P73N2M0B0.2C2/2C6 (R2)

Security Target Lite

Rev. 3.7 — 21 November 2023 **Product evaluation document**

COMPANY PUBLIC

Document information

Information	Content
Keywords	Security Target Lite, Crypto Library, Services Software, P73N2M0B0.2C2, P73N2M0B0.2C6
Abstract	This document is the Security Target Lite of P73N2M0B0.2C2/2C6 (R2). The TOE consists of the hardware “NXP High-performance secure controller P73N2M0B0.202” and the “Security Software on P73N2M0B0.202”, which is built upon this platform. Both parts are developed and provided by NXP Semiconductors. P73N2M0B0.2C2/2C6 (R2) complies with Evaluation Assurance Level 5 of the Common Criteria for Information Technology Security Evaluation Version 3.1 with augmentations.

Revision history

Revision number	Date	Description
3.7	2023-11-21	Derived from Security Target v3.7

Glossary

API	Application Programming Interface
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CRC	Cyclic Redundancy Check
ECB	Electronic Code Book (a block cipher mode of operation)
ECC	Elliptic Curve Cryptography
IT	Information Technology
PKC	Public Key Cryptography
PP	Protection Profile
SFR	Security Functional Requirement (CC context)
TOE	Target of Evaluation
TSF	Part of the TOE that realises the security functionality

1 ST Introduction

This chapter is divided into the following sections: "ST Identification", "TOE Overview" and "TOE Description".

1.1 ST Reference

“P73N2M0B0.2C2/2C6 (R2), Security Target Lite, Revision 3.7, NXP Semiconductors, 21 November 2023"

1.2 TOE Reference

The TOE is named "**P73N2M0B0.2C2/2C6 (R2)**". The TOE consists of:

- The hardware “NXP High-performance secure controller P73N2M0B0.202”
- The software “Security Software on P73N2M0B0.202” which is built upon this hardware platform.

The NXP High-performance secure controller P73N2M0B0.202 is named "P73N2M0B0.202" in short. The Security Software on P73N2M0B0.202 is named "Security Software" in short.

This Security Target builds on the Hardware Security Target [31], which refers to the “P73N2M0B0.202”, provided by NXP Semiconductors. Note that due to historical reasons the hardware platform provides a separate Security Target. In addition, the Security Software is addressed by the content of this Security Target. The superset of both Security Targets shall be considered to address the entire TOE. A self-sufficient version of the Security Targets would consist of all content of the two Security Targets copied into one document.

"P73N2M0B0.2C2/2C6 (R2)" uses the product naming scheme "P73N2M0B0.2wn" as introduced in [32]. With "*w*" being the NXP software combination identifier and "*n*" being the version identifier of the NXP software combination.

The TOE is configurable to

- **P73N2M0B0.2C2**
- **P73N2M0B0.2C6**

Both are evaluated configurations of the TOE that use the same underlying IC Hardware. They only differ in configuration data, IC Dedicated Support Software and Security Software stored to FLASH Memory.

1.3 TOE Overview

1.3.1 Introduction

The Hardware Security Target [31] contains, in Section 1.3 “TOE Overview”, an introduction about the P73N2M0B0.202 hardware TOE that is considered in the evaluation. The Hardware Security Target includes the P73N2M0B0.202 hardware platform provided with IC Dedicated Software.

The Security Software provides software that can be used by the Security IC Embedded Software. It consists of Services Software and Crypto Library.

Services Software

The Services Software consists of Flash Services Software and Services Framework Software. The Flash Services Software manages technical demands of the Flash memory and serves the Security IC Embedded Software with an interface for Flash erase and/or programming. The Services Framework Software represents a collection of different abstractions and utility functions that provide a runtime environment to the individual Services.

Crypto Library

The Crypto Library consists of several binary packages that are intended to be linked to the Security IC Embedded Software. The Security IC Embedded Software developer links the binary packages that he needs to his Embedded Software and the whole is subsequently implemented in arbitrary memory (Flash) of the hardware platform. The P73N2M0B0.202 provides the computing platform and cryptographic support by means of co-processors for the Crypto Library.

The Security Software of P73N2M0B0.2C2/2C6 provides the security functionality described below in addition to the functionality described in the Hardware Security Target [31] for the hardware platform. The Security Software uses hardware functionality that is covered by the scope of the platform evaluation like the PKC coprocessor.

The Crypto Library provides AES[1], DES[1], Triple-DES (3DES)[1], RSA, RSA key generation, RSA public key computation, ECDSA (ECC over GF(p)) signature generation and verification, ECDSA (ECC over GF(p)) key generation, ECDH (ECC Diffie-Hellmann) key-exchange, full point addition (ECC over GF(p)), ECDAA, standard security level SHA-224, SHA-256, SHA-384, SHA-512, SHA-3/224, SHA-3/256, SHA-3/384, SHA-3/512 algorithms, high security level SHA-224, SHA-256, SHA-384, SHA-512, SHA-3/224, SHA-3/256, SHA-3/384, SHA-3/512 algorithms, and HMAC algorithms.[2]

In addition, the Crypto Library implements a software (pseudo) random number generator which is initialized (seeded) by the hardware random number generator of the P73.

The Crypto Library also provides a secure copy routine, a secure memory move routine, a secure memory compare routine, cyclic redundancy check (CRC) routines, and includes internal security measures for residual information protection.

Note that the Crypto Library also implements KoreanSeed, Felica, OSCCA SM2, OSCCA SM3 and OSCCA SM4. However, KoreanSeed, Felica, OSCCA SM2, OSCCA SM3 and OSCCA SM4 are not in the scope of evaluation.

1.3.2 Life-Cycle

The Security Software is delivered in Phase 1 [3] as a software package (a set of binary files) to the developer of Security IC Embedded Software, to support its development process and to ensure compatibility when using the Security Software on the product.

The life cycle of the hardware platform as part of the TOE is described in Section 1.4.4 "Security During Development and Production" of the Hardware Security Target [31]. The

1 AES, DES, and Triple-DES can be used in ECB, CBC, CTR, CBC-MAC, or CMAC mode. In addition, AES can be used in GCM mode.
2 To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards).
3 For a definition of the Phases refer to Section 1.2.3 'TOE life cycle' of the Protection Profile [5]

Security Software uses the delivery process of the hardware platform, as the Security Software is preloaded to the Flash memory area of the IC.

The Security Software is stored separately from the Security IC Embedded Software to the Flash memory area under control of NXP.

Security during Development and Production

The development process of the TOE is part of the evaluation. The access to the implementation documentation, test bench and the source code is restricted to the development team of the TOE. The security measures installed within NXP, including a secure delivery process, ensure the integrity and quality of the delivered Security Software binary files.

1.3.3 Specific Issues of Hardware and the Common Criteria

Regarding the Application Note 2 of the Protection Profile [5] the TOE provides additional functionality which is not covered in the Protection profile [5] and the Hardware Security Target [31]. This additional functionality is added this Security Target (see Section 3.3).

1.4 TOE Description

The Target of Evaluation (TOE) consists of a hardware part (incl. IC Dedicated Software) and a software part:

- The hardware part "P73N2M0B0.202" consists of the P73N2M0B0.202 with IC Dedicated Software. The IC Dedicated Software of P73N2M0B0.202 comprises IC Dedicated Support Software. The IC Dedicated Support Software is composed of test software named Factory OS, boot software named Boot OS and memory driver software named Flash Driver Software. The P73N2M0B0.202 provides a programming interface (PI) for NXP, which gives access to the Flash Driver Software. For details, see [31]. The hardware part of the TOE includes dedicated guidance documentation [33].
- The software part "Security Software" is an extension of IC Dedicated Software that provides Services Software and Crypto Library, that can be operated on the hardware platform as described in this Security Target.

The hardware part of the TOE is not described in this document. Details are included in the Hardware Security Target [31] and therefore this latter document will be cited wherever appropriate.

The TOE configuration **P73N2M0B0.2C2** consists of all TOE components listed in Table 1 of the Hardware Security Target [31] plus all components listed in Table 1 and Table 3.

The TOE configuration **P73N2M0B0.2C6** consists of all TOE components listed in Table 1 of the Hardware Security Target [31] plus all components listed in Table 2 and Table 3.

Table 1. Components of the TOE specific for P73N2M0B0.2C2

Type	Name	Release	Form of Delivery
Services Software	Flash Services Software	**1.9.14**	Binary Services NVM image file encoded in Intel HEX format, stored to the Service Flash memory area of the die
	Services Framework Software		
Documents	Services User Manual, API and Operational Guidance	[34]	PDF document

Table 2. Components of the TOE specific for P73N2M0B0.2C6

Type	Name	Release	Form of Delivery
Services Software	Flash Services Software	**1.9.18**	Binary Services NVM image file encoded in Intel HEX format, stored to the Service Flash memory area of the die
	Services Framework Software		
Documents	Services User Manual, API and Operational Guidance	[34]	PDF document

Table 3. Components of the TOE common for P73N2M0B0.2C2 and P73N2M0B0.2C6

Type	Name	Release	Form of Delivery
Crypto Library	The Crypto Library consists of an entire set of individual Library Components, each providing an individual release version given below, that can be identified as decribed in [12] Crypto Library Components are:	**1.0.8**	Binary Crypto Library NVM image file encoded in Intel HEX format, stored to the Shared Flash memory area of the die
	`libphClRsa.a`	0x0100	
	`libphClRsaKg.a`	0x0107	
	`libphClEccGfp.a`	0x0010	
	`libphClEcdaa.a`	0x0004	
	`libphClSha.a`	0x0000	
	`libphClSecSha.a`	0x0000	
	`libphClSha3.a`	0x0000	
	`libphClSecSha3.a`	0x0000	
	`libphClRng.a`	0x0100	
	`phClRngHealthTest.a`	0x0100	
	`libphClUtils.a`	0x0100	
	`phClUtilsAsym.a`	0x0100	
	`libphClSymCfg.a`	0x0100	
	`libphClHmac.a`	0x0000	
	`libphClKoreanSeed.a`[1]	0x0000	
	`libphClFelica.a`[1]	0x0005	
	`libphClOscca.a`[1]	SM2: 0x0003 SM3: 0x0000 SM4: 0x0000	
Documents	User Guidance Manual	[12]	PDF document
	User Manual: RSA	[20]	PDF document
	User Manual: RSA Key Generation	[21]	PDF document
	User Manual: ECC over GF(p)	[22]	PDF document
	User Manual: ECDAA	[23]	PDF document
	User Manual: SHA	[14]	PDF document

Table 3. Components of the TOE common for P73N2M0B0.2C2 and P73N2M0B0.2C6 *...continued*

Type	Name	Release	Form of Delivery
	User Manual: SecSHA	[15]	PDF document
	User Manual: SHA3	[16]	PDF document
	User Manual: SecSHA3	[17]	PDF document
	User Manual: Hash	[18]	PDF document
	User Manual: RNG	[13]	PDF document
	User Manual: Utils	[24]	PDF document
	User Manual: SymCfg	[25]	PDF document
	User Manual: HMAC	[19]	PDF document
	User Manual: KoreanSeed[1]	[26]	PDF document
	User Manual: Felica[1]	[27]	PDF document
	User Manual: SM2[1]	[28]	PDF document
	User Manual: SM3[1]	[29]	PDF document
	User Manual: SM4[1]	[30]	PDF document

[1] However, KoreanSeed, Felica, OSCCA SM2, OSCCA SM3 and OSCCA SM4 are not in the scope of evaluation.

1.4.1 Hardware description

The NXP P73N2M0B0.202 hardware is described in Section 1.4.3.1 “Hardware Description” of the Hardware Security Target [31]. The IC Dedicated Software delivered with the hardware platform is described in Section 1.4.3.2 “Software Description” of the Hardware Security Target [31].

1.4.2 Software description

The Security Software consists of Services Software and Crypto Library.

1.4.2.1 Services Software

The Services Software comprises the Flash Services Software and Services Framework Software.

Flash Services Software

- The Flash Services Software manages technical demands of the Flash memory and serves the Security IC Embedded Software with an interface for Flash erase and/or programming.
- The Flash Services Software maintains the Flash with re-freshing, tearing-safe updates of Flash contents and wear leveling techniques to ensure integrity and consistency of its content and optimize its endurance.
- For more details, see [34].

Services Framework Software

- The Services Framework Software provides the utility functionality and interface for actual services. This comprises the control of services related functionality such as the resource management, patch handling, service and system configurations functionality.
- For more details, see [34].

1.4.2.2 Crypto Library

The Crypto Library (or parts thereof[4]) comprises a set of cryptographic functions.

AES

- The AES algorithm is intended to provide encryption and decryption functionality.
- The Crypto Library implements AES algorithm with different security configurations. For more details on those different configurations please refer the user guidance documentation of the Crypto Library [12].
- The following modes of operation are supported for AES: ECB, CBC, CTR, GCM, CBC-MAC and CMAC.

DES/TDES

- The DES and Triple-DES (TDES) algorithm are intended to provide encryption and decryption functionality.
- The Crypto Library implements DES algorithm with different security configurations. For more details on those different configurations please refer the user guidance documentation of the Crypto Library [12].
- The following modes of operation are supported for DES and Triple-DES: ECB, CBC, CTR, CBC-MAC and CMAC.

To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards). In particular this means that Single-DES shall not be used.

