PN560 - NFC Controller

SESIP Security Target

Rev. 1.0 — 2 August 2023 **Security target**

Document information

Information	Content
Keywords	SESIP, Security Target, PN560
Abstract	Evaluation of the PN560 developed and provided by NXP Semiconductors, according to SESIP Assurance Level 2 (SESIP2), based on SESIP methodology, version 1.1.

Revision history

Rev	Date	Description
v.1.0	20230802	Final version

1 Introduction

The PN560 NFC controller is designed for integration in devices compliant with NFC standards.

This document evaluates PN560 platform core security features against the GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.1 (document reference: GP_FST_070), SESIP Assurance Level 2 [1].

The PN560 solution is based on NFC superior RF performance and hardware security, enabling a wide range of applications in the domain of secure connectivity.

Note: *In this document, platform refers to PN560.*

1.1 ST reference

PN560 - NFC Controller SESIP Security Target, Revision 1.0, NXP Semiconductors, 2023-08-02

1.2 Protection profile reference and conformance claims

The security target claims conformance to the following SESIP profiles:

Table 1. Protection profiles reference and conformance claims

Reference	Value
For SESIP certification	
SESIP profile	This ST does not claim conformance to any SESIP profile
Assurance claim	SESIP assurance level 2 (SESIP 2)

1.3 Platform reference

Table 2. Platform reference

Reference	Value
Platform name	PN560 – NFC controller
Platform version	ROM: 01 FW: 01.2B
Platform identification	PN560 0xCA
Platform type	NFC reader with programmable microcontroller

1.4 Included guidance documents

Table 3 lists the documents included with the platform.

Table 3. Guidance documents

Document type	Name	Version
PN560 hardware design	PN560 [6]	0.1
Product data sheet	PN560 FO_WLP56 NFC controller [5]	3.0
Product data sheet	PN560 WLCSP40 NFC Controller	3.1
Demo board user manual	UM11585 SN220 Demoboard User Manual	1.1
User manual	UM11308 SN2x0 NFC User Manual [3]	1.10
Security target	PN560 NFC Controller SESIP Security Target [8]	1.0
Antenna design	PN560 – AN13556	1.2
Application note	AN13473 SN220 Dynamic Power Control	2.1
Scripts	PN560 NCI Scripts [7]	1.0
Application note	AN13422 SN220 Phase Compensation for Felica Applications	5.0
Application note	AN13076 SN220 Dynamic Load Modulation	3.1
Application note	AN13098 SN220 Low Power Card Detection Mode Configuration	1.1
Application note	AN 13045 SN220 RF Register Setting Guidelines	1.9
Technical specification	NFC Controller Interface (NCI)	2.0

1.5 Platform functional overview and description

NFC controllers are widely used in connected devices to enable wireless proximity communications between the device, the NFC controller (within the device), and the outside world (for example between IoT gateway and mobile phone). NFC controllers also enable the data communication between sensors, microcontrollers and other peripherals.

PN560 is one of NXP's family of NFC controllers that execute NXP's proprietary applications and firmware. PN560 can be configured through NCI API. Table 4 provides an overview of PN560 hardware and firmware components.

Table 4. Overview of PN560 hardware and firmware components

Hardware/ firmware	Component/ interface	Description
Hardware	CPU	Arm Cortex-M0+ MCU core running at a frequency up to 90 MHz
	On-chip memory	• 96 kB ROM • 192 kB Flash • 16 kB RAM
	Host interface	• I2C slave up to 3.4 Mbit/s
	Peripheral	• 1 timer and 1 watchdog timer • Up to 4 GPIO interfaces
	NFC	• 13.56 MHz reader/writer modes (PCD) compliant to ISO14443-3/4 A/B and ISO15693 • 13.56 MHz card modes (PICC) compliant to ISO14443-3/4A
Firmware	ROM firmware	• Firmware residing in ROM. Implements the boot flow including secure boot loader, firmware download and lifecycle management.
	FLASH firmware	• Firmware residing in the flash, partitioned into platform data/code and application settings configured via NCI API.

