P73N2M0B0.202

Security Target Lite

Rev. 2.4 — 2 November 2018

Evaluation document
COMPANY PUBLIC

Document information

Information	Content
Keywords	NXP, P73N2M0B0.202, Secure Microcontroller, Secure Processor, Common Criteria, Security Target Lite
Abstract	This document is the Security Target Lite of the NXP High-performance secure controller P73N2M0B0.202. The device is developed and provided by NXP Semiconductors. The TOE 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
2.4	02.11.2018	Derived from Security Target v2.4

1 ST Introduction

1.1 ST Reference

"*P73N2M0B0.202 Security Target Lite*", NXP Semiconductors, Revision 2.4, 2 November 2018

1.2 TOE Reference

The TOE is named "***NXP High-performance secure controller P73N2M0B0.202***". This TOE is an IC hardware platform with IC Dedicated Software and documentation describing the usage of the TOE.

In short from the TOE is named ***P73N2M0B0.202***.

1.3 TOE Overview

1.3.1 TOE physical configurations

The TOE is delivered in one physical configuration:

- **P73N2M0B0.202**

1.3.2 Usage and major security functionality

P73N2M0B0.202 is a microcontroller, which can be used as a Secure Element or as a Universal Integrated Circuit Card in mobile computing devices such as tablets, smartphones and mobile phones. P73N2M0B0.202 includes IC Dedicated Software and serves as a platform for Security IC Embedded Software.

The IC hardware of P73N2M0B0.202 incorporates an ARM SC300 processor, a Public-Key Cryptography (PKC) coprocessor and a Direct Memory Access (DMA) controller, which are all connected over a Memory Management Unit (MMU) to a bus system. This bus system gives access to memories, hardware peripherals and communication interfaces.

The ARM SC300 processor is a security enhanced variant of the ARM Cortex M3. It includes the SC300 core and the Nested Vector Interrupt Controller (NVIC). The core implements the ARMv7-M architecture, which supports a subset of the Thumb instruction set. The PKC coprocessor provides large integer arithmetic operations, which can be used by Security IC Embedded Software for asymmetric-key cryptography. Hardware peripherals include coprocessors for symmetric-key cryptography and for calculation of error-detecting codes, and also a random number generator. The DMA controller manages data transfers over communication interfaces like Single Wire Protocol (SWP) interface, ISO/IEC 7816 compliant interface, Serial Peripheral Interface (SPI) and I^2C interface. On-chip memories are Flash memory, ROM and RAMs. The Flash memory can be used to store data and code of Security IC Embedded Software. It is designed for reliable non-volatile storage.

P73N2M0B0.202 is offered with the NXP Trust Provisioning Service, which involves secure reception, generation, treatment and insertion of customer data and code at NXP.

The documentation of P73N2M0B0.202 includes a product data sheet, several product data sheet addenda, a user guidance and operation manual, and service documentation. This documentation describes secure configuration and secure use of P73N2M0B0.202 as well as the services provided with it.

The security functionality of P73N2M0B0.202 is designed to act as an integral part of a security system composed of P73N2M0B0.202 and Security IC Embedded Software to strengthen it as a whole. Several security mechanisms of P73N2M0B0.202 are completely implemented in and controlled by P73N2M0B0.202. Other security mechanisms must be treated by Security IC Embedded Software. All security functionality is targeted for use in a potential insecure environment, in which P73N2M0B0.202 maintains

- correct operation of the security functionality,
- integrity and confidentiality of data and code stored to its memories and processed in the device,
- controlled access to memories and hardware components supporting separation of different applications.

This is ensured by the construction of P73N2M0B0.202 and its security functionality.

P73N2M0B0.202 basically provides

- hardware to perform computations on multiprecision integers, which are suitable for public-key cryptography,
- hardware to calculate the Data Encryption Standard with up to three keys,
- hardware to calculate the Advanced Encryption Standard (AES) with different key lengths,
- hardware to support Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR) modes of operation for symmetric-key cryptographic block ciphers,
- hardware to support Galois/Counter Mode (GCM) of operation and Galois Message Authentication Code (GMAC) for symmetric-key cryptographic block ciphers,
- hardware to calculate Cyclic Redundancy Checks (CRC),
- hardware to serve with True Random Numbers,
- hardware to control access to memories and hardware components.

In addition, P73N2M0B0.202 embeds sensors, which ensure proper operating conditions of the device. Integrity protection of data and code involves error correction and error detection codes, light sensing and other security functionality. Encryption and masking mechanisms are implemented to preserve confidentiality of data and code. The IC hardware is shielded against physical attacks.

1.3.3 TOE Type

P73N2M0B0.202 is an IC hardware platform for various operating systems and applications with high security requirements.

1.3.4 Required non-TOE Hardware/Software/Firmware

None

1.4 TOE Description

1.4.1 Physical Scope of TOE

P73N2M0B0.202 is manufactured in an advanced 40nm CMOS technology. It is built of IC hardware and IC Dedicated Software, and includes documentation. A block diagram of the IC hardware is depicted in Figure 1.

