AN14540

Firmware update on PN7642

Rev. 2.0 — 3 July 2025

Application note

Document information

Information	Content
Keywords	PN7642, firmware update, esfwu, user application
Abstract	This documents explains the various options for performing a firmware update on the PN7642.

1 Introduction

The PN7642 consists of two main memory areas, one for the NXP secure firmware and another for the user application. This document explains how both can be updated by the user.

The firmware update process involves additional tools which are not explained in detail within this document. References to other documents provide guidance on how to install and use the respective tools. A certain amount of embedded programming knowledge is assumed.

- The NXP firmware is further referred to as "NXP firmware” or “firmware”.
- The user application is further referred to as “user application” or “application”.

Table 1. PN7642 memory map

Description	Size	Start - End
NXP firmware	32 kB	0x200000 - 0x207FFF
User application	180 kB	0x208000 - 0x234FFF
NXP firmware	44 kB	0x235000 - 0x23FFFF

A firmware update must only be performed in a controlled environment with a stable power source and without interruptions. An interrupted firmware update has the potential to break certain functionalities, which might limit the possibilities for further updates. The download mode (also referred to as Bootloader mode) of the PN7642 is ROM-based and available at all times. Updating via In-Application programming might not work if the firmware has been corrupted due to interruption, and the PN7642 stays in Bootloader mode.

2 Firmware overview

The PN76 firmware and tool compatibility are listed below in Table 2.

Firmware version

A firmware version is always 2 bytes: XX.YY

Where '*XX*' is the major version and '*YY*' is the minor version. A firmware version written as "2.1" is equal to "02.01", "1.0" is equal to "01.00" and so on.

It is not possible to downgrade a major version. A chip with firmware version 02.xx cannot be downgraded to firmware version 01.xx. A downgrade is only possible within minor version: 02.02 → 02.01; 01.0A → 01.00; and so on.

A firmware version with “F” in its minor version is the same as without the “F” except it does not update the RF and protocol settings. Firmware version "01.00" and 01.F0" are equal from a functional point of view, but one overwrites the settings while the other one, with “F”, will not modify RF settings.

SDK version

An SDK is bound to a certain firmware version. Make sure to use the right SDK version for the firmware version. An SDK upgrade is necessary if a firmware upgrade is made. Or the firmware is upgraded to the firmware version within the SDK.

This guarantees that the compiled application is running on the target firmware version, see Table 2.

NFC Cockpit version

The NFC Cockpit application binary (.bin), within the installation folder of the NFC Cockpit, is compiled for a certain firmware version.

Make sure to flash the correct NFC Cockpit application according to your firmware version.

Firmware backward compatibility

A firmwares backwards compatibility is not guaranteed. While a backward compatibility within minor versions is given (02.02 → 02.00), this is unlikely for major version changes (02.00 → 01.00).

Before performing a firmware update, check the release notes.

Compatibility table

Table 2. Firmware compatibility

FW version	SDK version	Comment
01.00 / 01.F0	2.12.1	Standard firmware on C100[1] ICs. DWL_REQ pin necessary to enter into the bootloader.
02.00 / 02.F0	2.12.3	Standard firmware on C101 ICs. DWL_REQ pin not necessary. Pin-less download active as default.
02.01 / 02.F1	2.12.4	Firmware officially withdrawn due to backward compatibility issues.
02.02 / 02.F2	2.12.5	Minor bug fixes. Backward-compatible to FW v02.00.
	2.15.000	New SDK structure to support VSC. Same content as v2.12.5
02.03 / 02.F3	2.15.002	See release notes of the SDK.
02.05 / 02.F5	2.15.003	See release notes of the SDK.
02.06 / 02.F6	2.15.004	See release notes of the SDK.

[1] C100/C101 being the part numbers of the PN7642.

Firmware release notes

See document RN00257 for the latest PN7642 firmware release notes.

3 Updating NXP firmware

The PN7642 NXP firmware is closed-source and only available for the user as an *.esfwu* file provided by NXP. The MCUXpresso SDK, NFC Cockpit and Firmware package (on nxp.com) contain these files.

The NXP firmware of the PN7642 can be updated through:

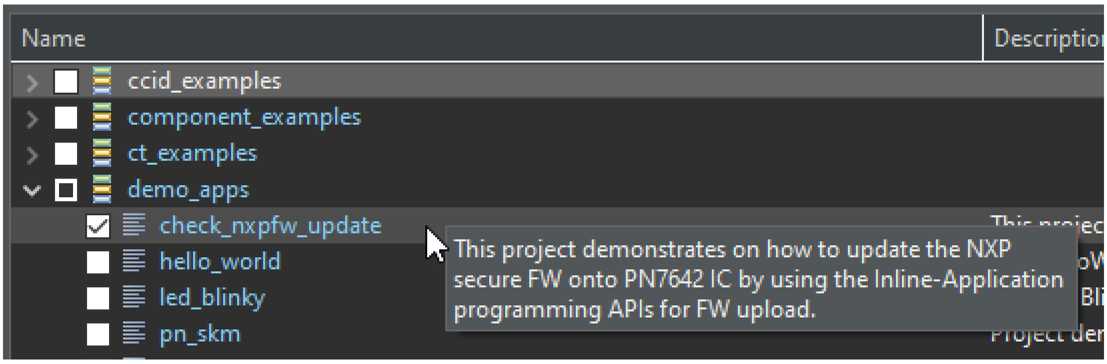
- IAP (In-Application Programming)
- the HIF (Host Interface) of another MCU
- the NXP NFC Cockpit (USB)

3.1 FW update via IAP

Prerequisites

- IDE: MCUXpresso
- PN7642 MCUXpresso SDK from nxp.com → PN7642 → software
- Evaluation board: OM27642
- Debugger: MCU-Link, MCU-Link Pro, or a J-Link debug probe.

