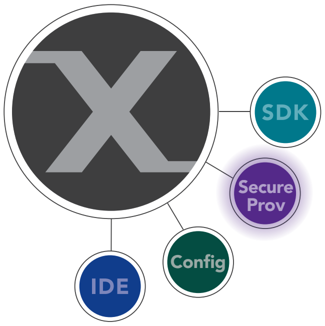
MCUXpresso Secure Provisioning Tool (SEC)

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. 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.

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 SPSDK is available in source form for the development of fully customized provisioning workflows.

Users can achieve advanced scripting by using the MCUXpresso SEC 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
- Device certificates harvesting
- 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 based on Secure Provisioning SDK application
- Manufacturing tool support with device provisioning and parallel programming support
- UI-based fuse programmer
- Production limit control
- Factory log for audit review

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.

Secure Provisioning SDK

The MCUXpresso Secure Provisioning Tool utilizes foundational security operations based on the Secure Provisioning SDK developed by NXP. This open-source python-based library is available on GitHub and includes a fully documented set of APIs and use case examples.

Precompiled command-line utilities developed with the Secure Provisioning SDK are provided as part of the MCUXpresso Secure Provisioning Tool installation. In addition to providing the underlying mechanisms of the Secure Provisioning Tool GUI, the Secure Provisioning SDK is available to advanced security users for development or prototyping of customized provisioning tools and workflows.

The Secure Provisioning SDK provides the following API modules:

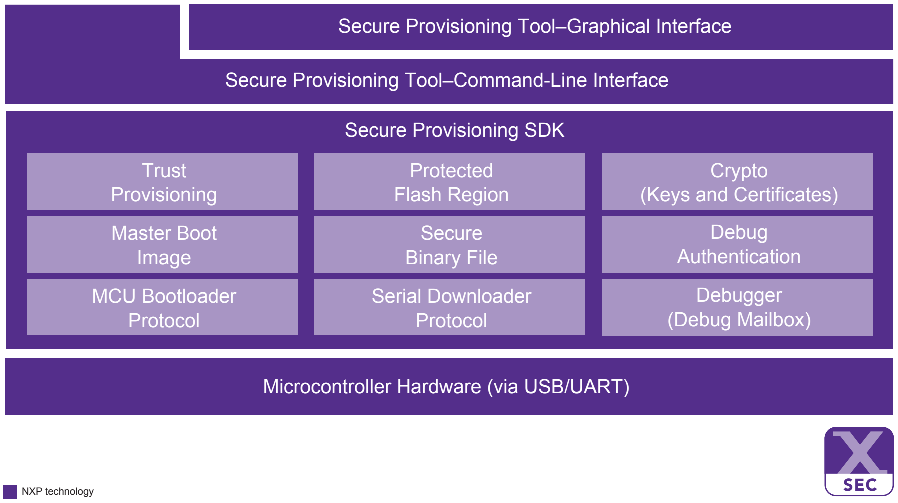
Trust Provisioning

- Production limit control
- Counterfeit device detection
- Secure device certificates generation and harvesting
- Factory audit log generation

Protected Flash Region

- APIs providing support for Protected Flash Region areas (CMPA, CFPA)

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)
NXP technology
X SEC

Crypto

- Generation and management of cryptographic keys and certificates

Master Boot Image

- APIs and utilities for mastering bootable image, including keystore, encryption, and trustzone

Secure Binary File

- APIs supporting the generation of a SB (Secure Binary) bootable files image
- Support provided for SBv2.0, SBv2.1, and SBv3.1

Debug Authentication

- Provides API for managing, provisioning, and responding to a securely authenticated debug path on supported devices leveraging a secure debug mailbox implementation

MCU Bootloader Protocol

- Provides communication APIs for interfacing with the target device
- Supported ROM based interfaces and supported Flashloader installations

Serial Downloader Protocol

- APIs for Serial Downloader Protocol used to install a Flashloader onto supported devices
- Supports UART and USB communication paths

Debugger

- Support for J-Link, PEmicro, and PyOCD debug probes

Get Started

Learn more:

www.nxp.com/mcuxpresso/secure

Join the MCUXpresso Secure Provisioning community:
https://community.nxp.com/t5/MCUXpresso-Secure-Provisioning/bd-p/mcux-secure-tool

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

www.nxp.com/mcuxpresso/secure