ProMik
Trusted Solutions

ProMik

Cyber Security

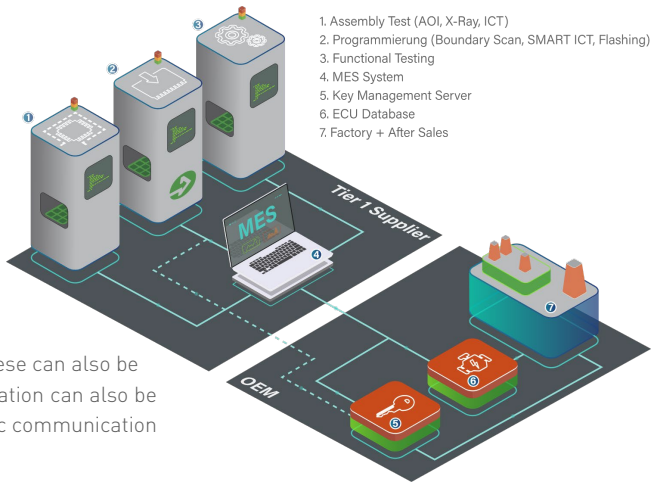
for Electronics Manufacturing

Cyber Security

Overview

The interface for transferring production and security data from the OEM to the production facility of Tier 1 is in many cases represented by a manufacturing execution system (4). Via this communication path, ECU-specific data can be transferred to the corresponding database at the OEM (6), as well as security-relevant data, for example, from a key management system (5).

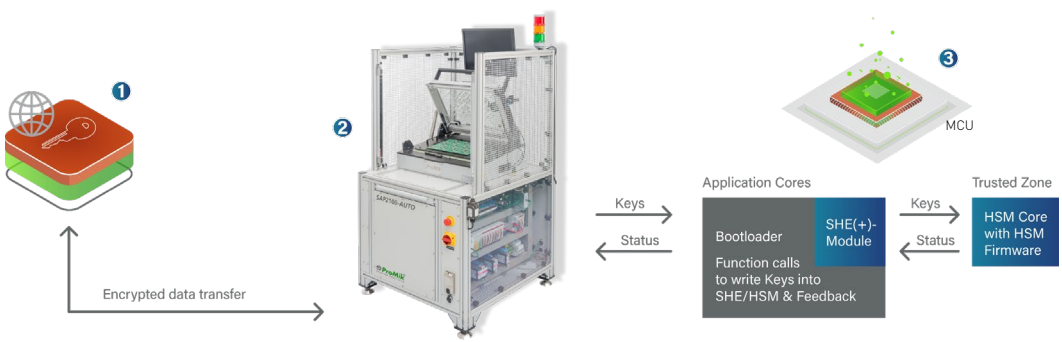
If key provisioning, i.e. the generation of keys, takes place at the Tier1, these can also be transferred to the back-end of the OEM. Alternatively, the security information can also be transferred directly, without an intermediate MES, using the OEM-specific communication interface.



Key Features

- Consulting & implementation of customer-specific cyber security requirements
- Secure OEM back-end connection via encrypted communication
- Encryption & decryption of the application software via MES, programmer and bootloader
- Mastering encryption methods like PGP, AES, RSA and „Elliptic Curve Algorithm"
- Software and programming hardware for cyber security relevant applications
- Device reprogramming with active security functions via fieldbus interfaces e.g. for software updates

Secure ECU production process



1. Key management server

- OEM ECU Data Base
- Key Provisioning Server
- MES

2. Programming of security relevant data

- Secure File Handling
- Encryption/Decryption
- Key Provisioning on Flash Station
- Seed & Key
- Cryptographic Support for: PGP, AES, ...

3. On-chip security feature

- HSM/SHE(+)
  - HSM Firmware Programming
  - Key Programming
  - Firmware Update
- Debug Interface Lock
- Flash Protection
- Secure Boot Activation
- Support Custom HSM Firmware (e.g Elektrobit, Vector, ...)