ProMik®
Trusted Solutions

hello, whitepaper

Cyber-Security in der Elektronikfertigung: Das ganzheitliche Konzept

Alles über Cyber-Security Lösungen, ProMiks detailliertes Leistungsspektrum, spannende Anwendungsbeispiele und vieles mehr!

Inhalt

Relevanz

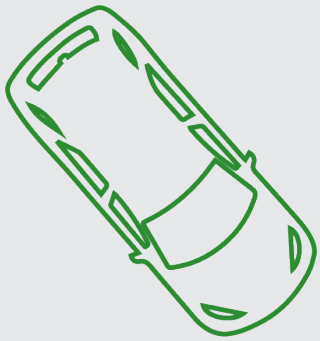
Stellen Sie sich vor – Sie sind mit Ihrem Auto auf dem Weg zur Arbeit. Musik läuft, während Sie beschleunigen. Plötzlich bläst Ihnen ein Wind entgegen. Die Klimaanlage hat sich auf frostige 16 Grad gestellt. Bevor Sie dies beheben können, schaltet sich Ihr Scheibenwischer ein und die Laustärke der Musik nimmt schlagartig zu. Sie wollen bremsen, doch anders als gewünscht gibt das Auto Gas. Ehe Sie realisieren, was passiert, geraten Sie von der Straße ab.

Ein solcher Vorfall hat sich 2015 ereignet, als Hacker Gaspedal, Bremse, Klimaanlage, Scheibenwischer sowie Radio eines Fahrzeugs manipulierten. Die Hacker wollten zu jener Zeit aufmerksam auf die Sicherheitslücken moderner Autos machen – mit Erfolg.

Damit demonstrieren sie die Relevanz von Cyber-Security in der Elektronikfertigung. Denn solche Eingriffe können verhindert werden, indem bereits während der Produktion in Sicherheitsmechanismen investiert wird. ProMik hat die erhöhten Anforderungen erkannt und die existierende Toolchain erweitert, um diesen gerecht zu werden.

Einsatzgebiete von Cyber-Security in der Elektronikfertigung

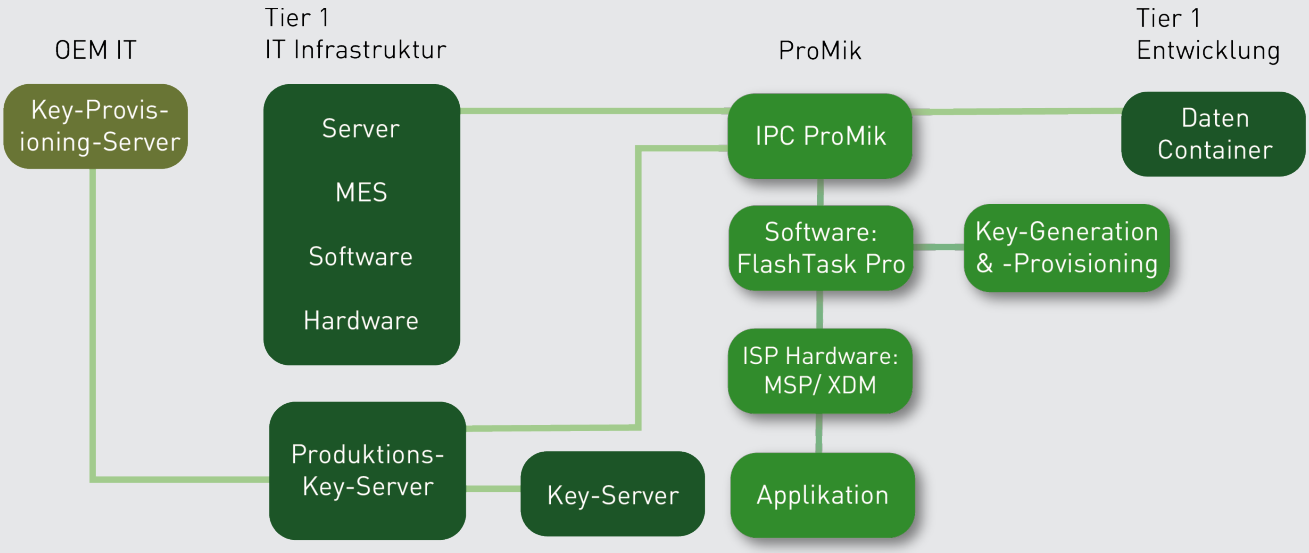
Im Automobil-Bereich gilt Cyber-Security in der Produktion bereits als wichtiger Standard. Denn durch die frühestmögliche Sicherung elektrischer Bauteile können Fahrzeugführer sowie weitere Verkehrsteilnehmer geschützt werden. Beispiele für Automotive-Applikationen sind Infotainment- und Batteriemanagement-Systeme, ADAS-Anwendungen und viele weitere.



