Preparing industrial device manufacturers for the upcoming EU CRA

from a secure embedded software development perspective

Terry London (MSc)

Product Manager of Device Security solutions

PROEKSPERT

proekspert.com

Visit our booth 4-380

Cloud connectivity for remote devices

- Industrial mobile apps
- Development, support and maintenance

Device cyber-security

- Secure Firmware Update
- IEC 62443 compliance analysis

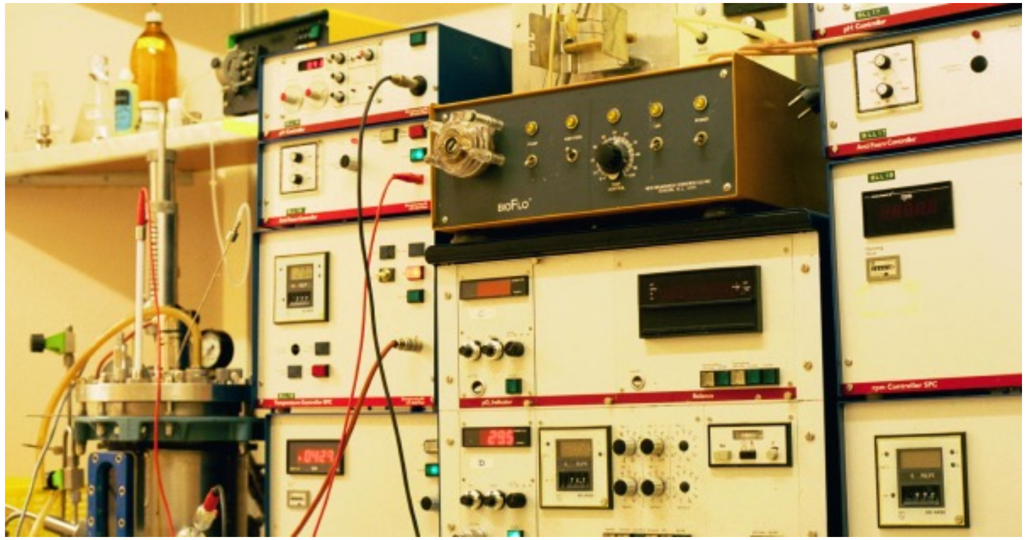
Why our experience matters

- 31 years
- 170+ people
- Software engineers' company

PROEKSPERT

Over **1 Million** manhours of embedded software development **since 1993**

Danfoss VLT® drives



Bioreactor control software for pharma
(***device remote control and monitoring***)

Smart Card and ATM banking software
(***device security and secure data transactions***)