RSA

- The RSA algorithm can be used for encryption and decryption as well as for signature generation, signature verification, message encoding and signature encoding.
- The RSA key generation can be used to generate RSA key pairs.
- The RSA public key generation computation can be used to compute the public key that belongs to a given private CRT key.

The TOE supports various key sizes for RSA up to a limit of 4096 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

ECDSA (ECC over GF(p))

- The ECDSA (ECC over GF(p)) algorithm can be used for signature generation and signature verification.
- The ECDSA (ECC over GF(p)) key generation algorithm can be used to generate ECC over GF(p) key pairs for ECDSA.
- The ECDH (ECC Diffie-Hellman) key exchange algorithm can be used to establish cryptographic keys. It can be also used as secure point multiplication.
- Provide secure point addition for Elliptic Curves over GF(p).

The TOE supports various key sizes for ECC over GF(p) up to a limit of 640 bits for signature generation, key pair generation and key exchange. For signature verification the TOE supports key sizes up to a limit of 640 bits. To fend off attackers with high attack

4 Crypto functions are supplied as a library rather than as a monolithic program, and hence a user of the library may include only those functions that are actually required – it is not necessary to include all cryptographic functions of the library in every Security IC Embedded Software. For example, it is possible to omit the RSA or the SHA-3 components. However, some dependencies exist; details are described in the User Guidance [12].

potential an adequate key length must be used (references can be found in national and international documents and standards).

ECDAA

- The ECDAA library component implements the ECDAA related functions as specified in the TPM2.0 [9] specification. TPM 2.0 specifies two functions related to ECDAA: EccCommitCompute and EcDaa.
- The EccCommitCompute consists of several point multiplications which can be efficiently and easily performed using the ECC component.
- For the EcDaa function of TMP 2.0, the ECDAA component provides the `phClEcdaa_Sign` function.

To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

SHA

- The SHA-224, SHA-256, SHA-384, SHA-512, SHA-3/224, SHA-3/256, SHA-3/384 and SHA-3/512 algorithms can be used for different purposes such as computing hash values in the course of digital signature creation or key derivation.
- The Crypto Library implements two versions of each SHA algorithm with different security level: standard and high. The difference between the standard and high security level of the SHA implementations is that the high security level SHA is protected against more side-channel attacks.

To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards).

HMAC

- The HMAC algorithm can be used to calculate Keyed-Hash Authentication code. The TOE supports the calculation of HMAC authentication code with SHA-224, SHA-256, SHA-384, SHA-512, SHA-3/224, SHA-3/256, SHA-3/384 or SHA-3/512 hash algorithms. The HMAC algorithm can use either the high security level or standard security level version of SHA, depending on required security level.

To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards).

The TOE supports various key sizes for HMAC. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

KoreanSeed

- The KoreanSeed library component implements the Korean SEED symmetric cipher. It supports 128 bit and 256 bit keys as well as ECB, CBC, CTR, and CBC_MAC operating modes.

Note that KoreanSeed is not in the scope of evaluation.

Felica

- The Felica library component implements the Felica DES and Felica AES symmetric cipher.

Note that Felica is not in the scope of evaluation.

OSCCA SM2

- The OSCCA SM2 library component can be used for signature generation and signature verification.

Note that OSCCA SM2 is not in the scope of evaluation.

OSCCA SM3

- The OSCCA SM3 library component can be used to compute hash values in the course of digital signature creation or key derivation.

Note that OSCCA SM3 is not in the scope of evaluation.

OSCCA SM4

- The OSCCA SM4 library component implements the OSCCA SM4 symmetric cipher.

Note that OSCCA SM4 is not in the scope of evaluation.

Resistance of cryptographic algorithms against attacks

The cryptographic algorithms are resistant against attacks as described in JIL, JIL-ATT-SC: Attack Methods for Smartcards and Similar Devices [50], which include Side Channel Attacks, Perturbation attacks, Differential Fault Analysis (DFA) and timing attacks, except for standard/high security level SHA and HMAC, which are only resistant against Side Channel Attacks and timing attacks.

More details about conditions and restrictions for resistance against attacks are given in the user documentation of the Crypto Library [12].

Random number generation

- Library component to access random numbers generated by a software (pseudo) random number generator and to perform a test of the hardware (true) random number generator at initialisation.

Further security functionality of the Crypto Library

- Internal security measures for residual information protection
- Secure Memory Copy routine
- Secure Memory Move routine
- Secure Memory Boolean Compare routine
- CRC16 & CRC32 routines for cyclic redundancy check calculation

Note that the TOE does not restrict access to the functions provided by the hardware: these functions are still directly accessible to the Security IC Embedded Software.

1.4.3 Documentation

The documentation for the NXP P73N2M0B0.202 hardware is listed in Section 1.4.3.3 “Documentation” of the Hardware Security Target [31].

The documentation for the Security Software is listed in the following sub-sections.

1.4.3.1 Services Software

The use and operation of Flash Services Software is documented in [34].

1.4.3.2 Crypto Library

The Crypto Library has associated user manuals and one user guidance documentation (see [12]). The user manuals contain:

- the specification of the functions provided by the Crypto Library,
- details of the parameters and options required to call the Crypto Library by the Security IC Embedded Software

and the user guidance document contains:

- Guidelines on the secure usage of the Crypto Library, including the requirements on the environment (the Security IC Embedded Software calling the Crypto Library is considered to be part of the environment).

1.4.4 Interface of the TOE

The interface to the NXP P73N2M0B0.202 hardware is described in Section 1.4.5 “Interface of the TOE” of the Hardware Security Target [31]. The use of this interface is not restricted by the use of the Security Software.

The interface to the P73N2M0B0.2C2/2C6 additionally consists of software function calls, as detailed in the “User Manual” documents of the Security Software. The developer of the Security IC Embedded Software will link the required functionality of the Security Software into the Security IC Embedded Software as required for his Application.

1.4.5 Life Cycle and Delivery of the TOE

The life cycle of the hardware platform as part of the TOE is described in Section 1.4.4 "Security During Development and Production" of the Hardware Security Target [31]. The Security Software uses the delivery process of the hardware platform, as the Security Software is preloaded to the Flash memory area of the IC:

- The Services Software is stored separately from the Security IC Embedded Software in the "Service Window" RAM area of the P73N2M0B0.202 (see [32]). The content is defined via electronic Order Entry Form under control of NXP.
- The Crypto Library is stored separately from the Security IC Embedded Software in the Shared Flash memory area of the P73N2M0B0.202 (see [32]). The content is defined via electronic Order Entry Form under control of NXP.

Additionally, the Security Software is delivered as part of Phase 1 [5] as a software package (a set of binary files) to the developer of Security IC Embedded Software, to support its development process and to ensure compatibility when using the Security Software on the product. To protect the Security Software during the delivery process, the Security Software is encrypted and digitally signed.

An overview of the sites involved during development and manufacturing of the TOE is given in Table 4.

Table 4. Development and Manufacturing sites

Site	Company Address	Description	Life Cycle Phase acc. [5]
NXP Semiconductors Hamburg	Beiersdorfstr.12 (formerly known as Troplowitzstr. 20), 22529 Hamburg, Germany	Development & Test Center	Phase 2 - IC Development
		Trust Provisioning	Phase 3 - IC Manufacturing and Testing

5 For a definition of the Phases refer to Section 1.2.3 'TOE life cycle’ of the Protection Profile [5]

Table 4. Development and Manufacturing sites*...continued*

Site	Company Address	Description	Life Cycle Phase acc. [5]
		IT Admin	Phase 1 to 4
NXP Semiconductors Mougins	E space Park - Bat. C, 45 allee des Ormes, 06250 Mougins, France	Development Center	Phase 2 - IC Development
NXP Semiconductors Eindhoven	HTC-46.3-west Building 46, High Tech Campus, 5656AE Eindhoven, NL	Development Center	Phase 2 - IC Development
		IT Admin	Phase 1 to 4
NXP Semiconductors Caen	2 Esplanade Anton Phillips, 14000 Caen, France	Development Center	Phase 2 - IC Development
NXP Semiconductors Gratkorn	Mikron-Weg 1, 8101 Gratkorn, Austria	Development Center	Phase 2 - IC Development
		Trust Provisioning	Phase 3 - IC Manufacturing and Testing
NXP Semiconductors Glasgow	Pegasus House, Scottish Enterprise Technology Park, Bramah Ave, East Kilbride, Glasgow G75 0RD, Scotland	Development Center	Phase 2 - IC Development
NXP Semiconductors San Jose	411 East Plumeria Drive, San Jose, CA, 95134, USA	Development Center	Phase 2 - IC Development
NXP Semiconductors Bangalore	Nagawara Village, Kasaba Hobli, Bangalore 560 045, India	Development Center	Phase 2 - IC Development
NXP Semiconductors Leuven	Interleuvenlaan 80, 3001 Leuven, Belgium	Development Center	Phase 2 - IC Development
GlobalLogic Wroclaw	Ul. Strzegomska 48A, 53-611 Wroclaw, Poland	Development Center	Phase 2 - IC Development
SII Gdansk	SII Sp. Z o.o. Olivia Prime Building (Floor 10) - Grunwaldzka 472E, 80-309 Gdansk, Poland	Development Center	Phase 2 - IC Development
NXP Semiconductors Kaohsiung (ATKH)	10 Chin 5th Road, N.E.P.Z., 81170 Kaohsiung, Taiwan	Assembly & Test	Phase 3 - IC Manufacturing and Testing Phase 4 - IC Packaging
NXP Semiconductors Nijmegen	Gerstweg 2, 6534 AE Nijmegen, Netherlands	Failure Analysis Lab	Phase 3 - IC Manufacturing and Testing
Advanced Mask Technology Center Gmbh & Co KG (AMTC)	Rähnitzer Allee 9, 01109 Dresden, Germany	Wafer Mask Production	Phase 3 - IC Manufacturing and Testing
Global Foundries Singapore	Pte Ltd. 60 Woodlands Industrial Park D, Street 2, 738406 Singapore	Wafer Production	Phase 3 - IC Manufacturing and Testing
ASE Kaoshiung	26, Jing 3rd Rd., Nantze Export Processing Zone, Kaohsiung, Taiwan 811, R.O.C.	Assembly & Test	Phase 3 - IC Manufacturing and Testing Phase 4 - IC Packaging
NXP Virtual IT Network and Administration Site (NXP Master IT)	NXP Semiconductors, HTC Building 60, High Tech Campus, 5656 Eindhoven, NL	IT Admin	Phase 1 to 4
Datacenter Akquinet Hamburg	Akquinet Location, Ulzburger Str.201, 22850 Norderstedt, Germany	Data Center	Phase 1 to 4
Datacenter AtlasEdge (formerly known as Datacenter Colt) Hamburg	Obenhaupstr.1, 22335 Hamburg, Germany	Data Center	Phase 1 to 4
Datacenter Digital Realty Phoenix	Digital Realty, 120 East Van Buren St, Phoenix, AZ 85004, USA	Data Center	Phase 1 to 4
Datacenter Equinix Singapore	EQUINIX, 20 Ayer Rajah Crescent, IBX SG1, Level 5 Unit 5, Ayer Rajah Industrial Park, 139964 Singapore, Singapore	Data Center	Phase 1 to 4

1.4.6 TOE Type and TOE intended usage

The TOE is an IC hardware platform for various operating systems and applications with high security requirements.

The intended use cases are described in the Hardware Security Target [31], section 1.3.2 “Usage and major security functionality”, extended by the functionality as described in this Security Target in Section 1.3.

Regarding to Phase 7 (for a definition of the Phases refer to Section ‘1.2.3 TOE life cycle’ of the Protection Profile [5]), the combination of the hardware and the Security IC Embedded Software is used by the end-user. The method of use of the product in this phase depends on the application. The TOE is intended to be used in an unsecured environment, that is, the TOE does not rely on the Phase 7 environment to counter any threat.

The Security Software is intended to support the development of the Security IC Embedded Software since the Security Software include countermeasures against the threats described in this Security Target. The used modules of the Security Software are implemented as an extention of the Security IC Dedicated Software in the memory of the hardware platform.

1.4.7 TOE User Environment

The user environment for the P73N2M0B0.2C2/2C6 is the Security IC Embedded Software, developed by customers of NXP, to run on the NXP P73N2M0B0.202 hardware.

1.4.8 General IT features of the TOE

The general features of the NXP P73N2M0B0.202 hardware are described in Section 1.3 “TOE overview” of the Hardware Security Target [31]. These are supplemented for the TOE by the functions listed in Section 1.3.1 of this Security Target.

2 Conformance Claims

2.1 Conformance Claim

This Security Target and P73N2M0B0.2C2/2C6 (R2) claim conformance to version 3.1 of Common Criteria for Information Technology Security Evaluation, which comprises

- "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001" [1]
- "Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002" [2]
- "Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003" [3]

The TOE is evaluated against this Security Target in consideration of the methodology in

- "Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004" [4]

This Security Target claims to be CC Part 2 extended and CC Part 3 conformant. Section 5 of this Security Target defines the security functional components, which are extended beyond CC Part 2, and also demonstrates that they are consistent with the above conformance claim.

This Security Target also claims strict conformance to Protection Profile

- "Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084-2014" [5]

This conformance claim includes the following packages of security requirements out of those for Cryptographic Services defined in the Protection Profile [5].