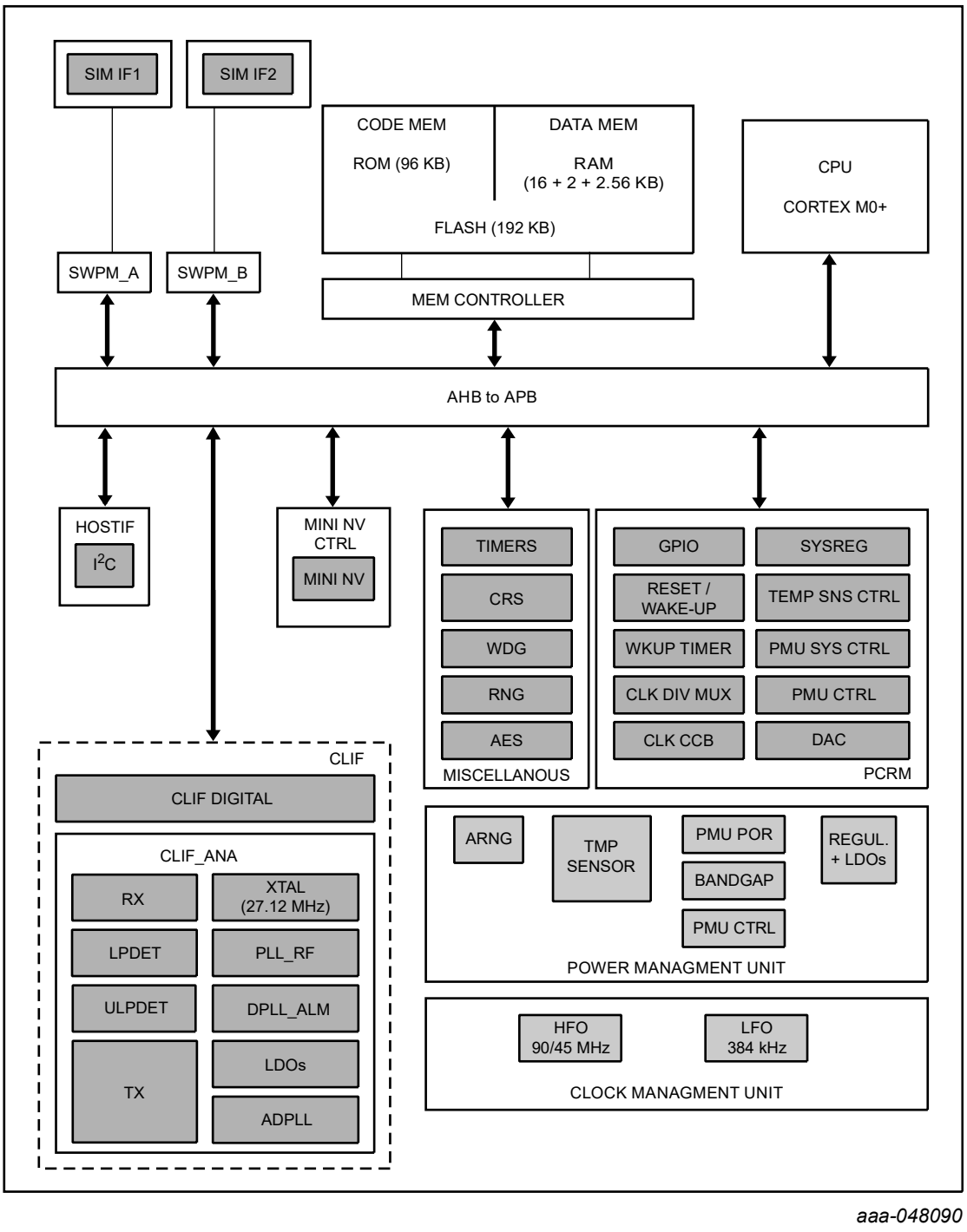

Figure 1. PN560 block diagram

1.5.1 Platform security features and scope

The main security features of the PN560 are described below.

Secure boot

After a reset, PN560 implements a secure initialization process of its components, and the hardware checks the integrity of the firmware image.

Secure update of firmware

To facilitate the improvement and bug-fixing to the platform, PN560 implements functionalities to update the firmware securely, even when the product is in the In-field Life-Cycle (LC) state.

Secure debugging

Debugging can be allowed but is disabled when the product is in the In-field Life-Cycle state. Debugging capabilities are only available during Development at NXP and in In-field Return Life-Cycle states. Both states require authentication with NXP credentials.

1.5.2 Platform scope and deliverables

The scope of the platform includes the IC hardware, ROM firmware, FLASH firmware as listed in Table 5.

Note: *No non-TOE hardware, software, or firmware is needed to run the target of evaluation (TOE).*

Table 5. Platform deliverables

Type	Name	Version	Form of delivery
IC hardware	PN560	CA	Silicon chip
Firmware	ROM firmware	01	On-chip ROM firmware
Firmware	FLASH firmware	01.2B	On-chip FLASH firmware

1.5.3 Life-Cycle

The platform manages the Life-Cycle (LC). The LC states are:

- **Creation**: The platform is in production. This state covers: silicon production, wafer test, assembly, and final test stage.
- **Development at NXP**: State for firmware development. In this state, the flash can be updated and debugged.
- **Operation In-field**: State of normal platform usage and most secure state with access to test mode. All debug options are disabled. The flash can be updated only through secure update.
- **Operation – Field Return**: State to diagnose failures in platforms returned from the field. To perform functional testing, authentication with an NXP credential is required to reenter the test mode for testing. The debug options are also reenabled in this state.

