AN13936

PN7642 frequently asked questions

Rev. 1 — 29 February 2024 Application note

Document information

Information	Content
Keywords	FAQ, PN76, PN7642, secure key mode (SKM), MbedTLS, Crypto, Secure Key Store, frequently asked questions
Abstract	This document covers frequently asked questions in a question-answer style.

1 Introduction

This document is a collection of frequently asked question about PN7642 environment.

Most of the questions are covered in greater detail in other documents. It is highly recommended to get yourself familiar with the PN7642 and related documentation.

2 Firmware

2.1 Can the firmware be downgraded to another version?

Downgrading is only possible with minor versions. You cannot downgrade to another major version.

Minor downgrade: v02.07 → v02.01 = **possible**

Major downgrade: v02.xx → v01.xx = **not possible**

2.2 What is the maximum size of an NXP firmware update file (*.esfwu*)?

Maximum size of secure firmware update file (includes secure flash code, RF settings) ==> (0xD240) ==> **53,824 bytes**

Maximum size of secure firmware update file including ROM area settings and log area ==> (0xD8C0) ==> **55,488 bytes**

Maximum size of secure firmware update file including ROM area settings, and log area, and NXP configuration area ==> 0xDD10 ==> **56,592 bytes**

2.3 If an invalid command with a valid CRC is received in download mode. Does PN7642 stay in download mode?

Yes. If a valid packet format is received, PN7642 stops the HIF-Timeout timer (per default 500 ms) and stays in download mode. Only a valid exit command or VEN rest puts PN7642 out of the download mode.

2.4 Do the TPT keys change on a firmware update?

PN7642 C100 device comes by default with firmware v01.00. If you update a PN7642 C100 device to a newer firmware version like v02.02, the TPT keys remain the same.

The TPT_KEY is bound to the device version and independent of the firmware version. Updating the firmware does not change any key within the secure key store.

2.5 What is the difference between "xx.0x" and "xx.Fx" firmware version?

NXP always publishes two different firmware files for one version. The firmware file with "F" in its name is not updating the user settings area. The firmware update file with "0" instead of "F" always updates all the user settings as well.

PN7642Firmware_02.**0**0.esfwu → Is updating user configuration. Can be used to revert to factory settings.

PN7642Firmware_02.**F**0.esfwu → Is not updating user configuration. Can be used after you have configured your PN7642 to your hardware.

2.6 What is the difference between PN7642 C100 and C101?

The PN7642 is available in two versions: C100 and C101. The major difference between the two versions is the default configuration of PN7642, and not necessarily the firmware version.

- **C100**
  - Firmware version: v01.00
  - *Pin-less download*: **disabled** by default
- **C101**
  - Firmware version: v02.00
  - *Pin-less download*: **enabled** by default

The *Pin-less download* feature sets whether PN7642 probes DWL_REQ at boot-up to go to bootloader mode or not.

- If *Pin-less download* is disabled, PN7642 goes to bootloader mode only if DWL_REQ is high while booting.
- If *Pin-less download* is enabled, at power-on reset (POR), PN7642 goes to bootloader mode. To listen for bootloader commands, PN7642 remains in bootloader mode for some time (500 ms by default).

If PN7642 version C100 is updated with the same firmware version as PN7642 version C101, both versions have the same functionality. The only difference is the default configuration of the *Pin-less download* feature.

For firmware version v02.00 and above, the *Pin-less download* feature can be enabled on PN7642 version C100 with the API *PN76_Sys_OTPConfigs_EnableDwnldReqLessBoot()*.

Note: *OTP stands for One Time Programmable and is not reversible!*

CAUTION: *If Pin-less download is enabled— either via the API on PN7642 version C100, or by default on PN7642 version C101— USB Mass-storage mode (USB download) is not available.*

3 Secure key store and cryptography

3.1 What is the SKM?

The acronym SKM stands for "Secure Key Mode". The secure key mode is a special mode of the PN7642, where you open a session to interact with the secure key store. Only if a valid session in the secure key mode is opened, keys can be provisioned, deleted, and purged from the secure key store.

3.2 When is the SKM authentication counter increased?

The authentication counter in SKM is increased:

1. If the challenge and response are proper.
2. If the challenge and response are not proper, or if invalid values are used for the key (128-bit or 256-bit key).
3. Any internal errors (failures) are returned by the crypto algorithms for decryption of the challenge, or for access to key store/internal SGI IPs.
4. Any internal error results in secure memory read comparison.

In all these conditions, the authentication counter is increased when APIs are called or when SKM boot mode is entered to work on keys.

3.3 Key store is locked, what can I do?

Once the key store is locked, it stays locked. There is no way to unlock the key store. All provisioned keys can be used and purged. But no new authentication to the key store is possible.

The counter for faulty authentications is not reset by any action. After ten unsuccessful authentications, the key store is locked.

Take special care with the examples, like the MIFARE DESFire example, that the correct TPT_KEYs are set.

