RN00257

PN7642 firmware release notes v02.06

Rev. 2.1 — 3 July 2025   **Release notes**

Document information

Information	Content
Keywords	PN7642, firmware, release notes
Abstract	Release notes of the PN7642 secure firmware. Covering issue fixes and new feature implementation.

1   Document purpose

The document describes the contents of the PN7642 IC secure firmware. It covers the release summary, release history, known issues, work-arounds, limitations, and recommendations.

2 Features supported in this release

2.1 System services

System services are APIs provided by NXP to the customer for the functions described below.

These APIs are implemented as part of a secure firmware embedded within the secure region of the flash that executes in secure CPU mode. These APIs shall be Non-Secure Callable.

The APIs can be broadly divided into the following categories.

Table 1. System services

Category	Services	Feature availability
In-application programming	Programming the application flash areas	Yes
In-application encrypted FW download	Encrypted FW download of NXP FW and customer FW for hostless designs	Yes
One-time programmable life cycle management	The customer can enable/disable the product life cycle parameters permanently at the various product development stages.	Yes
CLIF HAL/instruction	APIs to work with RF Interface system	Yes
PCRM HAL	APIs to work with Power and Clock configurations of the PN7642 family	Yes
Symmetric crypto wrapper	APIs to work with symmetric crypto operations (AES ECB, CBC 128/256, CTR, CCM, GCM/GMAC, 3DES, CMAC (for AES, 3DES) SHA(256,384,512), Secure SHA (256,384,512), HMAC, HKDF, RNG)	Yes
Asymmetric crypto wrapper	APIs to work with ECC operations (ECCKeyGen, ECDSASign, ECDSAVerify, and ECDH for curves SECP256-r1, SECP384-r1, BP256-r1, BP384-r1, Custom curves, EdDsa signature verification for Edward curve, EDDSaMont DH, RSA (keygen, encrypt, decrypt, sign, verify))	Yes
Symmetric key store	Symmetric Key Store (128/256) provisioning operations, loading, unloading, locking	Yes
Asymmetric key store	Asymmetric Key Store (ECC keys) provisioning operations, loading, unloading.	Yes
Utility/Helper interfaces	APIs to retrieve IC FW/SW component versions, CRC, and test bus components	Yes

2.2 System feature list

2.2.1 Bootloaders and key provisioning

Table 2. Bootloaders and key provisioning

Feature	System SW	Validation status
Encrypted secure firmware update of NXP code and data using NXP keys	Available	Functional verified
Encrypted secure firmware update of customer code and data using customer keys	Available	Functional verified

Table 2. Bootloaders and key provisioning...*continued*

Feature	System SW	Validation status
In-application encrypted secure firmware update of NXP code and data using NXP keys	Available	Functional verified
In-application encrypted secure firmware update of customer code and data using customer keys	Available	Functional verified
Plain firmware download of customer code and data using USB mass storage mode	Available	Functional verified
Secure key provisioning of customer download and application keys (symmetric and asymmetric)	Available	Functional verified

2.2.2 System interface (SysHAL)

Table 3. System interface (SysHAL)

Feature	System SW	Validation status
GPIO	Available	Functional verified
CLIF TX driver	Available	Functional verified
VDDPA LDO	Available	Functional verified
DC-DC control	Available	Functional verified
GPADC control	Available	Functional verified
RF clock control	Available	Functional verified
RNG	Available	Functional verified
CRC	Available	Functional verified
Secure Key Mode Provisioning (symmetric and asymmetric keys)	Available	Functional verified

2.2.3 Platform drivers (HAL) within MCUXpresso SDK

Table 4. Platform drivers (HAL)

Feature	System SW	Validation status
CLIF	Available	Functional verified
CRC	Available	Functional verified
Host interface (SPI, I2C, UART)	Available	Functional verified
NVIC	Available	Functional verified
SysTick	Available	Functional verified
General-purpose TIMER	Available	Functional verified
Watchdog Timer	Available	Functional verified
CLOCK, POWER	Available	Functional verified
USB	Available	Basic verified
GPIO	Available	Functional verified
SCT(PWM)	Available	Functional verified
Generic DMA	Available	Functional verified

RN00257

All information provided in this document is subject to legal disclaimers.