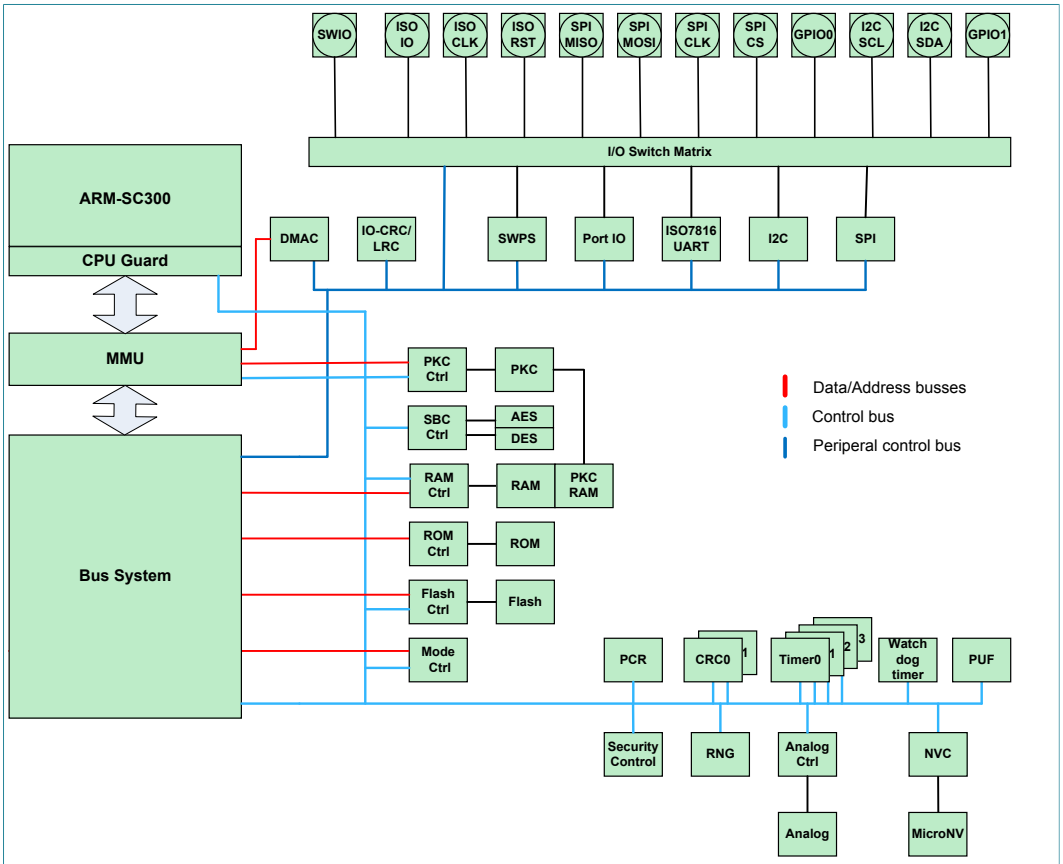

Figure 1. Block diagram of P73N2M0B0.202

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. All other software is called Security IC Embedded Software and is not part of the TOE.

Figure 2 shows the scope of P73N2M0B0.202, serving as a platform for Security IC Embedded Software of four different software component types named Library Software, Services Software, Bootloader OS and Customer OS.

P73N2M0B0.202 is available for NXP internal use only. It provides a programming interface (PI) for NXP, which gives access to the Flash Driver Software. This allows NXP to develop sales products composed of P73N2M0B0.202 and Services Software, which are out of scope of this Security Target.

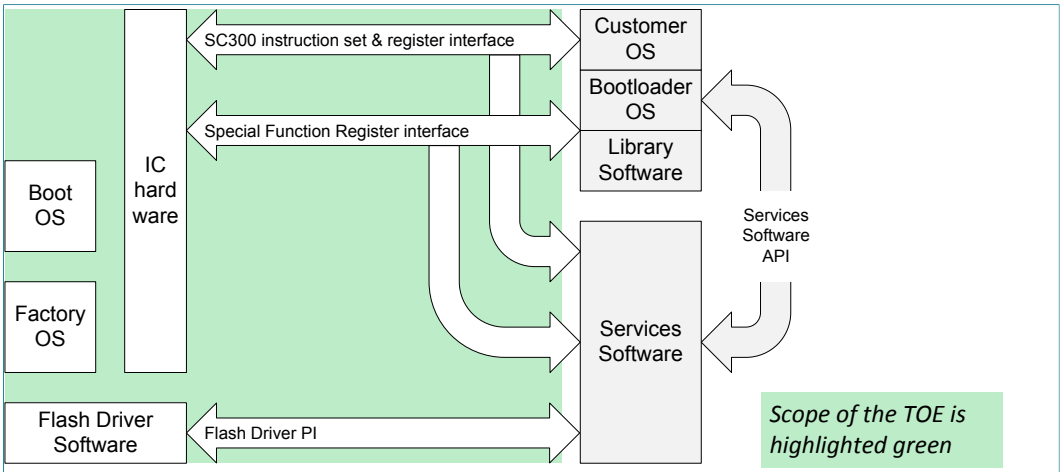

Figure 2. P73N2M0B0.202 Logical scope

All components of P73N2M0B0.202 are listed in Table 1.

Table 1. Components of P73N2M0B0.202

Category	Component	Version	Delivery form
IC Hardware	base layer and fixed metal masks	B0.2	Wafer
IC Dedicated Support Software: Test Software	Factory OS	1.4.4	On-chip software. Stored to the ROM of the TOE.
IC Dedicated Support Software: Boot Software	Boot OS	1.2.3 PL2 v8	On-chip software. Stored to the ROM of the TOE. Boot OS patch stored to the System page in the FLASH area of the TOE.
IC Dedicated Support Software: Memory Driver Software	Flash Driver Software	1.5.2	On-chip software. Stored to the ROM of the TOE.
Documentation, Product Data Sheet	P73N2M0, High-performance secure controller, Product data sheet, NXP Semiconductors, DocID: 297431	[18]	Electronic Document (PDF via NXP Docstore)
Documentation, Product Data Sheet Addendum	P73N2M0B, Wafer and Delivery Specification, Product data sheet addendum, NXP Semiconductors, DocID 328231	[19]	Electronic Document (PDF via NXP Docstore)
	P73 Family, SC300 User Manual, Product Data sheet addendum, NXP Semiconductors, DocID: 341410	[20]	Electronic Document (PDF via NXP Docstore)
	ARM®v7-M Architecture Reference Manual, ARM, DDI 0403E.b (ID120114)	[21]	Electronic Document (PDF via NXP Docstore)
	P73 Family, DMA Controller PL080 User Manual, Product data sheet addendum, NXP Semiconductors, DocID: 341510	[22]	Electronic Document (PDF via NXP Docstore)
Documentation, User Guidance and Operation Manual	P73N2M0B0.20n, Information on User Guidance and Operation	[17]	Electronic Document (PDF via NXP Docstore)
Order Entry Form	Electronic Order Entry Form, online document, NXP Semiconductors	[24]	Online Document

1.4.2 Evaluated Configurations

The physical configuration of the TOE must be chosen in the electronic Order Entry Form (OEF) for P73N2M0B0.202 as detailed in Table 2 .

Table 2. Order entry for evaluated physical scope of P73N2M0B0.202

Order entry item	Symbol	Evaluated values	Description
series	*srs*	P73	Series identifier in NXP product family SCP
development type	*ieee*	N2M0	Development type identifier in the series of the NXP product family
base layer	*x*	B	Base layer identifier of the development type
fixed metal masks	*y*	0	Fixed metal masks identifier of the development type
customizable metal masks	*z*	2	Customizable metal masks identifier of the development type, includes the IC Dedicated Software stored to ROM
NXP software combination	*wn*	02	• *w*: NXP software combination identifier of the development type, identifies the IC Dedicated Software stored to Flash • *n*: version identifier of the NXP software combination, identifies software version and configuration data stored to Flash

The symbols in the second column in Table 2 build the product name of a physical configuration according to the following rule:

srs ieee x y . z w n

Logical and further physical configuration options are provided for each configuration of P73N2M0B0.202, which do not modify the physical scope described in Section 1.4.1. Evaluated logical configuration options are all or a subset of the order entry options available in the electronic Order Entry Form. Table 3 identifies these evaluated logical configuration options.

