UG10241

Quick Start Guide for MCUXpresso Secure Provisioning Tool

Rev. 1 — 30 June 2025 User guide

Document information

Information	Content
Keywords	MCUXpresso Secure Provisioning Tool
Abstract	MCUXpresso Secure Provisioning Tool (SEC) is a GUI tool made to simplify the generation and provisioning of bootable executables on NXP MCU platforms. It is built upon the proven security enablement toolset provided by NXP and takes advantage of the breadth of programming interfaces provided by the BootROM library.

1 Overview

This Quick Start Guide provides a step-by-step overview to help you install, configure, and begin using the MCUXpresso Secure Provisioning Tool efficiently. Whether you are new to secure boot and encryption workflows or looking to integrate secure provisioning into your production process, this guide will help you get started quickly.

The MCUXpresso Secure Provisioning Tool (SEC tool) is a powerful utility developed by NXP to streamline the secure provisioning of embedded devices. Designed to support a wide range of NXP microcontrollers, this tool enables developers to configure security features, generate cryptographic keys, and securely program devices with minimal setup.

2 Hardware requirements

- It is recommended to start with the reference design board (FRDM/EVK) from NXP.
- Detailed requirements to start the MCUXpresso Secure Provisioning Tool are listed in MCUXpresso Secure Provisioning Tool Release Notes.

3 Software requirements

MCUXpresso Secure Provisioning Tool can be executed on Windows, Linux, or MacOS. The detailed requirements are listed in the MCUXpresso Secure Provisioning Tool Release Notes.

4 Installing and configuring the SEC tool

The MCUXpresso Secure Provisioning Tool installers are available for Windows, Linux, or MacOS, and can be downloaded from NXP Secure Provisioning web. For Windows and MacOS, the installers work as a wizard that guides you step by step through the installation process. The Debian package is available for Linux. The details about the installation can be found in the MCUXpresso Secure Provisioning Tool User Guide.

5 Using the tool

5.1 Prerequisites

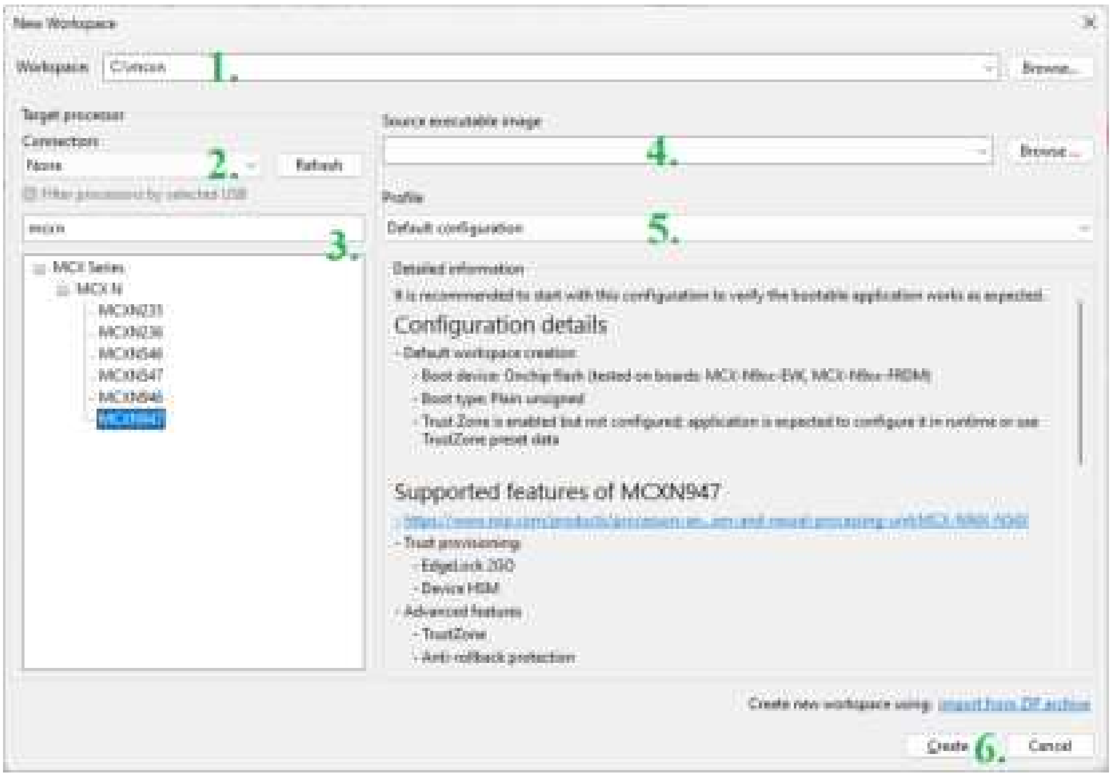
As an input for the tool, use an application binary (S19, HEX, ELF/AXF or BIN file format) that works on the processor. Based on the boot device, build the application either for RAM or for Flash. It is recommended to start with any MCUXpresso SDK example, which is already pre-configured for the right address. Before using the MCUXpresso Secure Provisioning Tool, run the application in debugger and check if it works as expected.