NXP guarantees secure provisioning of the NXP credentials and secure Life-Cycle configuration. Customers receive the platform in Operation In Field state. The Operation – Field Return state requires an NXP credential to reenter the test mode and reenable the debug options.

1.5.4 Use case environments

[Trusted code/trusted user]

PN560 NFC controller is integrated into a host device to support various applications in secure connectivity. In such applications, PN560 handle and transmits user data including sensitive information. The host can be a connected device, and PN560 a component of the connected device. As such, PN560 is the target of remote attacks that impact the capabilities of the platform such as debugging and firmware update. To address these threats, PN560 must have a controlled access to its internal resources. For example, via authentication to ensure that PN560 executes only trusted code from NXP.

Note: *The operational environment must ensure adequate protection against physical attacks. To prevent the physical access to PN560 of an attacker, customers must consider attacks in their risk analysis, and add mitigation at higher layers of the product or system.*

2 Security objectives for the operational environment

2.1 Platform objectives for the operational environment

To fulfill the security requirements of the platform, the operational environment (technical or procedural) must meet the objectives listed in Table 6.

Table 6. Platform objectives for the operational environment

Title	Description
Platform verification	The operating system or host application code checks the version of all the platform components, as described in *section 16.5* of [3].
Secure boot	The operating system or host application code uses the feature as described in Section 3.2.2.
Secure update	The operating system or the host application initiates the update of the platform firmware, as described in *section 16.5.7* of [3].
Secure use	Users ensure the secure and correct use of the platform according to the guidance documents (Section 1.4).
Software isolation	The operational environment must not allow the deployment of untrusted code as described in *section 16* of [3]. That means that all code running on the product is known to the product vendor and the product vendor can confirm that the code cannot harm the claimed security features. Code download is only done via secure update of platform as described in Section 3.2.4. All code is digitally signed.
Physical protection	The operational environment must protect the TOE against physical access of attackers as described in Section 1.5.4.

3 Security requirements and implementation

3.1 Security assurance requirements

The claimed assurance requirements package is: **SESIP 2** as defined in section 4 of GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.1 [1].

3.1.1 Flaw reporting procedures (ALC_FLR.2)

In compliance with flaw reporting procedures (ALC_FLR.2), the developers have defined the following procedure:

NXP has defined the product security incident response process (PSIRP). The product security incident response team (PSIRT) implements the PSIRP. The process is published at https://nxp.com/psirt. PSIRP includes four steps:

- **Reporting**. The process begins when the PSIRT becomes aware of a potential security vulnerability in an NXP product. The reporter receives an acknowledgment and updates throughout the handling process.
- **Evaluation**. The PSIRT confirms the potential vulnerability, assesses the risk, determines the impact, and assigns a processing priority. If the vulnerability is confirmed, the priority determines how the issue is handled throughout the remaining steps in the process.
- **Solution**. Working with PSIRT, the product team develops a solution that mitigates the reported security vulnerability. Solutions take different forms based on the vulnerability. Because of the nature of NXP products – mostly silicon products where the firmware is in ROM – often the solution is provided in the next version of the chips. The short-term solution consists of recommending security measures to be applied in systems using the NXP product.
- **Communication**. Because of the nature of the NXP products, often the solution to systems using the affected products must be found in other countermeasures in those systems. The communication on the vulnerability and solutions is mostly toward the affected customers. For previously unknown or unreported issues, NXP acknowledges the reporter of the issues (unless the reporter requests otherwise).

The secure boot feature of the platform:

- Verifies the integrity of the loadable firmware part.
- Checks the major version number of the firmware download (must be numerically greater than or equal to the existing firmware major version).

3.2 Security functional requirements

The platform fulfills the following security functional requirements.

3.2.1 Verification of the platform identity

Requirement

The platform provides a unique identification of the platform, including all its parts and their versions.

Conformance rationale:

The platform provides APIs for users to retrieve the identification information including versions of hardware and firmware parts as described in Table 5.

3.2.2 Secure initialization of the platform

Requirement

The platform ensures its authenticity and integrity during the platform initialization. If the platform authenticity or integrity cannot be ensured, the available modes for the platform are Test or Download modes.

Conformance rationale

The system boot module of the platform is started after each system reset. After the initialization of the hardware and firmware based on the Flash data configurations one operation modes is started.

