RN00062

PN7642 software package v01.00

Rev. 1.1 — 14 March 2023 Release notes

Document information

Information	Content
Keywords	PN7642, generic NFC open controller
Abstract	Contains information about a specific release product and component information

1 Revision history

Revision history

Rev	Date	Description
1.1	20230314	Security status changed into public
1.0	20230221	• First official release The master/slave replacement into controller/target in this document follows the recommendation of the NXP - I2C standards organization.

2 Document purpose

The document describes the contents of the PN7642 IC secure firmware and software release.

The release contains:

- PN7642 IC secure firmware
- LPC55s16 based host software demo examples to show the features of PN7642
- A separate MCUXpresso based SDK package available with example applications for PN7642

This document describes the release summary, release history, known issues, work-arounds, limitations, and recommendations.

3 PN7642 system software layers

System software components are delivered in this release as shown below:

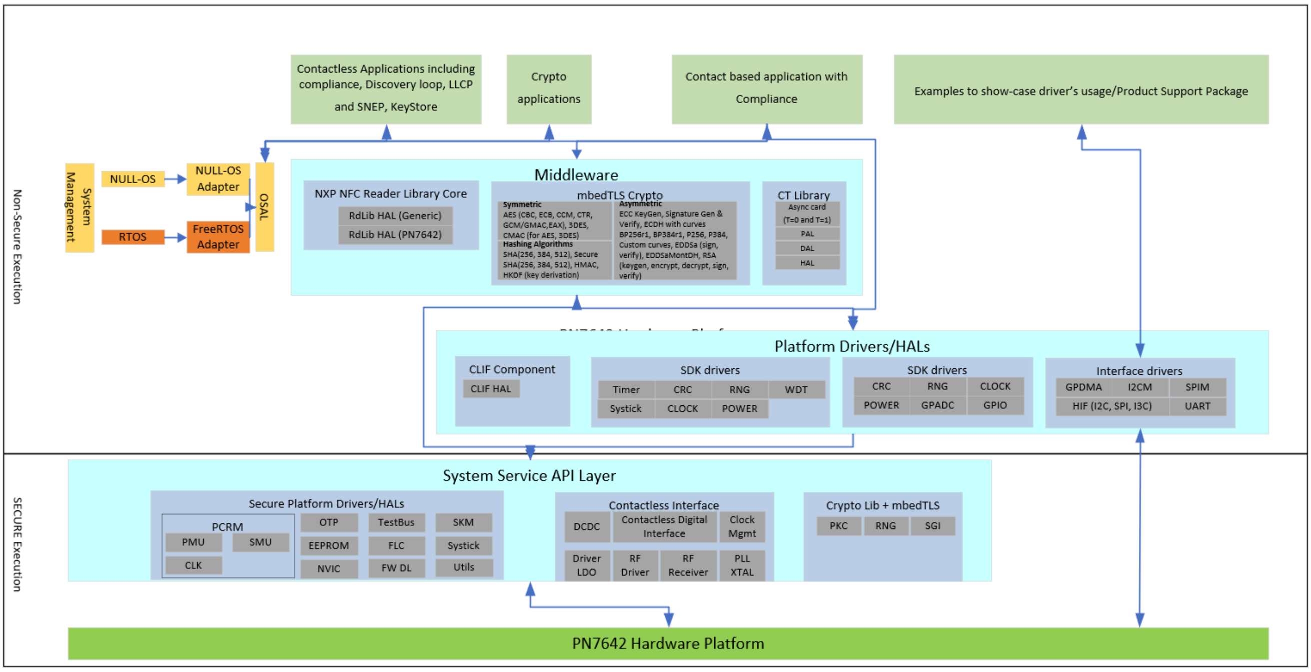

Figure 1. PN7642 system software layer

4 Validation platform used for testing the PN7642 software

Board / IC: PNEV7642FAMA revA board with PN7642 IC

PN7642 software package version (including host utilities): v01.00

NXP secure firmware version: v01.00

MCUXpresso SDK: SDK version: 2.12.1 (01.00.00 08.11.2022)

MCUXpresso IDE: v11.7.0

Host platform:

- Windows 10 Enterprise x86
- macOS X (ProductVersion: 10.14.6, BuildVersion:18G8012)
- Embedded Host Platform LPC55S16

Device platform: CortexM-33 based controller with FreeRTOS(version 10.4.3) integration and NullOS integration.

