PN7642EV - NFC reader with programmable MCU

SESIP Security Target

Rev. 1.4 — 22 November 2022 **Evaluation document**

Document information

Information	Content
Keywords	SESIP, Security Target, PN7642EV v01.00, PN7642EV/C100
Abstract	Security target for evaluation of the PN7642EV v01.00 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
0.1	15 October 2021	First released draft
0.2	10 November 2021	Second released draft
0.3	1 December 2021	Third released draft
0.4	17 March 2022	Switch to DITA format Add DRBG to the scope and siscellanous fixes
0.5	27 April 2022	Remove DRBG from the scope
0.6	24 May 2022	Update SFR Residual Information Purging
0.7	24 May 2022	Update guidance documents Update SFR Cryptographic Key Generation for RSA key generation
0.8	19 August 2022	Update SFR Cryptogrpahic Operation and Cryptographic Key Generation Update SFR Secure Update of Application Add references for objectives for operational environment Miscellanouse editorial fixes
0.9	23 August 2022	Update SFR Cryptogrpahic Key Store Update SFR Secure Update of Application
1.0	10 October 2022	Update Platform identification Update guidance references Replace SFR Secure Application Update with SFR Secure Install of Application Miscellaouse editorial fixes
1.1	27 October 2022	Further Update Platform identification Update guidance references Correct the definition for newer firmware version Miscellaouse editorial fixes
1.2	27 October 2022	Update reference for Quick Start Guide Add a note on updating firmware to the same version
1.3	7 November 2022	Update platform idenfication Update references for Datasheet and UM Add a note on USB download feature for SFR Secure Install of Application Update SWD levels for SFR Secure Debugging to be consistent with Datasheet
1.4	22 November 2022	Update Table 2 and 5 to correct platform idenfication

1 Introduction

This Security Target describes the PN7642EV - NFC reader with programmable MCU platform (PN7642EV v01.00 for short) and the exact security properties of the platform that are evaluated against GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), version 1.1, SESIP Assurance Level 2 (SESIP2) [1].

1.1 ST Reference

PN7642EV - NFC reader with programmable MCU, SESIP Security Target, Revision 1.4, NXP Semiconductors, 22 November 2022.

1.2 SESIP Profile Reference and Conformance Claims

Table 1. SESIP Profile Reference and Conformance Claims

Reference	Value
SP Name	GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs [2]
SP Version	Version 1.0
Assurance Claim	SESIP Assurance Level 2 (SESIP2)
Package Claim	Base SP, Package Secure Services, Package Software Isolation

1.3 Platform Reference

Table 2. Platform Reference

Reference	Value
Platform Name	PN7642EV - NFC reader with programmable MCU
Platform Version	v01.00, see also Table 5 for the versions of the platform components
Platform Identification	PN7642EV v01.00
Platform Type	NFC reader with programmable microcontroller

1.4 Included Guidance Documents

The following guidance documents are included with the platform:

Table 3. Guidance Documents

Document	Name	Version
Product Data Sheet	PN7642 Open NFC Controller - Objective Datasheet [3]	1.2
Application Note	AN13134 – PN76 Family Evaluation Board - Quick Start Guide [4]	2.2
Application Note	AN13719 – PN7642 Instruction Manual [5]	1.1
API Reference Manual	PN7642 Open NFC Controller - User API Documentation [6]	01.00
Product User Manual	UM11566 - PN76 family NFC Open Controller - User Manual [7]	1.4
Application Note	AN13720, PN7642 Secure Key Mode Demo [8]	1.1

1.5 Platform Overview and Description

NFC controllers are widely used in many connected devices to enable wireless proximity communications between the device, the NFC controller is included, and the outside world, *e.g.*, between IoT gateway and mobile phone. It also enables the data communication between sensors, microcontrollers and other peripherals.

PN7642EV v01.00 is NXP's family of open NFC controller with integrated crypto acceleration and secure key store, which allows customer applications to be present alongside with NXP's own applications and firmware. An overview of PN76 hardware and firmware components is given in the following Table.