- Package "TDES"
- Package "AES"

The minimum assurance level for the Protection Profile [5] is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

This Security Target claims conformance to assurance package **EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ALC_FLR.1, ATE_COV.3, ATE_FUN.2, ASE_TSS.2 and AVA_VAN.5.**. This claim includes and exceeds the minimum assurance level for the Protection Profile [5] as demonstrated in Section 6.2 of this Security Target.

The assurance level for evaluation and the functionality of the TOE are chosen in order to allow the confirmation that the TOE is suitable for use within devices compliant with the German Digital Signature Law.

2.2 Conformance Claim Rationale

According to chapter 2 this Security Target claims strict conformance to the Protection Profile [5]. As shown in 1.3 the TOE consists of hardware (Secure Controller IC) and software (IC Dedicated Software). This is identical to the TOE as defined in [5] and therefore the TOE type is consistent.

The Security Problem Definition in Section Section 3 of this Security Target includes all threats, organizational security policies and assumptions, which are identified in the Protection Profile [5], and this without any restrictions or modifications.

In addition, this Security Target contains additional threats, organizational security policies and assumptions. The additional assumptions neither mitigate any threat (or a part of it) nor fulfil any organizational security policy (or part of it). This is demonstrated in Section Section 3.4 of this Security Target.

The Security Objectives Rationale presented in Section Section 4.4 clearly identifies and justifies modifications and additions made to the rationale presented in the Protection Profile [5].

The Security Requirements Rationale presented in Section Section 6.3 has been updated with respect to the Protection Profile [5]. All PP requirements have been shown to be satisfied in the extended set of requirements whose completeness, consistency and soundness have been argued in the rationale sections of this Security Target.

3 Security Problem Definition

This Security Target claims strict conformance to the Security IC Platform protection profile [5]. The Assets, Assumptions, Threats and Organizational Security Policies of the Protection Profile are assumed here, together with extensions defined in chapter 3 “Security Problem Definition” of the Hardware Security Target [31].

In the following sub-sections the complete set of Assets, Assumptions, Threats and Organizational Security Policies will be listed.

3.1 Description of Assets

Since this Security Target claims strict conformance to the PP [5], the assets defined in Section 3.1 of the Protection Profile apply to this Security Target.

User Data and TSF data are mentioned as assets in the Hardware Securtiy Target [31].

Since the data computed by the Security Software contains keys, plain text and cipher text that are considered as User Data and e.g. blinding vectors that are considered as TSF data, the assets are considered as complete for this Security Target.

3.2 Threats

Since this Security Target claims strict conformance to the PP [5], the threats defined in Section 3.2 of the Protection Profile, and described in Section 3.2 “Threats” of the Hardware Security Target [31] are entirely valid for this Security Target.

All threats defined in section 3.2 of the Protection Profile [5], and threat T.Masquerade_TOE taken from package “Authentication of the Security IC” of the Protection Profile [5], as introduced in Hardware Security Target [31], are listed in Table 5.

Table 5. Threats defined in the Protection Profile

Name	Title
T.Malfunction	Malfunction due to Environmental Stress
T.Abuse-Func	Abuse of Functionality
T.Phys-Probing	Physical Probing
T.Phys-Manipulation	Physical Manipulation
T.Leak-Inherent	Inherent Information Leakage
T.Leak-Forced	Forced Information Leakage
T.RND	Deficiency of Random Numbers
T.Masquerade_TOE	Masquerade the TOE

Note 2. Within the Hardware Security Target [31], the threat T.RND has been used in a context where the hardware (true) random number generator is threatened. The P73N2M0B0.2C2/2C6 consists of both hardware (NXP P73N2M0B0.202) and software (Services Software and Crypto Library). The Crypto Library provides random numbers generated by a software (pseudo) random number generator. Therefore the threat T.RND explicitly includes both deficiencies of hardware random numbers as well as deficiency of software random numbers.

In compliance with Application Note 4 of the Protection Profile [5] the TOE provides security functionality that protects against the additional Threat introduced in Hardware Security Target [31], which is listed in Table 6. The definition and justification for that Threat are defined in the Hardware Security Target [31].

Table 6. Threats added in Hardware Security Target

Name	Title
T.Unauthorized-Access	Unauthorized Memory or Hardware Access

3.3 Organizational Security Policies

3.3.1 Security Policies from Protection Profile and Hardware Security Target

The organizational Security Policies defined in section 3.3, section 7.3.2 and section 7.4 of the Protection Profile [5] are listed in Table 7. They entirely apply to this Security Target.

Table 7. Organizational Security Policies defined in the Protection Profile

Name	Title
P.Process-TOE	Identification during TOE Development and Production
P.Crypto-Service	Cryptographic services of the TOE

In compliance with Application Note 5 of the Protection Profile [5] the Hardware Security Target [31] introduces security functionality, which requires an additional organizational Security Policy [6] that is listed in Table 8.

Table 8. Organizational Security Policies added in Hardware Security Target

Name	Title
P.Add-Components	Additional Specific Security Components

3.3.2 Security Policies specific to Crypto Library

The Crypto Library part of the TOE uses the AES co-processor hardware to provide AES security functionality, and the DES co-processor hardware to provide DES security functionality. In addition to the security functionality provided by the hardware and defined in the Hardware Security Target [31] the following additional security functionality is provided by the Crypto Library for use by the Security IC Embedded Software:

P.Add-Func — **Additional Specific Security Functionality**

The TOE provides the following additional security functionality to the Security IC Embedded Software:

- AES encryption and decryption,
- DES and Triple-DES encryption and decryption,

6 This Security Policy provides the following additional security functionality to the Security IC Embedded Software: Integrity support of content stored to Flash memory, computation of Cyclic Redundancy Checks, and support for Galois/Counter Mode (GCM) and GMAC

- RSA encryption, decryption, signature generation, signature verification, message encoding and signature encoding.
- RSA public key computation
- RSA key generation,
- ECDSA (ECC over GF(p)) signature generation and verification,
- ECC over GF(p) key generation,
- ECDH (ECC Diffie-Hellman) key exchange,
- ECC over GF(p) point addition,
- ECDAA (ECC-based Direct Anonymous Attestation),
- SHA-224, SHA-256, SHA-384, SHA-512, SHA-3/224, SHA-3/256, SHA-3/384 and SHA-3/512 Hash Algorithms,
- HMAC algorithm,
- access to the RNG (implementation of a software RNG),
- secure copy routine,
- secure move routine,
- secure compare routine,
- CRC16 and CRC32 routine,

In addition, the TOE shall

- provide protection of residual information, and
- provide resistance against attacks as described in Note 4 and in Security Architectural Information.

Regarding the Application Note 5 of the Protection Profile [5] there are no other additional policies defined in this Security Target.

3.4 Assumptions

Since this Security Target claims strict conformance to the PP [5], the assumptions defined in Section 3.4 of the Protection Profile (see Table 9), and defined in Section 3.4 “Assumptions” of the Hardware Security Target [31] (see Table 10) are entirely valid for this Security Target.

Table 9. Assumptions defined in the Protection Profile

Name	Title
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
A.Resp-Appl	Treatment of user data of the Composite TOE

Table 10. Assumptions defined in Hardware Security Target

Name	Title
A.Check-Init	Check of TOE identification data

4 Security Objectives

This chapter contains the following sections: “Security Objectives for the TOE”, “Security Objectives for the Security IC Embedded Software”, “Security Objectives for the Operational Environment”, and “Security Objectives Rationale”.

4.1 Security Objectives for the TOE

4.1.1 Security Objectives from the Protection Profile and the Hardware Security Target

The security objectives for the TOE defined in section 4.1, section 7.3.2 and section 7.4 of the Protection Profile [5] are listed in Table 11. They entirely apply to this Security Target.

Table 11. Security objectives for the TOE defined in the Protection Profile

Name	Title
O.Malfunction	Protection against Malfunctions
O.Abuse-Func	Protection against Abuse of Functionality
O.Phys-Probing	Protection against Physical Probing
O.Phys-Manipulation	Protection against Physical Manipulation
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Leak-Forced	Protection against Forced Information Leakage
O.RND	Random Numbers
O.Identification	TOE Identification
O.TDES	Cryptographic service Triple-DES
O.AES	Cryptographic service AES

In compliance with Application Note 9 of the Protection Profile [5] the TOE provides security functionality that results in the additional security objectives for the TOE as listed in Table 12. The security objectives in Table 12 are defined in the Hardware Security Target [31]. They entirely apply to this Security Target.

Table 12. Security Objectives for the TOE added in the Hardware Security Target

Name	Title
O.MEM-ACCESS	Memory Access Control
O.SFR-ACCESS	Special Function Register Access Control
O.FLASH-INTEGRITY	Integrity support of data stored to Flash memory
O.GCM-SUPPORT	Support for NIST Galois/Counter Mode and GMAC
O.CRC	Cyclic Redundancy Checks

4.1.2 Security Objectives specific to Crypto Library

Note 3. Within the Hardware Security Target [31], the objective O.RND has been used in context with the hardware (true) random number generator (RNG). In addition to this, the P73N2M0B0.2C2/2C6 also provides a software (pseudo) RNG. Therefore the objective

O.RND is extended to comprise also the quality of random numbers generated by the software (pseudo) RNG. See also Note 2 in Section 3.2, which extends T.RND in a similar way.

The O.RND defined in the HW ST is modified as follows:

O.RND	The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a sufficient entropy. The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys. This objective is applicable for both hardware (true) random number generator and software (pseudo) random number generator.

The following additional security objectives for the Crypto Library are defined by this ST, and are provided by the software part of the TOE:

O.SW_AES	The TOE includes functionality to provide encryption and decryption facilities of the AES algorithm, see Note 4
O.SW_DES	The TOE includes functionality to provide encryption and decryption facilities of the DES & Triple-DES algorithm, see Note 4
O.RSA	The TOE includes functionality to provide encryption, decryption, signature creation, signature verification, message encoding and signature encoding using the RSA algorithm, see Note 4.
O.RSA_PubExp	The TOE includes functionality to compute an RSA public key from an RSA private key, see Note 4.
O.RSA_KeyGen	The TOE includes functionality to generate RSA key pairs, see Note 4.
O.ECDSA	The TOE includes functionality to provide signature creation and signature verification using the ECC over GF(p) algorithm, see Note 4.
O.ECC_DHKE	The TOE includes functionality to provide Diffie-Hellman key exchange based on ECC over GF(p), see Note 4.
O.ECC_KeyGen	The TOE includes functionality to generate ECC over GF(p) key pairs, see Note 4.
O.ECC_Add	The TOE includes functionality to provide a point addition based on ECC over GF(p) , see Note 4.
O.ECDAA	The TOE includes functionality to provide the TPM 2.0 EccCommitCompute function and TPM 2.0 EcDaa function, see Note 4.
O.SHA	The TOE includes functionality to provide electronic hashing facilities using the SHA-224, SHA-256, SHA-384, SHA-512, SHA-3/224, SHA-3/256, SHA-3/384 and SHA-3/512 algorithms.
O.HMAC	The TOE includes the functionality to provide keyed-hash message authentication facilities using the HMAC algorithm.

O.COPY	The TOE includes functionality to copy memory content, see Note 4.
O.MOVE	The TOE includes functionality to move memory content, see Note 4.
O.COMPARE	The TOE includes functionality to compare memory content, see Note 4.
O.SW_CRC	The TOE includes functionality to privide Cyclic Redundancy Checks.
O.REUSE	The TOE includes measures to ensure that the memory resources being used by the TOE cannot be disclosed to subsequent users of the same memory resource.

Note 4. All introduced security objectives claiming cryptographic functionality and the security objectives for copy, move and compare are protected against attacks as described in the JIL, Attack Methods for s and Similar Devices [50], which include Side Channel Attacks, Perturbation attacks, Differential Fault Analysis (DFA) and timing attack. The following exceptions apply:

1. SHA-224, SHA-256, SHA-384, SHA-512, SHA-3/224, SHA-3/256, SHA-3/384 and SHA-3/512 are provided by the TOE with two implementations with different level of security:
   - One implementation does not contain protective measures against DPA and DFA
   - The other implementation does not contain protective measures against DFA but does contains protective measure against DPA
2. HMAC implementation do not contain protective measures against DFA.

This does not mean that the algorithm is insecure; rather at the time of this security target no promising attacks were found. More details about conditions and restrictions for resistance against attacks are given in the user documentation of the Crypto Library.

To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards).

4.2 Security Objectives for the Security IC Embedded Software

The security objectives for the Security IC Embedded Software defined in section 4.2 of the Protection Profile [5] are listed in Table 13. They entirely apply to this Security Target.

Table 13. Security objectives for the Security IC Embedded Software defined in the Protection Profile

Name	Title
OE.Resp-Appl	Treatment of user data of the Composite TOE

This Security Target does not add security objectives for the Security IC Embedded Software.

4.3 Security Objectives for the Operational Environment

The security objectives for the operational environment in section 4.3 of the Protection Profile [5] are listed in Table 14. They entirely apply to this Security Target.

Table 14. Security objectives for the operational environment defined in the Protection Profile

Name	Title
OE.Process-Sec-IC	Protection during composite product manufacturing

The Hardware Security Target [31] adds the security objectives for the operational environment listed in Table 15. The security objectives in Table 15 are defined in the Hardware Security Target [31]. They entirely apply to this Security Target.