The MCUXpresso SDK for the PN7642 has a demo application called "check_nxpfw_update". When this example is imported and run, it will automatically update the IC to the firmware version associated with this SDK version.

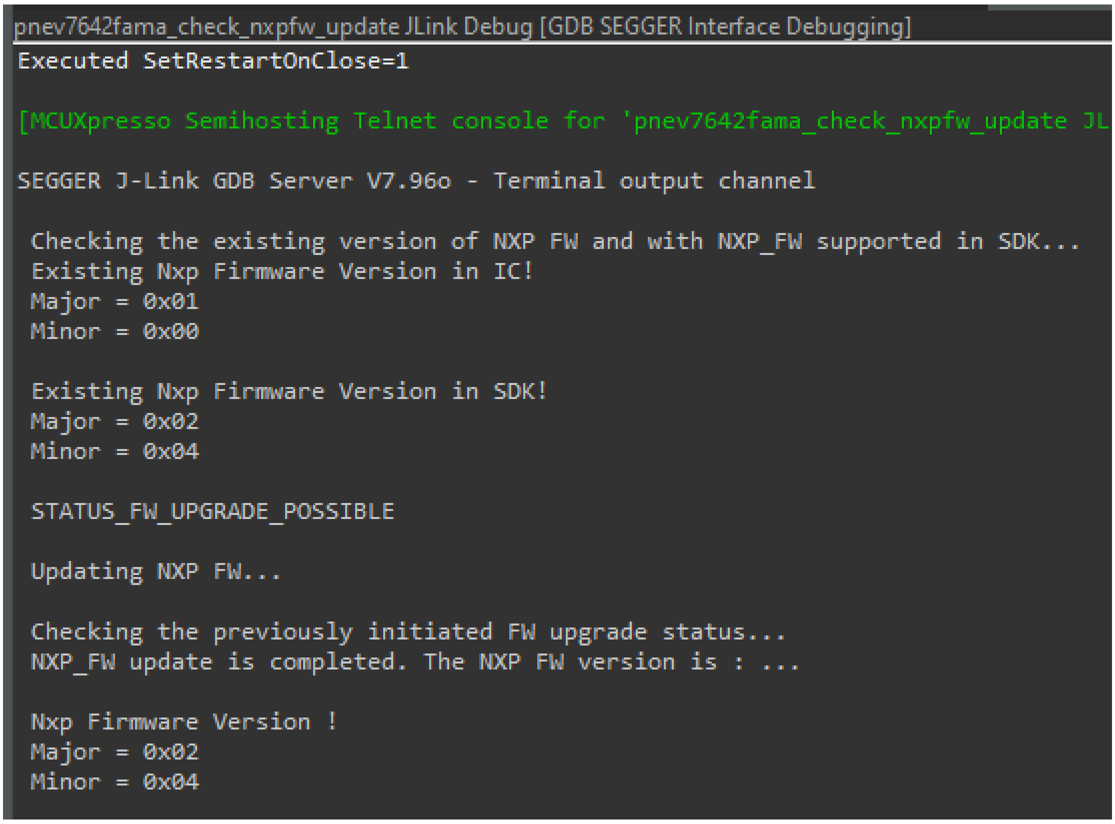


This project demonstrates on how to update the NXP secure FW onto PN7642 IC by using the Inline-Application programming APIs for FW upload.

Figure 1. Check NXP firmware Update Example

For example: If the SDK example is run on a PN7642 C100, default firmware v01.00, with SDK 2.15.000, it is automatically updated to firmware v02.02.

No firmware update is performed, if the versions match. Information about the chips firmware version, the SDK firmware version, and the progress is shown in the debug output.



```
pnev7642fama_check_nxpfw_update JLink Debug [GDB SEGGER Interface Debugging]
Executed SetRestartOnClose=1

[MCUXpresso Semihosting Telnet console for 'pnev7642fama_check_nxpfw_update JL

SEGGER J-Link GDB Server V7.96o - Terminal output channel

 Checking the existing version of NXP FW and with NXP_FW supported in SDK...
 Existing Nxp Firmware Version in IC!
 Major = 0x01
 Minor = 0x00

 Existing Nxp Firmware Version in SDK!
 Major = 0x02
 Minor = 0x04

 STATUS_FW_UPGRADE_POSSIBLE

 Updating NXP FW...

 Checking the previously initiated FW upgrade status...
 NXP_FW update is completed. The NXP FW version is : ...

 Nxp Firmware Version !
 Major = 0x02
 Minor = 0x04
```

Figure 2. Firmware update console output

To learn how to import and run an example, refert to the AN13134 PN76xx quick start guide.

The API used for the firmware update is part of the *System Service Interface Layer* and described in the PN7642 API Documentation.