Table 4. Overview of Platform Hardware and Firmware components

HW / FW	Name	Description
Hardware	CPU	• ARM Cortex M33 CPU with ARM TrustZone technology running at a frequency up to 90 MHz
	On-chip memory	• 256 kB ROM memory • 256 kB Flash memory (180 kB available to the user) • 32 kB RAM (20 kB available to the user)
	Security subsystem	• Accelerators supporting multiple symmetric and asymmetric cryptographic algorithms • Secure key storage • Secure key transfer unit • Random number generators • General-purpose CRC unit
	Host interface	• USB 2.0 Full-speed device controller • I2C slave up to 3.4 Mbit/s (High-speed mode) • SPI slave up to 15 Mbit/s • I3C slave up to 3.4 Mbit/s • UART up to 5.4 Mbit/s
	Peripheral	• 4 Timers and 1 WatchDog Timer • Up to 6 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 that implements the Secure Boot flow including Firewalling, Secure Boot Loader, Secure Key management , USB Mass Storage based Firmware Download and System APIs to access platform drivers for system-critical hardware resources (including power management, clock control, contactless interface, FLASH controller, etc.), lifecycle management, boot/ download configuration APIs, utility and other application programming APIs.
	FLASH firmware	• Firmware residing in FLASH partitioned into secure and application code/data. Secure Firmware provides APIs to access wrapper APIs for cryptographic operations, NFC APIs , In-Application Programming APIs and platform drivers for other system resources (including timer, host interfaces, etc.)

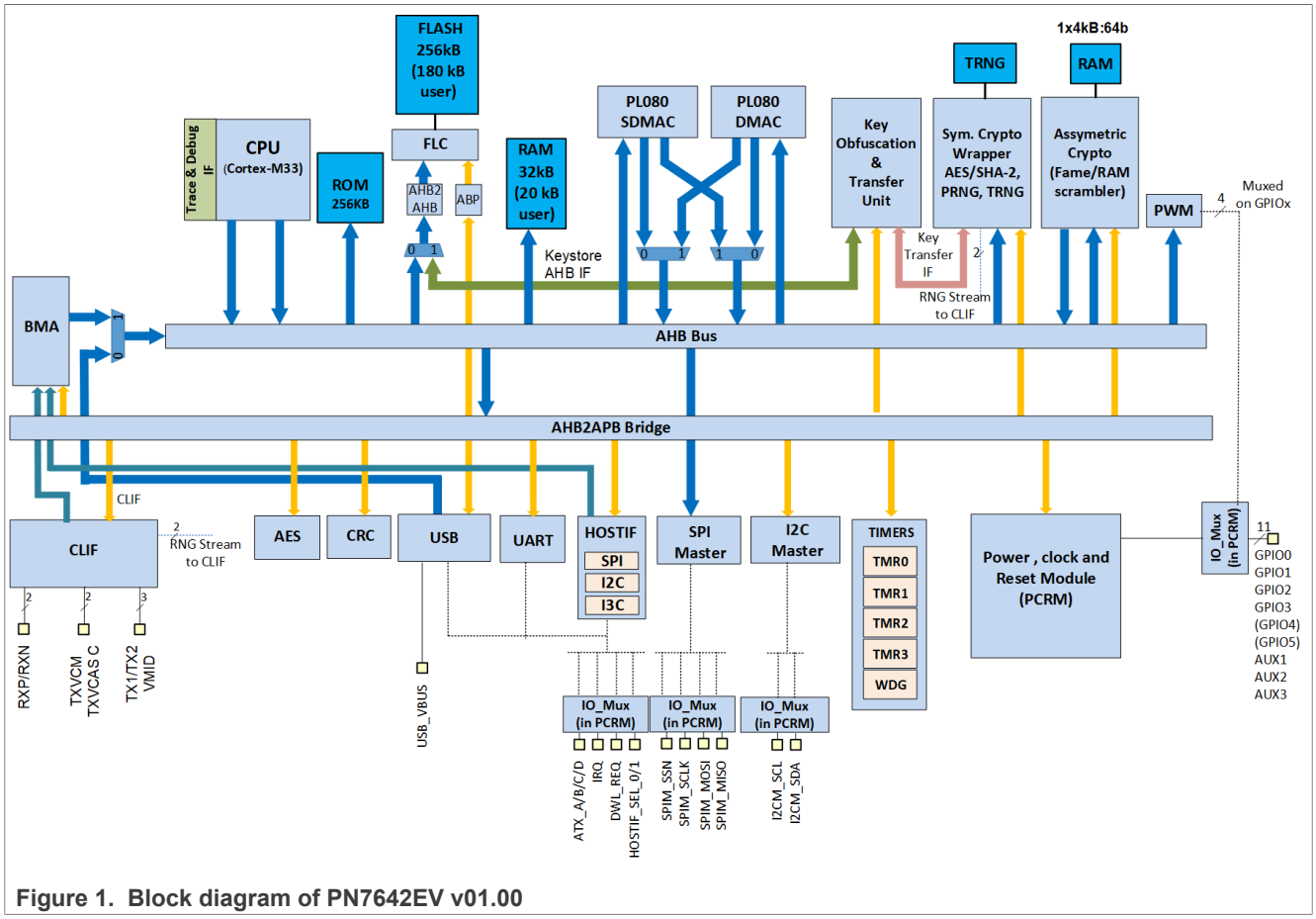

Figure 1. Block diagram of PN7642EV v01.00

1.5.1 Platform Security Features

The main security features of PN76 are described below.