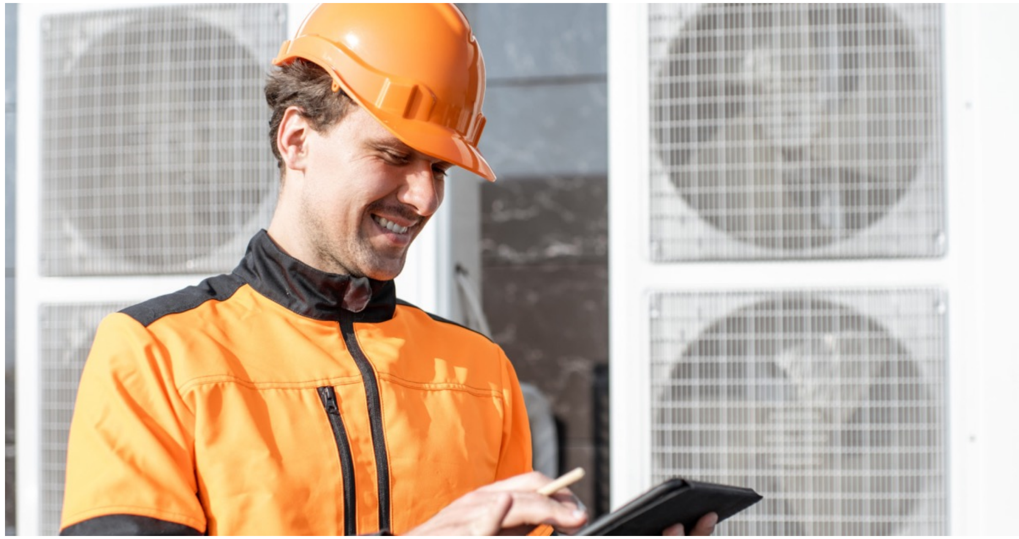
What we do today

PROEKSPERT

Custom software solutions for

Industrial Device Manufacturers

- Embedded software
- Device-cloud integration
- Technician apps



Danfoss

STIEBEL ELTRON

What is European Cyber Resilience Act (EU CRA)?

Unifies EU cybersecurity rules for more secure hardware and software products

Postponed until Q3 2024

https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

What the EU CRA wants to achieve?

- Protect the end-users of internet-connected devices against cyber-attacks
- Increase the responsibility of software developers and device manufacturers

Why it matters – cyber threats are real

Common myths about Industrial Control Systems

- We are offline from internet (https://www.shodan.io/)
- Control systems are behind a firewall
- Hackers don't understand control systems
- Our facility is not a target
- Our safety systems will protect us (Iranian steel mill attack 2022)

Target	Method
2010 Iran Uranium Enrichment	Stuxnet
2013 ICS Supply Chain attack	Havex
2014 German Steel Mill	spear phishing/ social-engineering
2015 Ukraine Power Grid	BlackEnergy KillDisk
2016 Ukraine Substation	CrashOverride
2017 Global shipping company	NotPetya
2017 IoT permanent DDos attack	BrickerBot
2017 Health care, Automotive, many others	WannaCry
2017 Saudi Arabia Petrochemical	TRITON/TRISIS
2019 Norwegian Aluminum Company	LockerGaga
2021 Colonial Pipeline	DarkSide
2022 Bridgestone Tire	ransomware
2023 DP World Australia	

EU CRA main requirements

- Get products assessed or certified
- Provide Software Bill of Materials
- Report vulnerabilities
- Provide security updates to fix the vulnerabilities

EU CRA certification requirements

Products must be assessed or certified

Common products

require **self-assessment**

- Smart home devices
- Toys

Critical products

require **3rd party assessment**

- Microcontrollers & processors
- General purpose operating systems
- Anti-virus software
- Firewalls
- VPN servers & clients
- Public key infrastructures

Highly critical products

require **certification**

- Smart cards
- Hardware devices with security boxes
- Smart meter gateways

EU CRA requirements for device manufacturers

Compile Software Bills of Materials (SBOM)

- Define software suppliers
- Define who is responsible of software modules & stages

