ProMik realisiert kundenspezifisches Cyber Security Projekt

Branche: Automotive
Anwendung: Hightech-Kamera

ProMik als Cyber Security Partner

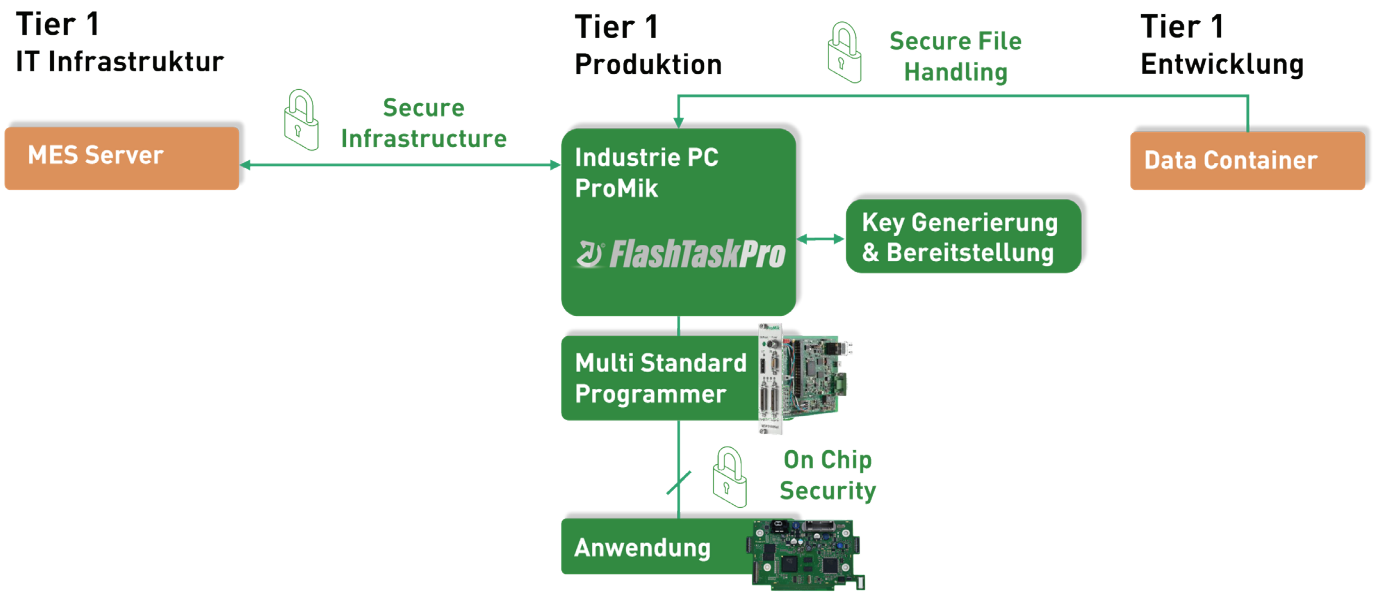
ProMik hebt sich von anderen Anbietern bei der Umsetzung von Cyber Security Anforderungen ab. Denn statt ausschließlich die Firmware Implementierung der Cyber Security bereitzustellen, bietet ProMik einen vollumfänglichen Support – Von ersten Produktionskonzepten über die Projektabwicklung bis hin zum Ramp-Up. Dieses Leistungsportfolio bestätigte ProMik zum wiederholten Mal in einem neuen Cyber-Security-Projekt, indem alle technischen Bedingungen erfüllt wurden. Hierbei wird zwischen applikativen - sowie IT-Datenstruktur-Voraussetzungen unterschieden.

Der Unterschied in der Produktion

- Beratung & Umsetzung kundenspezifischer Cyber Security Anforderungen in der Produktion
- Sichere OEM Backend-Anbindung mittels verschlüsselter Kommunikation
- Ver- & Entschlüsselung der Applikationssoftware via MES, Programmer und Bootloader
- Hardware für Cyber Security relevant Anwendungen
- Realisierung verschiedener Verschlüsselungsverfahren wie z.B. PGP, AES, RSA und „Elliptic Curve Algorithmen“
- Reprogrammierung von Bauteilen mit aktiven Security Funktionen z.B. Software Updates via Feldbus Schnittstellen

Voraussetzungen der IT-Datenstruktur

Die IT-Datenstruktur des Projekts war wie folgt gegeben:



Vorteile:

- Weniger Schnittstellen → schnellere Lösung
- Höhere Ausfallsicherheit
- Lösung aus einer Hand mit projektbezogenen Anpassungen

