TrustnGo
Plug & Play Security

TrustnSafe SDK

A Framework to Secure IoT & Embedded Products

In Brief

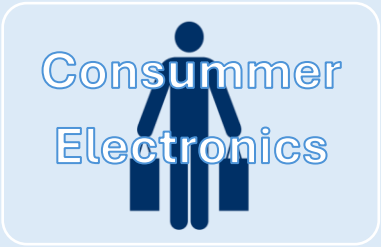
What could be worse than having your innovation stolen or seeing your product used to attack your customer's network ?

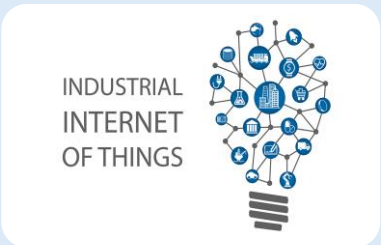
However, securing an embedded device can be a challenge due to constrained hardware & software, limited knowledges in cybersecurity technologies and a fast-changing market shaped by new regulations and customer expectations.

TrustnSafe SDK is a complete, portable & easy to use security framework designed to protect your MCU based products and fulfill requirements of new cybersecurity oriented regulations like the radio equipment directive 2014/53/EU or the Cyber Resilience Act.

Complete	•Secure Bootloader •Cryptographic Library •Secure Key & Data Storage
Portable	•Pure C source code •Any ARM Cortex-Mx & Cortex-M3x •Implements the Standardized PSA Interfaces
Simple	•Secure by Default •Comes with Provisioning Tools •No Proprietary Toolchain Required

Applications





Key features

Secure Bootloader

- Based on MCUboot
- Low footprint (< 64 KB)
- FW verification using ECDSA P-256/384 or RSA 3072
- FW encryption using AES128/256
- Anti-rollback
- Powerloss resistant update
- Support FW update from an external flash
- Relies on PSA Crypto API

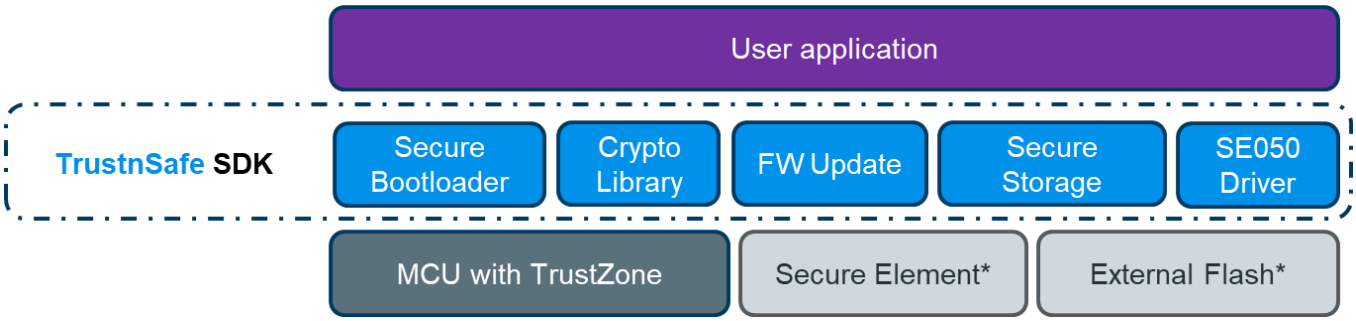
Crypto. Library

- Based on MbedTLS
- RSA 2048 to 4096
- ECDSA/ECDH
- AES 128/256
- Authenticated Encryption
  - AES-GCM/CCM
  - ChaCha20-Poly1305
- CMAC/HMAC
- TLS 1.2/1.3
- X509
- PSA Crypto interface

Supporting modules & tools

- Secure Storage
  - *ARM PSA ITS API*
- Secure Attestation
  - *ARM PSA Attestation API*
- Secure Update
  - *ARM PSA FWU API*
- Toolchain
  - *Image signing tool*
  - *Provisioning tool*
  - *PKI tool*

SDK Architecture



An *all-in-one* Software Development Kit

The **TrustnSafe SDK** includes all the software and guidance needed to secure your MCU based device against most common attack paths. Hence, it comes with an image signing tools which allows to protect your firmware signing keys. It also comes with simple and customizable PKI & provisioning tools that allow you to generate a small PKI and provision the issued certificates and keys into your devices.

Evaluation Kit, Training & Consulting

TrustnGo offers an evaluation kit for the **TrustnSafe SDK**. This evaluation kit includes the full SDK with a pre-programmed Nucleo-F439ZI board from ST Microelectronics.

Version 1.0

TrustnGo
Plug & Play Security

https://trustngo.tech
+33 781 765 448
sales@trustngo.tech

TrustnGo S.A.S
20 rue Paule Marrot
33300 Bordeaux