Report product vulnerabilities

- Monitor software components
- Reporting process yet to be defined

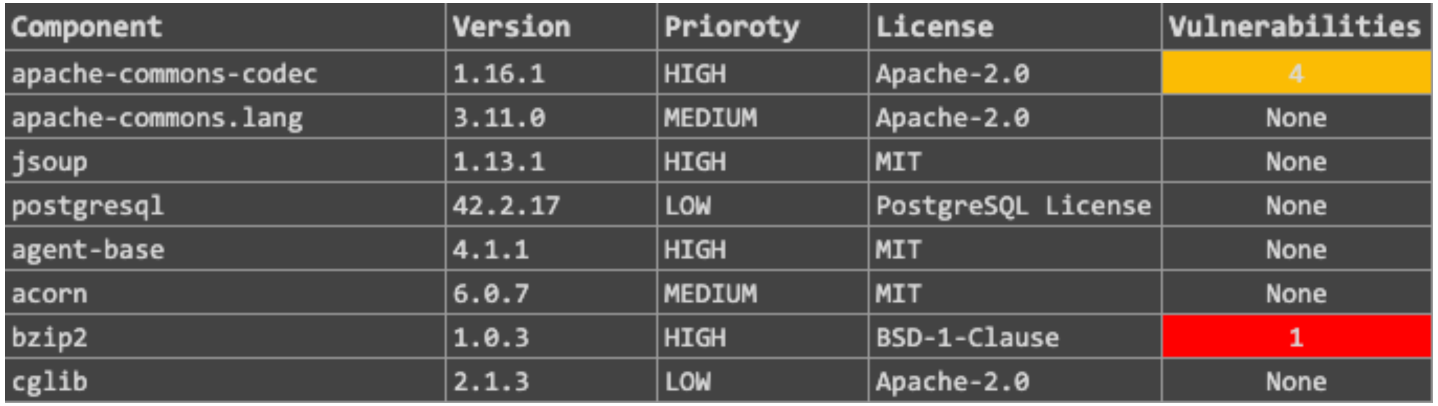
Ensure security updates

- Define intended purpose and requirements of the product
- Provide security updates over product lifetime (without delay and free of charge)

What is SBOM?

Software Bill of Materials (SBOM) is a list of all the open-source and third-party components present in a system's code

- Lists the licenses that govern the components, the versions of the components used in the code, and their patch status