Secure Boot

After reset, PN7642EV v01.00 implements a secure initialization process of its components. In particular, the hardware firewall is started with the most restricted setting early in the process. The result is a secure state, regardless of the initialization process was completed or not.

Secure Update of The Firmware

To facilitate the improvement and bug-fixing to the platform, PN7642EV v01.00 implements functionalities which enable its firmware to be securely updated even when the product is in the field.

Secure Debugging

During the development of customer applications, debugging can be allowed but is done in a secure manner such that the security of user data is protected.

Isolation of Platform

PN7642EV v01.00 separates user application and critical firmware parts into two execution environments: the Secure area (TEE) and the Application area (REE). This is enabled by ARM TrustZone technology and a hardware firewall.

Secure Install of Application

Customer applications can be securely installed onto the platform and replace the existing applications via a similar process to secure firmware update. The difference is that this process shall use the customer' own keys for encryption and signature.

Cryptographic Operations

PN7642EV v01.00 implements various cryptographic operations that user applications can make use of. These cryptographic operations include:

- AES encryption and decryption with 128-bit or 256-bit key sizes in ECB, CBC, CTR, CCM, GCM and EAX modes.
- Triple-DES encryption and decryption with 2-key (112-bit key) and 3-key (168-bit key) support in ECB and CBC modes.
- MAC generation algorithms AES-CMAC and TDES-CMAC.
- SHA-256, SHA-384 and SHA-512 cryptographic hash functions.
- HMAC algorithms.
- HMAC-based Key Derivation Function (HKDF) algorithm.
- RSA encryption, decryption, signature generation and signature verification with 1536-bit, 2048-bit and 3072-bit key sizes.
- ECDSA signature generation and verification with BrainpoolP256r1, BrainpoolP384r1, SECP256r1 and SECP384r1 curves.
- ECDH (Elliptic Curve Diffie-Hellman key exchange) algorithm with BrainpoolP256r1, BrainpoolP384r1, SECP256r1 and SECP384r1 curves.
- EdDSA (Edwards-curve Digital Signature Algorithm) signature generation and verification with Ed25519 curve.
- MontDH (Diffie Hellman key exchange on Montgomery curve over GF(p)) key exchange with Ed25519 curve.

Cryptographic Key Generation

PN7642EV v01.00 implements cryptographic key generation algorithms that are available for user applications as follows:

- RSA key generation with 1576-bit, 2048-bit and 3072-bit key sizes.
- ECC key generation with 256 or 384-bit key sizes.
- EdDSA key generation with 256 key size.
- MontDH (Diffie Hellman key exchange on Ed25519 Montgomery curve) key generation.

Cryptographic Key Store

PN7642EV v01.00 provides hardware components that securely store, protect and handle cryptographic keys with a dedicated FLASH memory segment. The handling of stored keys bypasses the CPU completely. For additional key store, a dedicated memory area in Flash is reserved for this purpose. This memory area is called extended key stiore and accessible in TEE only. The main key store can hold AES keys while the extended key store can hold both AES and ECC keys.

Random Number Generation

PN7642EV v01.00 implements the following random number generators:

- A True Random Number Generator (TRNG) that meets the quality metric of the AIS31 PTG.2 class as defined in [25]

1.5.2 Platform Scope and Deliverables

The scope of the platform includes the IC hardware, ROM firmware and FLASH firmware as listed in Table 5. Any additional firmware, OS or application software stored on the platform is not in scope of this evaluation.

Table 5. Platform Deliverables for PN7642EV v01.00

Type	Name	Version	Form of delivery
IC Hardware	PN7642EV/C100	0x53	Silicon chip
Firmware	ROM Firmware	0x03	On-chip ROM firmware
Firmware	FLASH Firmware	1.0	On-chip FLASH firmware
User Guidance	See Table 3	See Table 3	Pdf, secure download

1.5.3 Life Cycle

The life cycle (LC) is managed by the platform. The LC states are described in Table 6:

Table 6. Life Cycle States

LC State	Description
Creation	The platform is in production in NXP manufacturing. This state covers : silicon production, wafer test, assembly and final test stage.
Development at NXP	This is the state for firmware development, both Secure and Non-secure parts, by NXP. In this state, both NXP and User Flash can be updated and debugged.
Development at Customer	This is the state for customer software development. In this state, only User Flash can be updated and debugged.
Operaition - In Field	This is the state of normal platform usage and most secure state with access to Test Mode and all debug options disabled
Operation - Field Return	This is the state for diagnosing failures in platforms returned from the field. In order to perform functional testing, authentication with NXP credential is required to re-enter Test Mode to perform testing. In addition, partial or full debug options can also re-enabled in this state.