Table 15. Security Objectives for the operational environment added in the Hardware Security Target

Name	Title
OE.Check-Init	Check of TOE identification data

4.4 Security Objectives Rationale

4.4.1 Rationale for Security Objectives from Protection Profile and Hardware Security Target

Section 4.4 of the Protection Profile [5] and Section 4.4 of the Hardware Security Target [31] provide a rationale how the threats, organisational security policies and assumptions are addressed by the objectives that are subject of the PP. They entirely apply to this Security Target.

4.4.2 Rationale for Security Objectives specific to Crypto Library

The justification for the additional security objectives for Crypto Library are listed in Table 16 below. They are in line with the security objectives of the Protection Profile and supplement these according to the additional assumptions and organisational security policy.

Table 16. Additional Security Objectives versus threats, assumptions or policies for Crypto Library

Threat, Assumption/ Policy	Security Objective	Note
T.RND	O.RND	T.RND and O.RND address the modifications for software (pseudo) random number generation made in Section 3.3.2 and Section 4.1.2.

Table 16. Additional Security Objectives versus threats, assumptions or policies for Crypto Library *...continued*

Threat, Assumption/ Policy	Security Objective	Note
P.Add-Func	O.RND O.SW_AES O.SW_DES O.RSA O.RSA_PubExp O.RSA_KeyGen O.ECDSA O.ECC_DHKE O.ECC_KeyGen O.ECC_Add O.ECDAA O.SHA O.HMAC O.REUSE O.COPY O.MOVE O.COMPARE O.SW_CRC	O.RND addresses the modification for software (pseudo) random number generation made in Section 4.1.2.

Since the objectives O.SW_AES, O.SW_DES, O.RSA, O.RSA_PubExp, O.RSA_KeyGen, O.ECDSA, O.ECC_DHKE, O.ECC_KeyGen, O.ECC_Add, O.ECDAA, O.SHA, O.HMAC, O.COPY, O.MOVE, O.COMPARE, O.SW_CRC and O.REUSE require the TOE to implement exactly the same specific security functionality as required by P.Add-Func, the organizational security policy P.Add-Func is covered by the security objectives.

Since the extended definition of the objective O.RND require the TOE to implement a software RNG as required by P.Add-Func, the organizational security policy P.Add-Func is covered by the security objectives. In addition O.RNG addresses T.RNG in the same generic way as the Protection Profile [5].

Additionally, the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality required by P.Add-Func and therefore support P.Add-Func. These security objectives are also valid for the additional specific security functionality since they must also avert the related threats for the components added to the organisational security policy.

The justification of the additional policy and the additional assumptions show that they do not contradict with the rationale already given in the Protection Profile [5] for the assumptions, policy and threats defined there.

5 Extended Components Definition

The extended components defined in chapter 5 of the Protection Profile [5] are listed in Table 17. They entirely apply to this Security Target.

Table 17. Extended components defined in the Protection Profile

Name	Title
FCS_RNG	Generation of random numbers
FMT_LIM	Limited capabilities and availability
FAU_SAS	FAU_SAS Audit data storage
FDP_SDC	Stored data confidentiality

To define the IT Security Functional Requirements of the TOE an additional family (FDP_SOP) of the Class FDP (user data protection) is defined here. This family describes the functional requirements for basic operations on data in the TOE.

Note that the PP “Security IC Platform Protection Profile [5] also defines extended security functional requirements in chapter 5, which are included in this Security Target.

As defined in CC Part 2, FDP class addresses user data protection. Secure basic operations (FDP_SOP) address protection of user data when it is processed by Copy or Compare function, respectively. Therefore, it is judged that FDP class is suitable for FDP_SOP family.

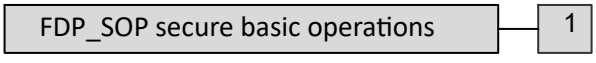
The reason for adding an extra family to FDP class is that existing families do not address protection of user data against all relevant attacks.

5.1 Secure basic operations (FDP_SOP)

Family Behaviour

This family defines requirements addressing the protection of data during security relevant basic operations inside the TSF. The data can comprise user data as well as TSF data. Appropriate separation between user data or TSF data shall be ensured by sequential, atomic processing of either TSF data or user data. The integrity and confidentiality of the data shall be protected during the processing of the basic operation against attacks. Each influence or interaction of the TOE that is not intended and/or specified is considered as attack.

Component levelling



FDP_SOP.1 requires the TOE to provide the possibility to perform basic secure operations on data

Management: FDP_SOP.1

There are no management activities foreseen.

Audit: FDP_SOP.1

There are no actions defined to be auditable.

FDP_SOP.1	**Secure Basic Operations**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SOP.1.1	The TSF shall provide basic operations [selection: *Copy, Move, Compare, ModMultiply, ModAddSub*] on objects stored in the TOE. The basic operation is applied between objects stored in [Selection: *memory location*][7] and [Selection: *memory location*][8].
FDP_SOP.1.2	The TSF shall protect the data against attacks from [selection: *disclosure, modification*] that can be inherently applied during the processing of the basic operations.
Application Notes:	The different memories are seen as possible objects.

The attacks addressed by disclosure and modification comprise side-channel attacks including timing attacks, fault injection attacks including manipulation of the basic operation result and attacks trying to violate the data separation based on the sequential operation.

7 [assignment: *list of memory locations*]
8 [assignment: *list of memory locations*]

6 Security Requirements

6.1 Security Functional Requirements

To support a better understanding of the combination Protection Profile and Security Target of the hardware platform (P73N2M0B0.202) vs. this Security Target (P73N2M0B0.2C2/2C6 (R2)), the TOE SFRs are presented in the following sections.

6.1.1 SFRs from the Protection Profile and the Hardware Security Target

The Security Functional Requirements (SFRs) for the TOE are specified in section 6.1 and in sections 7.4.1 and 7.4.2 of the Protection Profile [5]. They are defined in the Common Criteria [2] or in the Protection Profile [5].

Note 5. The requirements in Table 18 and Table 19 have been stated in the Hardware Security Target [31] and are fulfilled by the chip hardware, if not indicated otherwise in this section.

Table 18. Security functional requirements from the Hardware Security Target taken from Protection Profile

Name	Title
FRU_FLT.2	Limited fault tolerance
FPT_FLS.1	Failure with preservation of secure state
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FAU_SAS.1	Audit storage
FDP_SDC.1	Stored data confidentiality
FDP_SDI.2/AGE	Stored data integrity monitoring and action - Ageing
FDP_SDI.2/FLT	Stored data integrity monitoring and action - Faults
FPT_PHP.3	Resistance to physical attack
FDP_ITT.1	Basic internal transfer protection
FPT_ITT.1	Basic internal TSF data transfer protection
FDP_IFC.1	Subset information flow control
FCS_RNG.1/PTG.2	Random number generation - PTG.2
FCS_COP.1/TDES	Cryptographic operation - TDES
FCS_COP.1/AES	Cryptographic operation - AES
FCS_COP.1/GCM	Cryptographic operation - GCM
FCS_COP.1/CRC	Cryptographic operation - CRC
FCS_CKM.4/TDES	Cryptographic key destruction -TDES
FCS_CKM.4/AES	Cryptographic key destruction - AES

Table 19. Security functional requirements from the Hardware Security Target based on CC Part 2

Name	Title
FDP_ACC.1/MEM	Subset access control - Memories
FDP_ACC.1/SFR	Subset access control - Hardware components
FDP_ACF.1/MEM	Security attribute based access control - Memories
FDP_ACF.1/SFR	Security attribute based access control - Hardware components
FMT_MSA.1/MEM	Management of security attributes - Memories
FMT_MSA.1/SFR	Management of security attributes - Hardware components
FMT_MSA.3/MEM	Static attribute initialisation - Memories
FMT_MSA.3/SFR	Static attribute initialisation - Hardware components
FMT_SMF.1	Specification of Management Functions

6.1.2 Security Functional Requirements added in this Security Target

6.1.2.1 Crypto Library

The SFRs specific for Crypto Library are described in Table 20.

Table 20. SFRs defined in this Security Target for Crypto Library

Name	Title	Defined in
FCS_COP.1/SW_AES	Cryptographic operation - AES	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/SW_DES	Cryptographic operation - DES and TDES	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/RSA	Cryptographic operation (RSA encryption, decryption, signature and verification)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/RSA_PAD	Cryptographic operation (RSA message and signature encoding)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/RSA_PubExp	Cryptographic operation (RSA public key computation)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/ECDSA	ECDSA Cryptographic operation (ECC over GF(p) signature generation and verification)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/ECC_DHKE	ECDH Cryptographic operation (ECC Diffie-Hellman key exchange)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/ECC_Additional	ECC point addition	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/ECDAA	TPM 2.0 ECDAA operation	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/SHA	Cryptographic operation (SHA-224, SHA-256, SHA-384, SHA-512, SHA-3/224, SHA-3/256, SHA-3/384 and SHA-3/512)	CC Part 2 [2]; specified in this ST, see below.
FCS_COP.1/HMAC	Cryptographic operation (HMAC calculation)	CC Part 2 [2]; specified in this ST, see below.

Table 20. SFRs defined in this Security Target for Crypto Library*...continued*

Name	Title	Defined in
FCS_CKM.1/RSA	Cryptographic key generation (RSA key generation)	CC Part 2 [2]; specified in this ST, see below.
FCS_CKM.1/ECC	ECC Cryptographic key generation (ECC over GF(p) key generation)	CC Part 2 [2]; specified in this ST, see below.
FCS_CKM.4	Cryptographic Key Destruction	CC Part 2 [2]; specified in this ST, see below.
FDP_RIP.1	Subset Residual Information Protection	CC Part 2 [2]; specified in this ST, see below.
FCS_RNG.1/HYB-DET	Random number generation	PP Section 5.1 [5]; specified in this ST, see below.
FCS_RNG.1/HYB-PHY	Random number generation	PP Section 5.1 [5]; specified in this ST, see below.
FCS_COP.1/SW_CRC	Cryptographic operation - CRC	CC Part 2 [2]; specified in this ST, see below.

The requirements listed in Table 20 are detailed in the following sub-sections.

Additional SFR regarding cryptographic functionality

The TSF provides cryptographic functionality to help satisfy several high-level security objectives. In order for a cryptographic operation to function correctly, the operation must be performed in accordance with a specified algorithm and with a cryptographic key of a specified size. The following Functional Requirements to the TOE can be derived from this CC component:

FCS_COP.1/SW_AES	**Cryptographic operation - AES**
Hierarchical to:	No other components.
FCS_COP.1.1/SW_AES	The TSF shall perform *decryption and encryption* [9] in accordance with a specified cryptographic algorithm *AES in ECB, CBC, CTR, GCM, CBC-MAC or CMAC* [10] and cryptographic key sizes *128, 192 or 256 bit* [11] that meet the following *FIPS 197 [43], NIST SP 800-38A (ECB, CBC and CTR mode) [46], NIST SP 800-38D (GCM mode) [48], ISO 9797-1, Algorithm 1 (CBC-MAC mode) [49], and NIST SP 800-38B (CMAC mode) [47]* [12].
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [50].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/SW_DES	**Cryptographic operation - DES and TDES**
Hierarchical to:	No other components.

9 [assignment: *list of cryptographic operations*]
10 [assignment: *cryptographic algorithm*]
11 [assignment: *cryptographic key sizes*]
12 [assignment: *list of standards*]

FCS_COP.1.1/SW_DES	The TSF shall perform *encryption and decryption* [13] in accordance with a specified cryptographic algorithm *and Triple-DES in ECB, CBC, CTR, CBC-MAC or CMAC* [14] and cryptographic key sizes *1-key DES (56 bit), 2-key TDES (112 bit) or 3-key TDES (168 bit)* [15] that meet the following *FIPS Publication 46-3 (DES and TDES) [42] and NIST Special Publication 800-38A, 2001 (ECB, CBC and CTR mode) [46], ISO 9797-1, Algorithm 1 (CBC-MAC mode) [49], and NIST Special Publication 800-38B (CMAC mode) [47]* [16].
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [50]. To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards).
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/RSA	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/RSA	The TSF shall perform *encryption, decryption, signature and verification*[17] in accordance with the specified cryptographic algorithm *RSA*[18] and cryptographic key sizes *1024 bits to 4096 bits*[19] that meet the following: *PKCS #1, v2.2: RSAEP, RSADP, RSASP1, RSAVP1*[20].
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [50]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/RSA_PAD	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/RSA_PAD	The TSF shall perform *message and signature encoding methods*[21] in accordance with the specified

13 [assignment: *list of cryptographic operations*]
14 [assignment: *cryptographic algorithm*]
15 [assignment: *cryptographic key sizes*]
16 [assignment: *list of standards*]
17 [assignment: *list of cryptographic operations*]
18 [assignment: *cryptographic algorithm*]
19 [assignment: *cryptographic key sizes*]
20 [assignment: *list of standards*]
21 [assignment: *list of cryptographic operations*]

	cryptographic algorithm *EME-OAEP and EMSA-PSS*[22] and cryptographic key sizes *1024 bits to 4096 bits*[23] that meet the following: *PKCS #1, v2.2: EME-OAEP and EMSA-PSS*[24].
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [50]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/RSA_PubExp	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/RSA_PubExp	The TSF shall perform *public key computation*[25] in accordance with the specified cryptographic algorithm *RSA*[26] and cryptographic key sizes *1024 bits to 4096 bits*[27] that meet the following: *PKCS #1, v2.2*[28].
Application Notes:	(1) The security functionality is resistant against side channel analysis and other attacks described in [50]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards). (2) The computation will result in the generation of a public RSA key from the private key (in CRT format). As this key is implied by the private key, this is not true key generation, and, to prevent duplication in this ST, this has not been included as a separate FCS_CKM.1 SFR.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/ECDSA	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/ECDSA	The TSF shall perform *signature generation and verification*[29] in accordance with the specified cryptographic algorithm *ECDSA / ECC over GF(p)*[30] and

22 [assignment: *cryptographic algorithm*]
23 [assignment: *cryptographic key sizes*]
24 [assignment: *list of standards*]
25 [assignment: *list of cryptographic operations*]
26 [assignment: *cryptographic algorithm*]
27 [assignment: *cryptographic key sizes*]
28 [assignment: *list of standards*]
29 [assignment: *list of cryptographic operations*]
30 [assignment: *cryptographic algorithm*]

	cryptographic key sizes *128 to 640 bits*[31] that meet the following: *ISO/IEC 15946-2*[32].
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [50]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/ECC_DHKE	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/ECC_DHKE	The TSF shall perform *Diffie-Hellman Key Exchange*[33] in accordance with the specified cryptographic algorithm *ECC over GF(p)*[34] and cryptographic key sizes *128 to 640 bits*[35] that meet the following: *ISO/IEC 15946-3*[36].
Application Notes:	(1) The security functionality is resistant against side channel analysis and other attacks described in [50]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards). (2) The security functionality does not provide the complete key exchange procedure, but only the point multiplication which is used for the multiplication of the private key with the communication partner's public key. Therefore this function can be used as part of a Diffie-Hellman key exchange as well pure point multiplication.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/ECC_Additional	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/ECC_Additional	The TSF shall perform *a full point addition*[37] in accordance with the specified cryptographic algorithm *ECC over GF(p)*[38] and cryptographic key sizes *128 to 640 bits*[39] that meet the following: *ISO/IEC 15946-1*[40].