- Allows for quick identification of any security or license risk



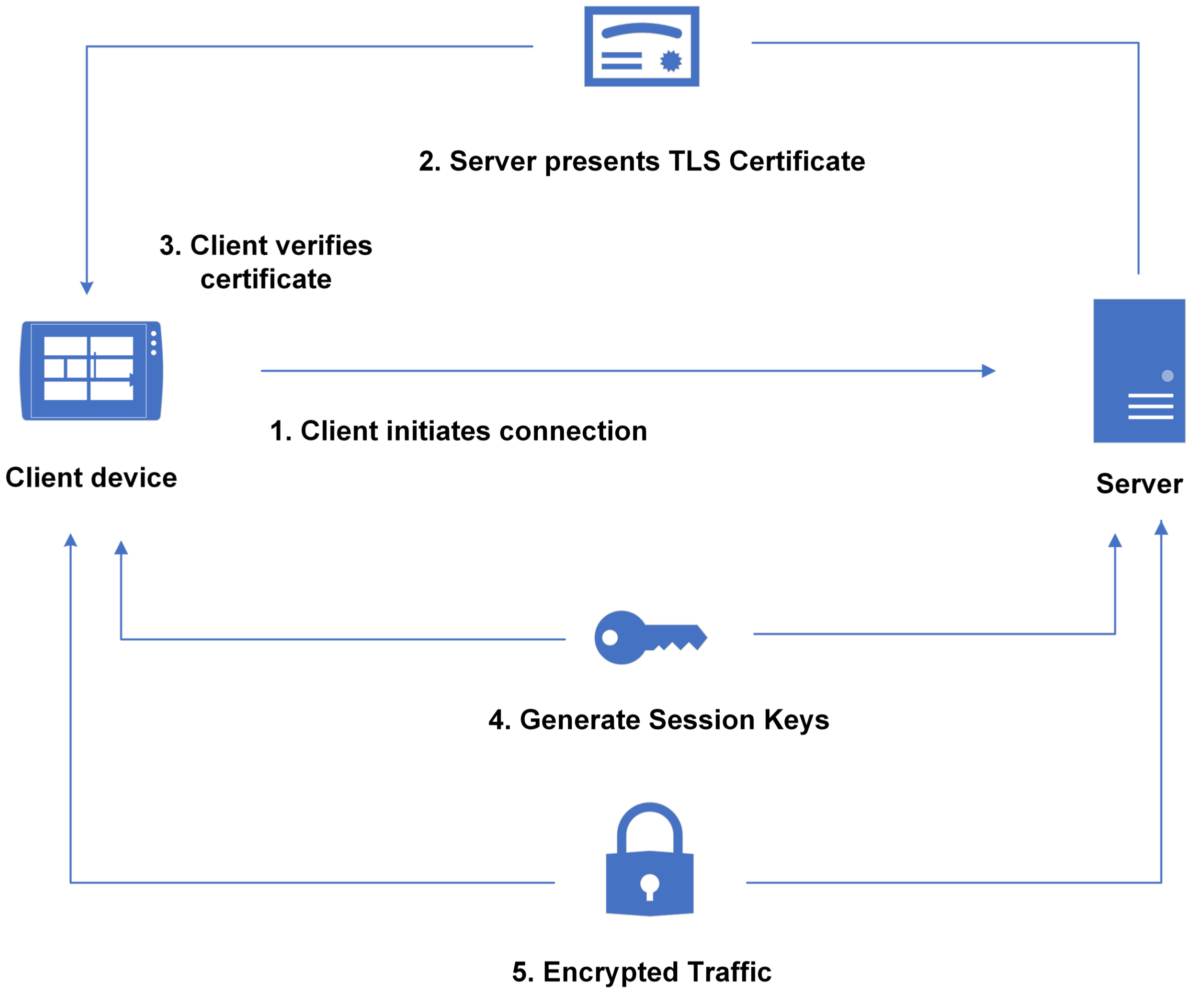
Component	Version	Prioroty	License	Vulnerabilities
apache-commons-codec	1.16.1	HIGH	Apache-2.0	4
apache-commons.lang	3.11.0	MEDIUM	Apache-2.0	None
jsoup	1.13.1	HIGH	MIT	None
postgresql	42.2.17	LOW	PostgreSQL License	None
agent-base	4.1.1	HIGH	MIT	None
acorn	6.0.7	MEDIUM	MIT	None
bzip2	1.0.3	HIGH	BSD-1-Clause	1
cglib	2.1.3	LOW	Apache-2.0	None