NXP ensures secure provisioning of the NXP credentials and secure life cycle configuration. The customer will receive the platform in *Development at Customer* state, and shall perform software installation and configuration and customer credential provision in this state. The platform shall then be configured to *Operation - In Field* state in their technical and/or procedural secure environment. The *Operation - In Field* state is the normal platform usage state and the only state it can switch to is the *Operation - Field Return* state which requires NXP credential to re-enter Test Mode and re-enable debug options.

1.5.4 Use Case

[trusted code]

Only trusted code is expected to run the platform. On the field, the platform contains NXP firmware and customer firmware which can be both updated. However, the update process must be done in a secure manner which protects the confidiality and integrity of the firmware.

[trusted user only]

As an open NFC controller, PN7642EV v01.00 is typically integrated into a host device (e.g., a mobile phone) which requires secure authentication and used for various applications including residential access (*e.g.*, lock), accessory authentication, closed-loop payment and ticketing. The host itself can be a connected device and therefore PN7642EV v01.00 is a component of the connected device and subject to remote logical attacks and attacks that may abuse the platform's capabilities such as debugging and firmware update. Given such use cases, only trusted users are expected to gain access to the platform.

Please note that, PN7642EV v01.00 does not provide protection against physical attacks by itself. Therefore, the operational environment shall be responsible for implementing sufficient protection against physical attacks. Some hints are provided in Section 20.3 of [7].

2 Security Objectives for the Operational Environment

2.1 Platform Objectives for the Operational Environment

For the platform to fulfill its security requirements, the operational environment (technical or procedural) must fulfill the following objectives:

Table 7. Platform Objectives for the Operational Environment

Title	Description	Reference
Platform Verification	The operating system or application code is expected to verify the correct version of all platform components that it depends on and any notice of firmware update.	Sections 20.1 of [7]
Key Management	Cryptographic keys and certificates outside of the platform are subject to secure key management procedures.	Sections 20.4 of [7]
Trust Provisioning	Any secret to be provisioned into the platform is generated securely (*e.g.*, via a standard compliant HSM) and subject to secure key management procedures. The provisioning process is done in secure sites with physical, logical security and organizational policies in place.	Sections 20.2 and 20.4 of [7]
Secure boot	The operating system or application code is expected to make use of the feature as described in the Section 3.2.1.2.	Sections 20.7 of [7]
Key Diversification	When applicable, keys must be diversified among different devices.	Section 20.2 of [7]
Lifecycle Management	The operational environment is expected to configure the platform correctly before deployment. In particular, the platform shall be in locked state (e.g., Test mode and debugging disabled, USB download mode disabled, etc.) when deployed.	Section 20.5 of [7]
Secure Testing	Production testing is expected to be done in a secure site with physical, logical security and organizational policies in place.	Sections 20.4 of [7]
Trusted Users	Actors in charge of platform management, for instance for encrypting and signing of firmware image to be updated, are trusted.	Sections 20.4 of [7]
Secure Update	Actors in charge of excising update of the platform firmware or applications are expected to securely initiate the update process. The update image is expected to be properly signed and distributed in a secure manner to ensure its confidentiality and authenticity.	Sections 20.6 of [7]
Crypto Use	Users are expected to ensure secure and correct use of cryptographic algorithms according to guidance.	[6] and [7]
SW integration	End users are expected to ensure secure and correct use of system service APIs.	[6]
Physical protection	The operational environment must protect the TOE against physical access of attackers as described in Section 1.5.4.	Sections 20.3 of [7]

3 Security Requirements and Implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP2** as defined in Chapter 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 accordance with the requirement for flaw reporting procedures (ALC_FLR.2), the developer has defined the following procedure:

NXP has defined a Product Security Incident Response Process (PSIRP), implemented by a dedicated team (PSIRT). This process provides a publicly available interface (https://nxp.com/psirt), and includes four major 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 will take different forms based on the vulnerability. Because of the nature of NXP products – mostly silicon products where the firmware is in ROM -, very often the solution can only be provided in a next version of the chips and the short-term solution will consist of recommending security measures to be applied in systems using the NXP product.
- **Communication**. As said above, because of the nature of the NXP products, the solution to systems using the affected products often needs to be found in additional countermeasures in those systems. The communication on the vulnerability and solutions will in most cases be done directly towards the affected customers. For previously unknown or unreported issues, NXP will acknowledge the reporter of the issues (unless the reporter requests otherwise).