31 [assignment: *cryptographic key sizes*]
32 [assignment: *list of standards*]
33 [assignment: *list of cryptographic operations*]
34 [assignment: *cryptographic algorithm*]
35 [assignment: *cryptographic key sizes*]
36 [assignment: *list of standards*]
37 [assignment: *list of cryptographic operations*]
38 [assignment: *cryptographic algorithm*]
39 [assignment: *cryptographic key sizes*]
40 [assignment: *list of standards*]

Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [50]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/ECDAA	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/ECDAA	The TSF shall perform *the TPM 2.0 EccCommitCompute function and TPM 2.0 EcDaa function*[41] in accordance with the specified cryptographic algorithm *ECC over GF(p)*[42] and cryptographic key sizes *128 to 640 bits*[43] that meet the following: *TPM Rev. 2.0*
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [50]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.
FCS_COP.1/SHA	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1/SHA	The TSF shall perform *hashing*[44] in accordance with the specified cryptographic algorithm *SHA-224, SHA-256, SHA-384, SHA-512, SHA-3/224, SHA-3/256, SHA-3/384 and SHA-3/512*[45] and cryptographic key size *none*[46] that meet the following: *FIPS 180-4 [40] and FIPS 202 [41]*[47].
Application Notes:	1) The security functionality is resistant against side channel analysis and timing attacks as described in [50]. To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards)..

41 [assignment: *list of cryptographic operations*]
42 [assignment: *cryptographic algorithm*]
43 [assignment: *cryptographic key sizes*]
44 [assignment: *list of cryptographic operations*]
45 [assignment: *cryptographic algorithm*]
46 [assignment: *cryptographic key sizes*]
47 [assignment: *list of standards*]

(2) The length of the data to hash has to be a multiple of one byte. Arbitrary bit lengths are not supported.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.

FCS_COP.1/HMAC **Cryptographic operation**

Hierarchical to: No other components.

FCS_COP.1.1/HMAC The TSF shall perform *keyed-hash message authentication code calculation*[48] in accordance with a specified cryptographic algorithm *SHA-224, SHA-256, SHA-384, SHA-512, SHA-3/224, SHA-3/256, SHA-3/384 and SHA-3/512*[49] and cryptographic key size *none*[50] that meet the following: *FIPS PUB 198-1 [39] and FIPS 202 [41]*[51]

Application Notes: The security functionality is resistant against side channel analysis and other attacks described in [50]. To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards)..

Dependencies: [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.

The TSF provides functionality to generate a variety of key pairs. In order for the key generation to function correctly, the operation must be performed in accordance with a specified standard and with cryptographic key sizes out of a specified range. The following Security Functional Requirements to the TOE can be derived from this CC component:

FCS_CKM.1/RSA **Cryptographic Key Generation**

Hierarchical to: No other components.

FCS_CKM.1.1/RSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA*[52] and specified cryptographic key sizes *1024 to 4096 bits*[53] that meet the following: *PKCS #1, v2.2 [52] and FIPS PUB 186-4 [44]*[54].

Application Notes: The security functionality is resistant against side channel analysis and other attacks described in [50]. To fend off attackers with high attack potential an adequate

48 [assignment: *list of cryptographic operations*]
49 [assignment: *cryptographic algorithm*]
50 [assignment: *cryptographic key sizes*]
51 [assignment: *list of standards*]
52 [assignment: *cryptographic key generation algorithm*]
53 [assignment: *cryptographic key sizes*]
54 [assignment: *list of standards*]

	key length must be used (references can be found in national and international documents and standards).
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1/ECC	**Cryptographic Key Generation**
Hierarchical to:	No other components.
FCS_CKM.1.1/ECC	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDSA (ECC over GF(p))*[55] and specified cryptographic key sizes *128 to 640 bits*[56] that meet the following: *ISO/IEC 15946-1 [35] , ANSI X9.62 [51] and FIPS PUB 186-4 [44].* [57].
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [50]. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FDP_RIP.1	**Subset Residual Information Protection**
Hierarchical to:	No other components.

This family addresses the need to ensure that information in a resource is no longer accessible when the resource is deallocated, and that therefore newly created objects do not contain information that was accidentally left behind in the resources used to create the objects. The following Functional Requirement to the TOE can be derived from the CC component FDP_RIP.1:

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from*[58] the following objects: *all objects (variables) used by the Crypto Library as specified in the user guidance documentation*[59].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

Note 6. The TSF ensures that, upon exit from each function, with the exception of input parameters, return values or locations where it is explicitly documented that values remain at specific addresses, any memory resources used by that function that contained temporary or secret values are cleared

55 [assignment: *cryptographic algorithm*]
56 [assignment: *cryptographic key sizes*]
57 [assignment: *list of standards*]
58 [selection: *allocation of the resource to, deallocation of the resource from*]
59 [assignment: *list of objects*]

FCS_CKM.4	**Cryptographic Key Destruction**
Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwrite*[60] that meets the following: *ISO11568*[61]
Application Notes:	The P73N2M0B0.2C2/2C6 (R2) provides the smartcard embedded software with library calls to perform various cryptographic algorithms that involve keys (e.g., AES, DES, RSA, etc.). Through the parameters of the library calls the smartcard embedded software provides keys for the cryptographic algorithms. To perform its cryptographic algorithms the library copies these keys, or a transformation thereof, to the working-buffer (supplied by the smartcard embedded software) and/or the memory/special function registers of the P73N2M0. Depending upon the algorithm the library either overwrites these keys before returning control to the smartcard embedded software or provides a library call to through which the smartcard embedded software can clear these keys. In the case of a separate library call to clear keys the guidance instructs the smartcard embedded software when/how this call should be used.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Note:	Clearing of keys that are provided by the smartcard embedded software to the Crypto Library is the responsibility of the smartcard embedded software.

The TOE shall meet the requirements “Random number generation” as specified below.

The hardware part of the TOE (NXP P73N2M0B0.202) provides a physical random number generator (RNG) that fulfils FCS_RNG.1 as already mentioned above in Section 6.1.1. The additional software part of the TOE (Crypto Library) implements a software (pseudo) RNG that fulfils FCS_RNG.1/HYB-DET (see below). This software RNG obtains its seed from the hardware RNG, after the TOE (Crypto Library) has performed a self test of the hardware RNG.

FCS_RNG.1/HYB-DET	**Random number generation**
Hierarchical to:	No other components.
FCS_RNG.1.1/HYB-DET	The TSF shall provide a *hybrid deterministic*[62] random number generator that implements: (K.4.1) a chi-squared test on the seed generator. (DRG.4.1) The internal state of the RNG shall use PTRNG of class PTG.2 (as defined in [7]) as random source.

60 [assignment: *cryptographic key destruction method*]
61 [assignment: *list of standards*]
62 *[selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]*

(DRG.4.2) The RNG provides forward secrecy (as defined in [7]).

(DRG.4.3) The RNG provides backward secrecy even if the current internal state is known (as defined in [7]).

(DRG.4.4) The RNG provides enhanced forward secrecy on demand (as defined in [7]).

(DRG.4.5) The internal state of the RNG is seeded by an PTRNG of class PTG.2 [63] (as defined in [7]).

FCS_RNG.1.2/HYB-DET

The TSF shall provide *random numbers* that meet:

(K.4.2) class K.4 of AIS20 [8].

(DRG.4.6) The RNG generates output for which 2^{48} strings of bit length 128 are mutually different with probability at least $1 - 2^{-24}$.

(DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A (as defined in [7]).

Application Notes:

(1) The security functionality is resistant against side channel analysis and similar techniques.

(2) The P73N2M0B0.2C2/2C6 (R2) provides the smartcard embedded software with separate library calls to initialise the random number generator (which includes the chi-squared test) and to generate random data. The user can call an initialisation function upon use of the random number generator.

Dependencies: No dependencies.

Note: Only if the chi-squared test succeeds the hardware RNG seeds the software RNG implemented as part of the Crypto Library on P73 (as part of security functionality SS.SW_RNG).

Note: The Crypto Library does not prevent the operating system from accessing the hardware RNG. If the hardware RNG is used by the operating system directly, it has to be decided based on the Smartcard Embedded Software's security needs, what kind of test has to be performed and what requirements will have to be applied for this test. In this case the developer of the Smartcard Embedded Software must ensure that the conditions prescribed in the Guidance, Delivery and Operation Manual for the NXP High-performance secure controller P73N2M0B0.202 are met.

The software (pseudo) RNG, which is implemented in the software part of the TOE (Crypto Library), fulfils FCS_RNG.1/HYB-PHY (see below) with a certain limitation.

63 *[assignment: list of security capabilities]*

This limitation can be given by the Security IC Embedded Software. For details on the limitation please refer the user guidance documentation of the Crypto Library [12].

FCS_RNG.1/HYB-PHY	**Random number generation**
Hierarchical to:	No other components.
FCS_RNG.1.1/HYB-PHY	The TSF shall provide a *hybrid physical*[64] random number generator that implements: (PTG.3.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure has been detected no random numbers will be output. (PTG.3.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source. (PTG.3.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG is started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 postprocessing algorithm have been finished successfully or when a defect has been detected. (PTG.3.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon. (PTG.3.5) The online test procedure checks the raw random number sequence. It is triggered *continuously* [65]. The online test is suitable for detecting nontolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time. (PTG.3.6) The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-processing algorithm shall not exceed its input data rate.
FCS_RNG.1.2/HYB-PHY	The TSF shall provide *numbers* [66] that meet: (PTG.3.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A (as defined in [7]).

64 [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]
65 [selection: *externally, at regular intervals, continuously, upon specified internal events*]
66 [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*]

	(PTG.3.8) The internal random numbers shall *use PTRNG of class PTG.2 as random source for the post-processing*[67].
FCS_COP.1/SW_CRC	**Cryptographic operation - CRC**
Hierarchical to:	No other components.
FCS_COP.1.1/SW_CRC	The TSF shall perform *calculation of cyclic redundancy checks* [68] in accordance with a specified cryptographic algorithm *CRC-16 resp. CRC-32* [69] and cryptographic key sizes *none* [70] that meet the following: *CRC-CCITT [10] resp. IEEE 802.3 [11]* [71].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction.

6.1.2.1.1 Extended Security Functional Requirements for Crypto Library

The SFRs in Section 6.1.2.1 are further supplemented by the following iterations of an extended SFR, as listed in Table 21.

Table 21. Extended SFRs defined for Crypto Library

Name	Title	Defined in
FDP_SOP.1/Copy	Secure Basic operations (secure copy)	Specified in this ST, see below.
FDP_SOP.1/Move	Secure Basic operations (secure move)	Specified in this ST, see below.
FDP_SOP.1/Compare	Secure Basic operations (secure compare)	Specified in this ST, see below.

The FDP_SOP.1 (secure basic operations) is introduced as a new component within a new family FDP_SOP consisting only of that new component

FDP_SOP.1/Copy	**Secure Basic Operations**
Hierarchical to:	No other components.
FDP_SOP.1.1/Copy	The TSF shall provide basic operations *Copy* on objects stored in the TOE. The basic operation is applied between objects stored in *ROM, RAM and Flash*[72] and *RAM*[73].
FDP_SOP.1.2/Copy	The TSF shall protect the data against attacks from *disclosure and modification* that can be inherently applied during the processing of the basic operations.
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [50].

