MCUXpresso Secure Provisioning Tool

MCUXPRESSO-SECURE-PROVISIONING

Last Updated: Apr 24, 2024

The MCUXpresso Secure Provisioning Tool is a GUI-based application provided to simplify generation and provisioning of bootable executables on NXP MCU devices.

The graphical interface provides a streamlined development flow, making it simpler to prepare, flash and fuse images while leveraging and providing access to existing utilities. Advanced scripting can be achieved using the command-line interface, while even more advanced secure provisioning flows can be accomplished by modifying scripts generated by the tool.

The latest releases of the Secure Provisioning Tool leverage low-level functionality based on the open-source Secure Provisioning SDK. The Secure Provisioning SDK (SPSDK) provides a unified software library replacing many of the existing security utilities to provide a solid feature-rich security foundation across the full range of supported devices. Additionally, the Secure Provisioning SDK is available in source form for the development of fully customized provisioning workflows. Full API documentation is available at the following link.

Smart Card Trust Provisioning and Device HSM Trust Provisioning are new security enablement of the MCUXpresso Secure Provisioning Tool for device provisioning and software IP protection.
MCUXpresso Secure Provisioning Tool Block Diagram

- Secure Provisioning Tool—Graphical Interface
- Secure Provisioning Tool—Command-Line Interface
- Secure Provisioning SDK
  - Trust Provisioning
  - Protected Flash Region
  - Crypto (Keys and Certificates)
  - Master Boot Image
  - Secure Binary File
  - Debug Authentication
  - MCU Bootloader Protocol
  - Serial Downloader Protocol
  - Debugger (Debug Mailbox)
- Microcontroller Hardware (via USB/UART)

View additional information for MCUXpresso Secure Provisioning Tool.

Note: The information on this document is subject to change without notice.