3.2 FW update via host

Prerequisites

- IDE: MCUXpresso
- LPC55S16 Host Software from: nxp.com → PN7642 → software
- Evaluation board: OM27642
- Evaluation board: LPC55S16-EVK
- NXP Firmware file (*.esfwu*):
  - Package "PN7642 Firmware vXX.YY" downloaded from: nxp.com → PN7642 → software
  - Or as part of the NXP NFC Cockpit installation: NFC Cockpit → firmware → PN7642_ESFWU

The PN7642 can be updated via the host interface (SPI, I2C, UART, etc.) by using the PN7642 ROM Bootloader and its HDLL command (see UM11905 Instruction Layer Manual).

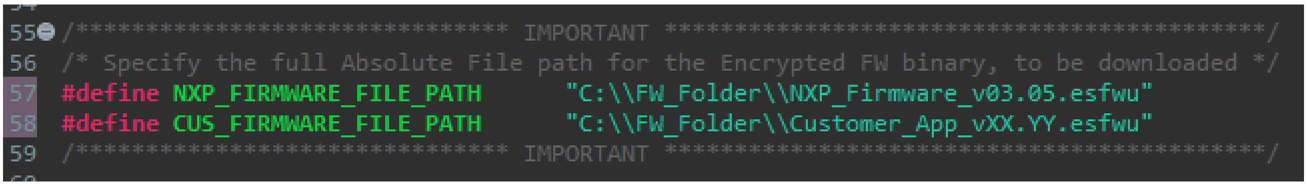
Refer to AN13134 PN76 quick start guide. for instructions on how to install and run the host examples as well as how to connect those the two boards.

3.2.1 Edit firmware location

At the top of the main file of *DownloadEx1*, the path to the firmware files is defined. This has to be changed to meet the individual path. For this example, a folder at the root of "C:" with the name "FW_Download" has been created, in which the downloaded *.esfwu* firmware file has been copied.

Users can either rename the firmware file to match the definition in the example or edit the definition in the example to match the firmware files name. The latter has the benefit of not losing important information in the name, such as the version, which can be useful if users have to repeat the update process later and might have forgotten what firmware file was previously used.

In this example, the path has been changed to match the firmware filename:



```
/******************************** IMPORTANT *******************************************/
/* Specify the full Absolute File path for the Encrypted FW binary, to be downloaded */
#define NXP_FIRMWARE_FILE_PATH      "C:\\FW_Folder\\NXP_Firmware_v03.05.esfwu"
#define CUS_FIRMWARE_FILE_PATH      "C:\\FW_Folder\\Customer_App_vXX.YY.esfwu"
/******************************** IMPORTANT *******************************************/
```

Figure 3. Firmware file path editing

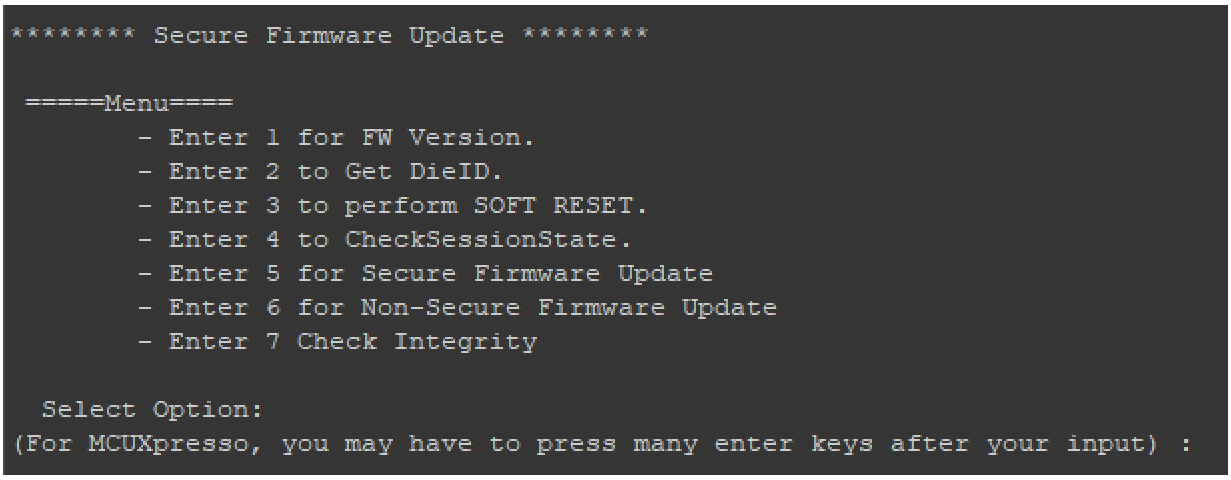
For updating the PN7642 firmware, the macro "FIRMWARE_FILE_PATH" has to match the location of the NXP secure firmware file.

Pay special attention to using a double backslash as a single backslash is marking a special character.

Note: *Depending on the Host Software package and its version the naming can be slightly different.*

3.2.2 Run firmware update

By running the example, there are several options printed in the console to be chose from.

