PROEKSPERT
Software, design and data services

Secure Firmware Updater technology

Proekspert helps to develop secure firmware (FW) update solutions tailored specifically for industrial device manufacturers. We are experienced in working with embedded software platforms and developing custom software, helping to customize the solution to your needs.

Key features

Secure and tamper-proof FW update process

Through security features like Secure Boot, data encryption and TrustZone®, our solution ensures that the whole FW update process is safe and cannot be modified or tampered with by external unauthorized parties.

Authentic FW verification

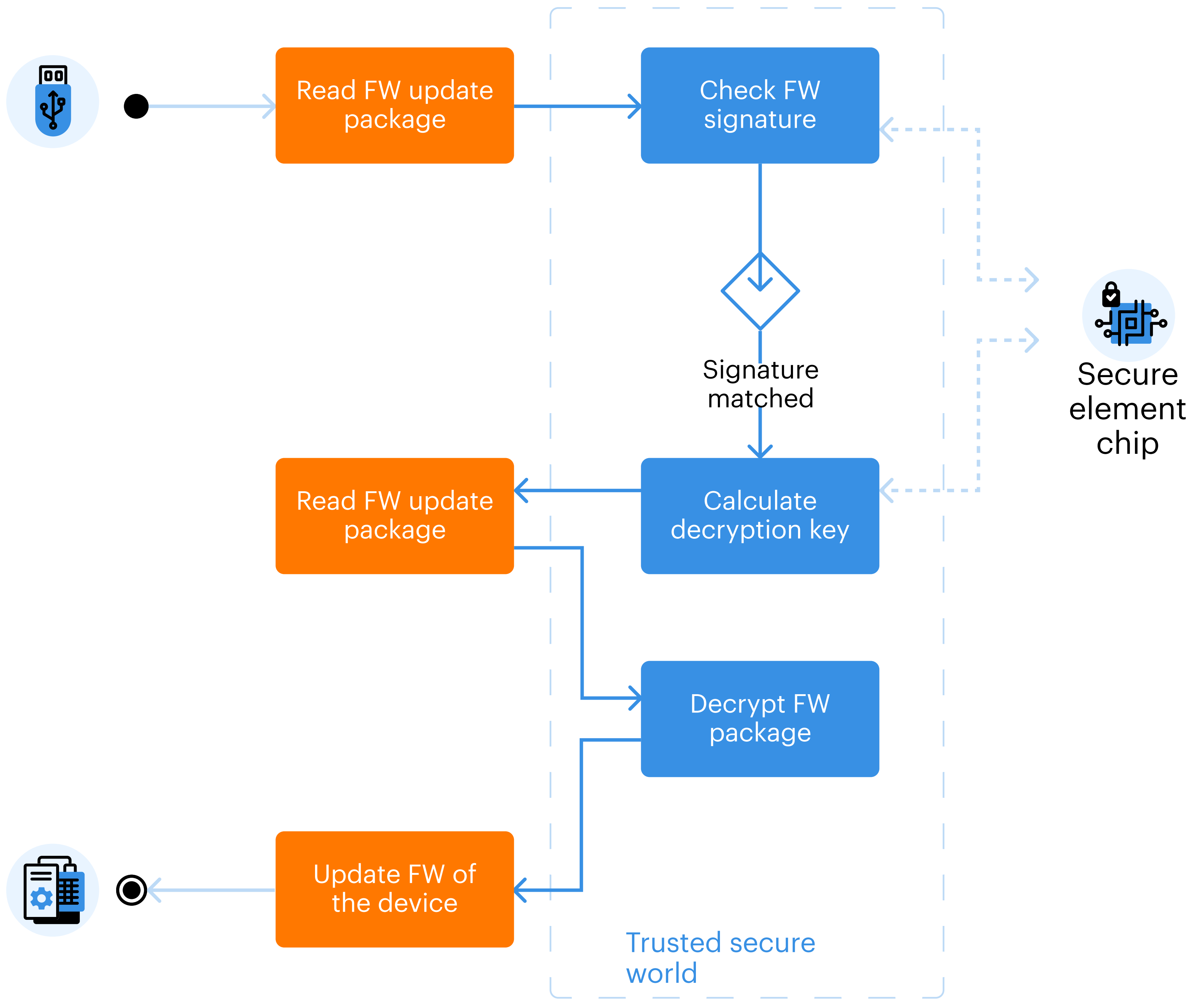
Integrity and authenticity of the FW is checked after reading the initial package, plus the signature is matched utilizing our secure element chip, making sure only authentic FW gets updated in the process.

USB / offline FW updating

An offline, on-site update process is used to ensure security right at the target device level and make FW updates possible in places without online connections.

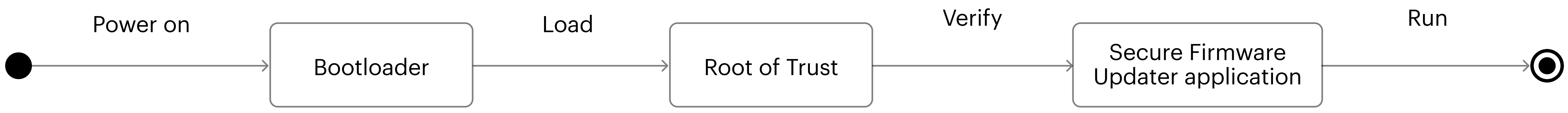
How does our Secure Firmware Updater work?

One of the key security features, TrustZone®, is used to separate sensitive cryptography-related operations into an isolated secure world. This adds an extra layer of security, since outside communication with the secure element takes place only through strictly defined interfaces, meant to minimize attack possibilities toward any sensitive data.



Enhanced security using Secure Boot

We use the Secure Boot process during the application startup phase to ensure that only trusted software components are loaded during the boot process. The process uses a root of trust, a trusted bootloader, and a series of verification steps to ensure only an authentic version of our application is allowed to run. The Secure Boot process, illustrated in the drawing below, can be customized or improved according to the client system's cybersecurity requirements.



Security features in our products

Our Secure Firmware Updater ensures safe FW updates by supporting major security features.

- **Secure Boot** – An extra layer of security which only allows the FW updater application to run when its integrity is verified against a trusted signature.
- **Secure Element** – a.k.a. the Trusted Platform Module (TPM) or crypto chip. A Secure Element provides a secure storage- and generation environment for encryption, decryption, and verification keys.
- **Data signing and encryption** – A firmware update package is encrypted and signed by the device manufacturer, ensuring that only trusted update packages are processed.
- **TrustZone®** – Technology which helps us separate the device into the "trusted secure world" and "normal world," so sensitive and critical operations such as data signature checks and decrypting the firmware can be handled securely and separately from regular operations.

Proekspert's supported MCUs and TPMs

Our Secure Firmware Updater ensures safe FW updates by supporting major security features.

MCU families supported:

- STM32F4
- STM32U5
- STM32L5

Secure Elements supported:

- STSAFEA110
- Infineon OPTIGA Trust M

Get in touch

Our experienced engineers can help assess and mitigate cyber risks concerning your product. Let's see if we are the right partner for you.

Terry London

Partner & Product Manager

terry.london@proekspert.ee

Terry London

Phone: +372 651 8700

Read more on our website:

proekspert.com/blog/connected-products/secure-firmware-updater-technology