Table 3. Evaluated logical configuration options

Name of order entry option	Evaluated values
P73_HWOPT_ENABLE_ISORESET	YES/NO
P73_HWOPT_ENABLE_SWPS_SWP	YES/NO
P73_HWOPT_ENABLE_MIFAREHW	YES/NO
P73_HWOPT_SELECT_RAM_HS_START	[0..0xFF]
P73_HWOPT_SELECT_RAM_HS_END	[0..0xFF]
P73_SWOPT_ENABLE_APPDISABLE	YES/NO
P73_SWOPT_ENABLE_CHMODE	YES/NO
P73_SWOPT_SELECT_MODE	ABL/BOR/AAP
P73_SWOPT_ENABLE_BL_RIGHTS_FOR_AP (short name: EN_BL_FOR_AP)	YES/NO

Name of order entry option	Evaluated values
P73_SWOPT_ENABLE_SV_AP (short name: EN_SV_AP)	YES/NO
P73_SWOPT_ENABLE_SV_BL(short name: EN_SV_BL)	YES/NO

The logical configuration options listed in Table 3 are detailed in [18] .

In addition to the logical configuration options given in Table 3 additional evaluated logical configuration options are available. They are under exclusive control of NXP.

Physical configuration options are delivery types. Evaluated delivery types and corresponding order entries in the electronic Order Entry Form are listed in Table 4 .

Table 4. Evaluated delivery types

Name of order entry option	Evaluated values	Description
Volume Delivery Type	*Up(p)*	Wafer not thinner than 50 um *p*(*p*) in column "Evaluated values" stand for one or two characters, which identify the wafer type

The security functionality of P73N2M0B0.202 is not affected by the package type. The package type varies in the pads of the die, which are connected to the package and thus defines the environment, in which the device can be used. The security of P73N2M0B0.202 does not rely on which pad is connected or not. A delivery of P73N2M0B0.202 as wafer even leaves this open.

The mapping of the evaluated configurations of the TOE to the commercial type names is done by applying the content of Table 6 to the naming scheme given in [18] . The mapping is given in Table 5 .

Table 5. Mapping of Commercial Type Name

TOE Physical Configuration	Commercial Type Name
P73N2M0B0.202	P73 N2M0 0 Up(p) / Z B 0 2 **2** ff[1]

[1] FabKey Number (FKN), which identifies the contents in AP-Flash at TOE Delivery, and the selection of logical configuration options

Table 6. Values of symbols in commercial type name

Symbol	Value	Description
srs	P73	Series in NXP product family SCP
ieee	N2M0	Development type in the series of NXP product family SCP
w	0	NXP software combination option
pp(*p*)	Up(p)	Volume Delivery type, see Table 4
m	Z	Manufacturer identifier
x	B	Base layer identifier
y	0	Fixed metal masks identifier
z	2	Customizable masks identifier

Symbol	Value	Description
n	2	NXP software combination version
ff	see FabKey Number (FKN) acc. to [18]	FabKey Number (FKN), which identifies the contents in AP-Flash at TOE Delivery, and the selection of logical configuration options

Information on how to order and identify P73N2M0B0.202 in its physical configuration and its definition of logical configuration options is described in [18] .

1.4.3 Logical Scope of TOE

1.4.3.1 Hardware Description

The hardware of P73N2M0B0.202 facilitates seven types of software components, which are depicted in Figure 3.

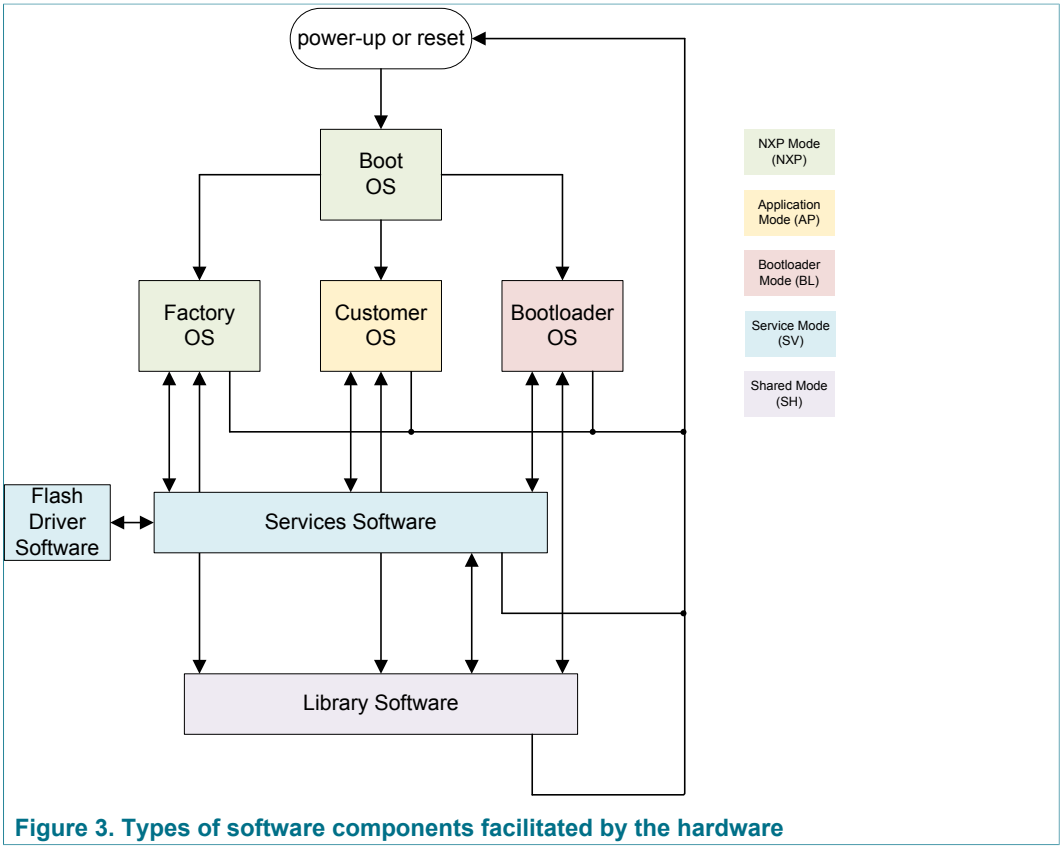

Figure 3. Types of software components facilitated by the hardware

The hardware always starts-up with executing the Boot OS. The Boot OS finally jumps to a start address in either Factory OS, Bootloader OS or Customer OS. The hardware provides no other way to start these operating systems but via power-up or reset of the device. Not more than one operating system out of Factory OS, Bootloader OS and Customer OS can be executed per start-up cycle. Each of the operating systems may interact with Services Software and with Library Software according to the programming interface they respectively provide.