© 2025 NXP B.V. All rights reserved.

Release notes **Rev. 2.1 — 3 July 2025**

Document feedback

4 / 22

Table 4. Platform drivers (HAL)...*continued*

Feature	System SW	Validation status
SPI controller with DMA	Available	Functional verified
I^{2}C controller with DMA	Available	Functional verified
UART with DMA	Available	Functional verified
GPADC	Available	Functional verified

2.2.4 Contactless interface

Table 5. Contactless interface

Feature	System SW	Validation status
Reader Mode ISO14443-A (106/212/424/848 kbit/s)	Available	Functional and RF performance verified
Reader Mode ISO14443-B (106/212/424/848 kbit/s)	Available	Functional and RF performance verified
Reader Mode FeliCa (212/424 kbit/s)	Available	Functional and RF performance verified
Reader Mode ISO15693	Available	Functional and RF performance verified
Reader Mode ISO18000p3m3	Available	Functional and RF performance verified
Card Mode ISO14443-A (106/212/424/848 kbit/s)	Available	Functional and RF performance verified
T4T	Available	Functional and RF performance verified
Dynamic Power Control (2.0, 3.0)	Available	Functional and RF performance verified
Automatic Waveshape Control	Available	Functional and RF performance verified
Automatic Receiver Control	Available	Functional and RF performance verified
Internal DC-DC for TX driver	Available	Functional and performance verified
Trimming of RF parameters	Available	Functional and RF performance verified
ISO10373-PCD digital compliance	Available	Verified with Micropross digital compliance
ISO10373-PICC digital compliance	Available	Verified with Micropross digital compliance
ISO14443-PCD analog compliance	Available	Verified with Micropross digital compliance
ISO14443-PICC analog compliance	Available	Verified with Micropross digital compliance
NFC Forum CR13 Reader digital compliance	Available	Verified with Micropross digital compliance

Table 5. Contactless interface...*continued*

Feature	System SW	Validation status
NFC Forum CR13 T4T Card mode digital compliance	Available	Verified with Micropross digital compliance
NFC Forum CR13 Reader analog compliance	Available	Verified with Micropross analog compliance
NFC Forum CR13 T4T Card mode analog compliance	Available	Verified with Micropross analog compliance

2.2.5 Contact interface

Table 6. Contact interface

Feature	System SW	Validation status
EMVCo digital compliance specification 4.3c for contact interface	Available	Functional and performance verified
ISO compliance for contact interface	Available	Functional and performance verified
Contact Interface for T=0, T=1 protocols	Available	Functional and performance verified
Multislot support for contact interface. Each slot supports EMVCo and ISO profiles.	Available	Functional and performance verified
Support for ID1 slot and SIM slot	Available	Functional and performance verified

2.2.6 USB interface

Table 7. USB Class drivers and compliance

Feature	System SW	Validation status
USB Mass storage class driver	Available	Functional verified
USB VCOM/CDC class driver	Available	Functional verified
USB CCID/PCSC class driver	Available	Functional verified for contactless interface and contact interface
USB 2.0 Digital Compliance	Available	Functional verified
USB 2.0 Electrical Compliance	Available	Functional verified with USB CCID Contactless class driver with internal PVDD configuration.

2.2.7 Mbed Crypto interfaces

Table 8. Mbed Crypto interfaces

Feature	System SW	Validation status
Encryption and decryption based on AES (128, 256) CBC mode	Available	Functional verified
Encryption and decryption based on AES (128, 256) ECB mode	Available	Functional verified
Encryption and decryption based on AES (128, 256) CCM mode	Available	Functional verified