The platform's secure update feature allows the platform's firmware to be updated to a newer version. Once updated, it is not possible to revert back to any older version of the firmware. The platform firmware's version is represented by two numbers: major version number and minor version number. A version is deemed the newer version than another version if the former has a higher major version number. This is enforced by the platform's secure update feature as described in Section 3.2.1.3

3.2 Security Functional Requirements

In the following Security Functional Requirements, the term **platform** covers the **PN7642EV v01.00 physical and logical scope**, and the term **application** refer to any additional firmware, OS or application software which is out of evaluation scope. It represents a part of the final connected device.

PN7642EV v01.00 fulfills the following security functional requirements:

3.2.1 Base SP Security Functional Requirements

3.2.1.1 Verification of 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 (refer to PN7642 Open NFC Controller - User API Documentation [6]) for users to retrieve identification information including versions of hardware and firmware parts as described in Table 5.

3.2.1.2 Secure Initialization of Platform

Requirement

The platform ensures its authenticity and integrity during the platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to a *limited availability mode in which only Test or Download modes, subject to further authentication, can be entered.*

Conformance rationale:

The system boot module of the platform is started after each system reset in Secure privileged mode.

After the initialization of the hardware and configuration of the IDAU and Firewall based on the Flash data configurations one of the three operation modes is started.

The boot sequence is present in ROM Memory and is executed in the Thread Mode of ARM Cortex M-33 as a part of reset handling sequence. All exceptions are disabled globally using the CPSID instruction. 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
- Initialize Firewall to highest security and SWD Disable
- Flash Controller HAL Initialization
- Create Block Structure for Code and data segments in Flash
  - Compute the CRC32 for 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 for Secure and Non-secure applications
  - Secure Key Mode
- Configure Firewall / IDAU for Application
- Jump to Secure Application Flash

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

3.2.1.3 Secure Update of Platform

Requirement

The platform can be updated to a newer version in the field such that the integrity, authenticity and confidentiality of the platform is maintained.

Conformance rationale:

Secure Update is the process used to securely update the firmware image in the field. For the firmware to be updated, the platform must enter the so-called Encrypted Download mode via a specific procedure. The platform shall stay in this mode until the whole firmware update process has been completed successfully. In addition, once in the Encrypted Download mode, NFC functionalities are disabled and only commands that are relevant for the secure firmware download operation are allowed. The firmware image to be downloaded is encrypted with AES cipher in CTR mode and signed using RSA-2048 algorithm so that its confidentiality and authenticity can be protected. To preserve the integrity of the updated firmware, an anti-tearing function is implemented for the downloading process such that any power supply removal or memory fault event can be detected. Finally, downgrading firmware is also prevented by version checking. Please note that, it is possible to update the platform firmware to the one with the same major version number (see the definition of older vs. newer version in Section 3.1.1). Version checking only prevents rolling back to any older version, *i.e.*, one with lower major version number.

3.2.1.4 Secure Debugging

Requirement

The platform only provides *Serial Wire Debug (SWD) interface with 2 debug levels* authenticated as specified in *Section 9.13.2.2 of PN7642 Open NFC Controller - Objective Datasheet* [3] with debug functionality.

The platform ensures that all data stored by the application, with the exception of *CPU core and other resources allowed by the firewall isolating TEE and REE*, is made unavailable.

Conformance rationale:

SWD access for debugging can be enabled by configuring a suitable SWD access level to allow SWD access. By default, the platform leaves production with SWD access level set to a configuration that allows debugging functionality of the REE. When the platform is ready for deployment, debugging can be disabled permanently by changing the configuration of SWD access level to No Access to prevent further access. This change is irreversible. Finally, the separation of TEE and REE by the TrustZone-based firewall is also applicable when debugging either TEE or REE. The configuration API to set SWD access level resides in the Secure area only to prevent it from being abused.

3.2.1.5 Residual Information Purging

Requirement

The platform ensures that *user data*, with the exception of *none*, is erased using the method specified in *PN7642 Open NFC Controller - User API Documentation* [6] before the memory is (re)used by the platform or application again and before an attacker can access it.

Conformance rationale:

An API PN76_Sys_SKM_Purge_AppKeys() (see PN7642 Open NFC Controller - User API Documentation [6]) is available for the customer to force the key de-commissioning from the application. Alternatively, user can also enter the so-called *Secure Key Mode (SKM)* and issue SKM_CMD_PURGE_APP_KEYS command. In addition, after TestOS authentication, all the application keys are erased by triggering the same API. This is the mechanism used for de-commissioning the customer keys upon Field-returns. The user data is deleted by overwriting with a constant value.

3.2.2 Package 'Security Services' Security Functional Requirements

3.2.2.1 Cryptographic Operation

The platform provides the application with *operations in* Table 8 functionality with *algorithms in* Table 8 as specified in *specifications in* Table 8 for key lengths *described in* Table 8 and modes *described in* Table 8.