ProMik realisiert kundenspezifisches Cyber Security Projekt

Branche: Automotive
Anwendung: Hightech-Kamera

Applikative Voraussetzungen

Bootloader-Entwicklung und Flashen der HSM-Firmware

Innerhalb des Projekts wurde zunächst ein spezieller ProMik Bootloader entwickelt. Dieser ist für das Flashen der Hardware-Security-Module- (HSM) Firmware zuständig.
Die HSM-Firmware realisiert eine spezielle Softwareanwendung, welche auf dem HSM-Kern läuft. Nur diese erlaubt es, Modifizierungen auf der HSM vorzunehmen. Dadurch wird zusätzlicher Schutz garantiert. Als Kundenanforderung wurde die HSM-Firmware eines externen Anbieters geflasht. Da ProMik in der Lage ist, mit beliebigen Firmware-Anbietern zusammenzuarbeiten, sind dem Kunden Freiheiten bei der Wahl der HSM-Firmware gegeben.
Im ersten Schritt des Flash-Prozesses wurde der Bootloader in den RAM des Microcontrollers (MCU) heruntergeladen. Anschließend initialisierte der Bootloader die HSM-Firmware und startete den HSM-Kern. Zuletzt wurden die restlichen Bereiche der MCU geflasht.

Aplication-Programming-Interface (API)

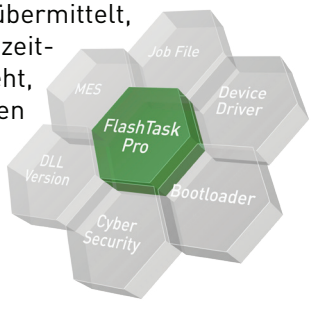
Zusätzlich zur Programmierung der HSM-Firmware erfolgte die Implementierung der API, welches zum einen zuständig für Firmwareupdates ist. Denn nach dem erstmaligen Flashen der HSM-Firmware kann die HSM nicht mehr extern aktualisiert werden. Dies kann nur noch durch Firmwareupdates via der API erfolgen.
Zum anderen wird das API beim Schreiben von Keys genutzt: Die HSM-Firmware-API ermöglicht das Generieren von Public Keys, wordurch Daten verschlüsselt werden. Diese verschlüsselten Daten können mittels der API in die HSM transferiert werden. Da die HSM unabhängig von anderen Modulen der MCU agiert, kann sie dafür verwendet werden, Private Keys zu generieren, welche allein für die HSM zugänglich sind. Diese Private Keys dienen dazu, die geteilten Public Keys ders API zu entschlüsseln.

Firmware-Signing

Für das Signing der Firmware, wurden zuvor Zertifikate generiert. Hierbei stellte ProMik sicher, dass diese während des Flash-Prozesses validiert werden können.

Generieren der Crypto Keys

Das Generieren der Crypto Keys erfolgte mittels einer der von ProMik unterstützten Verschlüsselungsmethoden auf der Flashstation selbst. Solche können beispielsweise PGP oder SHA-2 verschlüsselt sein. Im Anschluss wurden die Private Keys in einem Flash-Bereich auf dem HSM-Modul geschrieben. Die Public Keys können wiederum an beliebigen Orten wie zum Beispiel in dezentralen (IT-Infrastruktur) Datenbanken gespeichert werden.
Anschließend wurde mittels der FlashTask Pro von ProMik der Public Key des HSM-Firmware-APIs angefordert. Dieser wurde daraufhin zur zentralen Datenbank via das Manufacturing-Execution-System (MES) übermittelt, zusammen mit dem Data-Matrix-Code (DMC) des Steuergerätes. Daraus wurde eine Langzeit-Datenbank gebildet, die jedem DMC der Baugruppen einen Public Key zuordnet. Dies geschieht, falls in der Fertigung oder im Feld verschlüsselte Daten auf den Microcontroller geladen werden müssen



ProMik unterstützt im Bereich der Cyber Security ganzheitlich:

Es werden sowohl On-Chip Cyber Security Funktionen realisiert, als auch die Kommunikation und Interaktion mit der IT-Datenstrukturen ermöglicht. Die Vorteile von ProMiks Cyber Security umfassen eine höhere Ausfallsicherheit, die projektbasierte One Stop-Solution sowie weniger benötigte Schnittstellen und somit eine sichere Lösung.

Für mehr Informationen besuchen Sie unsere Webseite