Table 8. Mbed Crypto interfaces...*continued*

Feature	System SW	Validation status
Encryption and decryption based on AES (128, 256) CTR mode	Available	Functional verified
Encryption and decryption based on AES (128, 256) GCM/GMAC mode	Available	Functional verified
Encryption and decryption based on AES (128, 256) EAX mode	Available	Functional verified
Encryption and decryption based on 3DES ECB with key length 2key3DES, 3key3DES	Available	Functional verified
Encryption and decryption based on 3DES CBC with key length 2key3DES, 3key3DES	Available	Functional verified
CMAC for AES (128, 256) and 3DES	Available	Functional verified
CBC CMAC for 3DES	Available	Functional verified
SHA-256 Hash	Available	Functional verified
SHA-384 Hash	Available	Functional verified
SHA-512 Hash	Available	Functional verified
Secure SHA-256 Hash	Available	Functional verified
Secure SHA-384 Hash	Available	Functional verified
Secure SHA-512 Hash	Available	Functional verified
HMAC SHA-256 Hash	Available	Functional verified
HMAC Hash	Available	Functional verified
HKDF	Available	Functional verified
Random Number Generator	Available	Functional verified
Asymmetric key generation (ECCKeygen) for curves SECP256-r1, SECP384-r1, BP256-r1, BP384-r1, Generic custom curves	Available	Functional verified
Signature generation and verification based on Asymmetric key (ECDSASign, ECDSAVerify) for curves SECP256-r1, SECP384-r1, BP256-r1, BP384-r1, Generic custom curves	Available	Functional verified
ECDSA compute public key	Available	Functional verified
ECDH for curves SECP256-r1, SECP384-r1, BP256-r1, BP384-r1, Generic custom curves	Available	Functional verified
EdDsa signature generation and verification for Edward curve (25519)	Available	Functional verified
EdDsa MontDH generation and exchange for Edward curve (25519)	Available	Functional verified
RSAKeygen and RSA public/private operations with 1526, 2048 and 3076 key bits	Available	Functional verified
Encryption and decryption of PKCS1.5 with 1526, 2048 and 3076 key bits	Available	Functional verified
Signature generation and verification of PKCS1.5 with 1526, 2048 and 3076 key bits	Available	Functional verified

Table 8. Mbed Crypto interfaces...*continued*

Feature	System SW	Validation status
Encryption and decryption of OAEP with 1526, 2048 and 3076 key bits	Available	Functional verified
Signature generation and verification of OAEP with 1526, 2048 and 3076 key bits	Available	Functional verified
ECC point addition for curves SECP256-r1, SECP384-r1, BP256-r1, BP384-r1, generic custom curves	Available	Functional verified
ECC Math operations (DIVIDE, SECUREMODMULT, SECUREMODSUB, SECUREMODADD, SECUREMODINV, SECUREADD, SECURECOMPARE)	Available	Functional verified

2.2.8 Secure Key Management (Secure Key Mode and System Services APIs)

Table 9. Secure Key Management (Secure Key Mode and System Services APIs)

Feature	System SW	Validation status
Provisioning of APP_ROOT_KEY (128, 256-bit) storage in Secure Key Store	Available	Functional verified
Provisioning of APP_MASTER_KEY (128, 256-bit) storage in Secure Key Store	Available	Functional verified
Provisioning of APP_FIXED_KEY (128, 256-bit) in extended key store	Available	Functional verified
Update of APP_MASTER_KEY and APP_FIXED_KEY (128, 256-bit) for Modify and Delete operations	Available	Functional verified
Host authentication using APP_ROOT_KEY(128, 256-bit) for Key provisioning and update	Available	Functional verified
Locking of APP_ROOT_KEY (128, 256-bit) from further provisioning	Available	Functional verified
Provisioning of APP_ASYMM_KEY (for curves SECP256-r1, SECP384-r1, BP256-r1, BP384-r1, custom-curves) in extended software key store	Available	Functional verified
Deletion of APP_ASYMM_KEY (for curves SECP256-r1, SECP384-r1, BP256-r1, BP384-r1, custom-curves) operations in extended software key store	Available	Functional verified
Purge of Application keys (both symmetric and asymmetric keys)	Available	Functional verified

2.2.9 Example applications

For the full list of applications for PN7642, refer to SDK release notes.

2.2.9.1 Compliance applications

Table 10. Compliance applications

Feature	System SW	Validation status
Contactless NxpNfcRdLib EMVCo loopback Compliance App	Available	Functional verified

RN00257
Release notes

All information provided in this document is subject to legal disclaimers.

Rev. 2.1 — 3 July 2025

© 2025 NXP B.V. All rights reserved.