67 [selection: *use PTRNG of class PTG.2 as random source for the post-processing, have [assignment: work factor], require [assignment: guess work]*]
68 [assignment: *list of cryptographic operations*]
69 [assignment: *cryptographic algorithm*]
70 [assignment: *cryptographic key sizes*]
71 [assignment: *list of standards*]
72 [assignment: *list of memory locations*]
73 [assignment: *list of memory locations*]

FDP_SOP.1/Move	**Secure Basic Operations**
Hierarchical to:	No other components.
FDP_SOP.1.1/Move	The TSF shall provide basic operations *Move* on objects stored in the TOE. The basic operation is applied between objects stored in *ROM, RAM and Flash*[74] and *RAM*[75].
FDP_SOP.1.2/Move	The TSF shall protect the data against attacks from *disclosure and modification* that can be inherently applied during the processing of the basic operations.
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [50].
FDP_SOP.1/Compare	**Secure Basic Operations**
Hierarchical to:	No other components.
FDP_SOP.1.1/Compare	The TSF shall provide basic operations *Compare* on objects stored in the TOE. The basic operation is applied between objects stored in *ROM, RAM and Flash*[76] and *ROM, RAM and Flash*[77].
FDP_SOP.1.2/Compare	The TSF shall protect the data against attacks from *disclosure and modification* that can be inherently applied during the processing of the basic operations.
Application Notes:	The security functionality is resistant against side channel analysis and other attacks described in [50].
Dependencies:	No dependencies.

6.2 Security Assurance Requirements

Table 22 lists the security assurance requirements for the TOE. These security functional requirements are either copied from the Protection Profile [5] without modifications, or augmented from there, or newly added in this Security Target as indicated in column three of the table. This partly addresses Application Note 22.

Table 22. Security assurance requirements for the TOE

Name	Title	compared to PP
ADV_ARC.1	Security architectural description	as in PP
ADV_FSP.5	Complete semi-formal functional specification with additional error information	augmented from PP
ADV_IMP.2	Complete mapping of the implementation representation of the TSF	augmented from PP
ADV_INT.3	Minimally complex internals	added for EAL5
ADV_TDS.5	Complete semiformal modular design	augmented from PP

74 [assignment: *list of memory locations*]
75 [assignment: *list of memory locations*]
76 [assignment: *list of memory locations*]
77 [assignment: *list of memory locations*]

Table 22. Security assurance requirements for the TOE *...continued*

Name	Title	compared to PP
AGD_OPE.1	Operational user guidance	as in PP
AGD_PRE.1	Preparative procedures	as in PP
ALC_CMC.5	Advanced support	augmented from PP
ALC_CMS.5	Development tools CM coverage	augmented from PP
ALC_DEL.1	Delivery procedures	as in PP
ALC_DVS.2	Sufficiency of security measures	as in PP
ALC_FLR.1	Basic flaw remediation	not in PP, added for EAL5+
ALC_LCD.1	Developer defined life-cycle model	as in PP
ALC_TAT.3	Compliance with implementation standards - all parts	augmented from PP
ASE_CCL.1	Conformance claims	as in PP
ASE_ECD.1	Extended components definition	as in PP
ASE_INT.1	ST introduction	as in PP
ASE_OBJ.2	Security objectives	as in PP
ASE_REQ.2	Derived security requirements	as in PP
ASE_SPD.1	Security problem definition	as in PP
ASE_TSS.2	TOE summary specification with architectural design summary	augmented from PP
ATE_COV.3	Rigorous analysis of coverage	augmented from PP
ATE_DPT.3	Testing: modular design	augmented from PP
ATE_FUN.2	Ordered functional testing	augmented from PP
ATE_IND.2	Independent testing - sample	as in PP
AVA_VAN.5	Advanced methodical vulnerability analysis	as in PP

All refinements in section 6.2.1 of the Protection Profile [5] to security assurance requirements in Table 22, which are copied from the Protection Profile without modifications, entirely apply to this Security Target.

All refinements in section 6.2.1 of the Protection Profile [5] to security assurance requirements in Table 22, which are augmented from the Protection Profile, are discussed below in their applicability to this Security Target. This addresses Application Note 23 in the Protection Profile [5].

Refinements regarding ADV_FSP

Refinement no. 215 to ADV_FSP.4 in the Protection Profile [5] is not relevant for this Security Target since the TOE does not embed IC Dedicated Test Software.

The Factory OS is not considered as IC Dedicated Test Software but instead as IC Dedicated Support Software since it is **not** only used to support testing of the TOE during production and **does** provide security functionality to be used after TOE delivery, which both contradicts to abstract 12 on page 8 of the Protection Profile [5]. However, the Factory OS provides testing capabilities for production testing and analysis of field returns, which is under restricted access to NXP and not for usage by the Composite Product Manufacturer. Therefore, these testing capabilities are considered as "test tool",

which don't have to be described in the Functional Specification, but only be evaluated against their abuse after TOE delivery. Apart from that the Factory OS provides the Composite Product Manufacturer with some basic functional testing of the TOE and also with a readout of the identification flags of the TOE from System Page Common, which must be described in the Functional Specification.

Refinements no. 216, no. 217 and no. 218 to ADV_FSP.4 in the Protection Profile [5] are entirely applicable to ADV_FSP.5 since the refinements clarify the scope of the functional specification, and ADV_FSP.5 adds to this scope in accordance with the refinements.

Refinements regarding ADV_IMP

Refinement no. 223 to ADV_IMP.1 in the Protection Profile [5] is redundant since it is implicitly covered by the augmentation to ADV_IMP.2. First, ADV_IMP.2 requires the developer to provide the mapping between the TOE design description and the entire implementation representation instead of a sample of it only as in ADV_IMP.1. Second, ADV_IMP.2 requires the evaluator to confirm that, for the entire implementation representation and not only for a sample of it as in ADV_IMP.1, the information provided meets all requirements for content and presentation of evidence.

Refinements regarding ALC_CMC

Refinement no. 205 to ALC_CMC.4 in the Protection Profile [5] is entirely applicable to ALC_CMC.5 since the refinement clarifies the scope of configuration items in ALC_CMC.4, and ALC_CMC.5 does not touch this scope.

Refinement no. 206 to ALC_CMC.4 in the Protection Profile [5] is entirely applicable to ADV_CMC.5 since the refinement details requirements on configuration management of the TOE for ALC_CMC.4, which are not subverted in ADV_CMC.5.

Refinements regarding ALC_CMS

Refinement no. 199 to ALC_CMS.4 in the Protection Profile [5] is entirely applicable to ALC_CMS.5 since the refinement clarifies the scope of the configuration item "TOE implementation representation" on the configuration list of ALC_CMS.4, and ALC_CMS.5 adds new configuration items to the configuration list.

Refinements regarding ATE_COV

Refinements no. 226 and no. 227 to ALC_COV.2 in the Protection Profile [5] are entirely applicable to ALC_COV.3 since they define some particular requirements on the test coverage for ALC_COV.2, which are not subverted in ALC_COV.3.

6.3 Security Requirements Rationale

6.3.1 Rationale for the Security Functional Requirements

6.3.1.1 SFRs from the Hardware Security Target

Table 23 list the mapping of the security objectives to the security functional requirements from the Hardware Security Target [31]. This mapping entirely applies to this Security Target.

Table 23. Mapping of the security objectives to the security functional requirements of the Hardware Security Target

Security objective for the TOE	Security functional requirement of the TOE
O.Malfunction	FRU_FLT.2, FPT_FLS.1
O.Abuse-Func	FMT_LIM.1, FMT_LIM.2
	FRU_FLT.2, FTP_FLS.1
	FPT_PHP.3
	FDP_ITT.1, FPT_ITT.1, FDP_IFC.1
O.Phys-Probing	FPT_PHP.3
	FDP_SDC.1
O.Phys-Manipulation	FDP_SDI.2/FLT
	FPT_PHP.3
O.Leak-Inherent	FDP_ITT.1, FPT_ITT.1 , FDP_IFC.1
O.Leak-Forced	FRU_FLT.2, FPT_FLS.1
	FPT_PHP.3
	FDP_ITT.1, FPT_ITT.1, FDP_IFC.1
O.RND	FCS_RNG.1/PTG.2
	FRU_FLT.2, FPT_FLS.1
	FPT_PHP.3
	FDP_ITT.1, FPT_ITT.1 , FDP_IFC.1
O.Identification	FAU_SAS.1
O.TDES	FCS_COP.1/TDES
	FCS_CKM.4/TDES
O.AES	FCS_COP.1/AES
	FCS_CKM.4/AES
O.FLASH-INTEGRITY	FDP_SDI.2/AGE
O.GCM-SUPPORT	FCS_COP.1/GCM
O.CRC	FCS_COP.1/CRC
O.MEM-ACCESS	FDP_ACC.1/MEM
	FDP_ACF.1/MEM
	FMT_MSA.1/MEM
	FMT_MSA.3/MEM
	FMT_SMF.1
O.SFR-ACCESS	FDP_ACC.1/SFR
	FDP_ACF.1/SFR
	FMT_MSA.1/SFR
	FMT_MSA.3/SFR
	FMT_SMF.1

6.3.1.2 SFRs specific to Crypto Library

The rationale for the security functional requirements that are specific for Crypto Library is described below.

Note 7. O.RND has been extended if compared to the PP [5] to include also a software RNG (see also Note 3). The rationale given in the PP only covers the part of O.RND dealing with the hardware RNG. For O.RND additional functionality (software RNG) and additional requirements (FCS_RNG.1/HYB-DET, and FCS_RNG.1/HYB-PHY) have been added. The explanation following Table 24 describes this in detail.

This ST lists a number of security objectives and SFRs for P73N2M0B0.2C2/2C6, which are additional to both the PP and the Hardware ST. These are listed in the following table.

Table 24. Mapping of SFRs to Security Objectives for Crypto Library in this ST

Objective	TOE Security Functional Requirements
O.SW_AES	FCS_COP.1/SW AES ADV.ARC.1 (and underlying platform SFRs)
O.SW_DES	FCS_COP.1/SW DES ADV.ARC.1 (and underlying platform SFRs)
O.RSA	FCS_COP.1/RSA FCS_COP.1/RSA_Pad ADV.ARC.1 (and underlying platform SFRs)
O.RSA_PubExp	FCS_COP.1/RSA_PubExp ADV.ARC.1 (and underlying platform SFRs)
O.RSA_KeyGen	FCS_CKM.1/RSA ADV.ARC.1 (and underlying platform SFRs)
O.ECDSA	FCS_COP.1/ECDSA ADV.ARC.1 (and underlying platform SFRs)
O.ECC_DHKE	FCS_COP.1/ECC_DHKE ADV.ARC.1 (and underlying platform SFRs)
O.ECC_Add	FCS_COP.1/ECC_Additional ADV.ARC.1 (and underlying platform SFRs)
O.ECC_KeyGen	FCS_CKM.1/ECC ADV.ARC.1 (and underlying platform SFRs)
O.ECDAA	FCS_COP.1/ECDAA ADV.ARC.1 (and underlying platform SFRs)
O.SHA	FCS_COP.1/SHA ADV.ARC.1 (and underlying platform SFRs)
O.HMAC	FCS_COP.1/HMAC ADV.ARC.1 (and underlying platform SFRs)
O.COPY	FDP_SOP.1/Copy ADV.ARC.1 (and underlying platform SFRs)
O.MOVE	FDP_SOP.1/Move ADV.ARC.1 (and underlying platform SFRs)
O.COMPARE	FDP_SOP.1/Compare ADV.ARC.1 (and underlying platform SFRs)

Table 24. Mapping of SFRs to Security Objectives for Crypto Library in this ST*...continued*

Objective	TOE Security Functional Requirements
O.SW_CRC	FCS_COP.1/SW_CRC ADV.ARC.1 (and underlying platform SFRs)
O.REUSE	FDP_RIP.1 FCS_CKM.4
O.RND	FCS_RNG.1/HYB-DET FCS_RNG.1/HYB-PHY ADV.ARC.1 (and underlying platform SFRs)

The justification of the security objectives O.SW_AES, O.SW_DES, O.RSA, O.RSA_PubExp, O.RSA_KeyGen, O.ECDSA, O.ECC_DHKE, O.ECC_Add, O.ECC_KeyGen, O.ECDAA, O.SHA, O.HMAC, O.COPY, O.MOVE, O.COMPARE and O.SW_CRC are all as follows:

- Each objective is directly implemented by a single SFR specifying the (cryptographic) service that the objective wishes to achieve (see the above table for the mapping).
- The requirements and architectural measures that originally were taken from the Protection Profile [5] and thus were also part of the Security Target of the hardware (chip) evaluation support the objective:
  - ADV.ARC.1 (and underlying platform SFRs) supports the objective by ensuring that the TOE works correctly (i.e., all of the TOE's capabilities are ensured) within the specified operating conditions and maintains a secure state when the TOE is outside the specified operating conditions. A secure state is also entered when perturbation or DFA attacks are detected.
  - ADV.ARC.1 (and underlying platform SFRs) ensures that no User Data (plain text data, keys) or TSF Data is disclosed when they are transmitted between different functional units of the TOE (i.e., the different memories, the CPU, cryptographic co-processors), thereby supporting the objective in keeping confidential data secret.
- ADV.ARC.1 (and underlying platform SFRs) by ensuring that User Data and TSF Data are not accessible from the TOE except when the Security IC Embedded Software decides to communicate them via an external interface.