5 Development tools used for validation

Table 1. Development tools used for validation

Tool	Recommended version
Debugger Tool	SEGGER JLink/JTrace debugger software suite v7.82e* onwards (that includes SEGGER RTT viewer)
MCUXpresso IDE	Host software development and debug. MCUXpresso IDE v11.7.0 for Windows and macOS
Custom Scripts	Provided as part of the release package

6 Release package contents

Following table shows the locations of various components delivered in the release package, when it is extracted.

Table 2. Release package contents

Components	Location
Various documents to work with (application note, user guide and so on)	`<extracted_dir>\Docs`
PC-based Scripts/various inputs required to work with Host software examples	`<extracted_dir>\Host_Software\Scripts`
Examples and Demo applications to show the features of PN7642 on LPC55S16 platform Secure FW Downloader application Secure Key Mode Demo application on Host (LPC55S16) HIF Example Counterpart application	`<extracted_dir>\Host_Software\ucHost_Utils`
	`<extracted_dir>\Host_Software\ucHost_Utils\Secure_Fw_Downloader`
	`<extracted_dir>\Host_Software\ucHost_Utils\SKM_DemoApp`
	`<extracted_dir>\Host_Software\ucHost_Utils\HifEx_Counterpart`
Encrypted Secure Flash firmware for PN7642 IC	`<extracted_dir>\PN7642_FW`
PN7642 IC SDK	Release package available via NXP website

7 Features supported in this release

7.1 System services

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

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

The APIs can be broadly divided into following categories.

Table 3. 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 customers 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 (128/256) Store 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

7.2 System feature list

7.2.1 Boot loaders and key provisioning

Table 4. Boot loaders 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 4. Boot loaders 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

7.2.2 System interface (SysHAL)

Table 5. 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

7.2.3 Platform drivers (HAL) within MCUXpresso SDK

Table 6. 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

Table 6. Platform drivers (HAL)*...continued*

Feature	System SW	Validation status
SPI controller [1] with DMA	Available	Functional verified
I^{2}C controller [1] with DMA	Available	Functional verified
UART with DMA	Available	Functional verified
GPADC	Available	Functional verified

[1] The master/slave replacement into controller/target in this document follows the recommendation of the NXP - I2C standards organization.

7.2.4 Contactless interface

Table 7. Contactless interface

Feature	System SW	Validation status
Reader Mode ISO14443-A (106/212/424/848 Kbps)	Available	Functional and RF performance verified
Reader Mode ISO14443-B (106/212/424/848 Kbps)	Available	Functional and RF performance verified
Reader Mode FeliCa (212/424 Kbps)	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 Kbps)	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

Table 7. Contactless interface*...continued*

Feature	System SW	Validation status
NFC Forum CR13 Reader digital compliance	Available	Verified with Micropross digital compliance
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

7.2.5 Contact interface

Table 8. 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
Multi-slot 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

7.2.6 USB interface

Table 9. 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	The device is electrically passing USB2.0 requirements. For USB compliancy tests with most recent test requirements, FW update is required in future.

7.2.7 Mbed Crypto interfaces

Table 10. Mbed Crypto interfaces

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

Table 10. Mbed Crypto interfaces*...continued*

Feature	System SW	Validation status
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
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

Table 10. Mbed Crypto interfaces*...continued*

Feature	System SW	Validation status
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
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

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

Table 11. 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) for Key provisioning and update	Available	Functional verified
Locking of APP_ROOT_KEY (128/256) 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

7.2.9 Example applications

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

7.2.9.1 Compliance applications

Table 12. Compliance applications

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

7.2.9.2 Reader Library examples

Table 13. 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

7.2.9.3 Contact Reader Library examples

Table 14. 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

7.2.9.4 PN76 specific examples

Table 15. PN76 specific examples

Feature	System SW	Validation status
FreeRTOS Example	Available	Functional verified
Host Interface (SPI and I2C) Example	Available	Functional verified
Low-Power Mode Example Mode 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

7.3 Application software release package

The Application software package includes boards, CMSIS, devices, middleware, documentation, and OSAL support. This is provided as part of MCUXpresso SDK for quick customer integration of PN7642 IC into customers applications. Please refer to MCUXpresso PN7642 SDK manual.

