MCUXSPTRN

MCUXpresso Secure Provisioning Tool v.8 Release Notes

Rev. 6 — 11 January 2024 Release notes

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

MCUXpresso Secure Provisioning Tool (SEC) is a graphical user interface (GUI) tool covering secure boot process and trust provisioning capabilities primarily aimed at microcontroller customers. It provides a unified GUI front-end over SPSDK command-line tools.

2 Features

- Support for i.MX RT10xx, RT11xx, RT5xx, and RT6xx processors:
  - RT1010, RT1015, RT1020, RT1024, RT1040, RT1050, RT1060, and RT1064
  - RT116x, RT117x, RT118x
  - RT5xxS, RT685S
- Support for Kinetis W processors:
  - K32W148, KW45B41Zx
- Support for LPC55Sxx and LPC55xx processors:
  - LPC55S6x, LPC55S3x, LPC55S2x, LPC55S1x, and LPC55S0x
  - LPC553x, LPC552x, LPC551x, and LPC550x
- Support for MCX processors:
  - MCXN94x, MCXN54x
  - MCXA14x, MCXA15x
- Support for RW processors:
  - RW612, RW610
- Conversion of ELF executables, SREC, HEX, and raw binaries into bootable images files
- Credentials (keys, signatures, and certificates) generation and management associated with signed/encrypted images
- Target device connection via UART, USB-HID, SPI, and I2C
- Writing FlexSPI NOR, FlexSPI NAND, SEMC NAND, eMMC or SD card boot device including configuration of the boot device parameters
- Use of DCD/XMCD configuration for SDRAM images bootup
- Programming customizable eFuses per image and use case requirements
- Optional batch scripts generation for later use without the GUI
- Streamlined operation for general users
- Manufacturing Tool with the support of parallel execution
- Trust provisioning and device HSM provisioning for selected processors
- Flash programming GUI tool
- Debug authentication
- SB editor tool
- Detailed supported features for each processor in the user guide

3 System requirements

- One of the following Host Operating systems:
  - Microsoft(R) Windows(R) 10 (64-bit)
  - Mac OS 13 Ventura (Intel x86_64 or Aarch64)
  - Ubuntu 22.04 LTS 64 bit, with "OpenSSL 1.1.1f 31 Mar 2020"; GNOME is recommended
- 4 GB RAM or more

- Display with resolution 1366 x 768 or more; for lower resolution the font size should be set to 100 %
- P&E Micro debug probe users: install drivers from P&E web site or install MCUXpresso IDE
  - P&E Micro does not support Mac OS Aarch64
- MCU-Link or LPC-Link debug probe users: install drivers from NXP web site (see user guide for the links)

4 Known issues and limitations

- For more information, see chapter Troubleshooting in the documentation.
- User Guide is not updated for version 8, new features are not documented yet.

5 What is new

This chapter provides details on the versions of the tool.

5.1 Version 8.0, January 2024

- LPC55S3x, KW45xx, K32W1xx: added support for images executed in RAM (xip images)
- Added support for MCXN9xx/MCXN5xx/MCXA14x/MCXA15x processors
- Added support for i.MX RT118x processors with new option to include additional images into the build
  - RT1181 and RT1182 processors are not available in the release time, the tool was tested on preproduction silicon only
- Added support for RW61x processors (including shadow registers)
- Added support for SB 2.1 Editor, supported for i.MX RTxxx and LPC55Sxx processors
- Added an option to configure signature provider via a custom web server
- Added an option to specify separate FCB files for flash programming and runtime
- Supported ECC keys for i.MX RT116x/7x
- i.MX RT11xx bootable image can be used as the source image for the build (previously this was only for RT10xx)
- Added support for multiple monitors
- Integrated NXP Secure Provisioning SDK 2.x with the following highlighted changes:
  - elftosb tool removed, replaced by nxpimage; nxpkeygen tool replaced by nxpcrypto
  - updated changes in command-line arguments
  - several additional incompatible changes in configuration files
- LPC55S3x, KW45xx, K32W1xx: spsdk/nxpkeygen tool replaced by spsdk/nxpcrypto
- Removed legacy tools arm-none-eabi-objcopy, blhost, sdphost, elftosb, image_enc, and cst (fully replaced by spsdk tools)
- New installer for Mac OS with Apple M processor (previously Intel processor only was supported)
- Windows: the workspace can now be located on a drive with a letter other than the letter of the installed application.

