INFOSEC GLOBAL

Trust Management Root

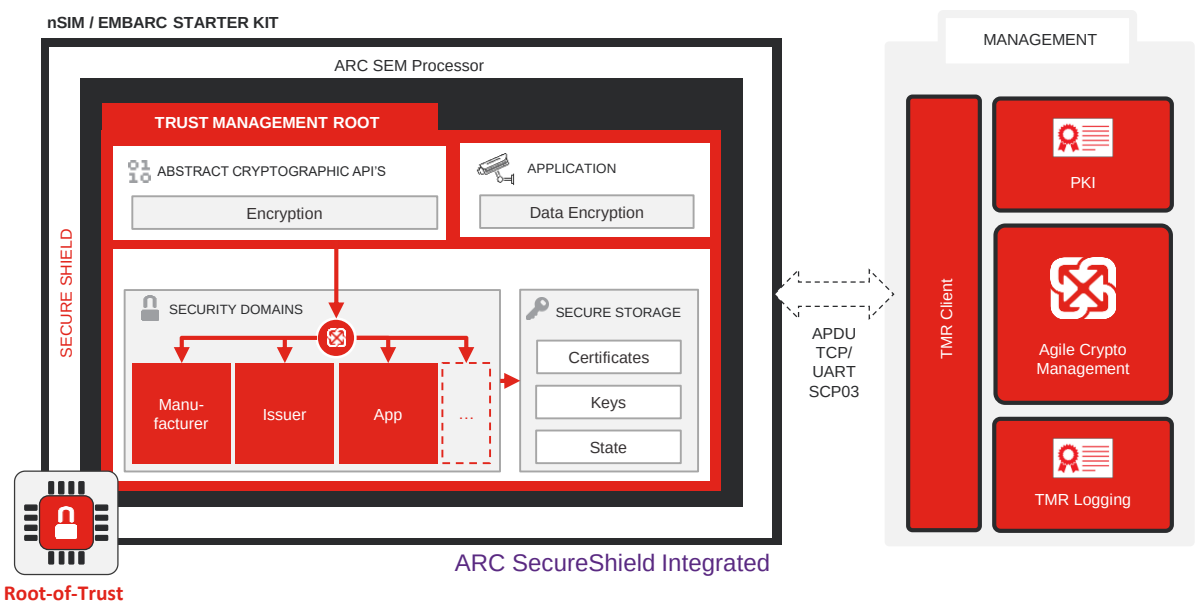
Agile Root-of-Trust for critical systems

Trust Management Root (TMR) Overview

- Create dedicated security domains
- Provision symmetric keys
- Provision public key certificates
- Establish secure management channel
- Encrypt application data
- Load dedicated crypto libraries at runtime
- Install new crypto libraries
- Use crypto within ARC applications

TMR Setup Overview

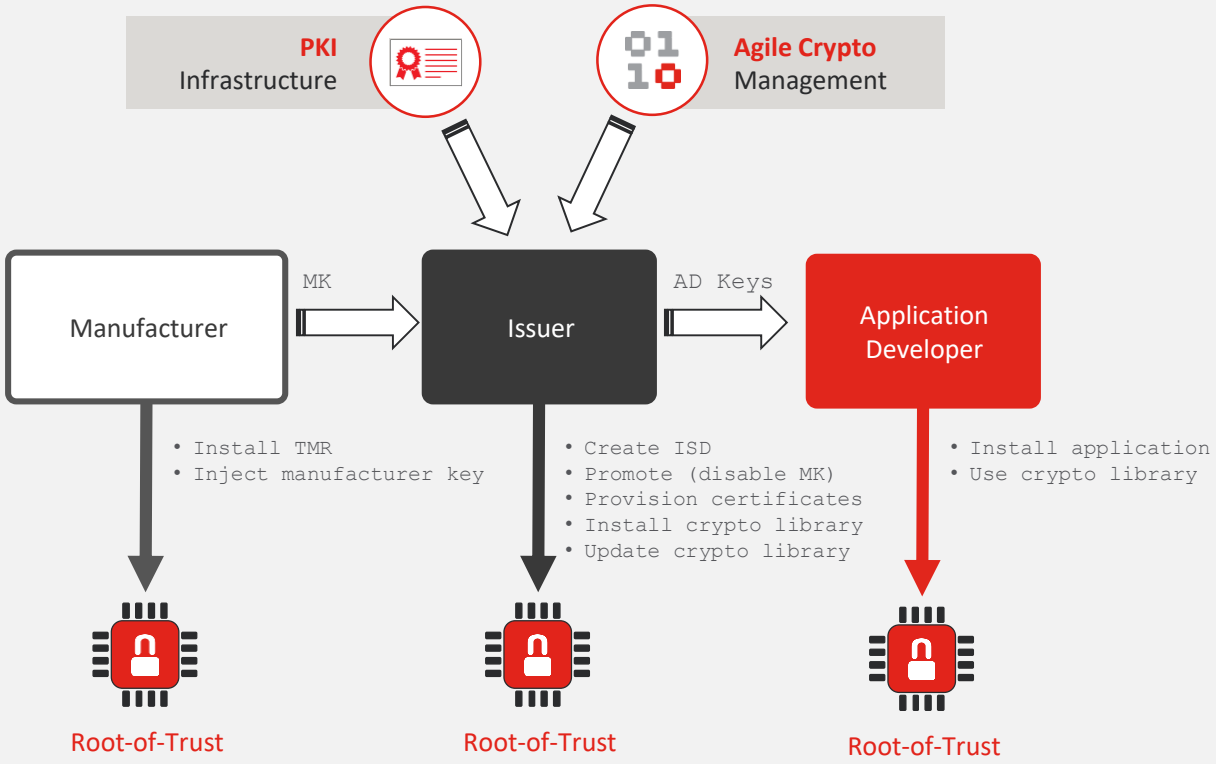
The Trust Management Root solution is composed by an end-point component, integrated within root-of-trust, and a management component, deployed within company infrastructure, to control lifecycle of keying material and cryptography. The architecture is as follows:



INFOSEC GLOBAL

TMR PROVISIONING & AGILE CRYPTO MANAGEMENT

Thanks to ISG unique agility layer, the root-of-trust can seamlessly support multiple keying material depending on the owners of security domains. This segregation make sure authorized entities can perform cryptographic functions using their own dedicated keying material.



KEY CAPABILITIES

The Key objectives of the ISG Trust Management Root is to deliver agility and control to organizations over sensitive keying material and cryptographic foundations used by their critical systems. The solution brings following state-of-the-art security capabilities to 3rd party systems coupled agile cryptography foundation:

Secure Provisioning
Make sure devices are securely enrolled with company keying material

Secure Identities
Make sure only trusted devices are able to access IoT network

Secure Data
Make sure sensitive data at-rest and in-transit are encrypted

Secure Updates
Make sure devices only accept system/firmware updates they can verify

Secure Key Store
Make sure sensitive keying material is stored in secure environment

Secure Execution
Make sure critical operations run in trusted execution environment

Secure Boot
Make sure only trusted software images can be executed

Security Lifecycle
Make sure to have pro-active security control of connected devices

Agile Cryptographic Foundation

For more information contact us

InfoSec Global | USA | Switzerland | Canada | www.infosecglobal.com