MTG

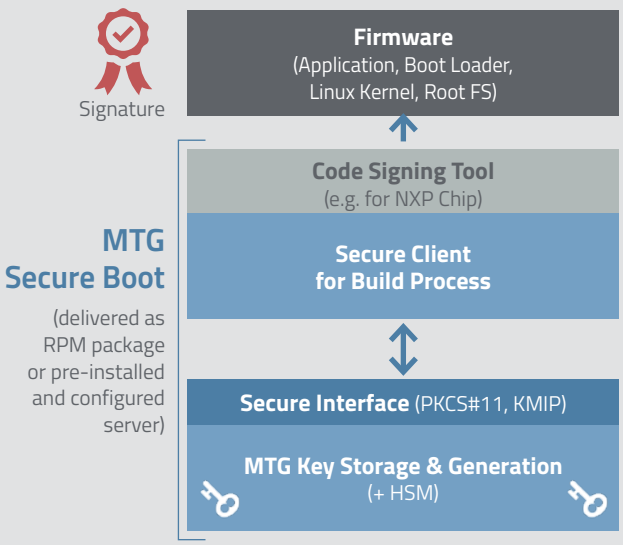
IT Security for Critical Infrastructures
Security Made in Germany

MTG Secure Boot

MTG Secure Boot is responsible for all crypto operations (encryption, signing, key generation ...), which are needed for secure boot, configuration and update of embedded systems.

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 required key material must be stored in a highly protected environment and only authorized users should have access to it. If this is not implemented consistently and end-to-end, there is a high risk of manipulation and misuse. The original software may run on faked hardware or, vice versa, faked or manipulated software may run on the original hardware.

MTG Secure Boot Process for Embedded Systems



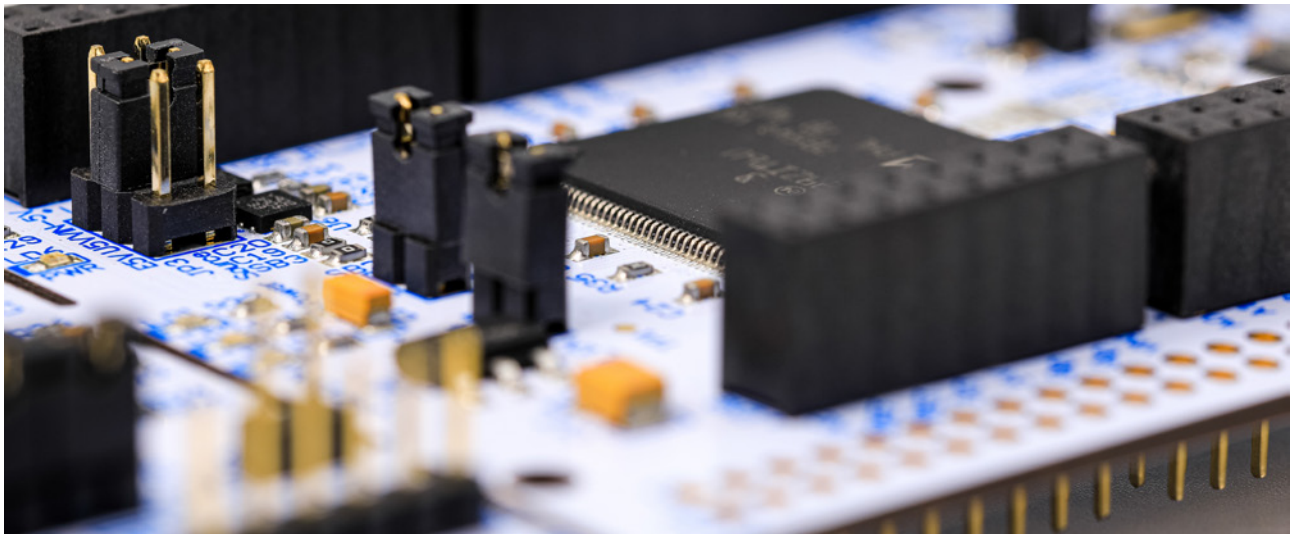
- All security related processes (Boot Loader, Linux Kernel and Root FS) will be protected by a digital signature
- MTG supports customers in IT security questions

- 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

Manage all crypto operations for a secure boot process



Booting of devices – a critical process

When an embedded device boots, it executes programs that are stored in its memory. If the code is not legitimate or incorrect this device will malfunction or endanger the infrastructure in which it is located. Therefore, booting of the device is a critical operation and needs to be secured to ensure that a device executes only legitimate software. During production the firmware needs to be protected by signature with private keys. This makes sure, that only the original firmware of the product is used.

MTG Secure Boot

MTG Secure Boot is responsible for all crypto operations (encryption, signing, key generation ...), which are needed for secure boot, configuration and update of embedded systems. The initial boot process will be secured with the customer encryption key. All required symmetric and asymmetric keys are securely protected in the MTG Key Storage respectively HSM.

Easy Integration

MTG Secure Boot is delivered as RPM package or on request on a pre-installed and configured server with a compatible HSM. It can be quickly and easily put into operation at a central and secure location. The connection of the development and production environment can be implemented very flexibly. Code signing tools of the chip manufacturers (e.g. NXP) are integrated into the system according to customer requirements. MTG provides support for all IT security relevant questions regarding the configuration of the firmware. The optional Hardware Security Modules are pre-configured and provided on a fail-safe basis.

Manufacturers of embedded systems should ensure that their devices only start with original and unmodified firmware

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

MANAGEMENTSYSTEM TÜV SAARLAND ISO 27001

MTG is a leading specialist for sophisticated encryption technologies in Germany. Our innovative IT security solutions effectively secure critical infrastructures and the Internet of Things.

MTG

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

mtg.de