5.2 Version 7.0, July 2023

- Smart card trust provisioning is supported for the LPC55S36 processor
- Smart card trust provisioning is supported only for smart card 1.2 or higher
- Redesigned configuration of boot memory; added support for user presets and custom-protected area
- Newly added dual image (ping/pong) boot support is extended to LPC55(S)3x, KW45xx, K32W1xx, and RT116x/7x
- Added support for SB 3.1 editor for LPC55S3x, KW45xx, and K32W1xx processors

- Improved configuration of IFR/ROMCFG for KW45xx and K32W1xx processors, now configured per 16-byte blocks
- i.MX RT116x/7x: legacy elftosb and image_enc tools are replaced by spsdk/nxpimage
- i.MX RT116x/7x: flashloader is updated and detection of locked fuses (via blhost get-property 31) is added
- i.MX RT116x/7x: eMMC is supported
- i.MX RT11xx: XMCD is supported, either via the link to the configuration file or via a simplified GUI editor
- i.MX RT10xx: support for SPI NAND is added
- Grouping of processors in the "New workspace" dialog is improved
- NXP Secure Provisioning SDK 1.10.2 is integrated

5.3 Version 6.0, March 2023

- Added KW45xx and K32W1xx processors
- Enabled support of the LPC55S36 processor
- Fixed configuration of boot device Macronix_MX25UM51345G_A.json, so it matches recommendations from reference manuals
- LPC55Sxx: DICE can be enabled by the user, UDS key initialized in the write script
- LPC55Sxx and i.MX RTxxx: It is possible to regenerate ROT certificates with a different serial number (for key revocation)
- LPC55Sxx: The CFPA content is verified before write and an error is reported if the version is not incremented (GUI only)
- LPC55Sxx: Added support for encrypted plain boot type
- Added i.MX RT1040 processor
- i.MX RT1060: a new EVK board revision supported: MIMXRT1060-EVKC
- i.MX RT107x: a new EVK board revision supported: RT1170-EVKB
- i.MX R685: a new EVK board supported: RT600-AUD-EVK
- i.MX RT5xx: Added support for dual image (ping/pong) boot with PUF key source
- i.MX RT5xx and RT6xx: Added support eMMC and SD card
- i.MX RT6xx: Added support for debug authentication
- Trust provisioning: added support for multiple smart cards, USB connection, and performance improvements
- Flash programmer performance improvements for higher buffer sizes
- Build view: displayed all generated files and their status
- Window locations and sizes are stored in preferences
- The tool display "dirty" flag; if settings are not saved on the disk; added new preference to save automatically
- Setting file `spt_settings.json` changed to `settings.sptjson`
- File extension `.sptjson` associated with the SEC tool, so it can be opened directly with the tool
- CLI: New argument in write scripts: erase_all - perform an erase of the entire flash memory instead erasing regions only
- Tool localized to Chinese
- Legacy blhost updated to v2.6.7
- LPC55S69: dropped support of trust provisioning firmware for silicon revision 8
- i.MX RT633S: the processor removed, no more supported
- Integrated NXP Secure Provisioning SDK 1.9.1

5.4 Version 5.0, November 2022

- Added support for LPC55xx and LPC553x processors (non-S)
- Added support for main menu > Tools > Flash Programmer