MEHR LESEN

Jedoch auch in weiteren Bereichen gewinnt Cyber-Security in der Elektronikfertigung immer mehr an Bedeutung. Denn durch den wachsenden Technologieanteil, welcher zudem immer komplexer wird, wird auch die Angriffsfläche für Hacker größer. Branchen, welche aus diesem Grund ebenfalls zu ProMiks Fachbereichen zählen, sind unter anderem das IOT, Industrial und Konsumgüter.

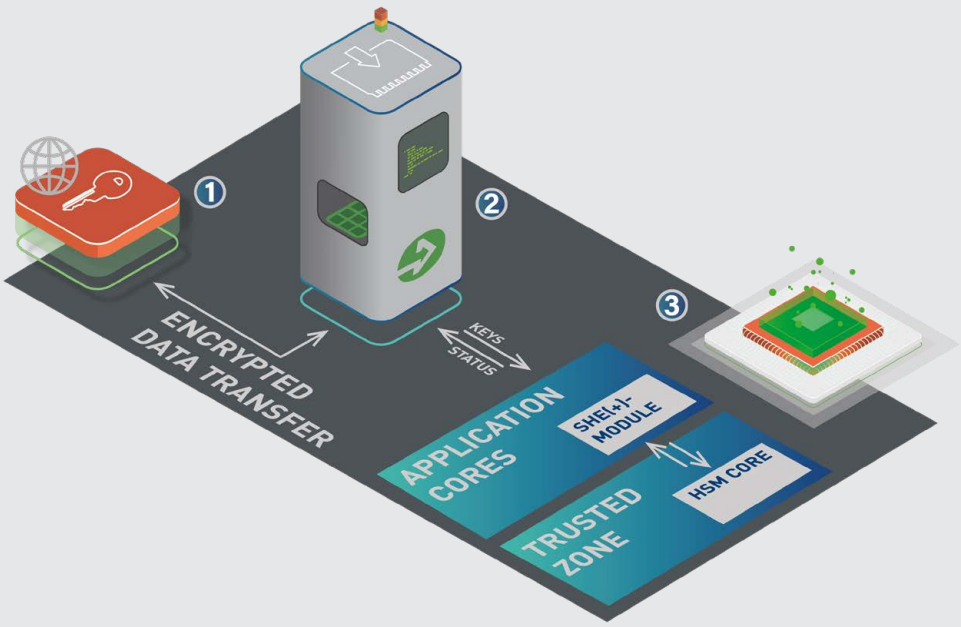
Cyber-Security-Infrastruktur



Die Cyber-Security-Infrastruktur von ProMik, Tier1 und OEM.