The justification of the security objective O.REUSE is as follows:

- O.REUSE requires the TOE to provide procedural measures to prevent disclosure of memory contents that was used by the TOE. This applies to the P73N2M0B0.2C2/2C6 (R2) and is met by the SFR FDP_RIP.1 and FCS_CKM.4, which requires the library to make unavailable all memory contents that has been used by it. Note that the requirement for residual information protection applies to all functionality of the Cryptographic Library.

The justification of the security objective O.RND is as follows:

- O.RND requires the TOE to generate random numbers with (a) ensured cryptographic quality (i.e. not predictable and with sufficient entropy) such that (b) information about the generated random numbers is not available to an attacker.
  1. Ensured cryptographic quality (sufficient entropy part) of generated random numbers is met by FCS_RNG.1.1/HYB-DET through the characteristic 'hybrid deterministic', by FCS_RNG.1.1/HYB-PHY through the characteristic 'hybrid physical', and by the random number generator meeting NIST SP 800-90A. Ensured cryptographic quality (not predictable part) of generated random numbers is met by FCS_RNG.1/HYB-DET through the characteristic 'chi-squared test

of the seed generator', by FCS_RNG.1/HYB-PHY through the characteristic 'cryptographic post-processing algorithm', and FCS_RNG.1 from the certified hardware platform.

2. Information about the generated random numbers is not available to an attacker is met through ADV.ARC.1, which prevent physical manipulation and malfunction of the TOE and support this objective because they prevent attackers from manipulating or otherwise affecting the random number generator.

6.3.2 Dependencies of security requirements

SFRs [FDP_ITC.1, or FDP_ITC.2 or FCS_CKM.1] are not included in this Security Target for FCS_COP.1/SW_AES, FCS_COP.1/SW_DES, FCS_COP.1/SHA and FCS_COP.1/HMAC since the TOE only provides a pure engine for these algorithms without additional features like the handling of keys or importing data from outside the TOE. Therefore the Security IC Embedded Software must fulfil these requirements related to the needs of the realized application.

Note that the requirement for residual information protection applies to all functionality of the Cryptographic Library. Therefore SFR FCS_CKM.4 fulfills dependencies of FCS_COP.1 for all its iterations SW_AES, SW_DES, RSA, RSA_PAD, RSA_PubExp, ECDSA, ECC_DHKE, ECC_Additional, ECDAA, SHA, HMAC and SW_CRC.

6.3.3 Rationale for the Security Assurance Requirements

The Protection Profile [5] targets EAL4 augmented with ALC_DVS.2, and AVA_VAN.5 and also gives a rationale for this choice, which is entirely applicable to this Security Target.

This Security Target augments from EAL4 to EAL5 in order to meet increasing assurance expectations of digital signature applications and electronic payment systems on the resistance to attackers with high attack potential. The augmentations to EAL4 in the Protection Profile [5] are mandatory for EAL5.

This Security Target augments EAL5 with ALC_FLR.1 and ASE_TSS.2 for the following reasons.

ALC_FLR.1 is added to cover policies and procedures that are applied to track and correct flaws and to support surveillance of the TOE.

ASE_TSS.2 is chosen to give architectural information on the security functionality of the TOE, which enhances comprehensibility.

In addition, this Security Target also augments EAL5 with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_TAT.3, ATE_FUN.2, and ATE_COV.3 for the following reasons.

ADV_TDS.5 is added to provide a complete semiformal modular design of the TOE.

ADV_IMP.2 is added to provide a complete mapping of the implementation representation of the TSF.

ADV_INT.3 is added to provide justification of the complexity of the TOE.

ALC_CMC.5 is added to fulfill ADV_IMP.2.

ALC_TAT.3 is added to adapt a complete compliance to relevant implementation standards.

ATE_FUN.2 is added to provide well-structured and well-documented tests.

ATE_COV.3 is added to confirm exhaustive tests performed on all interfaces.

7 TOE Summary Specification

This chapter describes the "IT Security Functionality".

7.1 IT Security Functionality

The evaluation of this P73N2M0B0.2C2/2C6 is performed as an evaluation, where the TOE comprises both the underlying hardware and the embedded software (Services Software and Crypto Library. The TOE of this evaluation therefore extends the security functionality already available in the chip platform (see Section 7.1 "Portions of the TOE Security Functionality" of the Hardware Security [31]).

Note 8. The security functionality SS.RNG implements the hardware RNG. The P73N2M0B0.2C2/2C6 also implements software RNG as part of security functionality SS.SW_RNG; for details see Section 7.1.1.2.14. The hardware RNG is not externally visible through the interfaces of the Crypto Library; instead users of the Crypto Library are intended to use the software RNG (SS.SW_RNG).

Note 9. The security functionality SF.LOG is extended by the P73N2M0B0.2C2/2C6 as described in Security Architectural Information.

The additional security functionality provided by the TOE is described in the following sub-sections.

The IT security functionalities directly correspond to the TOE security functional requirements defined in Section 6.1. The definitions of the IT security functionalities refer to the corresponding security functional requirements.

7.1.1 Security Services

7.1.1.1 Security Services of the hardware platform

The Security Services of the hardware platform P73N2M0B0.202 are described in the the Hardware Security Target [31] and are listed in Table 25. These Security Services entirely apply to the TOE.

Table 25. Security Services of the Hardware Security Target

Security Services	Name
SS.RNG	Random Number Generator
SS.TDES	Triple-DES coprocessor
SS.AES	AES coprocessor
SS.GCM	GCM coprocessor
SS.SBC	SBC interface functions
SS.CRC	CRC coprocessor

7.1.1.2 Security Services specific to Crypto Library

The security services for P73N2M0B0.2C2/2C6 include the security services for the hardware platform and, in addition, the following security services for Crypto Library.

7.1.1.2.1 SS.SW_AES

The TOE uses the P73 AES hardware coprocessor to provide AES encryption and decryption facility using 128, 192 or 256 bit keys.

The TOE implements additional countermeasures that are configurable at runtime and provides functionality for handling checksums over loaded keys.

The supported modes are ECB, CBC, CTR, GCM, CBC-MAC and CMACECB, CBC, CBC-MAC and CMAC (i.e. the CBC mode applied to the block cipher algorithm AES).

In addition, the TOE provides the ability to compute a CBC-MAC. The CBC-MAC mode of operation is rather similar to the CBC mode of operation, but returns only the last cipher text (see also [49], Algorithm 1).

SS.SW_AES is a basic cryptographic function which provides the AES algorithm as defined by the standard [43].

The interface to SS.SW_AES allows AES operations independent from prior key loading. The user has to take care that adequate keys of the correct size are loaded before the cryptographic operation is performed. Details are described in the user guidance [12] and the user manual [25].

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_COP.1/SW_AES

7.1.1.2.2 SS.SW_DES

The TOE uses the P73 Triple-DES hardware coprocessor to provide a DES encryption and decryption facility using 56-bit keys, and to provide Triple-DES encryption and decryption. The Triple-DES function uses double-length or triple-length keys with sizes of 112 or 168 bits respectively.

The TOE implements additional countermeasures that are configurable at runtime and provides functionality for handling checksums over loaded keys.

The supported modes are ECB, CBC, CTR, CBC-MAC and CMAC ECB, CBC, CBC-MAC and CMAC(i.e. the CBC mode applied to the block cipher algorithm TDES or DES).

In addition, the TOE provides the ability to compute a CBC-MAC. The CBC-MAC mode of operation is rather similar to the CBC mode of operation, but returns only the last cipher text (see also [49], Algorithm 1, or [45], Appendix F). Like ECB, CBC, and CTR, the CBC-MAC mode of operation can also be applied to both DES and TDES as underlying block cipher algorithm.

To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards). In particular this means that Single-DES shall not be used.

SS.SW_DES is a modular basic cryptographic function which provides the DES and Triple-DES algorithm (with two and three keys) as defined by the standard [42].

The interface to SS.SW_DES allows performing Single-DES or 2-key and 3-key Triple-DES operations independent from prior key loading. The user has to take care that adequate keys of the correct size are loaded before the cryptographic operation is performed. Details are described in the user manual [25]. All modes of operation (ECB,

CBC, CTR, CBC MAC) can be applied to DES, two-key TDES and three-key TDES for a total of nine possible combinations.

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_COP.1/SW_DES

7.1.1.2.3 SS.RSA

The TOE provides functions that implement the RSA algorithm and the RSA-CRT algorithm for data encryption, decryption, signature and verification. All algorithms are defined in PKCS #1, v2.2 (RSAEP, RSADP, RSAP1, RSAVP1) [52].

This routine supports various key lengths from 512 bits to 4096 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

The TOE contains modular exponentiation functions, which, together with other functions in the TOE, perform the operations required for RSA encryption or decryption. Two different RSA algorithms are supported by the TOE, namely the "Simple Straight Forward Method" (called RSA "straight forward", the key consists of the pair n and d) and RSA using the "Chinese Remainder Theorem" (RSA CRT, the key consists of the quintuple p, q, dp, dq, qInv).

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_COP.1/RSA

7.1.1.2.4 SS.RSA_Pad

The TOE provides functions that implement the RSA algorithm and the RSA-CRT algorithm for message and signature encoding. This IT security functionality supports the EME-OAEP and EMSA-PSS signature scheme. All algorithms are defined in PKCS #1, v2.2 (EME-OAEP, EMSA-PSS) [52].

This routine supports various key lengths from 512 bits to 4096 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_COP.1/RSA_PAD

7.1.1.2.5 SS.RSA_PublicExp

The TOE provides functions that implement computation of an RSA public key from a private CRT key. All algorithms are defined in PKCS #1, v2.2 [52].

This routine supports various key lengths from 512 bits to 4096 bits (CRT). To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_COP.1/RSA_PubExp

7.1.1.2.6 SS.ECDSA

The TOE provides functions to perform ECDSA Signature Generation and Signature Verification according to ISO/IEC 15946-2 [36].

Note that hashing of the message must be done beforehand and is not provided by this security functionality, but could be provided by SS.SHA.

The supported key length is 128 to 640 bits for signature generation and 128 to 640 bits for signature verification. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_COP.1/ECDSA

7.1.1.2.7 SS.ECC_DHKE

The TOE provides functions to perform Diffie-Hellman Key Exchange according to ISO/IEC 15946-3 [37].

The supported key length is 128 to 640 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_COP.1/ECC_DHKE

7.1.1.2.8 SS.ECC_Additional

The TOE provides functions to perform a full ECC point addition according to ISO/IEC 15946-1 [35] .

The supported key length is 128 to 640 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_COP.1/ECC_Additional

7.1.1.2.9 SS.ECDAA

The TOE provides the ECDAA related functions as specified in the TPM2.0 [9] specification: EccCommitCompute and EcDaa (see Part 4 of [9]).

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_COP.1/ECDAA

7.1.1.2.10 SS.RSA_KeyGen

The TOE provides functions to generate RSA key pairs as described in PKCS #1, v2.2 [52] and FIPS PUB 186-4 [44] (Algorithm acc. Appendix B.3.3). With this the TOE complies to the content of SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms [53].

It supports various key lengths from 512 bits to 4096 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Two different output formats for the key parameters are supported by the TOE, namely the "Simple Straight Forward Method" (RSA "straight forward") and RSA using the "Chinese Remainder Theorem" (RSA CRT).

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_CKM.1/RSA

7.1.1.2.11 SS.ECC_KeyGen

The TOE provides functions to perform ECC over GF(p) Key Generation according to ISO/IEC 15946-1 section 6.1 [35], “ANSI X9.62 [51] and FIPS PUB 186-4 [44]. With this the TOE complies to the content of SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms [53].

It supports key length from 128 to 640 bits. To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_CKM.1/ECC

7.1.1.2.12 SS.SHA

The TOE implements functions to compute the Secure Hash Algorithms SHA-224, SHA-256, SHA-384 and SHA-512 according to the standard FIPS 180-4 [40] and SHA-3/224, SHA-3/256, SHA-3/384 and SHA-3/512 according to the standard FIPS 202 [41]. The TOE implements functions to compute the Secure Hash Algorithms SHA-224, SHA-256, SHA-384 and SHA-512 according to the standard FIPS 180-4 [40]

and SHA-3/224, SHA-3/256, SHA-3/384 and SHA-3/512 according to the standard FIPS 202 [41].

To fend off attackers with high attack potential an adequate security level must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_COP.1/SHA

7.1.1.2.13 SS.HMAC

The TOE provides functions to perform HMAC Keyed-hash Message Authentication algorithm according to FIPS 198-1 [39].

There is no limitation on the supported key length except that it must be a multiple of 8 bits.

To fend off attackers with high attack potential an adequate key length must be used (references can be found in national and international documents and standards).

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_COP.1/HMAC

7.1.1.2.14 SS.SW_RNG

The TOE contains both a hardware Random Number Generator (RNG) and a software RNG; for the hardware RNG (SS.RNG) see the Note 8. SS.SW_RNG consists of the implementation of the software RNG and of appropriate online tests for the hardware RNG (as required for FCS_RNG.1/HYB-DET and FCS_RNG.1/HYB-PHY taken from the Protection Profile [5] and the proposal for AIS20/31 [7]):

The Crypto Library implements a software (pseudo) RNG that can be used as a general purpose random source. This software RNG has to be seeded by random numbers taken from the hardware RNG implemented in the P73 processor. The implementation of the software RNG is based on the standard NIST SP 800-90A as described in [38].