Table 8. Cryptographic Operations

Operation	Algorithm	Specification	Key Lengths	Modes / Curves
Encryption and decryption	AES	FIPS 197-2001 [10] NIST SP800-38A [14] NIST SP800-38A addendum [15] NIST SP800-38B [16] NIST SP800-38C [17] NIST SP800-38D [18] EAX Specification [31]	128, 256 bits	ECB, CBC, CTR, CCM, GCM, EAX
Encryption and decryption	TDES	NIST SP800-67 [19] NIST SP800-38A [14] NIST SP800-38A addendum [15]	112, 168 bits	ECB, CBC
Hashing	SHA256 SHA384 SHA512	FIPS 180-4 [9]	N/A	N/A
MAC generation	AES-CMAC	NIST SP800-38B [16]	128, 256 bits	N/A
MAC generation	TDES-CMAC	NIST SP800-38B [16]	112, 168 bits	N/A
MAC generation	HMAC-SHA256	FIPS 198-1 [11] RFC 2104 [12]	256 bits	N/A
Key derivation	HKDF	RFC 5869 [26]	N/A	N/A
Encryption and decryption	RSA	PKCS#1 v2.2 [21]	1536, 2048, 3072 bits	EME-OAEP, EME-PKCS1-V1_5

Table 8. Cryptographic Operations...*continued*

Operation	Algorithm	Specification	Key Lengths	Modes / Curves
Signature generation and verification	RSA	PKCS#1 v2.2 [21] PKCS#1 v2.1 [20] FIPS 186-4 [13]	1536, 2048, 3072 bits	EMSA-PSS, EMSA-PSS with salt option (extended PSS), EMSA-PKCS1-V1_5
Signature generation and verification	ECDSA	ANSI X9.62 [23] FIPS 186-4 [13] ISO/IEC 14888-3-2015 [22]	256, 384 bits	BrainpoolP256r1, BrainpoolP384r1, SECP256r1 and SECP384r1 curves
Signature generation and verification	EdDSA	RFC 8032 [27]	256 bits	Ed25519 curve
Key Exchange	ECDH	ANSI X9.63 [24] ISO/IEC 11770-3-2015 [28]	256, 384 bits	BrainpoolP256r1, BrainpoolP384r1, SECP256r1 and SECP384r1 curves
Key Exchange	MontDH	RFC 7748 [32]	256 bits	Ed25519 curve

Conformance rationale:

The platform provides Crypto Library that implements cryptographic functionalities. The Crypto Library resides in the Secure area. Users can access the provided cryptographic functionalities via CL wrapper APIs (refer to PN7642 Open NFC Controller - User API Documentation [6]) that reside in the Application area.

3.2.2.2 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in *algorithms in* Table 9 as specified in *specifications in* Table 9 for key lengths *described in* Table 9

Table 9. Cryptographic Key Generation

ID	Algorithm	Specification	Key Lengths
RSA	RSA Key Generation	BAnz AT 30.01.2015 B3 [30]	1536, 2048, 3072 bits
ECC	ECC Key Generation	ISO/IEC 15946-1-2008 [29] ANSI X9.62 [23] FIPS 186-4 [13]	256, 384 bits
EdDSA	EdDSA Key Generation	RFC 8032 [27]	256 bits
MontDH	MontDH Key Generation	RFC 7748 [32]	256 bits

Conformance rationale:

Cryptographic key generation is provided by Crypto Library which is accessible via wrapper APIs (refer to PN7642 Open NFC Controller - User API Documentation [6]).

3.2.2.3 Cryptographic Key Store

The platform provides the application with a way to store *cryptographic keys* such that not even the application can compromise the integrity, confidentiality of this data. This data can be used for the cryptographic operations *encryption, decryption, key derivation, signature generation*.

Conformance rationale:

The platform has dedicated hardware components to securely store and manage key material (*e.g.*, access rights, key operations like derivation, wrapping, unwrapping, etc) that belongs to either NXP or users. When needed, subject to proper access right, a key can be transferred directly (*i.e.*, bypassing CPU completely) to the symmetric crypto coprocessor for a cryptographic operation via a dedicated bus and the so-called Secure Key Transfer Unit (SKTU). The memory reserved for the key store subsystem is a dedicated 4kB segment of FLASH memory, which is protected by the hardware firewall blocking any access to this memory segment including access from the CPU. Only the SKTU has access to this memory segment via a dedicated bus that is not subject to the hardware firewall. There is also a dedicated anti-tearing mechanism implemented in this subsystem so that when a key is stored here, its integrity is guaranteed. Only AES keys can be stored in this key store. There is also an additional memory area in the regular FLASH for storing more keys (either AES or ECC keys). This area is called extended key store which is accessible from CPU but through secure access only, *i.e.*, it resides in secure world. They keys stored in the extended key store are encrypted by another key that is programmed into the platform during trust provisioning process.