Note: *In early versions of the SDK, the TPT_KEYs have not been set correctly. Running the MIFARE DESFire example without changing the TPT_KEY results in a failed authentication.*

3.4 When can I provision a APP_MASTER_KEY?

Provisioning of the secure key store is only possible if the secure key store is not locked and you must provision the APP_ROOT_KEY first.

- If the key store is locked, no further provisioning is possible. Keys within the key store are still valid and can be used, but no new key can be provisioned.
- If the APP_ROOT_KEY is not provisioned, the default TPT_KEYS (transport keys available in PN7642 data sheet) are still active. Provision both 128-bit and 256-bit APP_ROOT_KEYs before you provision any other key.

To obtain the SKM state, use the API "**PN76_Sys_SKM_Get_SKM_Info()**" which returns the SKM state (Figure 1).

◆ bSkmState

uint8_t PN76_SKM_Data_SKM_Info_t::bSkmState

Secure Key Mode locked out status.

Bits	Values	Description
[0]	0x00	SKM is not locked.
	0x01	SKM is locked. Application will not be able to operate on application keys.
[3:1]	0x00	Reserved for future use.
[5:4]	0x00	Application root key 128-bit is not provisioned.
	0x01	Application root key 128-bit is provisioned.
	0x02	Application root key 128-bit is locked from further provisioning.
	0x03	Application keys are purged.
[7:6]	0x00	Application root key 256-bit is not provisioned.
	0x01	Application root key 256-bit is provisioned.
	0x02	Application root key 256-bit is locked from further provisioning.
	0x03	Application keys are purged.

Figure 1. SKM state

For how to work with the secure key mode (SKM) to provision the key store, use *pnev7642fama_pn_skm* example available in the SDK. And read the application note [2].

4 Host interface

4.1 What can I do if PN7642 does not answer on HIF I2C?

In the bootloader, PN7642 uses the values of ATX_C (I^2C Adr Bit 0) and ATX_D (I^2C Adr Bit 1) to set the I^2C address.

For more information about I^2C addressing and the I^2C host interface functionality, refer to [1].

I^2C_ADR1	I^2C_ADR0	I^2C address (R/W = 0, write)	I^2C address (R/W = 0, read)
0	0	0x28	0x28
0	1	0x29	0x29
1	0	0x2A	0x2A
1	1	0x2B	0x2B

Figure 2. I^2C interface addressing

5 Software

5.1 Difference between *libintfs.a* and *intfs.a* in the SDK?

Both *libintfs.a* and *intfs.a* libraries are available in the SDK.

The two libraries serve the same purpose, have the same content, but comply with different toolchain requirements. If you must use one library, pick any of the two available in the SDK.

5.2 NFC Cockpit is not working. What can I do?

Refer to the section *Firmware overview* in [3].

The NFC Cockpit application (*.bin*) is compiled for a particular firmware version of PN7642. Major firmware versions are not compatible because of API address changes. For example, the NFC Cockpit application compiled for PN7642 FW v1.0 does not run on PN7642 with firmware v2.0.

5.3 Why is the SDK not working with VSC?

Even though the MCUXpresso Visual Studio Code (VSC) extension is available, not all SDK versions are compatible. For example, PN7642 SDK version vxx.*12*.xx is not compatible. To be supported by the VSC extension, the SDK minimum version must be 14 (xx.14.xx).

Updates are planned to make the PN7642 SDK VSC compliant. There is no timeline.

5.4 Why can't I see any output in the IDE console?

When importing an example from the SDK, you can choose the debug console. If the *SDK Debug Console* is 'Semihost', the debug output is in the IDE console. If *SDK Debug Console* is 'UART', the debug output can be grabbed on the debug UART.

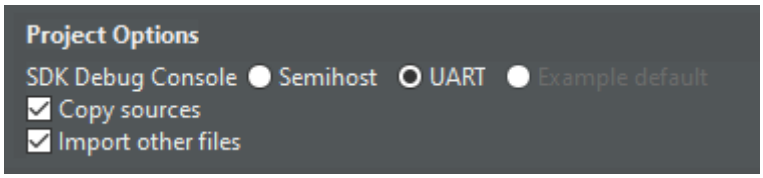

Figure 3. Example of project configuration for debug console

If you do not see any output in your MCUXpresso IDE console, cross-check the settings. You can change the settings for an example you have already imported.

- Go to the *Quickstart Panel*.
- Select *Quick Settings*.
- Select *SDK Debug Console*.
- Select *Semihost console* or *UART console*.