SBOM elements	
Supplier Name	The name of an entity that creates, defines and identifies components
Component name	Designation assigned to a unit of software defined by the original supplier
Version of the component	Identifier used by software component supplier
Other unique identifiers	Additional identifiers of the component
Dependency relationship	A relationship between two pieces of software where one piece of software relies on the other to function properly
Author of SBOM data	The name of the entity that creates the SBOM data for the component
Timestamp	SBOM data assembly timestamp

Ways of delivering security updates (securely)

- *Device PIN code/ username + password (not recommended)*

1. **Secure Over-the-Air (OTA) update (HTTPS/TLS)**
    1. IT standard for secure communication with Certificates
    2. Recommended in IEC 62443
2. **Device verifies the firmware (FW) package signature**


2. Server presents TLS Certificate
3. Client verifies certificate
Client device
1. Client initiates connection
Server
4. Generate Session Keys
5. Encrypted Traffic

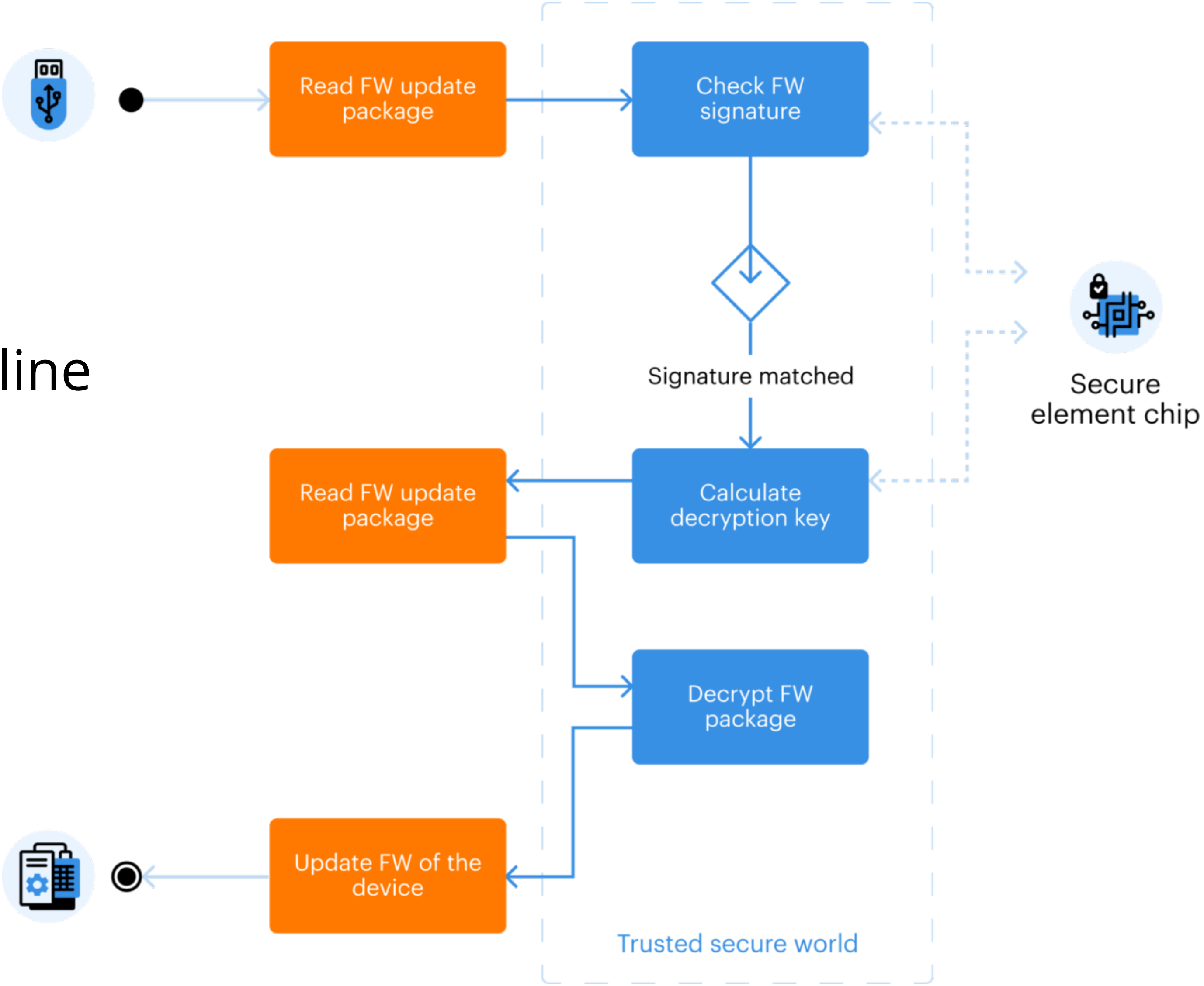
Devices as tamper-proof identities (1)

- Device-level encryption for offline security
- Integrated crypto chip provides hardware-level security
- MCUs with security features like TrustZone (e.g. PIC32CM LS60 or STM32L55)
- Full control over device firmware/ license

PROEKSPERT −−> booth 4-380

Devices as tamper-proof identities (2)

- Device-level encryption for offline security
- Integrated crypto chip provides hardware-level security
- MCUs with security features like TrustZone (e.g. PIC32CM LS60 or STM32L55)
- Full control over device firmware/ license



How we assist our clients (in security solutions)

- **Self-assessment** of device cyber-security risks (IEC 62443)
- **Software development processes** and tools (SBOM)
- **Implement security update delivery mechanisms** (Secure OTA update)