MEHR LESEN

On-Chip Cyber-Security



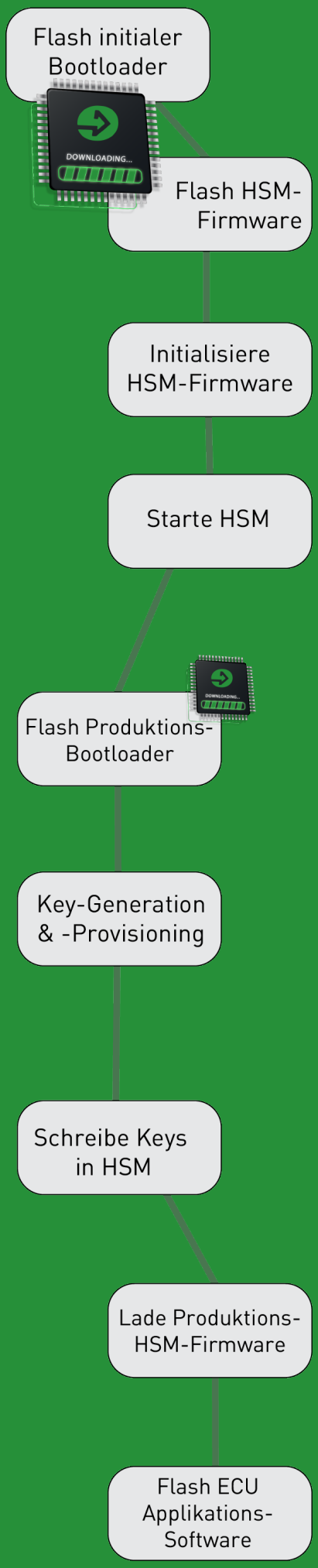
1. Key-Management-Server

2. Secure-Programming

3. On-Chip Cyber-Security

MEHR LESEN

Einordung der On-Chip Cyber-Security in den Produktionsprozess.



Die Schritte der On-Chip Cyber-Security.

Prozess

Zunächst wird der ProMik Bootloader entwickelt. Dieser führt die Flash-Programmierung der Firmware des Hardware-Security-Modules (HSM) aus, wodurch dieses initialisiert und gestartet wird.

Ein wichtiger Schritt in der On-Chip-Security stellt die Key-Generation und das Key-Provisioning dar. Die Key-Generation kann entweder durch ProMik oder durch den OEM erfolgen.

Anschließend werden die Keys mittels des ProMik Bootloaders in das HSM übertragen und dort abgespeichert. Dabei interagiert der Bootloader mit dem Secure-Hardware-Extension (SHE +) Module.

Während der gesamten Programmierung erfolgt ein Datenaustausch mit dem Manufacturing-Execution-System (MES). Dieses ist auch dafür verantwortlich, die Daten an die Electronic-Control-Unit (ECU)-Datenbank des OEMs zu übermitteln.

Nachdem die Programmierung durchgeführt wurde, wird die Vertrauenskette für den Secure-Boot konfiguriert. Das Steuergerät ist nun bereit für den Einsatz, um mit der Applikations-Software programmiert zu werden.

Mittels ProMiks Produktportfolio lassen sich alle Aufgaben der On-Chip-Security problemlos abdecken. Dazu gehört eine integrierte Spannungsversorgung, mit der sich die Applikation ganz einfach kontrollieren lässt.

Verschlüsselungsverfahren

Verschlüsselungsverfahren sind Methoden, um einen Klartext mithilfe kryptographischer Schlüssel in eine Zeichenfolge zu übersetzen. Man unterscheidet generell Public- und Private -Keys. Ersteres sind öffentliche Schlüssel, auf welche mehrere Parteien Zugriff haben. Private-Keys sind geheime Schlüssel, welche nur für einen Kommunikationspartner zugänglich sind.

MEHR LESEN

Bei Verschlüsselungsverfahren wird zwischen symmetrischen und asymmetrischen Methoden unterschieden. Symmetrische zeichnen sich dadurch aus, dass nur ein Private-Key für die Ver- und Entschlüsselung der Daten verwendet wird.
Bei Asymmetrischen Verfahren hingegen erzeugt jeder Kommunikationspartner ein eigenes Schlüsselpaar bestehend aus Public- und Private-Key.