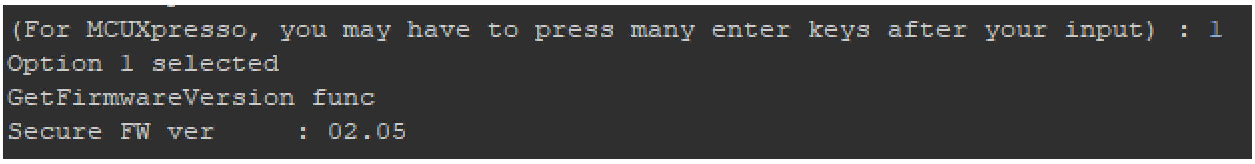


```
******** Secure Firmware Update ********

 =====Menu====
        - Enter 1 for FW Version.
        - Enter 2 to Get DieID.
        - Enter 3 to perform SOFT RESET.
        - Enter 4 to CheckSessionState.
        - Enter 5 for Secure Firmware Update
        - Enter 6 for Non-Secure Firmware Update
        - Enter 7 Check Integrity

  Select Option:
(For MCUXpresso, you may have to press many enter keys after your input) :
```

Figure 4. Firmware update options

Choosing the first option reads out the current firmware version of the PN7642. It is also a good check to see if the connection is working properly.

•

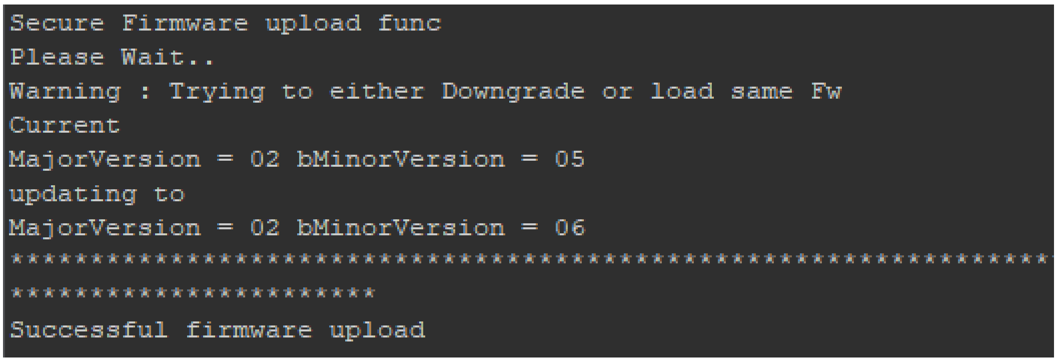


```
(For MCUXpresso, you may have to press many enter keys after your input) : 1
Option 1 selected
GetFirmwareVersion func
Secure FW ver      : 02.05
```

Figure 5. Read firmware version

- Secure FW Ver: represents the NXP firmware version on the PN7642
- Non-Secure FW ver: can be assigned by updating the user application space via download mode.

The connected PN7642 is running firmware version v02.05. If the path to the firmware file is correct and the firmware file itself is valid, running option 5 "Secure firmware update" starts the update process.



```
Secure Firmware upload func
Please Wait..
Warning : Trying to either Downgrade or load same Fw
Current
MajorVersion = 02 bMinorVersion = 05
updating to
MajorVersion = 02 bMinorVersion = 06
*****************************************************************
***********************
Successful firmware upload
```

Figure 6. Update firmware version

The update may take a while. At the end, a successful update is indicated by the prompt of "Successful firmware upload". To verify, a read firmware version can be executed once more.

3.3 FW update via NFC Cockpit

The PN7642 can also be updated by using the NFC Cockpit. Download and install it from nxp.com: NFC Cockpit

The PNEV7642 evaluation board does not come with the NFC Cockpit application preinstalled. The NXP NFC Cockpit application has to be flashed first.

Note: *Make sure to flash the application corresponding to your firmware version. As per default, the C100 and C101 have different firmware versions which are not compatible. C100 → v01.00 and C101 → v02.00*

Flashing the NFC Cockpit application can be done via the USB mass storage mode or with an external debugger (via SWD).

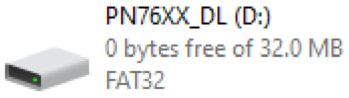
3.3.1 Bring to mass storage mode

To bring the PN76 development board into mass storage mode, the user must bring the DWL_REQ pin HIGH while resetting the board.

Follow the instructions below:

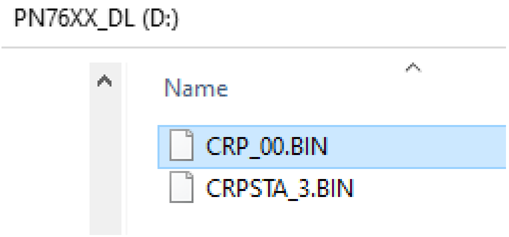
1. Press and hold SW3 "NFC_VEN".
   a. Found in the upper left corner. A small white pushbutton.
2. Press and hold SW2 "NFC_DWL_REQ".
   a. Found on the right side edge of the board. A small white pushbutton.
3. Release SW3 "NFC_VEN".
4. Release SW2 "NFC_DWL_REQ".

A new mass storage device will appear in your explorer, which holds two files *"CRP_00.BIN*" and *"CRPSTA_3.BIN*".