The Factory OS implements security functionality against unauthorized access in the field. Startup into Bootloader OS is blocked by the TOE with order entry option P73_SWOPT_SELECT_MODE = AAP until Customer OS explicitly unblocks this with next startup by changing the logical configuration to P73_SWOPT_SELECT_MODE = BOR. Then Bootloader OS can reactivate this blockage with changing back to P73_SWOPT_SELECT_MODE = AAP. Instead, order entry option P73_SWOPT_SELECT_MODE = BOR causes the TOE to start-up into Bootloader OS when a special sequence is applied to a pad.

Jumps between types of software components imply transformations in system operation modes, which are under control of the hardware. The hardware distinguishes among five such system operation modes. These are named NXP Mode (NXP), Application Mode (AP), Bootloader Mode (BL), Service Mode (SV) and Shared Mode (SH). Figure 3 gives the basic assignment of system operation modes to the seven types of software components.

Transformations among NXP Mode, Bootloader Mode, Application Mode and Service Mode are usually transitions from one to another system operation mode. Exceptions are with logical configurations EN_SV_AP=YES, EN_SV_BL=YES and/or EN_BL_FOR_AP=YES. Logical configuration EN_SV_AP=YES resp. EN_SV_BL=YES enable Bootloader OS to also activate Application Mode resp. Bootloader Mode when it jumps to Services Software. These configurations fit to the needs of update functionality in a Bootloader OS provided by NXP for third party operating systems. Such Bootloader OS itself is not in scope of this TOE. In logical configuration EN_BL_FOR_AP=YES the TOE always sets both, Application Mode and Bootloader Mode when jumping to Customer OS. This configuration is appropriate for NXP operating systems with integrated update functionality in the field. Such NXP operating systems themselves are not in scope of this TOE.

Shared Mode is always activated in addition to the system operation mode(s) of the software component type that jumps to Library Software. This allows to share Library Software among different types of software components.

System operation modes are used by the hardware to control access to memories and hardware components. The software component types are stored to different areas in the Flash memory, which are assigned with access rights that fit to their related software component type.

Furthermore, the ARM SC300 processor supports two CPU modes named "thread" and "handler", and also two CPU privilege levels named privileged and unprivileged (of which the latter one is also called "user" by ARM). These choices are combined to three valid CPU operation modes, which are privileged thread, unprivileged thread and privileged handler. The SC300 processor implements these CPU operation modes to control access to some of its configuration registers and instructions. Use of the two modes thread and handler is limited to the SC300 processor whereas the privilege levels are also used in the system to control access to memories and hardware components.

P73N2M0B0.202 implements 64 Kbytes ROM, 2 Mbytes Flash, 52 Kbytes System RAM, 5 Kbytes PKC RAM and a Buffer RAM for Flash erase/programming and for Flash read caching. All these memories are accessible over the bus system on data/address busses, and the PKC RAM can also be directly accessed by the PKC coprocessor on a separate data/address bus. PKC RAM accesses are arbitrated in the RAM Controller. The hardware controls access to the memories over the bus system. Direct access to the PKC RAM is controlled by way of access control to the hardware component PKC coprocessor. Access to the PKC RAM by the CPU and the PKC coprocessor over the bus system is adjusted accordingly.

The hardware controls write, read and execute access to the memories over the bus system against system operation modes. This is done based on segments in the logical address space. In this context the whole ROM address space is reserved for NXP.

The Flash address space is sectioned into an AP-Flash segment, a BL-Flash segment, an SV-Flash segment, an SH-Flash segment and a CFG-Flash segment. The AP-Flash segment is accessible in Application Mode without restrictions and blocked in Bootloader Mode for read and execute. The BL-Flash segment is accessible in Bootloader Mode without restrictions and completely blocked in Application Mode. Both segments are also blocked in Service Mode. The SV-Flash segment is accessible to Service Mode without restrictions. It is blocked in Application Mode and blocked in Bootloader Mode for read and execute. The SH-Flash segment is accessible for execute in Application Mode, Bootloader Mode and Service Mode, but blocked in all these system operation modes for read and write, except Bootloader Mode, which has write access when Shared Mode isn't also active. Library Software always has the same access rights like the software component from which it is executed and on top of that also has read access to the SH-Flash segment.

The CFG-Flash segment consists of several NXP areas, three System Pages and an area of the Buffer RAM for Flash erase/programming (PBRAM area), which are all under specific access control. The NXP areas are reserved for NXP. The three System Pages are combined of a System Page Application, which is blocked in Bootloader Mode and can be read in Application Mode, a System Page Bootloader, which is blocked in Application Mode and can be read in Bootloader Mode, and a System Page Common, which can be read in both, Bootloader Mode and Application Mode. All three pages are accessible in read and write in Service Mode so that write access to these in Application Mode and Bootloader Mode can be put under the control of service software. The PBRAM area isn't accessible in Application Mode, Bootloader Mode and Service Mode as long as it is unlocked. In this state, any allowed write access to an address in the Flash address space outside the PBRAM area immediately locks the PBRAM area to the accessing mode. In this context, Application Mode and Bootloader Mode are not distinguished, and they are overruled by Service Mode in case it is active together with one of these. In case the PBRAM area is locked to Application Mode and Bootloader Mode, and Service Mode is active together with one of these, the locking state is updated to Service Mode with any allowed write access to an address in the Flash address area inside or outside the PBRAM area.

The System RAM address space is composed of an AP-RAM segment, an SV-RAM segment and a PUF-RAM segment. The AP-RAM segment is available for use in Application Mode and in Bootloader Mode whereas SV-RAM segment and PUF-RAM segment are reserved for NXP.

The above described restrictions are valid by default for memory access over the bus system by the CPU. Such access by the PKC coprocessor and DMA controller is blocked completely by default, except for PKC coprocessor access to the PUF-RAM segment, which is reserved for NXP, and to the PKC RAM, which is accessible like for the CPU.

The Memory Management Unit can be utilized by software running in privileged level to open access windows over the bus system for PKC coprocessor and DMA controller to areas, which are blocked by default. Such windows for the PKC coprocessor are restricted to AP-Flash segment, BL-Flash segment, SV-Flash segment, SH-Flash segment and AP-RAM segment and for the DMA controller to the AP-RAM segment. The Memory Management Unit can also be utilized by software running in privileged level to open access windows over the bus system for the CPU. Such windows must be inside segments that are accessible to the software which then can block access to the underlying segments and by this restrict access beyond its default. Access rights to

all windows can be defined for system operation modes and CPU privilege levels. The Memory Management Unit therewith allows the software to protect its operating system and to implement an access control policy among its different applications.

P73N2M0B0.202 implements a wide range of hardware components. It embeds the Fast Accelerator for Modular Exponentiation of 3rd Generation (Fame3), which can be utilized by the software to accelerate computations required for public-key cryptography like such related to RSA, Elliptic Curve Cryptography (ECC), Secure Hash Function (SHA), Office of the State Commercial Cryptography Administration (OSCCA), Korean SEED.