Symmetrische Verschlüsselung

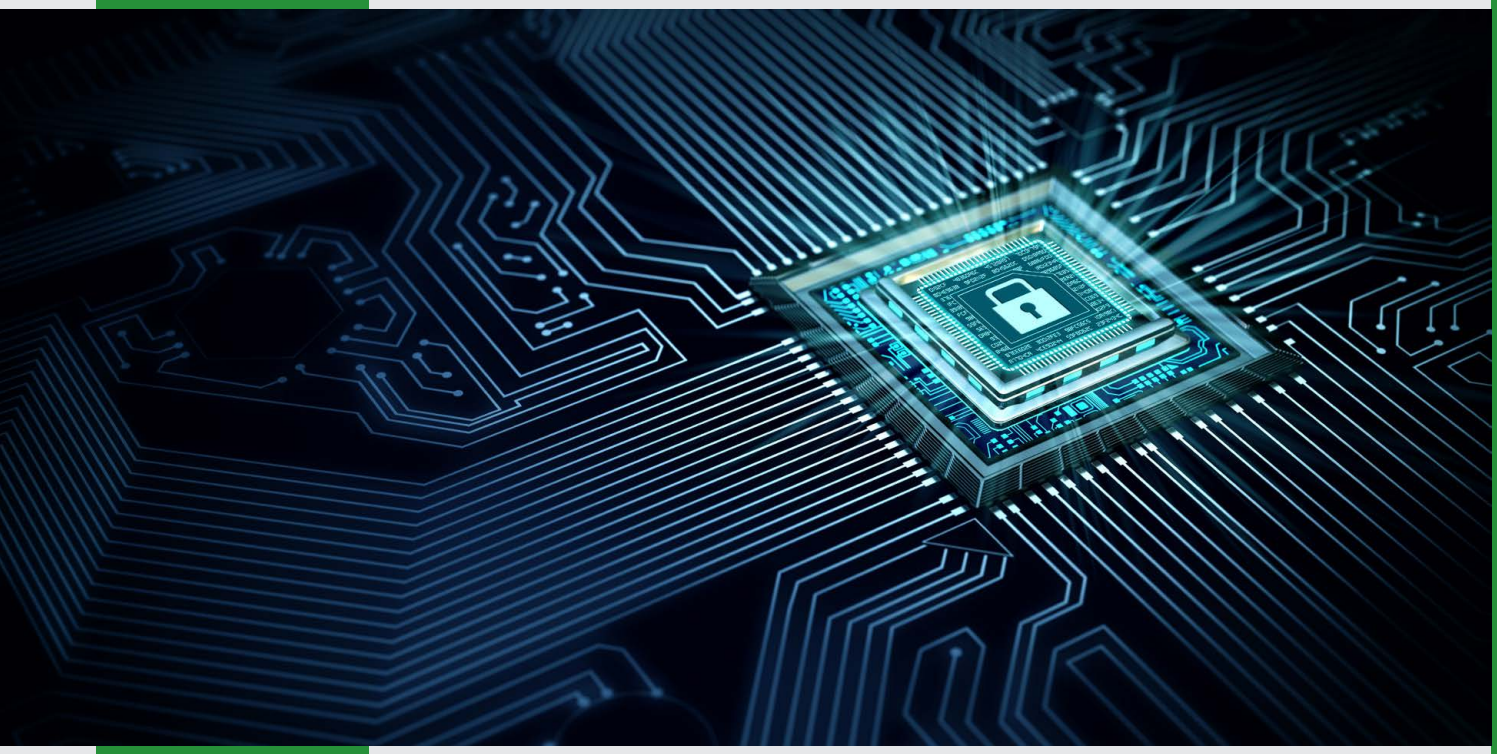
AES

Advanced-Encryption-Standard (AES) ist der Nachfolger des ebenfalls symmmetrischen Verschlüsselungsverfahrens Data-Encryption-Standard (DES). Es wird häufig für den verschlüsselten Datentransfer sowie bei Internet-Protocol-Security (IPsec) und Secure-Shell (SSH) verwendet.