PN76XX_DL (D:)
0 bytes free of 32.0 MB
FAT32

Figure 7. PN7642 mass storage device



PN76XX_DL (D:)

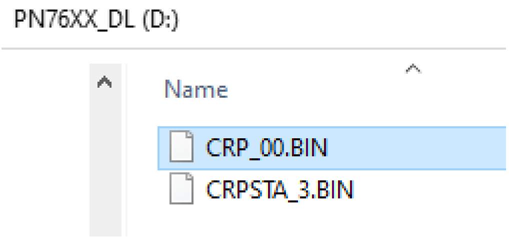
Name

CRP_00.BIN
CRPSTA_3.BIN

Figure 8. PN7642 content

3.3.2 Flash NFC Cockpit firmware

1. Open the PN76xx_DL mass storage device and delete the *"CRP_00.BIN*" file.



PN76XX_DL (D:)

Name

CRP_00.BIN

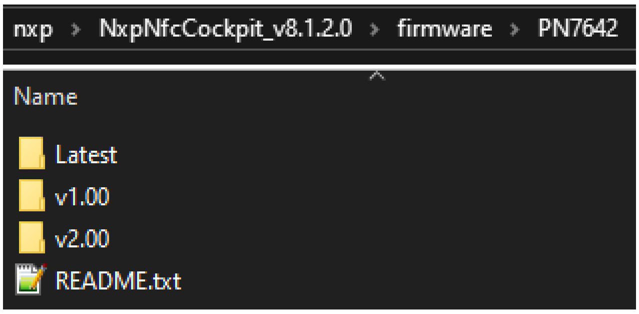
CRPSTA_3.BIN

Figure 9. Mass storage content

2. Go to your NFC Cockpit installation folder → firmware → PN7642 → v1.00/v2.00, see README.txt, and copy the *"NxpNfcCockpit_05_03_00.bin*"[1] onto the mass storage device.

Note: *Check chapter Section 2 to find the matching NFC Cockpit application version to the PN7642 firmware version in use.*

For the PN7642, use the PN7642 folder → firmware and read the "*README.txt*" to check which firmware versions are suitable.



nxp › NxpNfcCockpit_v8.1.2.0 › firmware › PN7642

Name

Latest

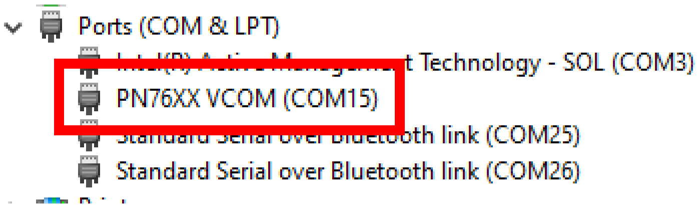
v1.00

v2.00

README.txt

Figure 10. NFC Cockpit firmware

3. The PN76xx_DL automatically restarts and a PN76XX VCOM device should appear in your device manager. If no VCOM appears and instead the mass storage device PN76xx_DL show up again, make sure DWL_REQ is low and reset the device again by pressing NFC_VEN.



Ports (COM & LPT)

Intel(R) Active Management Technology - SOL (COM3)

PN76XX VCOM (COM15)

Standard Serial over Bluetooth link (COM25)

Standard Serial over Bluetooth link (COM26)

Figure 11. PN7642 VCOM device

The PN76 has been successfully flashed with the NFC Cockpit firmware and can now be used with the NFC Cockpit application.

Depending on your system and previously installed drivers, there is a possibility that the PN76 VCOM port is displayed within another device category. This usually is no problem and the NFC Cockpit will function

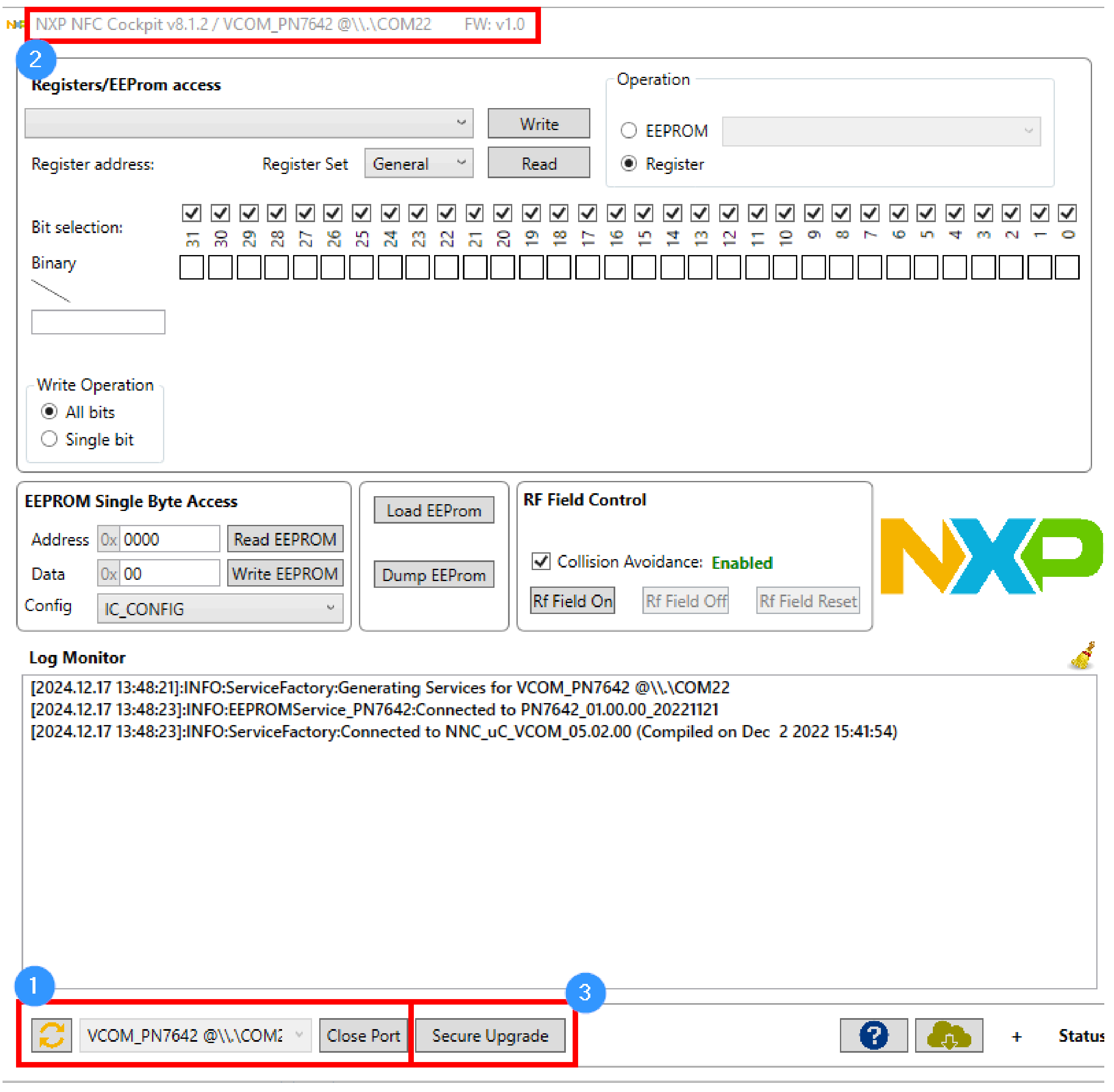
[1] The naming and/or version might be different depending on which NFC Cockpit version is used.