Hardware component Symmetric Block Cipher (SBC) serves the software with interfacing to a DES coprocessor and to an AES coprocessor. The DES coprocessor provides single DES calculation and also Triple-DES calculation in 2-key or 3-key operation with a length of 56 bits for each key. The AES coprocessor performs AES encryption and AES decryption calculations with key lengths of 128, 192 or 256 bits. The SBC supports Cipher Block Chaining Mode (CBC), Cipher Feedback Mode, (CFB) Output Feedback Mode (OFB), Counter Mode (CTR) and implements a Galois Field Multiplier to support Galois/Counter Mode (GCM) of operation.

Two CRC coprocessors each serve with checksum computation based on CRC generation polynomials CRC-8, CRC-16 and CRC-32. The Random Number Generator generates true random numbers, which are compliant to AIS31 and FIPS 140-2.

P73N2M0B0.202 also implements a watchdog counter with time-out mechanism that can be utilized by the software to abort irregular program executions, and provides a CPU Guard with several security functionality, which can be utilized by the software to secure its execution.

Hardware components of P73N2M0B0.202 can be controlled by software via Special Function Registers, which are accessible over the bus system on two separate busses. The peripheral control bus is provided for communication and thus gives access to the Special Function Registers of the DMA controller, the communication interfaces, the I/O switch matrix and a component for checksum computations over data streams of the communication interfaces. The Special Function Registers of all other hardware components are accessed on the control bus.

The hardware controls write and read access to its Special Function Registers to the point of single bits and this against Application Mode/Bootloader Mode, Service Mode, NXP Mode and against both privilege levels. This control does not distinguish between Bootloader Mode and Application Mode since these are separated via different start-up cycles in which Special Function Registers are reset to their default values. Also, this control does not consider Shared Mode since it is never stand-alone active. This is valid for accesses from the SC300 processor, whereas accesses from the PKC coprocessor are completely blocked for both busses and accesses from the DMA controller are completely blocked for the control bus.

Based on the above conditions the bus system can be utilized by software running in privileged level to further manage access to hardware components among Application Mode/Bootloader Mode and Service Mode as well as among the CPU privilege levels, which is then enforced by the hardware.

P73N2M0B0.202 implements complex security functionality to protect code and data during processing and while stored to the device. This includes appropriate memory encryptions and masking schemes to preserve confidentiality. This also includes error detection codes, the Flash Secure Fetch Plus and manifold light sensing to protect integrity. Active and passive shielding is present and operating conditions are monitored by sensors on temperature, power supplies and frequencies.

P73N2M0B0.202 operates with a single external power supply of 1.8 V or 3 V nominal voltage, which is applied to its supply pad. Normal operation is done in power mode ACTIVE, in which all hardware components are in operative condition. The device can be set into power modes SLEEP, DEEP SLEEP and DEEP POWER DOWN, which have different levels of reduced availability of hardware components with appropriately reduced power consumption.

1.4.3.2 Software Description

P73N2M0B0.202 is an IC hardware platform for Security IC Embedded Software. Such Security IC Embedded Software can be composed of software component types Customer OS, Bootloader OS, Library Software and Services Software.

Any operating systems and applications for particular utilizations of P73N2M0B0.202 in the field are implemented into type Customer OS.

P73N2M0B0.202 serves with hardware support for type Bootloader OS . It also provides hardware support for type Library Software so that its secure cryptographic functions can be shared among different types of Security IC Embedded Software. P73N2M0B0.202 also gives hardware support for type Services Software. Services Software is required at least to manage technical demands of the Flash memory and to serve other Security IC Embedded Software with an interface for Flash erase and/or programming. It may provide additional services to other Security IC Embedded Software.

Customer OS, Bootloader OS, Library Software and Services Software are stored to Flash, with Customer OS in the AP-Flash segment, Bootloader OS in the BL-Flash segment, Library Software in the SH-Flash segment and Services Software in the SV-Flash segment.

The IC Dedicated Software of P73N2M0B0.202 consists of the Factory OS, the Boot OS and the Flash Driver Software.

Boot OS, Factory OS and Flash Driver Software are stored to ROM.

The Factory OS provides controlled access to different levels of testing capabilities of P73N2M0B0.202. Full testing capabilities are under restricted access to NXP for production testing of P73N2M0B0.202 and also for in-depth analysis of field returns from particular utilizations of P73N2M0B0.202 with Customer OS. In addition, limited testing capabilities are accessible to NXP for basic analysis of field returns, which target to preserve the composite product in its original condition. Beyond that, the Factory OS provides the Composite Product Manufacturer with some basic functional testing of P73N2M0B0.202 and also with a readout of the identification flags of P73N2M0B0.202 from System Page Common. The Factory OS implements security functionality to protect from unauthorized access and measures that also authorized access cannot compromise confidentiality of content stored to AP-Flash, BL-Flash, SH-Flash and SV-Flash windows as well as System Page Application, System Page Bootloader and System Page Common.

The Boot OS is executed during start-up after power-on or reset of P73N2M0B0.202. It sets up the device and its configuration, and finally jumps to Customer OS, Bootloader OS or Factory OS.

The Flash Driver Software gives an interface for Services Software to the hardware that controls the Flash memory.

1.4.3.3 Documentation

The documentation of P73N2M0B0.202 is identified in Table 1 of Section 1.4.1.

Section 1.4.5 assigns the documentation to the interfaces of P73N2M0B0.202.

Proper use and operation of the hardware is described in [18] , with some details on particular hardware components in [20] and [22].

Usage and operation of the Flash Driver Software is documented in [23].

Particular information on secure use and operation of P73N2M0B0.202 is provided in [17] .

Information on packaging and delivery of P73N2M0B0.202 is given in [19] .

1.4.4 Security During Development and Production

The Security IC product life cycle is scheduled in phases, which are defined in the Protection Profile [5]. Phase 2 *IC Development* and phase 3 *IC Manufacturing and Testing* of this life cycle are part of this Security Target as well as phase 4 *IC Packaging* depending on TOE Delivery of P73N2M0B0.202. TOE Delivery is either at the end of phase 3 or at the end of phase 4, which is determined by the package type. The evaluated package types are identified in Section 1.4.2. The development environment of P73N2M0B0.202 always ranges from phase 2 *IC Development* to TOE Delivery. All other phases are part of the operational environment. This addresses Application Note 1 in in the Protection Profile [5].

In phase 2 *IC Development* of P73N2M0B0.202 access to sensitive design data of P73N2M0B0.202 is restricted to people, who are involved in the development of the product.

In phase 3 *IC Manufacturing and Testing* of P73N2M0B0.202 dice are produced and tested on wafers. Non-functional dice on a wafer are marked on a wafer map, which is provided to the Composite Product Manufacturer in electronic form. In this phase NXP also serves the Composite Product Manufacturer with storage of Customer OS to the Flash of P73N2M0B0.202. The NXP Trust Provisioning Service ensures confidentiality and integrity of Customer OS in this phase. This includes secure treatment and insertion of data and code received from the customer as well as random or derived data, which are generated by NXP.