Document feedback

8 / 22

Table 10. Compliance applications...*continued*

Feature	System SW	Validation status
Contactless NxpNfcRdLib ISO10373-PCD Compliance App	Available	Functional verified
Contactless NxpNfcRdLib ISO10373-PICC Compliance App	Available	Functional verified
Contactless NxpNfcRdLib EMVCo loopback Compliance App (Analog)	Available	Functional verified
Contactless NxpNfcRdLib EMVCo loopback InterOp App	Available	Functional verified
Contact Interface CtRdLib EMVCo loopback Compliance App	Available	Functional verified
NFC Forum DTA Compliance App	Available	Functional verified

2.2.9.2 Reader Library examples

Table 11. Reader Library examples

Feature	System SW	Validation status
Contactless NfcrdlibEx1_DiscoveryLoop	Available	Functional verified
Contactless NfcrdlibEx2_ECP	Available	Functional verified
Contactless NfcrdlibEx3_NFCForum	Available	Functional verified
Contactless NfcrdlibEx4_MIFAREClassic	Available	Functional verified
Contactless NfcrdlibEx5_ISO15693	Available	Functional verified
Contactless NfcrdlibEx6_LPCD	Available	Functional verified
Contactless NfcrdlibEx7_MIFAREPlus	Available	Functional verified
Contactless NfcrdlibEx8_HCE_T4T	Available	Functional verified
Contactless NfcrdlibEx9_NTagI2C	Available	Functional verified
Contactless NfcrdlibEx10_MIFAREDESFire_EVx	Available	Functional verified
Contactless Nfcrdlib_SimplifiedAPI_ISO	Available	Functional verified
Contactless NfcrdlibEx_TypeBprime	Available	Functional verified
USB-CCID Example with contactless interface	Available	Functional verified
USB Dual-CCID Example with contact and contactless interface	Available	Functional verified

2.2.9.3 Contact Reader Library examples

Table 12. Contact Reader Library examples

Feature	System SW	Validation status
Contact RdLib based Example with EMVCo supported contact cards	Available	Functional verified
Contact RdLib based Example with ISO7816 based contact cards	Available	Functional verified
USB CCID Example with contact interface	Available	Functional verified

2.2.9.4 PN76 specific examples

Table 13. PN76 specific examples

Feature	System SW	Validation status
FreeRTOS Example	Available	Functional verified
Host Interface (SPI and I2C) Example	Available	Functional verified
NFC configuration Example	Available	Functional verified
Low-Power Mode execution Example	Available	Functional verified
EmbedCrypto Example(Symmetric, hash and Asymmetric)	Available	Functional verified
PRBS(Pseudo Random Binary Sequence) Example	Available	Functional verified
Secure Key Mode Example	Available	Functional verified
User data download Example	Available	Functional verified
Secondary bootloader with Host-less secure FW update Example	Available	Functional verified

RN00257

Release notes

All information provided in this document is subject to legal disclaimers.

Rev. 2.1 — 3 July 2025

© 2025 NXP B.V. All rights reserved.

Document feedback

10 / 22

3 Release history

The following sectiosn provide a list of issues resolved, changes performed, and features implemented in the according releases.

3.1 v02.06

Table 14. Firmware updates from v02.05 to v02.06

SI No.	Description
1	Resolved the issue of IAP download of NXP FW/Customer FW.
2	Resolved the issue of LPCD and ULPCD wake-up timer variation issue at corner cases.
3	Improvement in handling of FW version update during FW download/IAP download mode.
4	Resolved the issue of higher power consumption in ULP modes.
5	Resolved the implementation of the PN76_Sys_Hal_SoftReset() API. Now in-line with documentation.
6	Increased the secure stack availability for application tasks from existing 1792 (0x700) to 2560 (0xA00) bytes.
7	Resolved the inconsistency in behaviour of ARC, if DPC is disabled.

3.1.1 SI No. 1

Summary:

Resolved the issue of IAP download of NXP FW/Customer FW.

Details:

The In-Application Programming (IAP) download from user application space is using the same bootloader routine as the firmware update via host-interface. The bootloader is checking the host interface buffers and if a valid command code is found the PN7642 is switched to host interface polling mode. From this point onwards, a firmware update is only possible by using the host-interface as the chip does not boot into application mode.

With this update, the host interface buffers are not probed by using IAP download.

