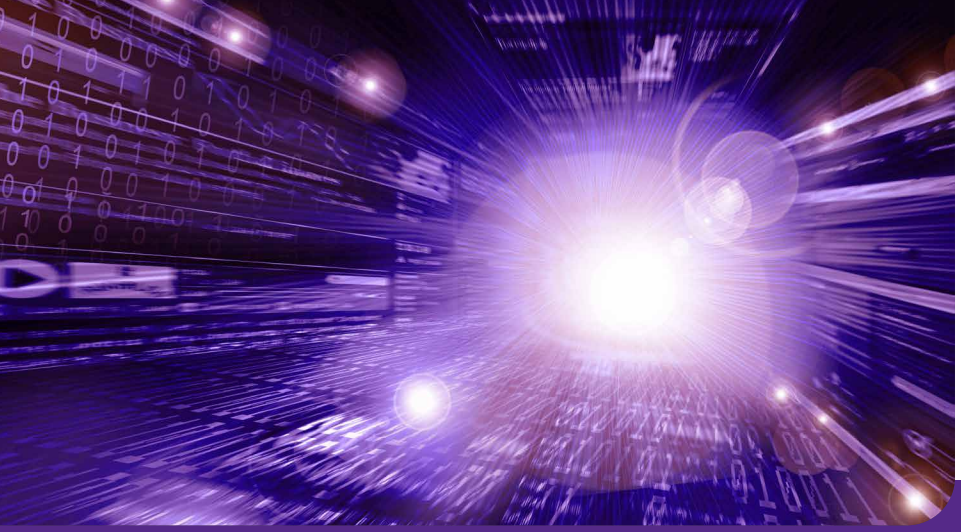


Secure provisioning for general-purpose NXP® microcontrollers

MCUXpresso Secure Provisioning Tool (SEC)

The MCUXpresso Secure Provisioning tool is a programming and secure provisioning tool for certificate and key management, secure image preparation and device provisioning and programming.

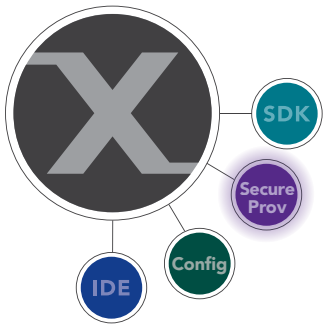
MCUXpresso SECURE PROVISIONING TOOL

NXP created the MCUXpresso SEC, a GUI-based application, to help simplify the generation and provisioning of bootable executables on NXP MCU devices. It is built upon existing security enablement utilities and takes advantage of the breadth of programming interfaces provided by the BootROM available for security-focused devices. The graphical interface provides an intuitive image preparation flow, making it simple to prepare and flash secure applications and program fuses and OTP memory, while leveraging and providing access to existing utilities (sdphost, blhost, elftosb, cst/srktool).

Users can achieve advanced scripting by using the command-line interface. They can customize even more advanced secure provisioning flows by modifying scripts the tool generated.

The MCUXpresso SEC provides:

- Support for i.MX RT crossover MCUs and LPC5500 MCUs based on Arm® Cortex®-M33 cores
- Support for target connectivity via UART and USB-HID serial download modes
- Support for multiple user application image formats (ELF/SREC/binary)
- Automated conversion of bare images to bootable images
- Downloading a bootable image in the target boot device
- Customization of the boot device either via GUI, or predefined flash configuration blocks
- Optional inclusion of device configuration data (DCD) per specific device and application initialization needs
- Generation of certificate trees for image signing and encryption
- Importing of existing user-supplied certificates
- Generation of signed and optionally encrypted executables
- Support for development (unsigned) boot mode
- Support for authenticated (signed) and encrypted boot modes
- Key provisioning and fusing as dictated by boot mode
- Command line interface for customized boot flows
- Additional command-line utilities for low-level interaction with the device



MCUXpresso

The MCUXpresso secure provisioning tool is part of the cohesive suite of MCUXpresso software and tools and is inherently compatible with the MCUXpresso software development kit (SDK), the MCUXpresso config tools, and the MCUXpresso IDE.

