PROEKSPERT

Software, design and data services

Our solution

Device identity management solution

Scale your product reach

Innovate with balanced product cost

Reduce product maintenance costs

Proekspert has over 20 years of experience securely integrating payment terminals with banking backend services. Today, we use our expertise to implement device security solutions in the industrial device manufacturing world.

Device identity management is used in two case scenarios:

Scenario 1. Establishing the authenticity of connected devices and services

Establishing identities for endpoints like devices with extremely high risk and responsibility: payment terminals, national ID-cards, life-critical devices, electronics with safety features.

Scenario 2. Securely exchanging data between services and connected devices

Reconfiguring and updating critical devices. Exchanging high-risk confidential data or monetary value.

Common risks when communicating with remote devices

Unverified sources

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

Lack of trained specialists

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

Malicious users

Malicious users may tamper with a device by spoofing it or replacing data packages sent to the server.

Unintended features

A wrong firmware version may ruin a user experience, break important features, or even brick the device.

Key features and benefits of our solution

Enabling secure remote device 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 and data against malicious usage and network attacks

Enabling device-level software licenses policies and certificate updates

How it works

To ensure security, data exchange between a device and the outside world is encrypted with a data encryption key (DEK).

To guarantee the DEK's authenticity, it is generated using certificates and private keys that are securely placed before the device leaves the factory.

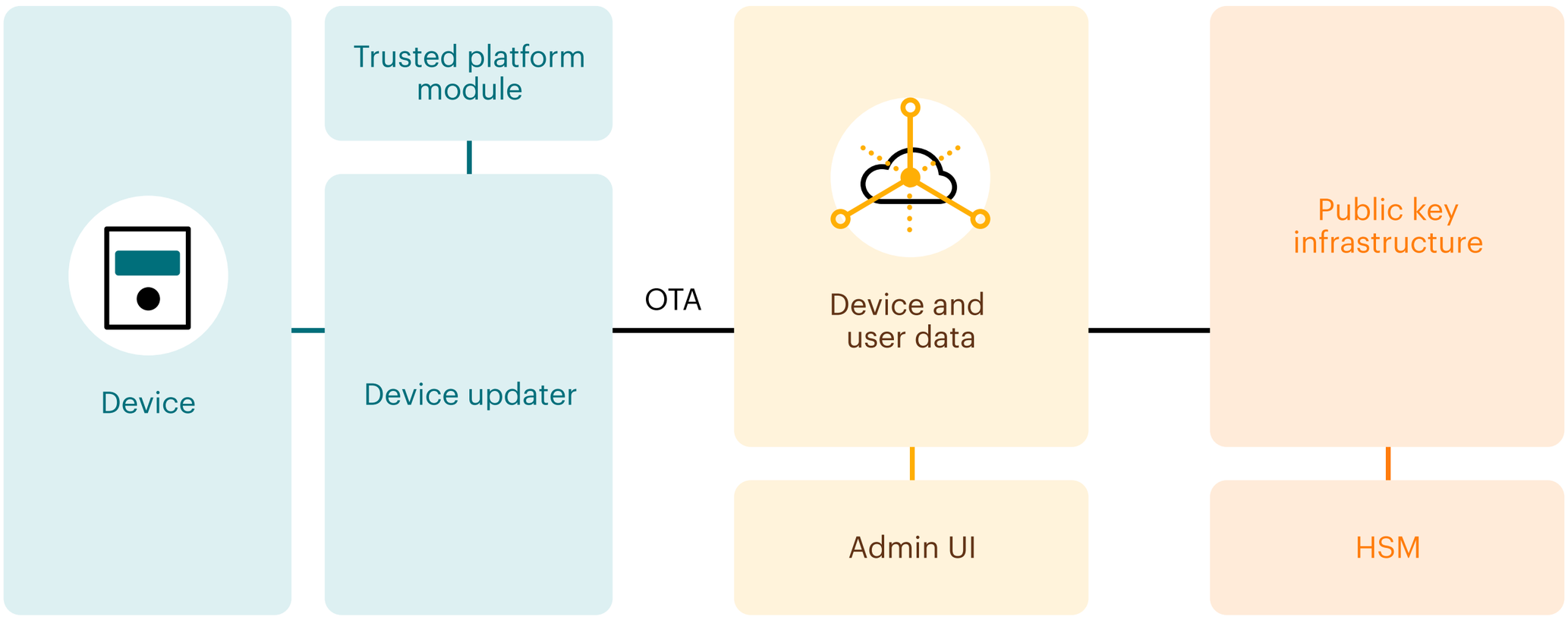
The aforementioned certificates are also employed to verify the origin of the data.

Key features and benefits of our solution

Strong embedded device security is built with secure elements and TPMs that enable unique identities for devices.

Remote device management over the cloud enables over-the-air (OTA) firmware updates and secure device connectivity over the internet.

A device identity management system is required when you have to manage many devices with unique identities in your organization.



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.

Michele Macrì
Devices Business Unit Lead

michele.macri@proekspert.com
Michele Macrì
Phone: +372 651 8700

Read more about this solution on our website:

proekspert.com/device-identity-management-solution