The delivery processes between all involved sites provide accountability and traceability of the dice.

An overview of the sites involved during development and manufacturing is given in Table 7.

Table 7. Development and Manufacturing sites

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

Site	Company Address	Description	Life Cycle Phase acc. [5]
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	Strzegomska 56B Street, 53-611 Wroclaw, Poland	Development Center	Phase 2 - IC Development
SII Gdansk	SII Sp. Z.o.o. Olivia Star Building (Floor 17) - Grunwaldzka 472C, 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
AMKOR Technology Philippines ATP3/4	119 North Science Avenue, Special Economic Processing Zone, Laguna Technopark, Binan Laguna, 4024, Philippines	Assembly & Test	Phase 3 - IC Manufacturing and Testing Phase 4 - IC Packaging
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

1.4.5 Interface of the TOE

The electrical interface of P73N2M0B0.202 are the pads, which connect power supply and ground, and the 12 communication pads of which 11 ones have generic I/O capabilities and one is specific for SW I/O. The communication pads can be configured to establish communication with the device via the following interfaces.

- ETSI TS 102 613 compliant SWP interface
- SWP interface in dual pad configuration by use of ETSI TS 102 613 protocol
- Serial Peripheral Interface (SPI)
- I^2C interface
- ISO/IEC 7816 compliant interface by use of ISO/IEC 7816 UART
- GPIO interface by use of Special Function Registers

The logical interface of P73N2M0B0.202 is composed of the following.

- SC300 instruction set and register interface acc. to [21], which is accessible to Security IC Embedded Software running on P73N2M0B0.202.
- Special Function Registers interface , which is accessible to Security IC Embedded Software of types Customer OS, Bootloader OS as well as Library Software executed from these running on P73N2M0B0.202.
- Flash Driver Software programming interface acc. to [23], which is accessible to Security IC Embedded Software of type Services Software running on P73N2M0B0.202.
- The command interface to the Factory OS , which is accessible via the ISO/IEC 7816 compliant interface and the I^2C interface.

The chip surface must be considered as an interface of P73N2M0B0.202. This interface could be exposed to environmental stress or physically manipulated by an attacker.

2 Conformance Claims

2.1 Conformance Claim

This Security Target and P73N2M0B0.202 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 4, September 2012, CCMB-2012-09-001" [1]
- "Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002" [2]
- "Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003" [3]

P73N2M0B0.202 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 4, September 2012, CCMB-2012-09-004 [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 für 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 Security Assurance Requirements for the TOE of this Security Target.

2.2 Conformance Claim Rationale

P73N2M0B0.202 is the type of TOE defined in Section 1.3.3 of this Security Target. Its components are detailed in Section 1.4.1 of this Security Target. These descriptions are consistent with the TOE definition in section 1.2.2 of the Protection Profile [5].

The security problem definition in 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 new threats, organizational security policies and assumptions. The new 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 3.4 of this Security Target.

3 Security Problem Definition

3.1 Description of Assets

The assets and emanating high-level security concerns in section 3.1 of the Protection Profile [5] entirely apply to this Security Target. In compliance with Application Note 8 in the Protection Profile [5] this Security Target identifies the access restrictions of the TOE to its memories and hardware as a further asset. The high-level security concerns of this Security Target are summarized below.

- SC1 Integrity of user data of the Composite TOE and of Security IC Embedded Software, while being executed/processed and while being stored in the TOE's protected memories
- SC2 Confidentiality of user data of the Composite TOE and of Security IC Embedded Software, while being executed/processed and while being stored in the TOE's protected memories
- SC3 Correct operation of the security services provided by the TOE for Security IC Embedded Software
- SC4 Deficiency of Random Numbers
- SC5 Correct operation of access restrictions to memories and hardware as provided by the TOE for Security IC Embedded Software

To be able to protect the assets the TOE shall protect its TOE security functionality. Critical information about the TOE security functionality shall be protected by the development environment and the operational environment. Critical information includes the following.

- Logical design data
- Physical design data
- IC Dedicated Software
- Configuration data
- Initialization data and pre-personalization data
- Specific development aids
- Test and characterization related data
- Material for software development support
- Photomasks

3.2 Threats

The threats defined in section 3.2 of the Protection Profile [5] are listed in Table 8. They entirely apply to this Security Target. In addition, threat T.Masquerade_TOE in package "Authentication of the Security IC" of the Protection Profile [5] is applicable to this Security Target.

Table 8. 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

Name	Title
T.Leak-Inherent	Inherent Information Leakage
T.Leak-Forced	Forced Information Leakage
T.RND	Deficiency of Random Numbers
T.Masquerade_TOE	Masquerade the TOE

Threat T.Masquerade_TOE may threaten the unique identity of the TOE as described in policy P.Process-TOE or the property as being a genuine TOE without unique identity. This threat is applicable because the TOE embeds Flash memory for storage of Security IC Embedded Software, which can be written, instead of ROM, which cannot be written.

In compliance with Application Note 4 of the Protection Profile [5] the TOE provides security functionality that protects against the additional threat listed in Table 9.

Table 9. Threats added in this Security Target

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

The threat in Table 9 is defined below.

T.Unauthorized-Access **Unauthorized Memory or Hardware Access**

Adverse action: An attacker may try to read, modify or execute code or data stored to restricted memory areas. An attacker may try to access or operate restricted hardware components by executing code that accidentally or deliberately accesses these restricted hardware components.

- Any code executed or data used in a system operation mode, with and without Shared Mode, may accidentally or deliberately access code or data or hardware components restricted to other system operation modes.
- Any code executed or data used in unprivileged level may accidentally or deliberately access code or data or hardware components restricted to privileged level.
- Any code executed or data used in unprivileged level, which is assigned to a certain application, may accidentally or deliberately access code or data or hardware components restricted to unprivileged level of the same system operation mode but assigned to another application.

Threat agent: Attacker with high attack potential and access to the TOE.

Asset: Code and data belonging to Security IC Embedded Software as well as code and data belonging to IC Dedicated Software.

The TOE provides security functionality for control of access to its memories and hardware components. This control targets to prevent

- Boot OS and Factory OS from being compromised by other software component types,

- Flash Driver Software and Services Software from being compromised by other Security IC Embedded Software - and vice versa,
- Customer OS from being compromised by Bootloader OS - and vice versa,
- Security IC Embedded Software assigned to privileged level from being compromised by Security IC Embedded Software assigned to unprivileged level,
- separate applications of Security IC Embedded Software, which are assigned to unprivileged level of the same system operation mode, from being compromised by each other.