Downgrade:

Due to the IAP fix, a downgrade, to v02.XY, will not succeed at 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 (see ref.[3]).

A consecutive update to the desired firmware version will succeed.

Note: It is not recommended to downgrade form v02.06 to any previous version.

3.2 v02.05

Table 15. Firmware updates from v02.03 to v02.05

SI No.	Description
1	Resolved the issue of an GPADC_READY_TIMEOUT error at ULPCD operation by relaxing internal timings and crystal requirements to give a bigger margin and window of operation.
2	LPCD and ULPCD wake-up timer variation issue minimized by adding LFO and ULFO trimming.
3	New EEPROM configuration for enabling LFO and ULFO trimming added. `ENABLE_ULFO_TRIM_CALIBRATION(068E)` and `ENABLE_LFO_TRIM_CALIBRATION(068F)`
4	RFLD and NFCLD calibration is moved from `PN76_Sys_Clif_Init()` to a new NSC API `PN76_Sys_Configure_RFLD_NFCLD`. Application must call this API as part of configuration of PN7642.
5	Fixed an issue of interference of RF with UART RX signal when the UART as HIF is used.
6	System service APIs `mbedtls_ecdsa_sign_stz()` and \ref `mbedtls_ecdsa_verify_stz()` are deprecated. Instead, the application must use APIs `mbedtls_ecdsa_sign_stz_flash()` and `mbedtls_ecdsa_verify_stz_flash()` if these are being used by the applications. If applications use standard mbedTLS interfaces, no changes are required.

3.2.1 SI No. 1

Summary:

Resolved the issue of GPADC_READY_TIMEOUT error at ULPCD operation by relaxing internal timings and crystal requirements to give a bigger margin and window of operation.

Details:

After thorough investigation, NXP has concluded that strict GPADC timing requirements and the variety of crystals available in the market have triggered GPADC_READY_TIMEOUT error. During the investigation, the complete crystal block has been reanalyzed and validated by NXP.

During this validation campaign, we also adjusted GPADC timings to relax the requirements of crystals and give margin to temperature drifts and manufacturing spread for crystal/clock startup circuit stability. This adjustment of the GPADC timing is incorporated in firmware v02.05.

ref.[2] mentions NXP recommended crystals which are fully validated by NXP. Adjusting GPADC timing may allow a broader range of crystals as well, however, NXP has not validated them. In this case, customers are required to perform thorough validation in their design with these crystals.

3.2.2 SI No. 4

Summary:

RFLD and NFCLD calibration is moved from `PN76_Sys_Clif_Init()` to a new NSC API `PN76_Sys_Configure_RFLD_NFCLD`. Application must call this API as part of the configuration of PN7642.

Details:

The FW version **v02.05/v02.F5** consists of a change in the behavior of API `PN76_Sys_Clif_Init()`. The RFLD/NFCLD calibration is moved to a new API `PN76_Sys_Configure_RFLD_NFCLD()`. If FW version **v02.05/v02.F5** is used, the application must ensure that RFLD/NFCLD calibration is performed after the FW update to this version. Failure to perform this operation may result in suboptimal NFC performance.

RN00257

All information provided in this document is subject to legal disclaimers.

© 2025 NXP B.V. All rights reserved.

Release notes

Rev. 2.1 — 3 July 2025

Document feedback

12 / 22

3.3 v02.04

Not publicly released. Changes are part of v02.05.

3.4 v02.03

Table 16. Firmware updates from v02.02 to v02.03

Sl No.	Description
1	Fixed an issue of instability of detecting load change during static conditions of card detection.

3.5 v02.02

Table 17. Firmware updates from v02.00 to v02.02

Sl No.	Description
1	This FW is compatible with FW v02.00.
2	Fixed issues in card mode of operation.
3	Fixed an issue where in call to API `PN76_Sys_UpdateRfConfiguration()` and `PN76_Sys_RetrieveRfConfiguration()` fails when used for TX index `E_PN76_LOADRF_TX_ISO180003M3_TARI_9_44_ASK` and `E_PN76_LOADRF_TX_ISO180003M3_TARI_18_88_ASK`.
4	USB download mode is disabled when the pinless download mode feature is enabled, even if USB_VBUS is present.
5	New APIs `PN76_Sys_Set_HIF_Timeout()` and `PN76_Sys_Get_HIF_Timeout()` added to update/get the timeout values for waiting for HIF commands in case the pinless download feature is enabled.
6	Implemented CT as a wake-up source during standby wake-up.
7	New API `PN76_Sys_Configure_TestBus_MultipleDigital()` for configuring multiple available digital test bus signal on selected pad configurations.