- Added support for trust provisioning using Smart Card for LPC55S0x/1x processors
- Added support for device HSM provisioning for i.MX RT6xx processors
- Added support for dual image (ping/pong) boot for i.MX RTxxx processors with OTP key source
- Legacy elftosb is replaced by elftosb from SPSDK for i.MX RTxxx processors
- OTP Configuration is moved from the **Write image** page to the **Build image** page
- `write_parameters.json` is generated for write with parameters reused from build; CLI parameters updated
- Added support for burning fuses in SB file for i.MX RTxxx processors
- Added support for debug authentication for LPC55Sxx and i.MX RTxxx processors
- Added support for OTFAD encrypted boot mode with master key for i.MX RT1011 processor
- Added support for FlexSPI NAND boot for i.MX RT117x/RT116x processors
- Added support for localization, Manufacturing Tool is localized to Chinese (see Preferences)
- Added "MX25U51245G_B" boot device configuration for i.MX RT600-AUD-EVK
- The command "main menu> File > Generate Scripts" is removed, it was replaced by the link on **Build image** and **Write image** views
- Integrated SPSDK 1.7 with the following highlighted changes:
  - new tools: nxpimage and nxpcrypto
  - elftosb: added support to burn fuses in the SB file

5.5 Version 4.1.1, July 2022

- Trust provisioning tools are updated from NXP Secure Provisioning SDK 1.6.3

5.6 Version 4.1, June 2022

- LPC55S69: 2 versions of trust provisioning firmware for different silicon revisions are now supported.
- Ubuntu 22.04 LTS is supported

5.7 Version 4.0.1, May 2022

- Windows: Fix for LPC55Sxx write script in sealing the CMPA page
- Updated terminology in GUI and documentation

5.8 Version 4.0, May 2022

- Added support for Trust Provisioning using Smart Card for LPC55S6x/2x
- Added support for "life cycle" selection instead of the "Enable security" checkbox (for all processors)
- Added support for Encrypted (HAB) and Encrypted (IEE) boot modes for RT11xx
- Added support for FlexSPI instance selection for i.MX RT11xx processors
- Added support for OTFAD encrypted boot mode with user keys for i.MX RT1010 processors
- Added support for SPI and I2C connection types (for LPC55Sxx and i.MX RTxxx)
- Improved fields and bits names in PFC Configuration for LPC55Sxx processors
- Improvements on the Manufacturing Tool: Added counter of successful operations and a "Test connection" button
- Improved layout of PFR Configuration dialog for improving the user experience on Linux
- Several fixes and improvements for write script for i.MX RTxxx processors
- Added a "Clear CMPA" button into the PFR configuration dialog
- CLI command "clear-security" was removed. It was replaced by the PFR configuration and a "Clear CMPA" button

- Windows: Fixed the problem that the Secure Provisioning Tool does not run with some region settings
- Integrated SPSDK 1.6 with the following highlighted changes:
  - Additional CLI tools added: tpconfig, tphost, nxpcertgen, nxpdevhsm, shadowregs, nxpdevscan
  - blhost:
    - The performance of the "receive-sb-file" command was significantly improved; however, if it fails, the reported error code might not be correct; use the parameter "--check-errors" to see the detailed problem information
    - The command "efuse-program-once" automatically verifies the written value to avoid problems on i.MX RT11xx processors, where the write failure was reported as a successful operation (see also --verify/--no-verify option)
  - pfr, pfrc:
    - The names of the fields and their bits were updated without preserving backward compatibility.

5.9 Version 3.1, August 2021

- Support for Mac OS X Big Sur (version 11) is added; support for Microsoft(R) Windows(R) 7 is dropped.
- support for i.MX RT1171, RT1172, RT1173, RT1175, RT1165, RT1166 is added.
- The CLI command "write_fuses" was removed, it was replaced by OTP Configuration
- [LPC55Sxx] support for PFR Configuration GUI is added.
- [LPC55Sxx] support for PRINCE encryption of "Whole image" without the necessity to enter an exact address range is added.
- [RTxxx, RT11xx] support for OTFAD encryption is added.
- support for i.MX RT1010: Unsigned and Authenticated (HAB) modes is added.

