Complete HSE/ HSM Activation Process through ProMik

Bootloader as well as HSM Programming, including Secure Generation and Provisioning of Cryptographic Keys

ProMik
Trusted Solutions

ProMik
Programmiersysteme für die
Mikroelektronik GmbH
Südwestpark 100
90449 Nuremberg, Germany

Phone: +49 (0) 911-25 26 65-0
Fax: +49 (0) 911-25 26 65-66
Email: info@promik.com
www.promik.com

Certified according to:
- ISO 9001
- ISO 14001

Cyber security for the production of modern applications is becoming an increasingly relevant topic. In order to be protected reliably against cyber attacks, not only the IT infrastructure including communication and storage of keys must be secure, but also the electronic control units (ECUs) specifically. Today's microcontrollers (MCUs) and system-on-chips (SoCs) obtain hardware security modules (HSMs) with dedicated firmware. These represent a trust zone on the device on which data can be securely stored and retrieved. The activation process of these HSMs is a critical process that requires professional know-how. ProMik enables the activation process through many years of industry experience and guarantees the highest level of cyber security for your production.

First, a bootloader and the initial HSM firmware are installed and then activated by the user configuration block (UCB). After the HSM has been restarted, the ProMik bootloader is able to access the HSM firmware via the SHE (+) interface. The HSM is initialized, and the unique identifier (UID) is read, which is required for generating keys. It is then necessary to update the HSM firmware. This requires both the HSM profile and the signed HSM firmware. Finally, this is deactivated via the UCB.

The figure on the right shows the entire HSM activation process. The process can also be divided into several steps and multiple stations. In this case, a first HSM activation sequence takes place on the needle bed and a second end-of-line. This has the advantage of being able to check the compatibility of the device with the hardware requirements in the meantime.

ProMik enables customers to handle the entire HSM or HSE activation process and implements any OEM requirements. Benefit from in-depth expertise and other services in the field of cyber security and implement your customer-specific project.

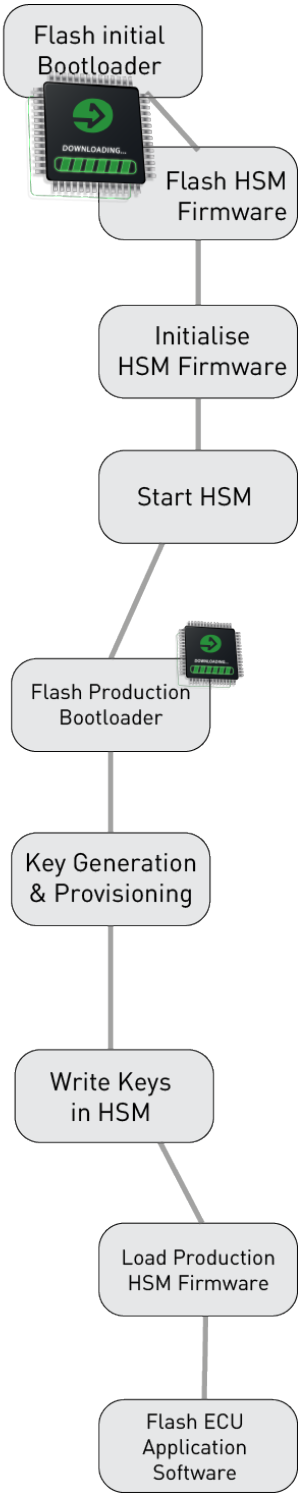

FIGURE 1: HSM ACTIVATION PROCESS