3.6 v02.01

Not publicly released. Changes are part of v02.02.

3.7 v02.00

Table 18. Firmware updates from v01.00 to v02.00

Sl No.	Title
1	PN7642 FW maintenance release. This FW is not compatible with FW v01.00. Applications must be recompiled with this FW.
2	Updated support for FreeRTOS kernel V10.5.0 from FreeRTOS kernel LTS Patch 2.
3	Added support for USB-CCID class suspend and resume operation for USB certification (chapter9 and electrical compliance). Added new API `PN76_Sys_Hal_USB_Suspend()`: Provides functionality for a USB suspend operation and resume after suspend.
4	Added new API `PN76_Sys_GetPartId()`: Provides information about the PN7642 IC part number.
5	Added a new API `PN76_Sys_OTPConfigs_EnableDwnldReqLessBoot()`: Provided for entering into HIF polling mode (download mode/Secure Key mode) without DWL_REQ pin configuration.
6	Added support for FW upgrade with Chunk-bit in frame header.

Note: *Default firmware of chip C101.*

3.8 v01.00

Table 19. Initial firmware v01.00

SI No.	Title
1	Production PN7642 FW release.
2	Corrected USB-PID and USB-VID for PN7642.
3	Added support for adding delay to cover inrush current when PVDD LDO is enabled.
4	Added support for FreeRTOS kernel V10.4.3 LTS Patch 2.

Note: *Default firmware of chip C100.*

RN00257

All information provided in this document is subject to legal disclaimers.

© 2025 NXP B.V. All rights reserved.

Release notes **Rev. 2.1 — 3 July 2025**

Document feedback

14 / 22

4 Firmware upgradeability and downgradeablity

A firmware upgrade is possible, without replacing the earlier provisioned application keys.

Once a firmware upgrade is completed, a downgrade is only possible within a minor version.

Refer to ref.[1] for more information about firmware updates.

Note: There are known limitations for downgrading from firmware v02.06 to v02.XY. See Section 3.1.1 "SI No. 1".

5 Known limitations and recommendations

Table 20. Known limitations, precautions, and recommendations

Limitation	Recommendation
TX driver may be damaged due to overcurrent.	Do not disable DPC on PN7642.
OTP settings are not applied properly.	When working with OTP group APIs, it shall be executed under stable power conditions. VEN toggling, VBAT loss during OTP API execution, may result in performance degradation or IC not booting to application main().
Application mode is not entered after USB FW upload interruption.	Retry USB FW upload again under stable power conditions.
PN7642 IC not entered into application main().	Halt the IC and check the PC. If it is 0x20003002, then the valid application reset vector table is not present. Try if re-flashing the FW solves the issue.
Firmware downgrade from v02.06 to v02.XY	See Section 3.1.1 "SI No. 1".

6   References

[1]   Application note – AN14540 – Firmware update on PN7642 (link)
[2]   Application note – AN14518 – Crystal Oscillator Design Guide (link)
[3]   User Manual - UM11905 - PN7642 instruction layer manual (link)

7 Revision history

Table 21. Revision history

Document ID	Release date	Description
RN00257 v.2.1	3 July 2025	• Added firmware v02.06 downgrade notes in Section 3.1.1 "SI No. 1", Section 5 "Known limitations and recommendations" and Section 4 "Firmware upgradeability and downgradeablity".
RN00257 v.2.0	21 May 2025	• Section 2.2.9.1 "Compliance applications": "NFC Forum DTA Compliance App" added. • Section 3 "Release history": Section 3.1 "v02.06" added.
RN00257 v.1.0	30 January 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.

RN00257

All information provided in this document is subject to legal disclaimers.

© 2025 NXP B.V. All rights reserved.

Release notes

Rev. 2.1 — 3 July 2025

Document feedback

19 / 22

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

Contents