7.4 Host utilities

As part of the software package for PN7642, few utilities running on host microcontroller (in this case it is LPC55S16) are provided.

These host utilities contain the various host-based applications and scripts to generated required key data to be used with SKM demo application.

Project files under the respective utility shall be loaded into MCUXpresso IDE, build, and download onto LPC55S16.

These host utilities provide support to use either I2C, SPI, I3C, and UART as HIF.

Host utilities provided with this package are as below:

Table 16. Host utilities

Utility	Location
Secure FW Downloader	`<extracted_dir>/Host_Software/ucHost_Utils/Secure_Fw_Downloader`
SKM DemoApp	`<extracted_dir>/Host_Software/ucHost_Utils/SKM_DemoApp`
Host Interface to PN7642 IC	`<extracted_dir>/Host_Software/ucHost_Utils/HifEx_Counterpart`

7.4.1 Secure FW downloader

Host utility provides secured encrypted firmware (esfwu file present in `<extracted_dir>/PN7642_FW` directory) The secure firmware can be downloaded onto the PN7642 IC. Refer to `<extracted_dir>/Host_Software/ucHost_Utils/Secure_Fw_Downloader/README.txt` for more information on the steps required to download the secure firmware image.

7.4.2 SKM DemoApp (Secure Key Mode Demo application)

This utility can be used to work with the secure key mode of PN7642 IC to provision the application keys on to the device. For more information on this application, refer to a separate application note provided with the release.

7.4.3 Host interface to PN7642 IC

The counterpart application to be run on the µC host (LPC55S16), to be able to run the HIF example application on the PN7642 IC. The HIF example demonstrates the use of the SPI, I2C, and UART command-response protocol to exchange data with the µC Host (LPC55S16) via the host interface.

7.5 PC scripts/utilities

As part of the software package for PN7642, few scripts are provided which run on host PC. These scripts demonstrate to generate the required keys, information required for using with different boot modes of PN7642 IC.

A readme file is provided in the respective script directory on the usage front.

PC scripts provided with this package are as below:

Table 17. PC Scripts/utilities

Script/utility	Location
Scripts/utility to generate encrypted FW file for application binary	`<extracted_dir>/Host_Software/Scripts/EsfwuMaker`
Scripts to generate/working on keys for use in SKM	`<extracted_dir>/Host_Software/Scripts/Crypto_Scripts`

8 Release history

8.1 PRs / CRs solved in this release

Following are the list of issues resolved and change request/features implemented in this release.

8.1.1 PN7642 secure firmware

8.1.1.1 v01.00

Table 18. v01.00

Sl 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.

8.1.1.2 v00.06

Table 19. v00.06

Sl No.	Title
1	First PN7642 CES/CQS Release.

9 Firmware upgradability

Firmware upgrade is possible to this FW version, without replacing the earlier provisioned application keys.

Once firmware upgrade is completed, downgrade older version of FW not possible.

Refer to Section 7.4.1 on how to upgrade the PN7642 IC firmware.

10 Known limitation and recommendations

Table 20. Known limitation and pre-cautions, 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.
Application mode is not entered after USB FW upload interruption	Retry USB FW upload again under stable power conditions.
USB compliancy	For customer USB compliancy, FW update is required in future.
FW upgrade with Chunk-bit in frame header does not work	Send the whole frame contents without Chunk-bit set. FW update is required for Chunk-bit support.

11 Legal information

11.1 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.

11.2 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 http://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.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

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.

11.3 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.

11.4 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.

DESFire — is a trademark of NXP B.V.

EdgeVerse — is a trademark 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.

NTAG — is a trademark 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'.

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

Date of release: 14 March 2023
Document identifier: RN00062