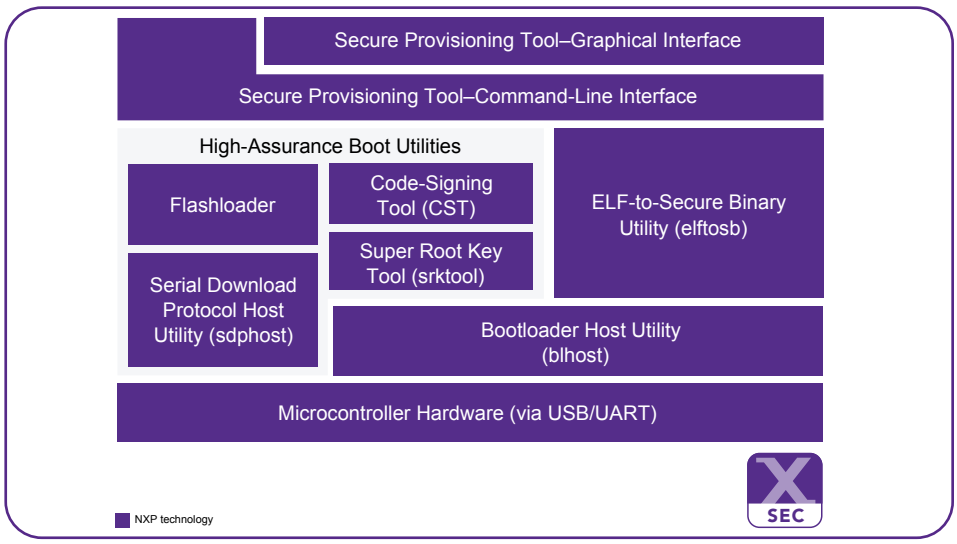
FUNDAMENTAL PROVISIONING UTILITIES

- MCU Bootloader Host Application (blhost)
  - The blhost application is used on a host computer to issue commands to an NXP platform running an implementation of the MCU bootloader. The blhost application, in conjunction with the MCU bootloader, allows a user to program a firmware application onto the MCU device without a programming tool.
- ELF to Secure Binary Conversion Tool (elftosb)
  - The elftosb tool creates a binary output file that contains the user's application image along with a series of bootloader commands.

HAB-SPECIFIC UTILITIES (required for i.MX RT MCUs)

- Serial Download Protocol Host Application (sdphost)
  - The sdphost tool provides a command line interface to send serial download protocol commands to NXP's i.MX RT devices enumerated on the host PC via USB-HID or UART interfaces.
- Code-Signing Tool (CST)
  - The CST implements the signing or encrypting of an embedded software application. For use with NXP MCUs supporting high-assurance boot (HAB), the CST can be used to ensure that only genuine or authenticated software is permitted to run on the end product.
- Super Root Key Tool (srktool)
  - The srktool is used to generate the super root key table and e-FUSE files derived from the corresponding certificates used with the CST.

MCUXpresso SECURE PROVISIONING TOOL BLOCK DIAGRAM



SEC FEATURES

- Graphical User Interface
  - Easy-to-use configuration of secure provisioning project settings
  - Enables direction communication with attached device for provisioning and programming
  - Supports generation of executable scripts for production use
- Command-Line Interface
  - Unified command-line interface to the underlying utilities that can be used to create custom provisioning and production processing
- Key/Certificate Management and Generation
  - Leverages OpenSSL or externally specified keys, signatures, and certificates
  - OpenSSL libraries are pre-bundled with Windows® and Mac installations for seamless installation
- Secure Image Preparation
  - Encrypting and signing of ELF (AXF) executables, SREC, and raw binaries
- Alignment with MCUXpresso Config Tools
  - Supports importing DCD and Arm TrustZone® configurations generated from the MCUXpresso Config Tools suite
- Device Provisioning and Programming
  - Programming of e-FUSEs and one-time-programmable flash regions
  - Direct connection to the target via UART, USB-HID for provisioning and programming
- Support for Windows 32/64-bit, Linux® 64-bit and MacOS

GET STARTED

Learn more:
www.nxp.com/mcuxpresso/secure

Join the MCUXpresso Secure Provisioning community:
https://community.nxp.com/community/mcuxpresso/mcuxpresso-secure-provisioning-tool

Professional Support and Services:
www.nxp.com/services

www.nxp.com/mcuxpresso/secure

Document Number: MCUXPRESSOSPFS REV 1