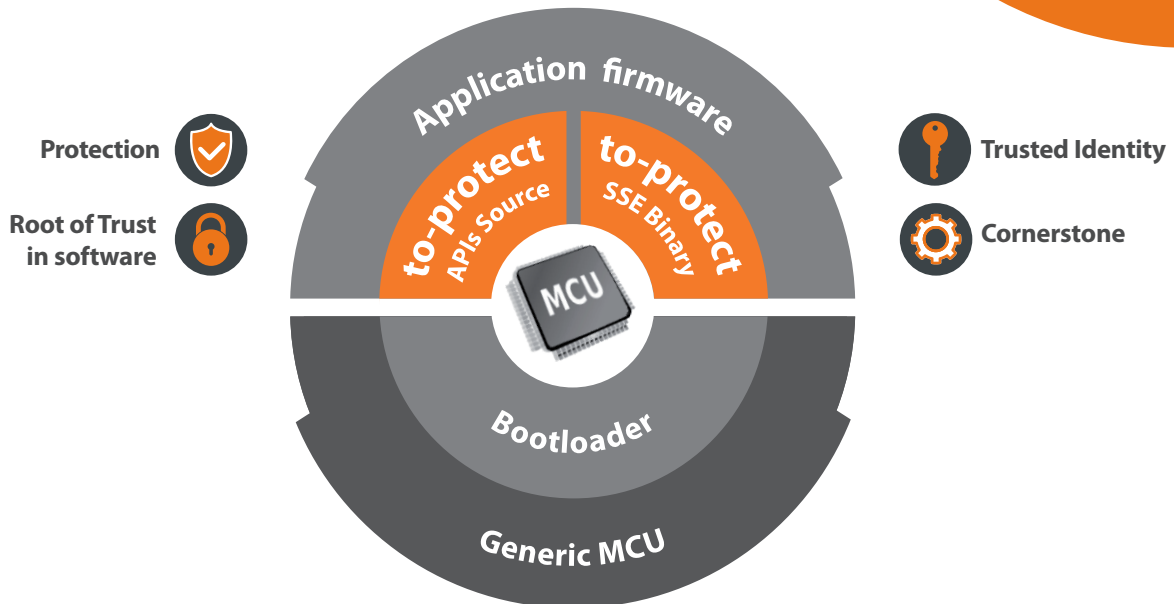


to-protect

Software Secure Element for *MCU-based systems

- ▶ **Protection** of IoT devices and data against security attacks
- ▶ **Root of Trust in software** for all devices based on generic MCU
 - ▶ **Trusted Identity** enabler, including for tiny MCU with no intrinsic security features
 - ▶ **Cornerstone** for edge to cloud security services