as expected. In rare cases, it might be necessary to look closer to similar drivers and de-install/install them manually.

3.3.3 Update firmware with the NFC Cockpit

Open the NFC Cockpit application. If a single NXP device has been detected, it will automatically connect to it. Otherwise, manually choose to which NXP device you want to open the connection.

Figure 12 shows a cropped capture of an opened and connected NXP NFC Cockpit to a PN7642.


NXP NFC Cockpit v8.1.2 / VCOM_PN7642 @\\.\COM22 FW: v1.0

Register Set: General

Operation: ○ EEPROM ● Register

Bit selection: ☑ 31 to ☑ 0

Write Operation: ● All bits ○ Single bit

EEPROM Single Byte Access: Address 0x 0000; Data 0x 00; Config IC_CONFIG

RF Field Control: ☑ Collision Avoidance: Enabled

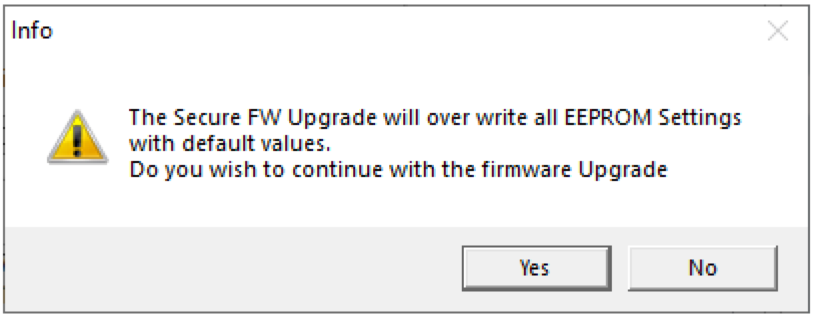
```
[2024.12.17 13:48:21]:INFO:ServiceFactory:Generating Services for VCOM_PN7642 @\\.\COM22
[2024.12.17 13:48:23]:INFO:EEPROMService_PN7642:Connected to PN7642_01.00.00_20221121
[2024.12.17 13:48:23]:INFO:ServiceFactory:Connected to NNC_uC_VCOM_05.02.00 (Compiled on Dec  2 2022 15:41:54)
```

VCOM_PN7642 @\\.\COM2

Figure 12. NXP NFC Cockpit opened

1. The drop-down menu shows all available NXP VCOM devices. Choosing one VCOM port will automatically try to connect to it. With "Close Port" the connection will be closed which also triggers a soft reset of the connected device.
2. General information about the NFC Cockpit version and the connected device. Such as:
   a. Name: VCOM_PN7642
   b. COM Port: COM22
   c. Firmware Version: FW v1.0
3. Secure Upgrade button. With this button you can update the NXP firmware of the connected device. In this case of the connected PN7642.

To update the NXP firmware of the PN7642 click the "Secure Upgrade" [3] button. A warning pops up to inform the user that all EEPROM settings are overwritten with their default values, to proceed "Yes" must be clicked.

