

SEAL BOX SECURE PROVISIONING IN MANUFACTURING

Currently enforced by major standards (Matter, EV-charging, US Cyber Trust Mark...) Digital Identity Provisioning is an essential first step in production to ensure security throughout the device lifecycle



Secure

- Secure and simplify the personalization process
- Remove room for human errors
- Ensure trust in the manufacturing operations



Cost Effective

- Aggregate various data from different sources at same step.
- Shorten manufacturing time cycle



Automate & Scale

- Fully automate the personalization and provisioning operation
- Fit with volume increase in production



Flexible

- Can be used with any device or chipset
- Easily integrated with most of programming equipment and test bench

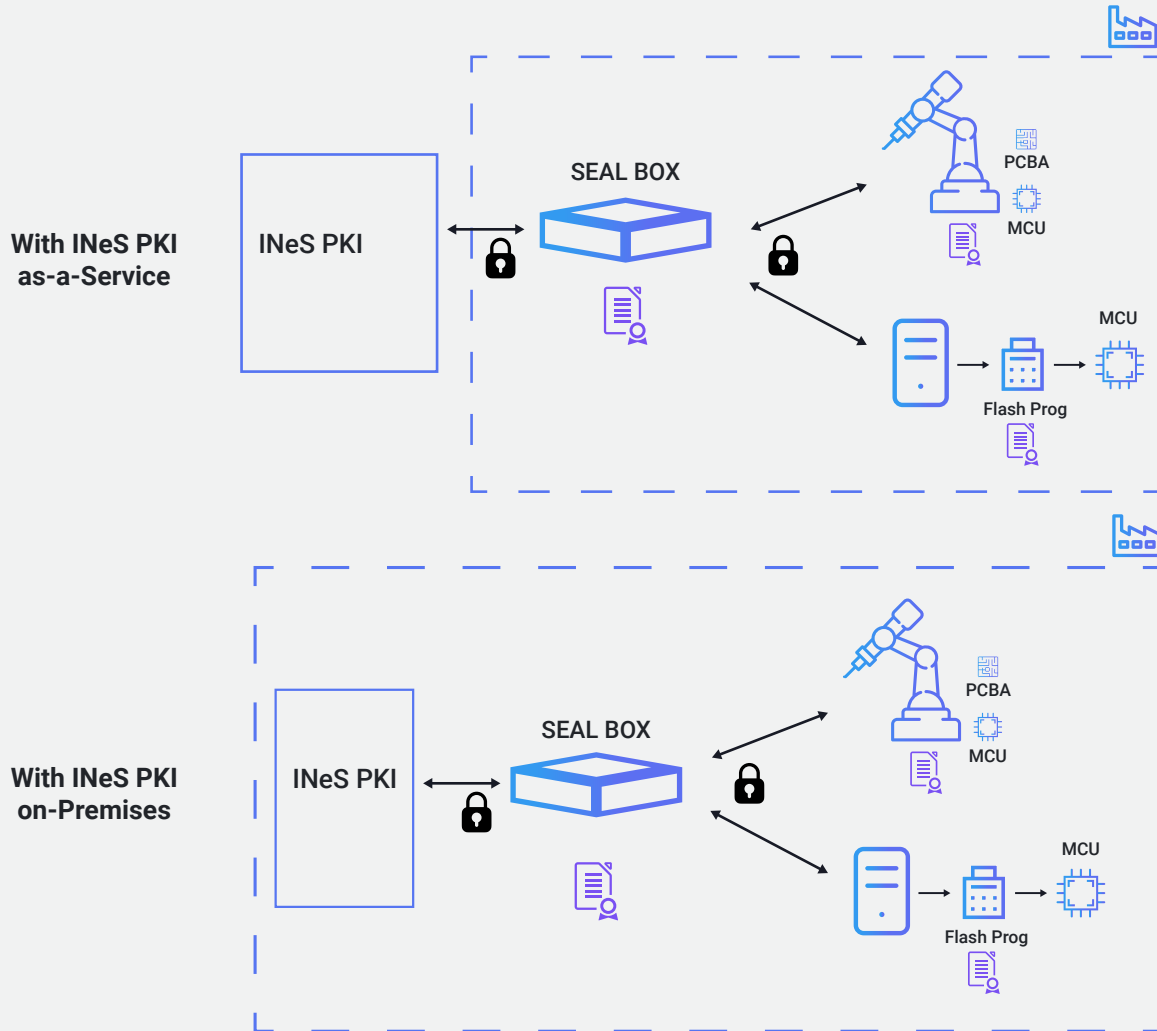


Product Services

- Generate and inject unique data per device (Private key, Certificate, Serial number, MAC address...)
- Generate and inject common data per device (firmware, common configuration parameters...)
- Generate random data
- Provision data from input file
- Concatenate various data from different sources and generate unique data for personalization
- Encrypt data before programming
- Secure storage in the programming facility
- Overproduction control: signed whitelist and blacklist, signed batch report
- Commissioning of the application server

Digital Identities Provisioning in Production

- Address identities provisioning needs of manufacturers and integrators (OEM, ODM, EMS...) for connected devices.
- Target connected devices based on programmable components (MPU, MCU, FPGA...).



Programmer Interfaces

Option to interface with various programmers for instance ESP-prog, STM32



SEALBOX

Secure computer :

- Portable industrial computer
- 256 GB SSD
- TPM 2.0 / HSM
- Secure OS and SW update
- Secure connection to the device programmer
- Application server with User interface (UI)
- Credits for a preset number of certificate provisioning
- Technical support for installation
- Full set of documentation