3.3 Organizational Security Policies

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 10. They entirely apply to this Security Target.

Table 10. 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 TOE provides security functionality, which requires an additional organizational security policy that is listed in Table 11.

Table 11. Organizational security policies added in this Security Target

Name	Title
P.Add-Components	Additional Specific Security Components

The organizational security policy in Table 11 is defined below.

P.Add-Components **Additional Specific Security Components**

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

- Integrity support of content stored to Flash memory
- Computation of Cyclic Redundancy Checks
- Support for Galois/Counter Mode (GCM) and GMAC

3.4 Assumptions

The assumptions defined in section 3.4 of the Protection Profile [5] are listed in Table 12. They entirely apply to this Security Target.

Table 12. 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

In compliance with Application Notes 6 and 7 of the Protection Profile [5] the TOE provides security functionality, which requires an additional assumption that is listed in Table 13.

Table 13. Assumptions added in this Security Target

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

The assumption in Table 13 is defined below.

A.Check-Init — **Check of TOE identification data**

It is assumed that either the Security IC Embedded Software implements a function, which checks the TOE identification data, or the Composite Product Manufacturer uses the command interface to the Factory OS of the TOE to check the TOE identification data. The TOE identification data are part of the initialization data. They are defined with the order entry of the TOE from the Composite Product Manufacturer and are injected by the TOE Manufacturer into the Flash memory of the TOE. TOE identification data can be used to identify and to trace a certain instantiation of the TOE.

Assumption A-Check-Init is defined to ensure correct receipt of the TOE in phases 1, 4, 5 and 6 of the Security IC product life cycle. Therefore it does not mitigate any threat or fulfil any organizational security policy or parts of such.

4 Security Objectives

4.1 Security Objectives for the TOE

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 14. They entirely apply to this Security Target.

Table 14. 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 listed in Table 15.

Table 15. Security Objectives for the TOE added in this 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

The security objectives in Table 15 are defined below.

O.MEM-ACCESS **Memory Access Control**

The TOE controls access of the SC300 processor, the DMA Controller and the PKC coprocessor over the bus system to ROM, Flash address space, System RAM and PKC RAM. The TOE also controls access of the PKC coprocessor over its Direct Memory Access (DMA) channel to PKC RAM. Control of access is enforced on these ports by generic limitations as well as restrictions based on system operation modes and CPU privilege levels.

O.SFR-ACCESS	**Special Function Register Access Control** The TOE controls access of the SC300 processor, the DMA Controller and the PKC coprocessor over the bus system to the Special Function Registers of the hardware components. Control of access is enforced on these ports by generic limitations as well as restrictions based on system operation modes and CPU privilege levels.
O.FLASH-INTEGRITY	**Integrity support of data stored to Flash memory** The TOE preserves integrity of content stored to its Flash memory with wearout detection capabilities.
O.GCM-SUPPORT	**Support for Galois/Counter Mode and GMAC** The TOE provides secure hardware based multiplication operation on blocks and incrementing function for the Galois/Counter Mode (GCM) and GMAC.
O.CRC	**Cyclic Redundancy Checks** The TOE provides secure hardware based computation of Cyclic Redundancy Checks (CRC).

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 16. They entirely apply to this Security Target.

Table 16. 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 17. They entirely apply to this Security Target.

Table 17. Security objectives for the operational environment defined in the Protection Profile

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

This Security Target adds the security objectives for the operational environment listed in Table 18.

Table 18. Security Objectives for the operational environment added in this Security Target

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

The security objectives in Table 18 are defined below.

OE.Check-Init — **Check of TOE identification data**

The Security IC Embedded Software or the Composite Product Manufacturer shall check the TOE identification data after receipt of the TOE from NXP. The TOE identification data are stored to System Page Common of the Flash. They can be used to identify and to trace a certain instantiation of the TOE.

4.4 Security Objectives Rationale

Table 19 traces the security objectives for the TOE in Section 4.1 back to the threats countered by them and the organisational security policies enforced by them. The table also traces the security objectives for the Security IC Embedded Software and for the operational environment in Section 4.2 and Section 4.3 back to the assumptions they uphold.

Table 19. Tracing of security objectives

Name of threat, org. security policy or assumption	Name of security objective	Applied to life cycle phases
T.Malfunction	O.Malfunction	
T.Abuse-Func	O.Abuse-Func	
T.Phys-Probing	O.Phys-Probing	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Inherent	O.Leak-Inherent	
T.Leak-Forced	O.Leak-Forced	
T.RND	O.RND	
T.Masquerade_TOE	O.Abuse-Func	
	OE.Process-Sec-IC	
T.Unauthorized-Access	O.MEM-ACCESS	
	O.SFR-ACCESS	
P.Process-TOE	O.Identification	phases 2 to 3 and optional phase 4
P.Crypto-Service	O.TDES	
	O.AES	
P.Add-Components	O.FLASH-INTEGRITY	
	O.GCM-SUPPORT	
	O.CRC	
A.Process-Sec-IC	OE.Process-Sec-IC	phases 5 to 6 and optional phase 4
A.Resp-Appl	OE.Resp-Appl	
A.Check-Init	OE.Check-Init	phase 1 and phases 4 to 6

The green and blue colored cells in Table 16 show how the Protection Profile [5] traces its security objectives back to its threats, organizational security policies and assumptions, see section 4.4 and section 7.4. Green marks this for the mandatory security requirements of the protection profile, blue marks this for the augmentations. Section 4.4 of the Protection Profile [5] also gives the security objective rationale for the tracings colored in green.

Security objective O.Abuse-Func counters threat T.Masquerade_TOE as it requires to protect the TOE's testing capabilities including download from unauthorized use. Also, security objective OE.Process-Sec-IC counters threat T.Masquerade_TOE with TOE identification data that can be used after TOE delivery and also in phase 7 of the Security IC product life cycle to distinguish genuine TOEs from faked ones.

Security objectives O.TDES and O.AES together enforce organizational security policy P.Crypto-Service since they target such kind of cryptographic services defined in P.Crypto-Service.

O.MEM-ACCESS and O.SFR-ACCESS counter threat T.Unauthorized-Access for two reasons. First, O.MEM-ACCESS targets to control all access ports available in the TOE to its memories and O.SFR-ACCESS targets to control all access ports available in the TOE to the Special Function Registers of its hardware components. Secondly, both objectives target to control accesses via these ports based on system operation modes, which are used to separate software component types from each other and based on CPU privilege levels, which can be used by a software component type to separate its operating system from the applications it may implement and also to separate its applications from each other.

Security objectives O.FLASH-INTEGRITY, O.GCM-SUPPORT and O.CRC together enforce organizational security policy P.Add-Components since they target at the components defined in P.Add-Components.

Security objective OE.Check-Init upholds assumption A.Check-Init since it requires the operational environment to implement the measure assumed in assumption A.Check-Init.

