MTG

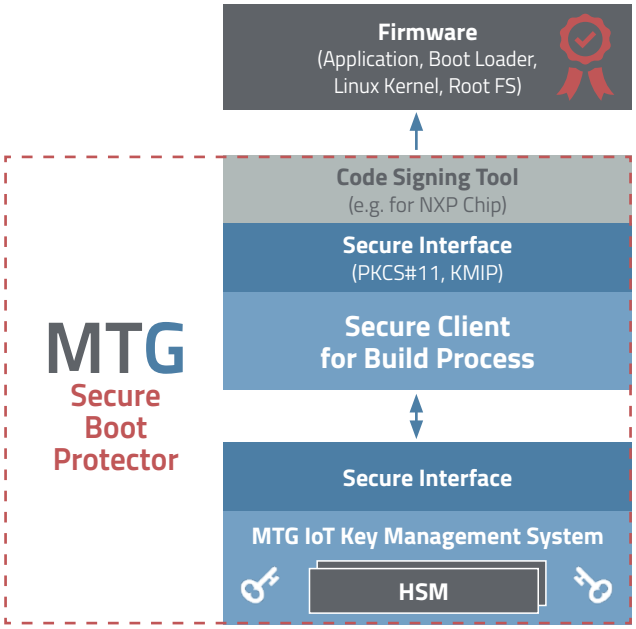
Enterprise Resource Security
Mastering Cryptographic Key Lifecycles

Foto: © MTG

MTG Secure Boot Protector

Secure Lifecycle Management of digital certificates & secret keys needed for the secure boot management process.

Manufacturers of embedded systems should ensure that their devices only start with original and unmodified firmware and that only authorized configuration files and updates can be used. The original software may run on counterfeit hardware or, vice versa, counterfeit or manipulated software may run on the original hardware. The challenge here is to protect the system in such a way that malicious code is detected by the secure boot mechanism and is not executed.



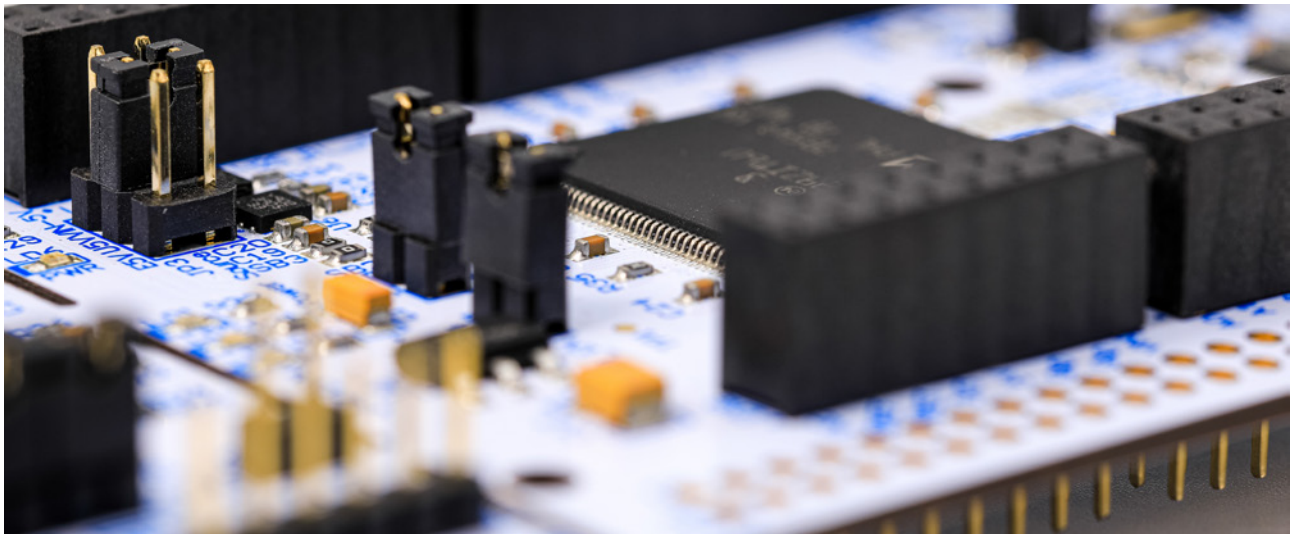
- All security related processes (Boot Loader, Linux Kernel and Root FS) will be protected by a digital signature
- MTG supports customers in IT security questions

- Signing tools which are supplied by Chip manufacturers will be integrated in the process
- MTG´s Secure Client manages the build process and is connected to the MTG Key Storage via standard interfaces

- Private Keys are securely generated & stored
- HSM integration to protect cryptographic keys in a highly secure way against possible attacks

MTG Secure Boot Protector

Manage all crypto operations for a secure boot process



MTG Secure Boot Protector

MTG Secure Boot Protector is responsible for all crypto operations (encryption, signing, key generation ...), which are needed for secure boot, configuration and update of embedded systems. It covers all needed elements to fully protect the firmware:

> Boot process
> Update process
> Protection of secret keys
> Protection of bootloader and operating system
> Encryption of the executed code
(e. g., bootloader or Linux Kernel)

Easy Integration with MTG IoT Key Management System

The Integration of all necessary processes is very simple thanks to the MTG IoT Key Management system. This also avoids complex configuration tasks when using hardware security modules. The solution can be shared centrally for different embedded devices using different chip manufacturers. This simplifies reliably the management of all necessary processes. The integration of a PKI for the variable generation of X.509 certificates is possible. Different CA hierarchies (Root CA, Sub CA) and signature algorithms are supported.

MTG Secure Boot Protector enables the secure life cycle management of digital certificates and secret keys needed for the secure boot management process

MTG AG is a leading specialist for sophisticated encryption technologies „Made in Germany". We simplify and centralize the management of cryptographic keys and identities throughout the complete key management lifecycle.

MTG AG · Dolivostraße 11 · 64293 Darmstadt · Germany
Tel +49 6151 8000-0 · contact@mtg.de

mtg.de