3.2.2.4 Cryptographic Random Number Generation

The platform provides the application with a way based on *True Random Number Generator (TRNG)* to generate random numbers as specified in *Quality metric for AIS31 PTG.2 class (PTG.2.6)*[25].

Conformance rationale:

The TRNG with the entropy source being ARNG (Analog RNG) is implemented in the symmetric crypto accelerator and accessible via either TRNG data register or a wrapper API (refer to PN7642 Open NFC Controller - User API Documentation [6]).

3.2.3 Package 'Software Isolation' Security Functional Requirements

3.2.3.1 Software Attacker Resistance: Isolation of Platform

The platform provides isolation between the application and itself, such that an attacker able to run code as an application on the platform cannot compromise any other claimed security functional requirements.

Conformance rationale:

The platform distinguishes between two execution environments which are enabled by ARM TrustZone technology: the Secure area (TEE) and the Application area (REE). This is so that NXP’s security-sensitive code running on the platform can be isolated from other code including user applications as well as other code owned by NXP. Most parts of the NXP firmware are running in the Secure area. In contrast, user applications and non-critical parts of NXP firmware are running in the Application area. Every time a peripheral from the secure firmware needs to be accessed (*e.g.*, accessing the contactless interface or the security subsystem), a context switch from the Application area to the secure area has to happen. In order to provide a controlled interface from the Secure area

to the Application area, the System Service API Layer is implemented into the NXP firmware. This API layer is the only possibility to exchange data between Application and secure execution environments. Also based on ARM TrustZone, the platform implements a hardware firewall which provides memory segmentation and management of access rights to the memory segments. This firewall also restricts access to critical hardware resources including crypto accelerators, key store, *etc*. from code running in the Application area.

3.2.4 Additional Security Functional Requirements

3.2.4.1 Secure Install of Application

The application can be installed in the field such that the integrity, authenticity and confidentiality of the application is maintained.

Conformance rationale:

Secure install of user applications can be done in Encrypted Download mode in the same way with secure update of platform firmware (but with a different set of keys for image encryption and signing). The installation process will overwrite the application that currently resides on the platform. There is no need for any management of installation and the installed application can be loaded once the installation process is successful. The platform also provides USB Download mode which does not require encrypted and signed firmware image. As a result, this feature does not contribute to the fulfillment of this SFR. On the field, the USB Download mode shall be disabled completely by setting the Code Read Protection Levels (CRP) and Code Write Protection (CWP) to restricted values (see Section 9.13.2.3 and 9.13.2.2 of PN7642 Open NFC Controller - Objective Datasheet [3]). In addition, the customer is also able to lock the read/write access to Customer firmware via USB Download by calling `PN76_Sys_OTPConfigs_LockSettings` (see [6]).

4 Mapping and Sufficiency Rationales

4.1 SESIP2 Sufficiency

Table 10. SESIP2 Sufficiency

Assurance Class	Assurance Family	Covered By	Rationale
ASE: Security target evaluation	ASE_INT.1 ST Introduction	Section 1	The ST reference is in Section 1.1, the TOE reference in Section 1.3, the TOE overview and description in Section 1.5.
	ASE_OBJ.1 Security requirements for the operational environment	Section 2	The objectives for the operational environment in Section 2 refer to the guidance documents.
	ASE_REQ.3 Listed security requirements	Section 3	All SFRs in this ST are taken from [1]. SFR "Secure Update of Platform" is is additionally included.
	ASE_TSS.1 TOE Summary Specification	Section 3	All SFRs are listed per definition, and for each SFR the implementation is defined in the SFR.
ADV: Development	ADV_FSP.4 Complete functional specifications	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: Test	ATE_IND.1 Independent testing: conformance	Material provided to evaluator.	The evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	N.A. A vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.	The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the evaluator assuming an attack potential of Basic.

4.2 SESIP Profile Conformance Mapping

This section provides rationales of conformance claimed in Section 1.2

Table 11. SESIP Profile for Secure MCUs and MPUs Sufficiency

Package Claimed	Security Functional Requirements	Covered By
Base	Verification of Platform Identity	Section 3.2.1.1
	Secure Initialization of Platform	Section 3.2.1.2
	Secure Update of Platform	Section 3.2.1.3
	Residual Inforamtion Purging	Section 3.2.1.5
	Secure Debugging	Section 3.2.1.4
Security Services	Cryptographic Operation	Section 3.2.2.1
	Cryptographic Key Generation	Section 3.2.2.2
	Cryptographic KeyStore	Section 3.2.2.3
	Cryptographic Random Number Generation	Section 3.2.2.4
Software Isolation	Software Attacker Resistance: Isolation of Platform	Section 3.2.3.1

5 Bibliography

5 . 1 Evaluation Documents

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

[2] GlobalPlatform Technology SESIP Profile for Secure MCUs and MPUs, Version 1.0, GPT_SPE_150.