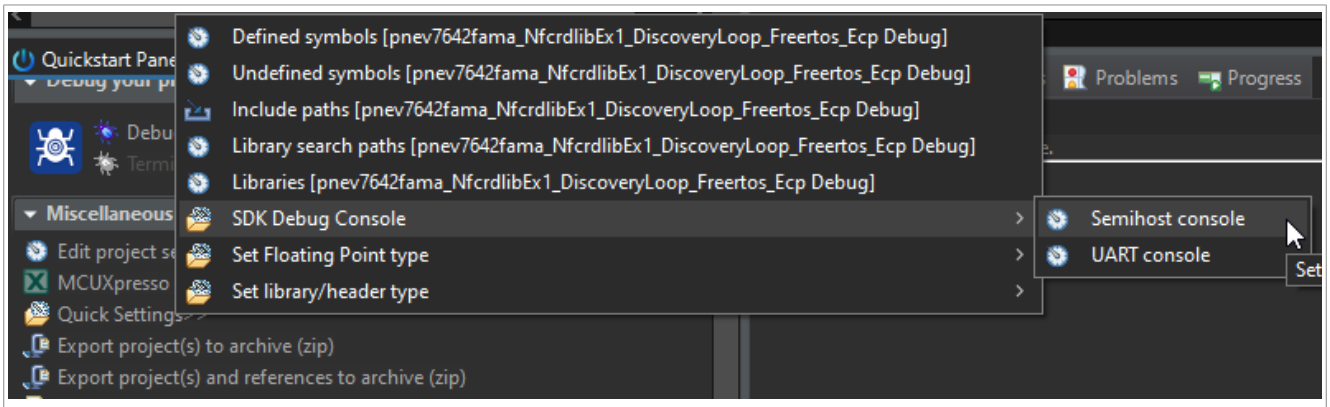

Figure 4. Quick settings for debug console

5.5 My examples are crashing. What to do?

Most examples rely on the underlying libraries. The libraries are built for a specific PN7642 firmware version. If the firmware version of PN7642 does not match the firmware version used by the SDK, all kinds of issues and unexpected behavior can occur.

For details on compatibility, refer to the section *Firmware overview* in [3]. And either update the firmware of your PN7642 to the SDK firmware, or use the correct SDK version for you PN7642.

6 Documentation

6.1 Where do I find the API documentation?

The *PN7642 NFC Controller User API Documentation* is part of the SDK package. If you and open

- Unzip the SDK package.
- Open the *docs* directory.
- Unzip *PN76-FW-apiguide.zip*.
- Open the *index.html* file.

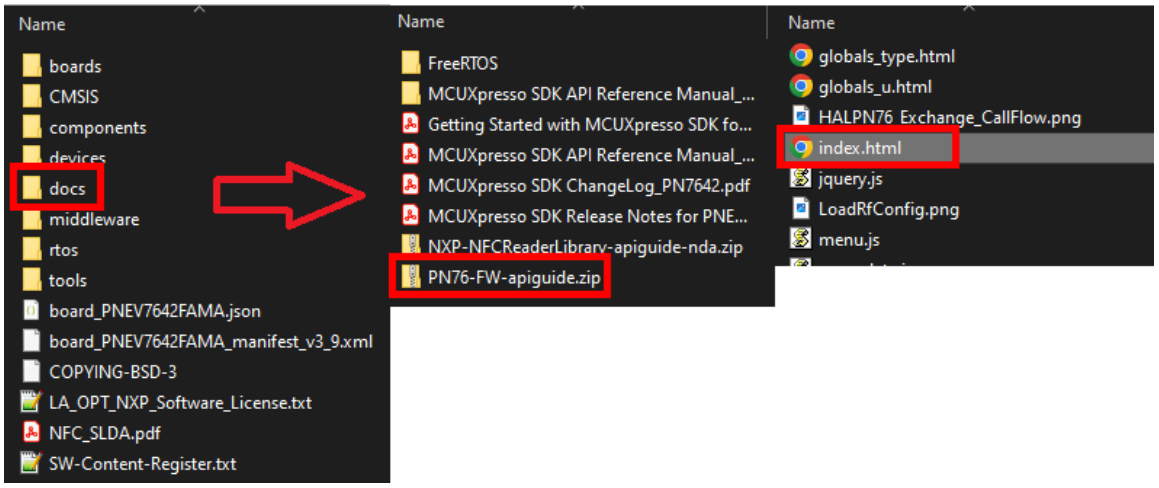

Figure 5. PN7642 API documentation location

The API documentation is generated with DoxyGen out of the actual SDK source code.

7 Abbreviations

Table 1. Abbreviations

Acronym	Description
ESFWU	Encrypted secure firmware update
HIF	Host interface
KS	Key store
OTP	One time programmable
POR	Power-on reset
SKM	Secure key mode
TPT_KEY	Transport key

8 References

[1] Data sheet - PN7642 - Single chip solution with high-performance NFC reader, customizable MCU, and security toolbox
[2] AN13720 - PN7642 Secure Key Mode demo application
[3] AN13134 - PN76 family evaluation board quick start guide

9 Revision history

Table 2. Revision history

Document ID	Release date	Description
AN13936 v.1	29 February 2024	• 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.

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.

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.

DESFire — is a trademark of NXP B.V.

EdgeVerse — is a trademark of NXP B.V.

FeliCa — is a trademark of Sony Corporation.

ICODE and I-CODE — are trademarks of NXP B.V.

I2C-bus — logo is a trademark of NXP B.V.

MIFARE — is a trademark of NXP B.V.

MIFARE Classic — is a trademark of NXP B.V.

MIFARE Plus — is a trademark of NXP B.V.

MIFARE Ultralight — is a trademark of NXP B.V.

Tables

Figures

Contents

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

Date of release: 29 February 2024
Document identifier: AN13936