For FRDM and EVK boards, there are sample applications provided in the binary form that usually blinks the onboard LED. It can be used to evaluate the tool functionality even if you do not have any specific application yet.

To load the application into the board, switch the board into In-System-Programming (ISP) mode. For details on how to do that, check documentation for the board or reference manual of the processor.

5.2 New workspace

When you start the MCUXpresso Secure Provisioning tool for the first time, it will ask you to create a new workspace, the folder with all files needed for your project. You can also create a new workspace later using command: **main menu > File > New Workspace**.



Workspace: C:\mcux

Connection: None

mcxn

Profile: Default configuration

It is recommended to start with this configuration to verify the bootable application works as expected.

Configuration details

- Default workspace creation:
  - Boot device: Onchip flash (tested on boards: MCX-N9xx-EVK, MCX-N9xx-FRDM)
  - Boot type: Plain unsigned
  - Trust Zone is enabled but not configured: application is expected to configure it in runtime or use TrustZone preset data

Supported features of MCXN947

- [illegible]
- Trust provisioning:
  - EdgeLock 2GO
  - Device HSM
- Advanced features:
  - TrustZone
  - Anti-rollback protection

Create new workspace using: import from ZIP archive

Figure 1. New Workspace

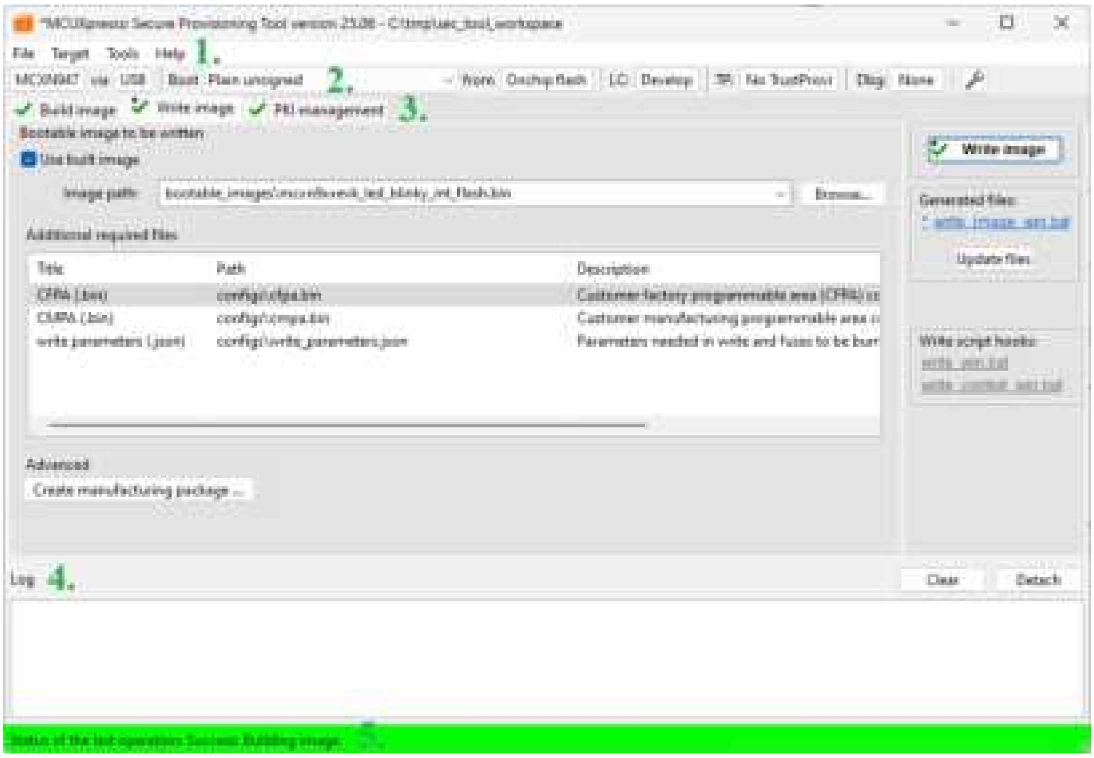
To create the workspace, fill in the following parameters:

1. Select the workspace path on the disk. It is recommended to create a new folder for each project.
2. Connect the device to your computer and select the connection used such as UART COM port or USB. Using a USB connection allows the tool to automatically select the processor series.
3. Select the processor either directly from tree or use the search bar.
4. Select the path to your application as a source executable image.
   Note: for the NXP board, the tool includes pre-complied SDK examples that can be selected from the drop down list.
5. To verify the build and write process with your application, use the default profile that application code is unsigned and plain (not encrypted). Later, when you already have the application tested in the tool, you can select secure profile, and the tool generates a keys and pre-generates a configuration for the secure boot.
6. Click the **Create** button to create the workspace.