5.10 Version 3.0, April 2021

- Support for i.MX RT1176: Unsigned and Signed modes is added.
- Support for i.MX RT5xx/RT6xx: Unsigned/CRC/Signed boot modes is added.
- Support for PRINCE encryption for LPC55Sxx processors is added.
- Support for OTP configuration is added.
- Support for Manufacturing Tool is added.
- [LPC55Sxx] CMPA/CFPA.bin files generated using the PFR tool; CMPA/CFPA.json used as an input
- [LPC55Sxx] The initial version of CFPA for Signed boot mode (0x02000_0000 to 0x0000_0002) is fixed.
- i.MX RT10xx/RT11xx: support for restricted data is added.
- RT5xx/RT6xx: the ability to use Shadow registers instead of using FUSEs
- Support for Ubuntu 20.04 is added.
- blhost and sdphost utilities are replaced with SPSDK alternatives; new CLI utilities: pfr, nxpkeygen, and nxpdebugmbox (Debug Authentication) in tools/spsdk are added.
- LPC55Sxx Key Store: The key store is initialized only once in the device life cycle and after that SBKEK cannot be changed.
- i.MX RT10xx GPx fuse lock: lock for the GPx fuse provided in previous versions was removed in V3 as the lock is not required for a bootable image;
  Note: *However, it is still recommended to lock the fuse; see "OTP Configuration"*

5.11 Version 2.1, December 2020

- Support for i.MX RT1015, i.MX RT1024, LPC55S06, and LPC55S04 is added.
- Mac OS X - fixed saving the workspace setting in case the App Menu "securep | Quit securep" is used.
- Mac OS X - fixed connection dialog freeze in case a wrong UART is used.

- [LPC55Sxx] several improvements for Signed LPC images
- LPC55Sxx Trust Zone - CLI allows setting/overriding the Trust Zone Settings
- Other minor improvements and bug-fixes

5.12 Version 2.0, August 2020

- Support for i.MX RT1020 and i.MX RT1064 is added.
- Support for LPC55S6x, LPC55S2x, and LPC55S1x is added.
  - Unsigned, Unsigned CRC, and Signed boot modes
  - TrustZone support (bin + json)
  - Key Management - Secure Boot, Generation of ROT keys
- BEE boot for i.MX RT10xx
  - OTPMK
  - SW-GP2/GP4
- Import/Export Keys between workspaces
- The connection dialog is improved, it supports UART test connection, processor detection and detection of fuse status are improved.

5.13 Version 1.0.1, January 2020

- Support for Mac OS X Catalina (10.15) + Ubuntu 18.04 is added.
- Termination of subprocesses of long-running tasks is fixed.

5.14 Version 1.0, December 2019

- Initial version with i.MX RT1050 and i.MX RT1060; for Windows

6 Revision history

Table 1. Revision history

Document ID	Release date	Description
MCUXSPTRN v.6	11 January 2024	Features for v.8 are added
MCUXSPTRN v.5	20 July 2023	Features for v.7 are added
MCUXSPTRN v.4	15 March 2023	Features for v.6 are added
MCUXSPTRN v.3	30 September 2022	Features for v.5 are added
MCUXSPTRN v.2	24 June 2022	Features for v.4.1 are added
MCUXSPTRN v.1	10 May 2022	Features for v.4.0.1 are added
MCUXSPTRN v.0	28 April 2022	Initial release

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.

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.

AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, μVision, Versatile — are trademarks and/or registered trademarks of Arm Limited (or its subsidiaries or affiliates) in the US and/or elsewhere. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. All rights reserved.

Apple — is a registered trademark of Apple Inc.

i.MX — is a trademark of NXP B.V.

Intel, the Intel logo, Intel Core, OpenVINO, and the OpenVINO logo — are trademarks of Intel Corporation or its subsidiaries.

Kinetis — is a trademark of NXP B.V.

MCX — is a trademark 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'.

For more information, please visit: https://www.nxp.com

Date of release: 11 January 2024
Document identifier: MCUXSPTRN