Asymmetrische Verschlüsselung

ECC

Elliptic-Curve-Cryptography (ECC) verwendet Operationen auf elliptischen Kurven über endliche Körper. Da ECC als eine der effizientesten Methoden gilt, wird sie zumeist anderen asymmetrischen Verfahren vorgezogen.



RSA

RSA ist nach dem Erfinder Rivest Shamir Adleman benannt. Nach der Generierung der Schlüssel wird der Public-Key verschickt, mit welchem der Empfänger die Daten verschlüsseln kann. Der Public-Key ist alleinig zum Verschlüsseln zuständig, sodass er einzeln unbrauchbar ist. Die Daten können ausschließlich mit dem passenden Private-Key des Empfängers entschlüsselt werden.

Keys für die Cyber-Security

Key-Lifecycle-Management (KLM) beschreibt die Erstellung, die Pflege, den Schutz und das Löschen kryptographischer Schlüssel. Der Prozess ist in einzelne Aufgaben zu unterteilen.

Das Key-Lifecycle-Management

Die Relevanz des KLMs zeigt sich darin, dass Schlüssel mit der Zeit an Sicherheit verlieren. Das liegt daran, dass immer mehr Personen Zugriff auf die Keys haben, jedoch auch, da diese veraltet oder kompromittiert sein können. Aus diesem Grund müssen die Schlüssel regelmäßig ausgetauscht werden.

MEHR LESEN

Bei der Key-Generation werden die kryptographischen Schlüssel erzeugt sowie anschließend in die Produktionsumgebung übertragen (Key-Provisioning). Dort werden die Keys beispielsweise in die HSM oder SHE(+) abgespeichert (Key-Storage) und je nach Verschlüsselungsverfahren unterschiedlich genutzt (Key-Usage).
Das Generieren neuer Keys und Ersetzen ungültiger wird als Key-Rotation bezeichnet. Hierbei werden ungültige Schlüssel zunächst während Key-Revocation widerrufen und zuletzt gelöscht (Key-Destruction).

ProMik: Experte für Cyber-Security in der Elektronikfertigung

Seit mehr als 25 Jahren ist ProMik Flash- und Testexperte in der Mikroelektronik. Durch tiefgreifendes Knowhow und das homogene Produktportfolio können Kunden state-of-the-art Security-Mechanismen in ihre Produktion implementieren.

DATENBLATT

Die Absicherung von Steuergeräten in der Produktion bringt einige Herausforderungen mit sich. Hierbei unterstützt ProMik seine Kunden und setzt individuelle Anforderungen unter Berücksichtigung aktueller Cyber-Security-Standards wie beispielsweise ISO 21434 um. ProMik überzeugt mit einem ganzheitlichen Konzept: Von der Bestimmung des Sicherheitskonzepts bis hin zur Erstellung des Schutzkonzeptes in der Applikation.

Dadurch besitzt ProMik ein umfassendes Technologiewissen über Secure-Boot, Sicherheitsmodule, Key-Management und viele weitere Themen der Cyber-Security. Mit den Plug- & Play-Lösungen ist es zudem ganz einfach ProMiks Lösungen in die Produktion des Kunden zu implementieren.

CONTACT

Use Case: Cyber-Security Implementierung einer ADAS-Applikation

In einem innovativen Projekt unterstützte ProMik bei der Realisierung einer High-tech Kamera. Sowohl das Flashing, Testing als auch die Cyber-Security-Implementierung der Applikation wurden durchgeführt. Im Bereich der Cyber-Security überzeugte ProMik mit dem vollumfänglichen Leistungsportfolio. Dazu gehörte die Entwicklung eines speziellen Bootloaders, die Programmierung der HSM und vieles weiteres.

Der Unterschied in der Produktion

- Flashing, Testing und Cyber-Security aus einer Hand
- Verschlüsselungsverfahren wie z.B. RSA und ECC
- Hochperformante ProMik Bootloader

MEHR LESEN

Erfahren Sie mehr über Cyber-Security in der Elektronikfertigung

ProMik®
Trusted Solutions