In addition, the Crypto Library implements appropriate online tests according to the Hardware User Guidance Manual [33] for the hardware RNG, which fulfils the functionality class P2 defined by the AIS31 [6] and class PTG.2 defined by the proposal for AIS20/31 [7], as required by SFR FCS_RNG.1/HYB-DET and SFR FCS_RNG.1/HYB-PHY. The interface of SS.SW_RNG allows to test the hardware RNG and to seed the software RNG after successful testing.

This security functionality covers:

- FCS_RNG.1/HYB-DET
- FCS_RNG.1/HYB-PHY

7.1.1.2.15 SS.COPY

The security service SS.COPY implements functionality to copy memory content in a secure manner protected against attacks.

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FDP_SOP.1/Copy

7.1.1.2.16 SS.MOVE

The security service SS.MOVE implements functionality to move memory content in a secure manner protected against attacks.

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FDP_SOP.1/Move

7.1.1.2.17 SS.COMPARE

The security service SS.COMPARE implements functionality to compare different blocks of memory content in a manner protected against attacks.

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FDP_SOP.1/Compare

7.1.1.2.18 SS.SW_CRC

SS.SW_CRC serves the Security IC Embedded Software with calculation of of cyclic redundancy checks as defined in [10] for 16 bits and in [11] for 32 bits.

Attack resistance for this security functionality is discussed in Security Architectural Information.

This security functionality covers:

- FCS_COP.1/SW_CRC

7.1.2 Security Features

7.1.2.1 Security Features from the hardware platform

The Security Features of the hardware platform P73N2M0B0.202 are described in the the Hardware Security Target [31] and are listed in Table 26. These Security Services entirely apply to the TOE.

Table 26. Security Features of the Hardware Security Target

Security Features	Name
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation
SF.LOG	Logical Protection

Table 26. Security Features of the Hardware Security Target*...continued*

Security Features	Name
SF.FOS-USE	Factory OS use restrictions
SF.MEM-ACC	Memory Access Control
SF.SFR-ACC	Special Function Register Access Control
SF.FLSV-SUP	Flash Services Software support

7.1.2.2 Crypto Library

The security features for P73N2M0B0.2C2/2C6 include the security features for the hardware platform and, in addition, the following security features for Crypto Library.

7.1.2.2.1 SF.Object_Reuse

The TOE provides internal security measures which clear memory areas used by the Crypto Library after usage. This functionality is required by the security functional component FDP_RIP.1 and FCS_CKM.4, taken from the Common Criteria Part 2 [2].

These measures ensure that a subsequent process may not gain access to cryptographic assets stored temporarily in memory used by the TOE.

This security functionality covers:

- FDP_RIP.1
- FCS_CKM.4

7.2 Security Architectural Information

Details deleted here, available only in the full version of the Security Target.

8 Annexes

8.1 Further Information contained in the PP

The Annex of the Protection Profile ([5], chapter 7) provides further information. Section 7.1 of the PP describes the development and production process of smartcards, containing a detailed life-cycle description and a description of the assets of the Integrated Circuits Designer/Manufacturer. Section 7.6 of the PP gives examples of Attack Scenarios.

8.2 Glossary and Vocabulary

Note: To ease understanding of the used terms the glossary of the Protection Profile [5] is included here.

Application Data	All data managed by the Security IC Embedded Software in the application context. Application data comprise all data in the final Security IC.
Authentication reference data	Data used to verify the claimed identity in an authentication procedure.
Authentication verification data	Data used to prove the claimed identity in an authentication procedure.
Composite Product Integrator	Role installing or finalizing the IC Security IC Embedded Software and the applications on platform transforming the TOE into the unpersonalized Composite Product after TOE delivery. The TOE Manufacturer may implement IC Security IC Embedded Software delivered by the Security IC Embedded Software Developer before TOE delivery (e.g. if the IC Security IC Embedded Software is implemented in ROM or is stored in the non-volatile memory as service provided by the IC Manufacturer or IC Packaging Manufacturer).
Composite Product Manufacturer	The Composite Product Manufacturer has the following roles (i) the Security IC Embedded Software Developer (Phase 1), (ii) the Composite Product Integrator (Phase 5) and (iii) the Personalizer (Phase 6). If the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice) he has the role of the IC Packaging Manufacturer (Phase 4) in addition. The customer of the TOE Manufacturer who receives the TOE during TOE Delivery. The Composite Product Manufacturer includes the Security IC Embedded Software developer and all roles after TOE Delivery up to Phase 6 (refer to Figure 2 on page 10 and Section 7.1.1).
End-consumer	User of the Composite Product in Phase 7.
IC Dedicated Software	IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional

	services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.
Initialization Data	Initialization Data defined by the TOE Manufacturer to identify the TOE and to keep track of the Security IC's production and further life-cycle phases are considered as belonging to the TSF data. These data are for instance used for traceability and for TOE identification (identification data).
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
Memory	The memory comprises of the RAM, ROM and the Flash of the TOE.
Memory Management Unit	The MMU maps the virtual addresses used by the CPU into the physical addresses of RAM, ROM and Flash. This mapping is done based on memory partitioning. Memory partitioning is fixed.
MIFARE	Contact-less smart card interface standard, complying with ISO14443A.
Pre-personalization Data	Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases.
Security IC	(as used in this Protection Profile) Composition of the TOE, the Security IC Embedded Software, user data of the Composite TOE and the package (the Security IC carrier).
Security IC Embedded Software	Software embedded in a Security IC and normally not being developed by the IC Designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3 or in later phases of the Security IC product life-cycle. Some part of that software may actually implement a Security IC application others may provide standard services. Nevertheless, this distinction doesn't matter here so that the Security IC Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.

Security IC Product	Composite product which includes the Security Integrated Circuit (i.e. the TOE) and the Security IC Embedded Software and is evaluated as composite target of evaluation in the sense of the Supporting Document
Secured Environment	Operational environment maintains the confidentiality and integrity of the TOE as addressed by OE.Process-Sec-IC and the confidentiality and integrity of the IC Security IC Embedded Software, TSF data or user data associated with the product by security procedures of the product manufacturer, personaliser and other actors before delivery to the end-user depending on the life-cycle.
Test Features	All features and functions (implemented by the IC Dedicated Test Software and/or hardware) which are designed to be used before TOE Delivery only and delivered as part of the TOE.
TOE Delivery	The period when the TOE is delivered which is (refer to Figure 2 on page 10) either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.
TOE Manufacturer	The TOE Manufacturer must ensure that all requirements for the TOE (as defined in Section 1.2.2) and its development and production environment are fulfilled (refer to Figure 2 on page 10). The TOE Manufacturer has the following roles: (i) IC Developer (Phase 2) and (ii) IC Manufacturer (Phase 3). If the TOE is delivered after Phase 4 in form of packaged products, he has the role of the (iii) IC Packaging Manufacturer (Phase 4) in addition.
TSF data	Data for the operation of the TOE upon which the enforcement of the SFR relies. They are created by and for the TOE, that might affect the operation of the TOE. This includes information about the TOE's configuration, if any is coded in non-volatile non-programmable memories (ROM), in non-volatile programmable memories (for instance E2PROM or flash memory), in specific circuitry or a combination thereof.
User data of the Composite TOE	All data managed by the Security IC Embedded Software in the application context.
User data of the TOE	Data for the user of the TOE, that does not affect the operation of the TSF. From the point of view of TOE defined in this PP the user data comprises the Security IC Embedded Software and the user data of the Composite TOE.

9 Bibliography

9 . 1 Evaluation documents

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

[5] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0084-2014

[6] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitaetsklassen und Evaluationsmethodologie fuer physikalische Zufallszahlengeneratoren, Version 2.1, 02.12.2011, Bundesamt fuer Sicherheit in der Informationstechnik

[7] A proposal for: Functionality classes for random number generators, Version 2.0, 18 September 2011

[8] AIS20: Anwendungshinweise und Interpretationen zum Schema (AIS), Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1, December 2nd, 1999

[9] TPM Rev. 2.0: Trusted Platform Module Library Specification, Family "2.0", Level 00, Revision 01.07- March 2014

[10] "SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATION Public data networks – Interfaces, Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit", International Telecommunication Union, ITU-T Recommendation X.25, October 1996

[11] "IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications", IEEE Computer Society, IEEE Std 802.3™-2005, Dec-12, 2005

9 . 2 Developer documents

[12] P73N2M0 Crypto Library: Information on Guidance and Operation, DocID: 402814

[13] P73N2M0 Crypto Library: User Manual – RNG Library, DocID: 401411

[14] P73N2M0 Crypto Library: User Manual – SHA Library, DocID: 401710

[15] P73N2M0 Crypto Library: User Manual – Secure SHA Library, DocID: 401810

[16] P73N2M0 Crypto Library: User Manual – SHA-3 Library, DocID: 402010

[17] P73N2M0 Crypto Library: User Manual – Secure SHA-3 Library, DocID: 402110

[18] P73N2M0 Crypto Library: User Manual – HASH Library, DocID: 403810

[19] P73N2M0 Crypto Library: User Manual – HMAC Library, DocID: 401310

[20] P73N2M0 Crypto Library: User Manual – Rsa Library (Rsa), DocID: 401510

[21] P73N2M0 Crypto Library: User Manual – RSA Key Generation Library (RsaKg), DocID: 401610
[22] P73N2M0 Crypto Library: User Manual – ECC over GF(p) Library, DocID: 401210
[23] P73N2M0 Crypto Library: User Manual – ECDAA, DocID: 402410
[24] P73N2M0 Crypto Library: User Manual – Utils Library, DocID: 402210
[25] P73N2M0 Crypto Library: User Manual – Symmetric Cipher Library (SymCfg), DocID: 401110
[26] P73N2M0 Crypto Library: User Manual – Korean SEED Library, DocID: 402310
[27] P73N2M0 Crypto Library: User Manual – FELICA, Version 1.0
[28] P73N2M0 Crypto Library: User Manual – OSCCA-SM2 over GF(p) Library, DocID: 402510
[29] P73N2M0 Crypto Library: User Manual – OSCCA-SM3 Library, DocID: 402610
[30] P73N2M0 Crypto Library: User Manual – OSCCA-SM4 Library, DocID: 402710
[31] Security Target, P73N2M0B0.202, Version 2.5, 21.11.2023, NXP Semiconductors
[32] P73N2M0, High-performance secure controller, Product Data Sheet, DocID: 297432, NXP Semiconductors
[33] Information on Guidance and Operation, P73N2M0B0.20n, Version 1.01, 18.04.2017, NXP Semiconductors
[34] P73 Services User Manual, API and Operational Guidance
For P73N2M0B0.2C2 (Services 1.9.14): Revision 2.0, 13.04.2017, NXP Semiconductors
For P73N2M0B0.2C6 (Services 1.9.18): Revision 2.2, 19.01.2018, NXP Semiconductors

9 . 3 Standards

[35] ISO/IEC 15946-1: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General, 2008
[36] ISO/IEC 15946-2: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures, 2003
[37] ISO/IEC 15946-3-2006: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key Establishment, 2006
[38] NIST Special Publication 800-90A, Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015, Elaine Barker and John Kelsey, National Institute of Standards and Technology
[39] FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication, July 2008, US Department of Commerce/National Institute of Standards and Technology
[40] FIPS PUB 180-4: Secure Hash Standard, Federal Information Processing Standards Publication, February 2011, US Department of Commerce/National Institute of Standards and Technology
[41] FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, Federal Information Processing Standards Publication, August 2015, US Department of Commerce/National Institute of Standards and Technology
[42] FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION DATA ENCRYPTION STANDARD (DES) Reaffirmed 1999 October 25

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

[44] FIPS PUB 186-4: Digital Signature Standard, Federal Information Processing Standards Publication, 2013, July, National Institute of Standards and Technology

[45] FIPS PUB 81: DES modes of operation, Federal Information Processing Standards Publication, December 2nd, 1980, US Department of Commerce/National Institute of Standards and Technology

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

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

[48] NIST Special Publication 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

[49] ISO/IEC 9797-1: 2011 Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher

[50] JIL-ATT-SC: Attack Methods for Smartcards and Similar Devices, Joint Interpretation Library, Version 1.5, February 2009

[51] ANSI X9.62: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Standard (ECDSA), American National Standard, November 16th, 2005

[52] PKCS #1, v2.2: RSA Cryptography Standard, RSA Laboratories, October 2012

9 . 4 Other documents

[53] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, SOG-IS Crypto Working Group, Version 1.0, May 2016

10 Legal information

10.1 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.

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.

10.2 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

Adelante, **Bitport**, **Bitsound**, **CoolFlux**, **CoReUse**, **DESFire**, **EZ-HV**, **FabKey**, **GreenChip**, **HiPerSmart**, **HITAG**, **I²C-bus** logo, **ICODE**, **I-CODE**, **ITEC**, **Labelution**, **MIFARE**, **MIFARE Plus**, **MIFARE Ultralight**, **MoReUse**, **QLPAK**, **Silicon Tuner**, **SiliconMAX**, **SmartXA**, **STARplug**, **TOPFET**, **TrenchMOS**, **TriMedia** and **UCODE** — are trademarks of NXP B.V.

HD Radio and **HD Radio** logo — are trademarks of iBiquity Digital Corporation.

Tables

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: 21 November 2023