PROEKSPERT

Software, design and data services

Our solution

Secure firmware update solution

Scale your product reach

Innovate with balanced product cost

Reduce product maintenance costs

Proekspert helps device manufacturers to prepare for upcoming EU Cyber Resilience Act

We help device and machine manufacturers develop intelligent products and focus on customers through value-adding digital services. We do this by combining data science and software development expertise with a design thinking approach.

The secure firmware update solution is used in two case scenarios.

Scenario 1. Preventing unintended device firmware updates

Updating devices over the internet or on-site by a technician poses risks of malicious usage and simple human error and may render a device inoperable, causing enormous expense, especially when the device is in a difficult to reach or remote location.

To give device manufacturers more control in the software update process, Proekspert has developed a hardware-level device firmware authenticity validation solution.

Scenario 2. Licensing device firmware

Device makers need control over software that is run on their devices. Proekspert has developed a hardware-level license verification solution to determine if an end-user is eligible for software updates or new features.

Common risks when updating device software

Unverified sources

Offline devices cannot verify if the specific firmware image is coming from an authentic source.

Lack of trained specialists

Updating device software manually on site is costly for maintenance service providers.

Malicious users

Malicious users may tamper with the device by altering the original firmware update package.

Unintended features

Wrong firmware version may ruin the user experience or break important features.

Key features and benefits of our solution

Enabling secure remote updates Over-the-Air and via Ethernet.

Preventing human errors by protecting a device against manual invalid FW updates online and offline.

Protecting device software against malicious usage and network attack.

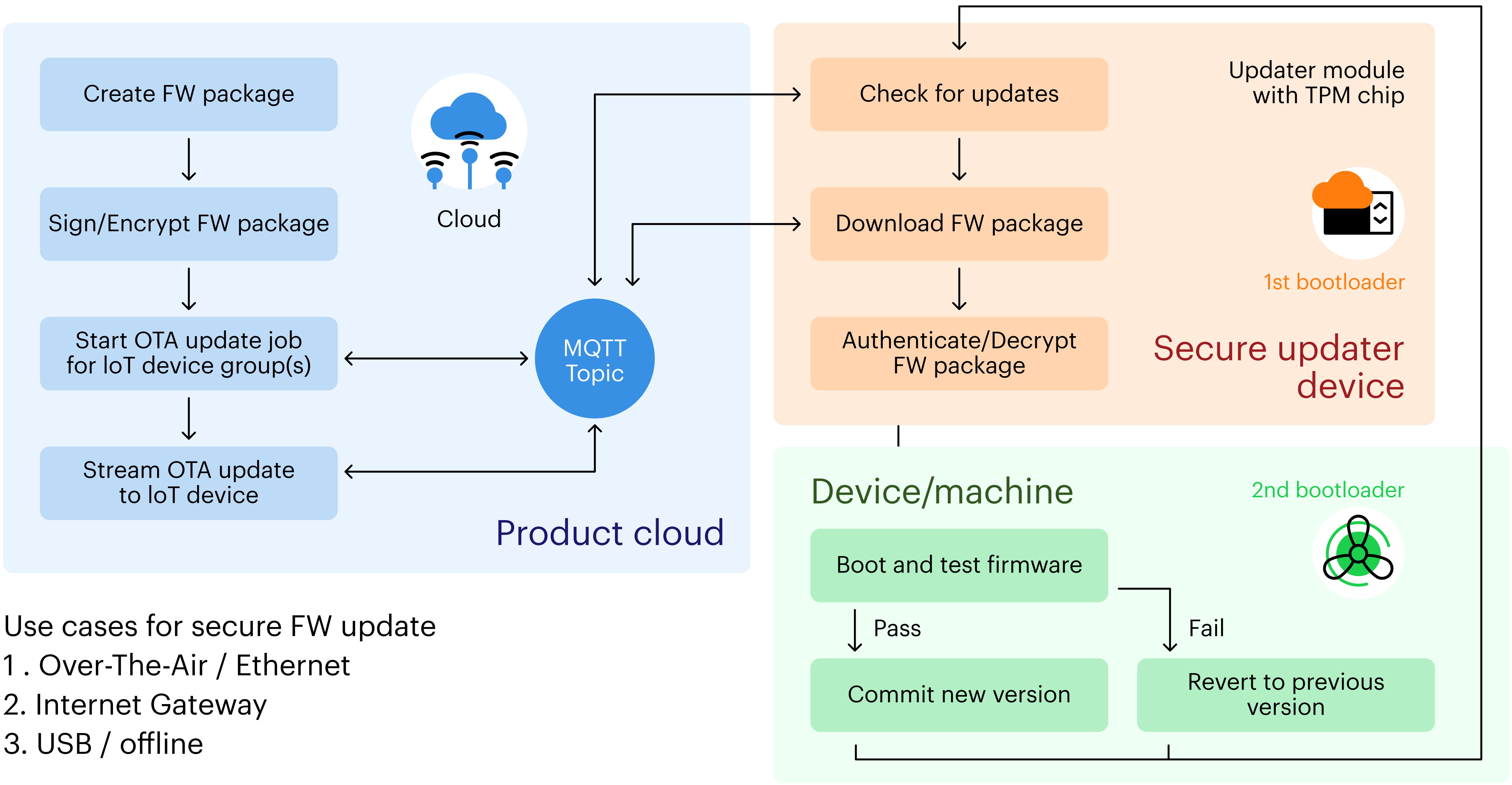
Enabling device-level software licenses.

How it works

Proekspert's firmware authenticity verification software uses a crypto processor chip (TPM) integrated with a device's motherboard to automatically verify an update file signature and/or decrypt a previously encrypted firmware update package.

Each TPM is unique, so on the device software development side the firmware is signed or encrypted for devices one by one. When a device updater discovers firmware with an incorrect signature or encryption, the update process halts without altering already installed software.

Secure FW update from a cloud service



Use cases for secure FW update
1 . Over-The-Air / Ethernet
2. Internet Gateway
3. USB / offline

Get in touch

We have tens of years of experience in developing secure software by design. Keeping the balance between security and end-user experience is a common practice for us.

Let's see if we are the right partner for you to prepare your devices and infrastructure for CRA.

Read more about this solution
on our website:

proekspert.com/secure-firmware-update-solution

Jukka Antero
Halttunen

Devices Business Unit Lead

jukkaantero.halttunen@proekspert.ee

jukka-halttunen

Phone: +372 5621 6173