5 . 2 Developer Documents

[3] PN7642 Open NFC Controller - Objective Datasheet, Rev. 1.2, NXP Semiconductors.

[4] AN13134 – PN76 Family Evaluation Board - Quick Start Guide, Rev. 2.2, NXP Semiconductors.

[5] AN13719 – PN7642 Instruction Manual, Rev. 1.1, NXP Semiconductors.

[6] PN7642 Open NFC Controller - User API Documentation, Rev. 01.00, NXP Semiconductors.

[7] UM11566 - PN76 family NFC Open Controller - User Manual, Rev. 1.4, NXP Semiconductors.

[8] AN13720, PN7642 Secure Key Mode Demo, Rev. 1.1, 25 October 2022, NXP Semiconductors.

5 . 3 Standards

[9] FIPS PUB 180-4: Secure Hash Standard (SHS), Federal Information Processing Standards Publication, Information Technology Laboratory, National Institute of Standards and Technology, August 2015.

[10] FIPS PUB 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/National Institute of Standards and Technology, 26 November 2001.

[11] FIPS PUB 198-1-2008: The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication, July 2008, US Department of Commerce/National Institute of Standards and Technology.

[12] RFC 2104 - HMAC: Keyed-Hashing for Message Authentication, February 1997, IETF.

[13] FIPS PUB 186-4: Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, US Department of Commerce/National Institute of Standards and Technology, July 2013.

[14] NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Morris Dworkin, National Institute of Standards and Technology, December 2001.

[15] Addendum to NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, National Institute of Standards and Technology, October 2010.

[16] NIST SP 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, National Institute of Standards and Technology, May 2005.

[17] NIST SP 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, July 2007, Morris Dworkin, National Institute of Standards and Technology.

[18] NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/ Counter Mode (GCM) and GMAC, November 2007, Morris Dworkin, National Institute of Standards and Technology.

[19] NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised January 2012, National Institute of Standards and Technology.

[20] PKCS#1: RSA Cryptography Standard, Version 2.1.

[21] PKCS #1: RSA Cryptography Standard, Version 2.2, October 27, 2012, RSA Laboratories

[22] ISO/IEC 14888-3:2015: Information technology â€“ Security techniques â€“ Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms, 2016.

[23] ANSI X9.62-2005: Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute (ANSI), 2005.

[24] ANSI X9.63: Public Key Cryptography for The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, December 2011, American National Standards Institute.

[25] A proposal for: Functionality classes for random number generators, Wolfgang Killmann, T-Systems GEI GmbH, Werner Schindler, Bundesamt für Sicherheit in derInformationstechnik (BSI), Version 2.0, 18 September 2011.

[26] RFC 5869, HMAC-based Extract-and-Expand Key Derivation Function (HKDF), https://www.ietf.org/rfc/rfc5869.txt.

[27] RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA), https://www.rfc-editor.org/rfc/rfc8032.

[28] ISO/IEC 11770-3-2015: Information technology – Security techniques – Key management -- Part 3: Mechanisms using asymmetric techniques, 2015.

[29] ISO/IEC 15946-1-2008: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2008.

[30] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German “Bundesanzeiger“, , BAnz AT 30.01.2015 B3.

[31] The EAX Mode of Operation: A Two-Pass Authenticated-Encryption Scheme Optimized for Simplicity and Efficiency, M. Bellare, P.Rogaway, D. Wagner, March 2004.

[32] RFC 7748: Elliptic Curves for Security, https://www.rfc-editor.org/rfc/rfc7748.html.

6 Legal information

6.1 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.

6.2 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.

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.

Suitability for use in automotive applications — This NXP product has been qualified for use in automotive applications. If this product is used by customer in the development of, or for incorporation into, products or services (a) used in safety critical applications or (b) in which failure could lead to death, personal injury, or severe physical or environmental damage (such products and services hereinafter referred to as "Critical Applications"), then customer makes the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. As such, customer assumes all risk related to use of any products in Critical Applications and NXP and its suppliers shall not be liable for any such use by customer. Accordingly, customer will indemnify and hold NXP harmless from any claims, liabilities, damages and associated costs and expenses (including attorneys' fees) that NXP may incur related to customer's incorporation of any product in a Critical Application.

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.

Translations — A non-English (translated) version of a 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.

6.3 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
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 22 November 2022