*MCU: Microcontroller Unit



to-protect key features

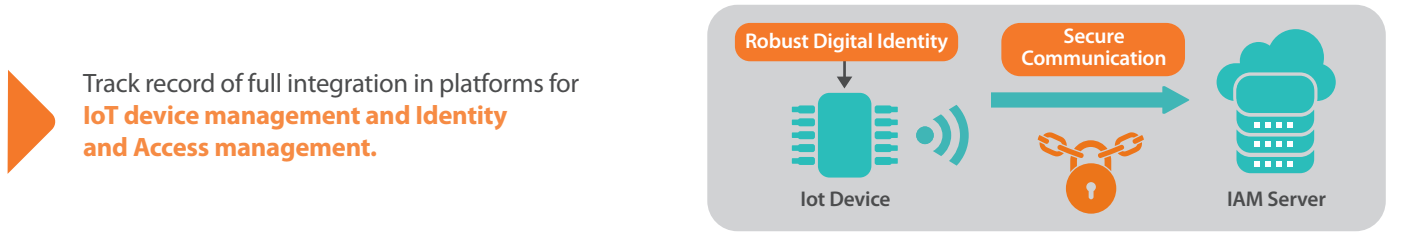
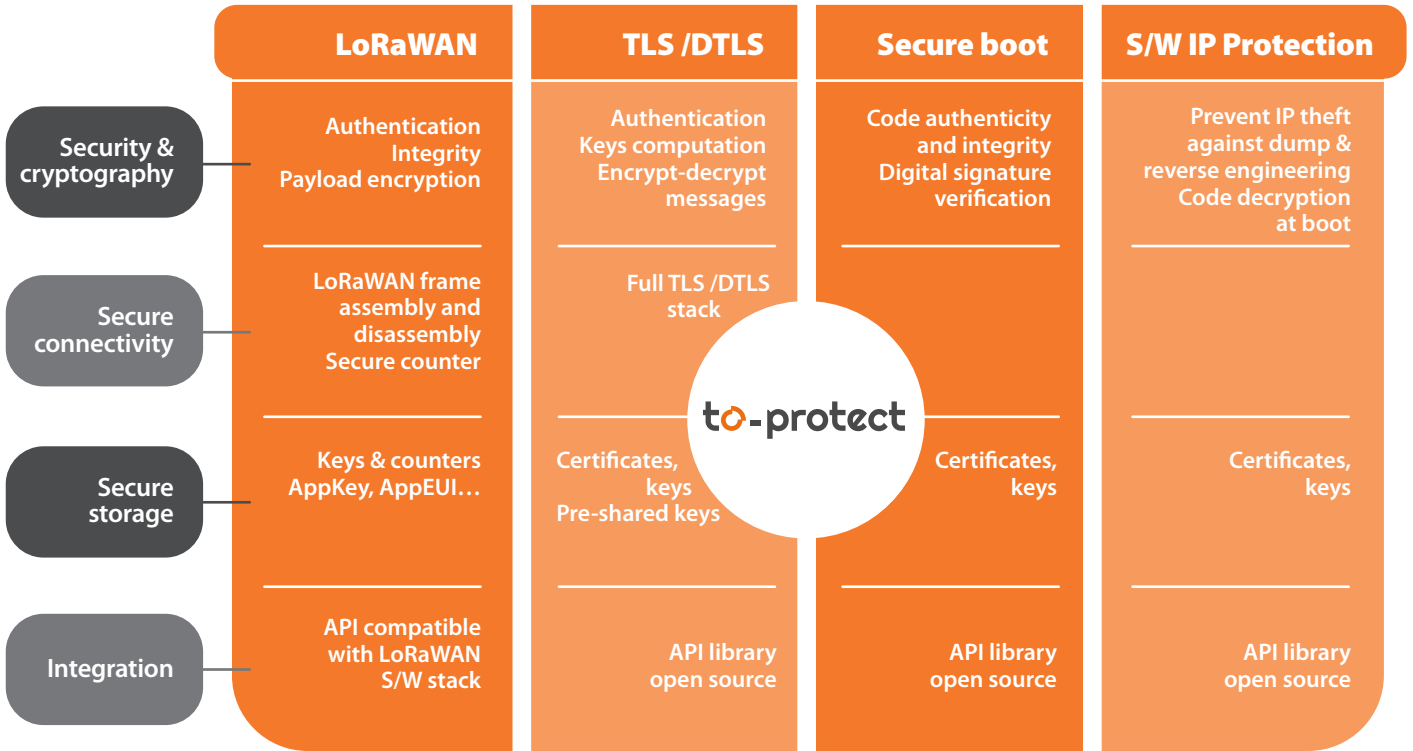
- **Security and cryptography operations:** secure authentication, data integrity and confidentiality, secure storage and more.
- **Secure connectivity:** LoRaWAN, TLS, DTLS secure implementation.
- **Secure storage:** keys, certificates.
- **Reduced code size,** no impact on device performances.
- **Run with tops,** a provisioning solution for secure manufacturing.

to-protect benefits

- **Running on generic MCU:** ARM Cortex, RISC V...
- **Prevention** against logical and physical security attacks.
- **Compatible with existing hardware:** no impact on the BOM.
- **Easy security retrofit** for devices already in the field with FUOTA mechanism (*Firmware update over the air*).
- **Easy to integrate** into security management platforms.

to-protect

Overview of **to-protect** secure software libraries family



▶ **Evaluation kit**
Evaluation version downloadable free of charge from our web site.
Production version under licensing model.