5.3 Tool GUI

After you create a workspace, the tool main window will be shown. The main window contains:

1. main menu
2. toolbar
3. tabs “Build image”, “Write image”, and “PKI management”
4. log view
5. status line


*MCUXpresso Secure Provisioning Tool version 25.06 - C:\tmp\sec_tool_workspace

MCXN947 via USB | Boot: Plain unsigned | from: Onchip flash | LC: Develop | TP: No TrustProv | Dbg: None

Bootable image to be written

☑ Use built image

Image path: bootable_images\mcxn9xxevk_led_blinky_int_flash.bin

Additional required files

Title	Path	Description
CFPA (.bin)	config\cfpa.bin	Customer factory programmable area (CFPA) c
CMPA (.bin)	config\cmpa.bin	Customer manufacturing programmable area c
write parameters (.json)	config\write_parameters.json	Parameters needed in write and fuses to be bur

Generated files: * write_image_win.bat

Write script hooks: write_win.bat, write_context_win.bat

Status of the last operation: Success: Building image.

Figure 2. Tool GUI

As a first step, double-check that the configuration on the toolbar matches your requirements. You will find there:

1. selected processor (already selected in the wizard)
2. connection to the processor (already selected in the wizard)
3. boot mode (already selected in the wizard)
4. boot memory
5. life cycle (it is recommended to start with the default value)
6. trust provisioning (it is recommended to start with the default value)
7. debug probe (for most processors you will not need this; it might be used to set up shadow registers used instead of fuses) 8 quick fix button

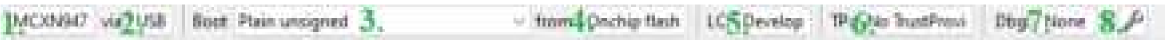

MCXN947 via USB | Boot: Plain unsigned | from: Onchip flash | LC: Develop | TP: No TrustProv | Dbg: None

Figure 3. Toolbar

5.4 Check connection

Either use command **main menu > Target > Connection** or click the connection button in the toolbar and select button **Test connection** in the connection configuration dialog. This pings the processor in ISP mode and checks whether the connection can be established. If the connection is successfully established, the dialog shows the detected status of the connected processor.

If the connection does not work, check if the board is configured to ISP/SDP mode and reset the board.

5.5 Build bootable image

If you create a workspace using the wizard, there should not be any error on the build page. The errors are displayed using red color and the description of the problem is displayed in the tooltip, so if there are any errors indicated, fix them. **Note:** Ignore the error on the Write page, there will be an error until you build the image.

Click the **Build image** button to build the bootable image. The progress is shown in the log. In case there was any problem, read the log and fix it. The files generated as a part of the process are shown below the button. The most important is listed as the first one. It is called the “build_image” script, a script executed during the build process. It is possible to click it and check the content.

5.6 Test bootable image

Once the bootable image is built, you can continue to the **Write image** page and write it into the boot memory. Double-check that there are no errors reported and click the **Write image** button to start the process. The write process works similar to the build process. It will do pre-checks and if no problem is found, it will generate the write script. If the write script does any irreversible changes in the processor, the GUI displays a confirmation dialog with the list of changes. After that, the write script is executed, and the details are listed in the log view.

Once the application is written, verify it boots correctly (switch from ISP to RUN mode and reset).

5.7 What is next

Once you have a bootable application working, it is possible to add additional security configurations, for example:

- secure boot with signed or encrypted image
- dual image boot
- anti-roll back configuration
- configuration of One-Time-Programamble (OTP)
- etc

It is recommended to check the application after each change. If the application does not boot, revert and figure out what change causes the problem. The tool provides various checks to prevent invalid configurations. Errors (red) are blocking issues, to prevent any invalid configuration to be applied to the processor. Warnings (yellow) are unusual/not recommended settings, but they are non-blocking.

Once the secure configuration of the application is finalized and stable, you con continue to manufacturing. The tool can generate a manufacturing package - a ZIP file with all files needed for the manufacturing. In the manufacturing facility, import the package and apply (the manufacturing tool allows applying it to several boards in parallel).

5.8 Processor-specific workflows

There are some processor-specific features that need to be configured. This is the reason there is a processor-specific workflow described in the MCUXpresso Secure Provisioning Tool User Guide, section “Processor-specific workflows” that contains a step-by-step process how to configure different secure configurations.

6 References

6.1 Release Notes

https://docs.mcuxpresso.nxp.com/secure/latest/release_notes.html

MCUXpresso Secure Provisioning Tool Release Notes (document MCUXSPTRN)

6.2 User Guide

https://docs.mcuxpresso.nxp.com/secure/latest/01_introduction.html

MCUXpresso Secure Provisioning Tool User Guide (document MCUXSPTUG)

6.3 NXP Secure Provisioning web

https://nxp.com/mcuxpresso/secure

6.4 Community, forum, knowledge base

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

7 Revision history

Document ID	Release date	Description
UG10241 v.1	30 June 2025	Initial version.

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.