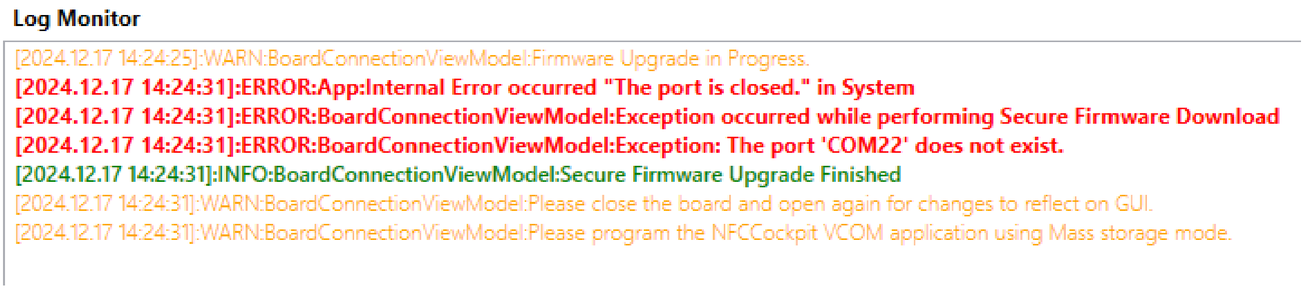


Info

The Secure FW Upgrade will over write all EEPROM Settings with default values.
Do you wish to continue with the firmware Upgrade

Figure 13. NNC Warning

Next, the firmware to which the PN7642 shall be upgraded must be chosen. This can be either from the NFC Cockpit package or from any other location. The firmware file must be an NXP provided and signed *.esfwu* file.



Log Monitor

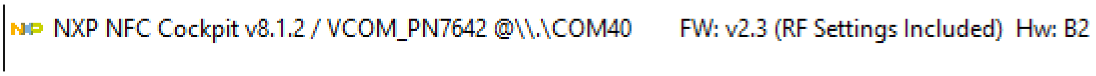
```
[2024.12.17 14:24:25]:WARN:BoardConnectionViewModel:Firmware Upgrade in Progress.
[2024.12.17 14:24:31]:ERROR:App:Internal Error occurred "The port is closed." in System
[2024.12.17 14:24:31]:ERROR:BoardConnectionViewModel:Exception occurred while performing Secure Firmware Download
[2024.12.17 14:24:31]:ERROR:BoardConnectionViewModel:Exception: The port 'COM22' does not exist.
[2024.12.17 14:24:31]:INFO:BoardConnectionViewModel:Secure Firmware Upgrade Finished
[2024.12.17 14:24:31]:WARN:BoardConnectionViewModel:Please close the board and open again for changes to reflect on GUI.
[2024.12.17 14:24:31]:WARN:BoardConnectionViewModel:Please program the NFCCockpit VCOM application using Mass storage mode.
```

Figure 14. Log monitor update success

By updating the PN7642 restarts, the NFC Cockpit will lose connection and needs to be connected again.

After a firmware update from v01.00 to v02.03 the NFC Cockpit application in the user application space is **not** compatible any longer. A new NFC Cockpit application must be flashed. See chapter Firmware overview for a compatibility list.

Flash the new NFC Cockpit application with the procedure from Flash NFC Cockpit firmware. After that, reopen the NFC Cockpit and the updated device will appear:



NXP NFC Cockpit v8.1.2 / VCOM_PN7642 @\\.\COM40 FW: v2.3 (RF Settings Included) Hw: B2

Figure 15. Device info after update

From this point on the PN7642 is updated to FW v02.03. Make sure the MCUXpresso SDK in use is compatible with the used firmware.

4 Downgrading NXP firmware

A firmware downgrade (for example, v01.04 → v01.02, v02.05 → v02.02) is possible within minor versions. Major version downgrades (for example, v02.XY → v01.XY) are not possible. The procedure for the downgrade is the same as for the firmware upgrade. Just the firmware file is not of a newer version but instead of the desired older version.

Important Note:

Due to the In-Application Programming fix in firmware version v02.06, a downgrade will not succeed on the first try. At the very end of the download session the DL_COMMIT (internally issued) is failing. The download session will remain open. As a result the PN7642 remains in bootloader mode and will not boot into application space. Any further interaction with the PN7642 must be via the host-interface and HDLL.

A downgrade of v02.06 to a previous version is not recommended.

5 Updating the user application

The user application, which resides in the user flash space (0x208000 - 0x234FFF), can be updated in multiple ways. The usefulness of each option depends on the users application.

- Debugger interface (SWD):
  - Using the SWD interface to write the flash. This option is useful during the development phase but is usually not usable for updates in the field.
- Host interface using primary NXP ROM bootloader:
  - The primary NXP ROM bootloader can be used to update the user flash space via the host interface.
- USB mass storage:
  - The application flash can be written by using the USB mass storage device and replacing the content with the application binary (*.bin*).
- Secondary bootloader:
  - Hosting a secondary bootloader in the user space.

5.1 Update via SWD

While SWD is used in development all the time to write the user application space, it is strongly recommended to disable SWD access after production. A enabled SWD interface is a potential entry point for malicious mischief. To write the application space via SWD a debugger of some sort is necessary which is usually spared on production hardware.

In theory, every M33 capable debugger could write the flash space of the PN7642. Officially supported are MCU-Link, MCU-Link Pro and SEGGER J-Link devices.

To update the user space via SWD, connect a debugger to SWDIO (B8), SWD_CLK (C8). On the PNEV7642 evaluation board this would be connector J21 "NFC_DEBUG".

5.2 Update via HIF

A user application space update via the host interface uses the same download mode as the NXP firmware update. For the instructions for performing the update, see Section 3.2 "FW update via host".

