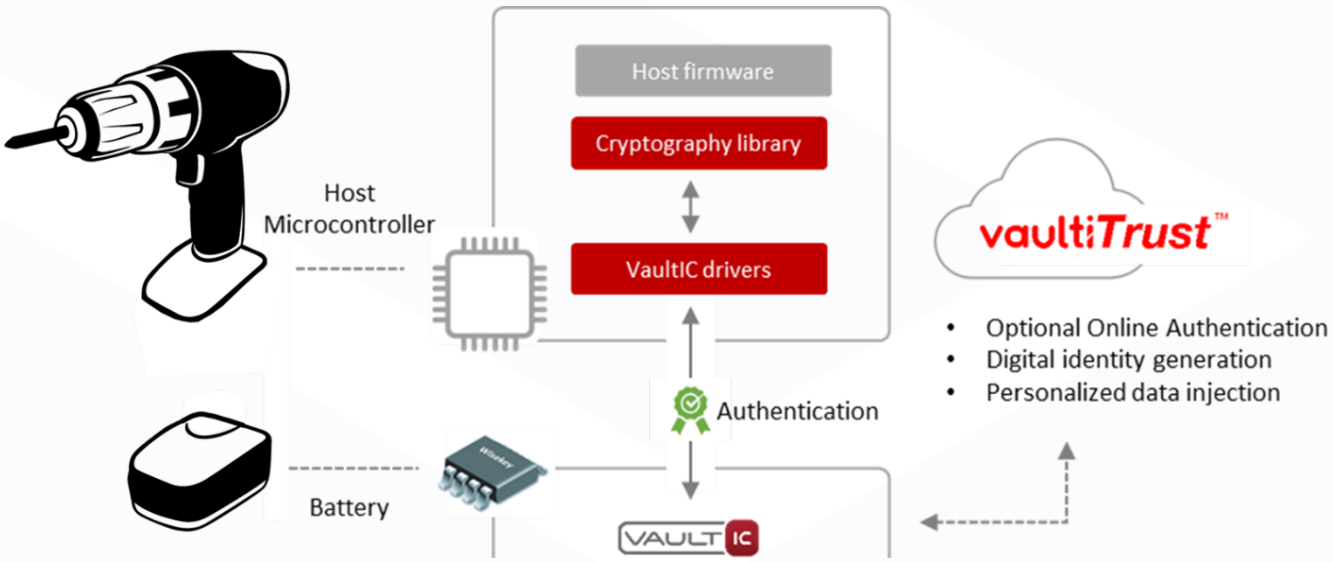
- One Wire Interface (OWI) up to 100 kbps (VaultIC186) or I²C interface up to 400kbps (VaultIC183)

- Tamper-resistant secure hardware (derived from Common Criteria EAL5+ certified product family) including:
    - Protection against side channel attacks
    - Monitoring of environmental parameters
    - Protected memory

- 1.62V-5.5V power supply

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

- 6-DFN (2mm x 3mm) or custom package



BatterySEAL architecture for power tools battery protection