# ProMik realizes customer-specific cyber security project

Branche: Automotive
Anwendung: High-tech camera

## ProMik as cyber security partner

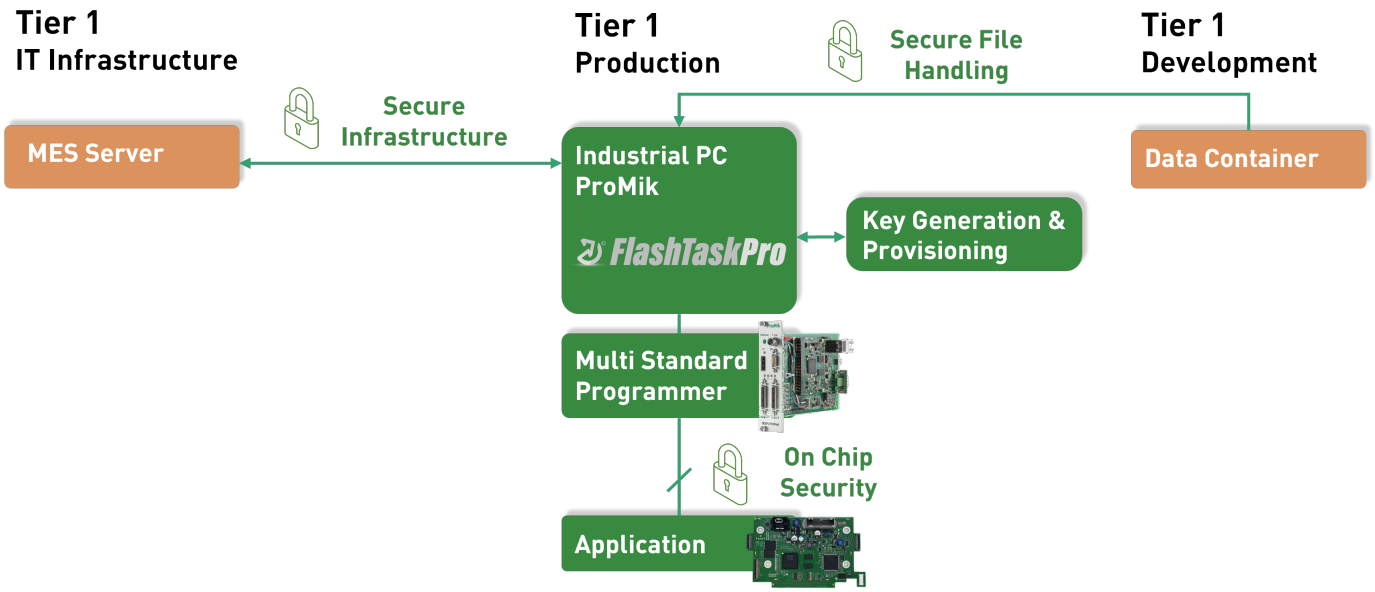
ProMik stands out from other suppliers when it comes to implementing cyber security requirements. Instead of providing only the firmware implementation of cyber security, ProMik offers full support - From initial production concepts to project execution and ramp-up. ProMik demonstrated this service portfolio once again in a new cyber security project by fulfilling all technical conditions. In this case a distinction is made between application and IT data structure requirements.

## The difference in production

- Consulting and implemenation of customer-specific cyber security requirements
- Secure OEM back-end connection via encrypted communication
- Encryption and decryption of the application software via MES, programmer and bootloader
- Hardware for cyber security relevant applicationn
- Mastering encryption methods like PGP,AES,RSA and „Elliptic Curve Algorithmen"
- Device re-programming with active security functions via feldbus interfaces e.g. software updates

## IT-data structure requirements

The IT-Data structure was predefined as following:




## Advantages

- Less interfaces → faster solution
- More fail-safe
- One-stop solution including project-based adaption

# ProMik realizes customer-specific cyber security project

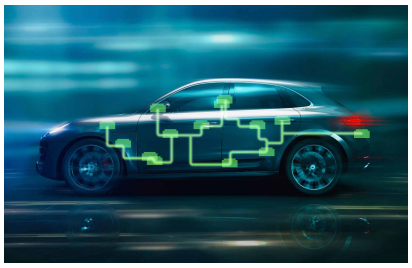
Branche: Automotive
Anwendung: Hightech-Kamera

## Applicative requirements

### Bootloader development and flashing of the HSM-firmware

Within the project, a special ProMik bootloader was first developed. It is responsible for flashing the hardware security module (HSM) firmware. The HSM firmware realizes a special software application that runs on the HSM core. Only this allows modifications to be made to the HSM. This guarantees additional protection. As a customer requirement, the HSM firmware of an external supplier was flashed. Since ProMik is able to work with any firmware provider, the customer is given freedom in choosing the HSM firmware.
In the first step of the flash process, the bootloader was downloaded into the microcontroller's (MCU) RAM. Then the bootloader initialized the HSM firmware and started the HSM core. Finally, the remaining areas of the MCU were flashed.

### Application-Programming-Interface (API)



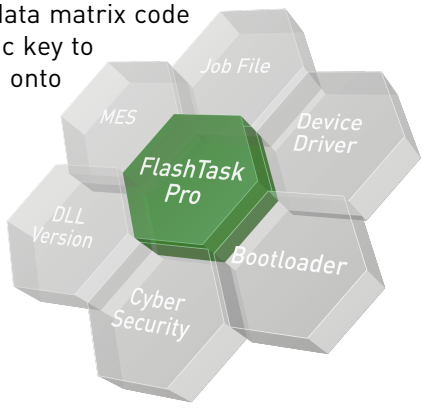
In addition to programming the HSM firmware, the API was implemented, which is responsible for firmware updates. After the first flashing of the HSM firmware, the HSM can no longer be updated externally. This can only be done by firmware updates via the API.
On the other hand, the API is used when writing keys: The HSM firmware API allows to generate public keys, which encrypt data. This encrypted data can be transferred to the HSM via the API. Since the HSM acts independently of other modules of the MCU, it can be used to generate private keys that are accessible only to the HSM. These private keys are used to decrypt the shared public keys of the API.

### Firmware-Signing

For the signing of the firmware, certificates were generated beforehand. ProMik ensured that these could be validated during the flash process.

### Generating the Crypto Keys

The generation of Crypto Keys was done using one of the encryption methods supported by ProMik on the flash station itself. Such methods can be PGP or SHA-2 encrypted. The Private Keys were then written to a flash area on the HSM module. In turn, the Public Keys can be stored in any location such as decentralized (IT infrastructure) databases.
he public key of the HSM firmware API was then requested using ProMik's FlashTask Pro. This was then transmitted to the central database via the Manufacturing Execution System (MES), together with the data matrix code (DMC) of the ECU. From this, a long-term database was created that assigns a public key to each DMC of the assemblies. This is done in case encrypted data needs to be loaded onto the microcontroller in manufacturing or in the field.




## ProMik provides holistic support in the area of cyber security:

Both on-chip cyber security functions are realized and communication and interaction with the IT data structures are enabled. The advantages of ProMik's cyber security include higher fail-safety, the project-based one-stop solution as well as less required interfaces and thus a secure solution.

For more information visit our website