The PN7642 in download mode only accepts encrypted secure firmware update files (*.esfwu*). For the user application space, the *.esfwu* file must be created by the user.

The application note AN13800 describes in detail how such a *.esfwu* file is sent to the PN7642. This application note is accessed under an NDA.

Generation of ESFWU files

The generation of such files is assisted with an example python script, “Host Crypto Scripts”, provided by NXP. It can be download from PN7642 → Software → Secure → Host Crypto Scripts.

CONNECTIVITY SOFTWARE

Host Crypto Scripts v01.03

PDF Rev 1.1 Sep 5, 2023 SW810311 English

Access Granted ⓘ

Figure 16. Host Crypto Scripts

The tool is available as source code and nothing is hidden. Read the *README.pdf* for information about the configuration. The PN7642 comes with a default RSA key which must be rotated by the user to their own RSA key. This RSA key has a special place and cannot be accessed via the SKM.

5.3 Update via mass storage

The PN7642 offers a USB mass storage device which accepts application binaries. Those binaries must be unencrypted as they are directly copied into the user flash space.

How to bring the PN7642 into USB mass storage is explained in Bring to mass storage mode and the AN13134 PN76xx evaluation board quick start guide.

Flashing your application binary is as easy as deleting the existing *"CRP_00.bin*" and copying in your binary *(.bin*). After the transfer is completed, the PN7642 will restart automatically and present mass-storage again. By resetting the PN7642, it boots to application mode.

5.4 Update via a secondary bootloader

The PN7642 is based on a Cortex-M33 which can remap the vector table (VTOR). This makes the usage of a secondary bootloader easy and feasible. In the PN7642 MCUXpresso SDK, an example of a secondary bootloader is provided.

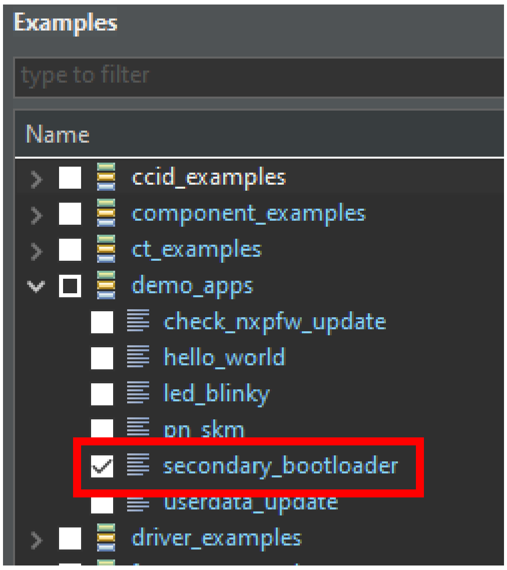


Figure 17. Example import secondary bootloader

To learn how to use MCUXpresso, import, and run examples, read the AN13134 PN76xx evaluation board quick start guide.

The example "pnev7642fama_secondary_bootloader" is a basic example, and it is assumed that a customer who wants to use a secondary bootloader has the knowledge and capability to write/enhance it on their own. A secondary bootloader is a delicate piece of software and shall be developed with utter care.

Using a secondary bootloader gives freedom regarding the update possibilities to the user, and every functionality of the PN7642 can be used to assist or enhance such a bootloader. Encrypted updates via NFC, Double-bank approaches, hashing mechanism and many more.

6 Abbreviations

Table 3. Abbreviations

Acronym	Description
ESFWU	Encrypted Secure Firmware Update
FW	Firmware
IAP	In-Application Programming
HIF	Host Interface
NNC	NXP NFC Cockpit
SWD	Single Wire Debug
SKM	Secure Key Mode
SDK	Software Development Kit
VTOR	Vector Table Offset Register

7 References

[1] Software – MCUXpresso Integrated Development Environment (IDE) (link)

[2] Web page – PN7642 – Single-Chip Solution with High-Performance NFC Reader, Customizable MCU and Security Toolbox (link)

[3] Resources – PN7642 NFC Controller User API Documentation

[4] User manual – UM11905 – PN76 family instruction manual (link)

[5] Application note – AN13134 – PN76 family evaluation board quick start guide (link)

[6] Application note – AN13800 – PN76 family encrypted application firmware download reference

[7] Software – NFC Cockpit Configuration Tool for NFC ICs (link)

8 Revision history

Table 4. Revision history

Document ID	Release date	Description
AN14540 v.2.0	3 July 2025	• Section 3.2.1 "Edit firmware location": updated • Section 3.2.2 "Run firmware update": updated • Section 3.3.1 "Bring to mass storage mode": updated • Section 3.3.2 "Flash NFC Cockpit firmware": updated • Section 3.3.3 "Update firmware with the NFC Cockpit": updated • Section 4 "Downgrading NXP firmware": added
AN14540 v.1.0	19 February 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.

Licenses

Purchase of NXP ICs with NFC technology — Purchase of an NXP Semiconductors IC that complies with one of the Near Field Communication (NFC) standards ISO/IEC 18092 and ISO/IEC 21481 does not convey an implied license under any patent right infringed by implementation of any of those standards. Purchase of NXP Semiconductors IC does not include a license to any NXP patent (or other IP right) covering combinations of those products with other products, whether hardware or software.

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.

Tables

Figures

Contents

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