PROEKSPERT --> booth 4-380

Visit our booth 4-380

Cloud connectivity for remote devices

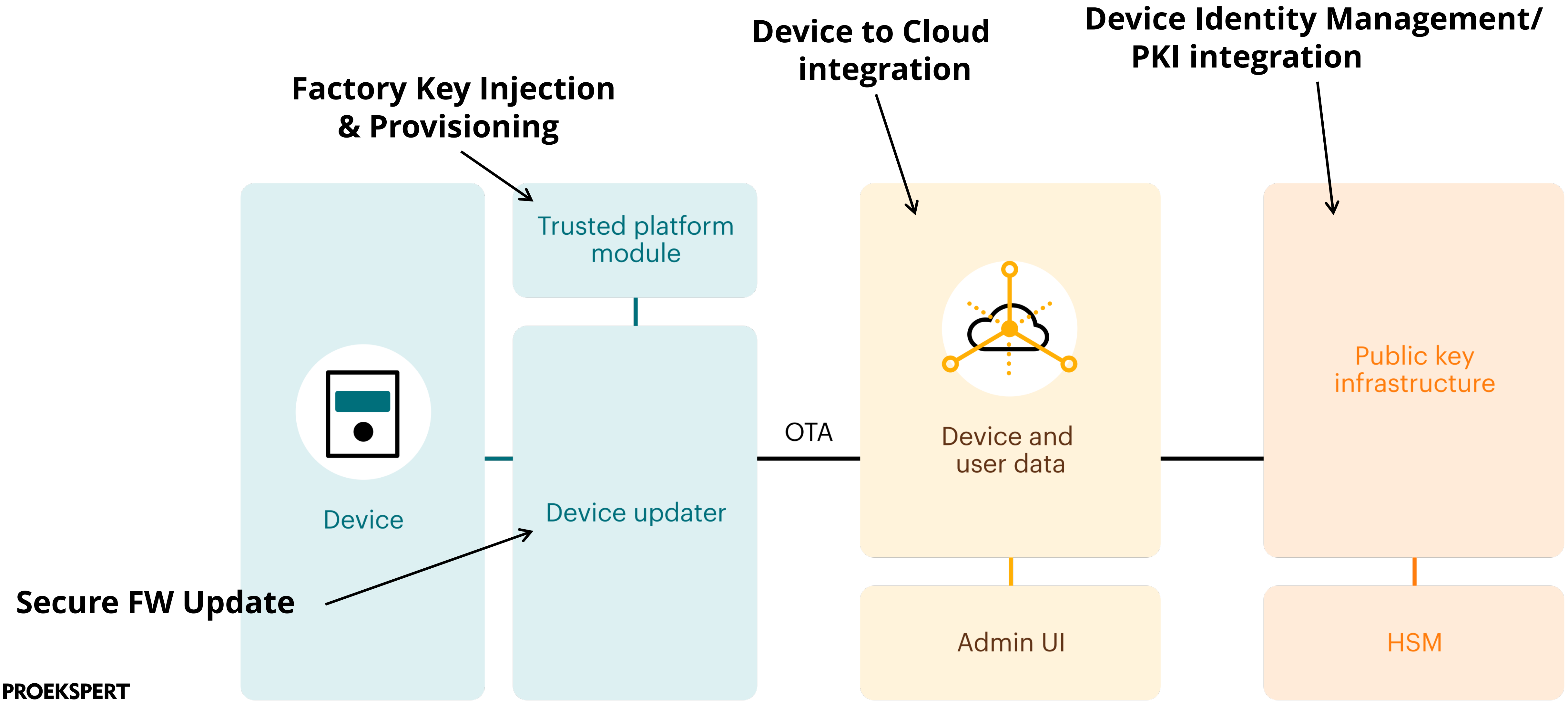
- Industrial mobile apps
- Development, support and maintenance

Device cyber-security

- Secure Firmware Update
- IEC 62443 compliance analysis

More device security materials in our web: https://proekspert.com/secure-firmware-update-solution/

Our secure solutions



Device Identity Management/
PKI integration

Device to Cloud
integration

Factory Key Injection
& Provisioning

Secure FW Update

Trusted platform
module

Device

Device updater

OTA

Device and
user data

Public key
infrastructure

Admin UI

HSM

Thank you!

You are welcome to meet me at both 4-380

Terry London

Device security solutions

For more info, please visit https://proekspert.com/

terry.london@proekspert.com

and don’t hesitate to ask me at Linkedin

https://www.linkedin.com/in/terry-london/