The boot sequence is present in the ROM memory and is executed as a part of reset handling sequence. All exceptions are disabled globally. Exceptions and interrupts are enabled only by the respective code of the boot target modes. The boot sequence is as follows:

- Initialize base system
- Clock Initialization
- CRC initialization
- Flash controller initialization
- Creation of the block structure for the code and data segments in the flash
  - Compute the CRC32 for the data and code areas
- Pad configuration and basic PMU initialization
- Anti-tearing check to have a reliable lifecycle and session byte
- Load patches
- Boot strap
  - TestOS mode
  - Encrypted secure firmware download mode
- Jump to application flash

During the initialization process above, if any check fails, the platform will be only available for Test mode, which requires authentication to enter, or Download modes.

3.2.3 Verification of the platform instance identity

Requirement

The platform provides a unique identification of the specific instantiation of the platform, including all its parts and their versions.

Conformance rationale

The platform provides APIs (refer to section 16.5.5 in [3]) for users to retrieve the identification information including hardware and firmware versions and the unique die ID.

3.2.4 Secure update of the platform

Requirement

To maintain the integrity, authenticity, and confidentiality of the platform, the platform firmware can be updated to an equal or newer version in the field.

Conformance rationale

The secure update process ensures the secure firmware image in the field. For the firmware to be updated:

- The platform must enter the secured firmware upload mode, and remain in this mode until the firmware update process is complete.
  - NFC features are disabled.
  - Only commands that are relevant for the secure firmware download operation are allowed.
- The firmware image to be downloaded is encrypted with an AES cipher in CTR mode and signed using the RSA-3072 algorithm.
- An anti-tearing function is implemented for the download process so any power supply removal or memory fault event can be detected.
- The major version number of the firmware is checked against the existing firmware major version number (prevents a firmware downgrade).

3.2.5 Secure debugging

Requirement

The platform provides a serial wire debug (SWD) interface with debug functionality. The interface is authenticated as specified in section 3.2.2.9 of [9].

The platform ensures that all data stored by the application, except for none, is made unavailable.

Conformance rationale

The debugging of the platform is restricted to NXP engineering teams. The debug capabilities are disabled while the platform is in the IN-FIELD state and can only be enabled using NXP credentials in the FIELD_RETURN state.

The Field Return of Platform SFR is not claimed because the TOE does not store any application data.

4 Mapping and sufficiency rationales

4.1 SESIP2 sufficiency

Table 7. Rationale for SESIP2 sufficiency

Assurance class	Assurance family	Covered by	Rationale
ASE: Security Target Evaluation	ASE_INT.1 ST Introduction	Section 1	ST reference: see Section 1.1 Platform reference: see Section 1.3 Platform overview and description: see Section 1.5
	ASE_OBJ.1 security requirements for the operational environment	Section 2	Objectives for the operational environment: see Section 2
	ASE_REQ.3 listed security requirements	Section 3	All SFRs in this ST are taken from [2].
	ASE_TSS.1 TOE summary specification	Section 3	All SFRs are listed per definition, and for each SFR the implementation and rationale are provided in the SFR.
ADV: Development	ADV_FSP.4 Complete functional specification	Section 1.4	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AGD: Guidance documents	AGD_OPE.1 operational user guidance	Section 1.4	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	Section 1.4	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section 3.1.1	The flaw reporting and remediation procedure is described.
ATE: Tests	ATE_IND.1 Independent testing: conformance	Performed by evaluator	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA_VAN.2	AVA_VAN.2 Vulnerability analysis	N/A. A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.	To confirm that the potential vulnerabilities cannot be exploited in the operational environment for the platform, the evaluator performs penetration testing, assuming an attack potential of Basic.

5 Bibliography

5.1 Evaluation documents

[1] *GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.1, GP_FST_070*

5.2 Developer documents

[3] *UM11308 – SN2x0 NFC User Manual*

[4] *NFCForum-TS-NCI-2.0*

[5] *PN560 FO-WLP56 NFC Controller Product Data Sheet*

[6] *PN560 Hardware Design*

[7] *PN560 NCI Scripts*

[8] *PN560 – NFC Controller SESIP Security Target*

[9] *Module Specification*

6 Acronyms and abbreviations

Table 8. Abbreviations

Acronym	Description
IC	Integrated circuit
LC	Life-Cycle
NFC	Near field communication
PSIRP	Product security incident response process
PSIRT	Product security incident response team
SFR	Security functional requirement
SWD	Serial wire debug
TOE	Target of evaluation

7 Legal information

7.1 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.

7.2 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.

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.

7.3 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

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

Date of release: 2 August 2023
Document identifier: PN560