5 Extended Components Definition

The extended components defined in chapter 5 of the Protection Profile [5] are listed in Table 20. They entirely apply to this Security Target.

Table 20. 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

This Security Target does not define additional extended components.

6 Security Requirements

6.1 Security Functional Requirements for the TOE

6.1.1 General

Security functional requirements from the Protection Profile [5] are applied to this Security Target as described in Section 6.1.2. In compliance with Application Note 12 in the Protection Profile [5] this Security Target adds security functional requirements as detailed in Security Functional Requirements added in this Security Target.

6.1.2 Security Functional Requirements from Protection Profile

Table 21 lists the security functional requirements for the TOE, which are defined in section 6.1 and in sections 7.4.1 and 7.4.2 of the Protection Profile [5]. They entirely apply to this Security Target.

Some of these security functional requirements are taken from CC Part 2 [2], others are newly defined in the Protection Profile [5]. This is denoted in the third column of the table. The fourth column indicates whether a security functional requirement is subject to refinement, selection, assignment and/or iteration operations in the Protection Profile [5] and/or in this Security Target.

Table 21. Security functional requirements from the Protection Profile

Name	Title	defined in	operations done in
FRU_FLT.2	Limited fault tolerance	CC	PP
FPT_FLS.1	Failure with preservation of secure state	CC	PP
FMT_LIM.1	Limited capabilities	PP	PP
FMT_LIM.2	Limited availability	PP	PP
FAU_SAS.1	Audit storage	PP	PP and ST
FDP_SDC.1	Stored data confidentiality	PP	ST
FDP_SDI.2	Stored data integrity monitoring and action	CC	ST
FPT_PHP.3	Resistance to physical attack	CC	PP
FDP_ITT.1	Basic internal transfer protection	CC	PP
FPT_ITT.1	Basic internal TSF data transfer protection	CC	PP
FDP_IFC.1	Subset information flow control	CC	PP
FCS_RNG.1	Random number generation	PP	PP and ST
FCS_COP.1	Cryptographic operation	CC	PP and ST
FCS_CKM.4	Cryptographic key destruction	CC	PP and ST

FPT_FLS.1 requests the TSF to preserve a secure state when the TOE is exposed to operating conditions which may not be tolerated according to FRU_FLT.2. The TOE detects such operating conditions and forces itself into a secure state as long as

these conditions are valid. This secure state is enforced by security feature SF.OPC as described in Section 7.1.3. This addresses Application Note 14 in the Protection Profile [5].

The TOE does not generate audit data for FRU_FLT.2 and/or FPT_FLS.1. This addresses Application Note 15 in the Protection Profile [5].

FPT_PHP.3 requests the TSF to resist physical manipulation and physical probing by responding automatically such that the security functional requirements are always enforced. The TOE implements two types of such automatic responses. One type of response is permanent and implicitly hampers exploitability or already incidence of physical attacks. The other type of response is conditional upon a failed check and explicitly detects physical attacks. Such type of response stops operation of the TOE or the attacked parts of it. These responses are enforced by security feature SF.PHY as described in Section 7.1.3. This addresses Application Note 19 in the Protection Profile [5].

Refinement, selection, assignment and iteration operations on the security functional requirements in Table 21 are performed in this Security Target as detailed below. Iteration operations are notified by a slash, which is appended to the name of the security functional requirement and followed by an identifier. Selection and assignment operations are denoted in italics. Refinements are denoted just as described in the Protection Profile [5].

This Security Target performs one selection and two assignment operations on FAU_SAS.1 according to Application Note 17 in the Protection Profile [5].

FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the test process before TOE Delivery with the capability to store *the Initialisation Data, Pre-personalisation Data and other user data*[1] in the *Flash memory* [2].

This Security Target performs one assignment operation on FDP_SDC.1 according to Application Note 18 in the Protection Profile [5].

FDP_SDC.1	**Stored data confidentiality**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SDI.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *Flash memory, the System RAM, the PKC RAM and the Buffer RAM* [3].

This Security Target performs two iteration operations on FDP_SDI.2, which comply with section 8.1 in CC Part 1 [1], and also performs two assignment operations on each iteration according to Application Note 18 in the Protection Profile [5].

FDP_SDI.2/AGE	**Stored data integrity monitoring and action - Ageing**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring

1 [selection: *the Initialisation Data, Pre-personalisation Data, [assignment: other data]*]
2 [assignment: *type of persistent memory*]
3 [assignment: *memory area*]

Dependencies:	No dependencies.
FDP_SDI.2.1/AGE	The TSF shall monitor user data stored in containers controlled by the TSF for *integrity violations due to ageing* [4] on all objects, based on the following attributes: *ageing check information associated with the data including code stored to the Flash memory* [5].
FDP_SDI.2.2/AGE	Upon detection of a data integrity error, the TSF shall *raise a wearout failure* [6].
FDP_SDI.2/FLT	**Stored data integrity monitoring and action - Faults**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1/FLT	The TSF shall monitor user data stored in containers controlled by the TSF for *modification, deletion, repetition or loss of data* [7] on all objects, based on the following attributes: *integrity check information associated with the data including code stored to the Flash memory, the ROM, the System RAM, the PKC RAM and the Buffer RAM* [8].
FDP_SDI.2.2/FLT	Upon detection of a data integrity error, the TSF shall *correct the error or trigger a security reset or raise a non-maskable interrupt* [9].

This Security Target performs an iteration operation on FCS_RNG.1, which complies with section 8.1 in CC Part 1 [1]. It also performs two assignment operations on each iteration of FCS_RNG.1 according to Application Note 21 in the Protection Profile [5]. The operations follow the example and its Application Note 44 in section 7.5.1 of the Protection Profile [5] in consideration of the updated documents [6] and [7].

FCS_RNG.1/PTG.2	**Random number generation - PTG.2**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
Note:	This security functional requirement complies with PTG.2 in [7]
FCS_RNG.1.1/PTG.2	The TSF shall provide a *physical* [10] random number generator that implements: *(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.* *(PTG.2.2) 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.*

4 [assignment: *integrity errors*]
5 [assignment: *memory area*]
6 [assignment: *action to be taken*]
7 [assignment: *integrity errors*]
8 [assignment: *memory area*]
9 [assignment: *action to be taken*]
10 [selection: *physical, hybrid physical, hybrid deterministic*]

	(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected. *(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.* *(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.* [11]
FCS_RNG.1.2/PTG.2	The TSF shall provide *octets of bits or packages of 32 bits*[12] that meet *(PTG.2.6) Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.* *(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.* [13]

Sections 7.4.1 and 7.4.2 of the Protection Profile [5] perform operations on two iterations of each, FCS_COP.1 and FCS_CKM.4 for package "TDES" and for package "AES", which entirely apply to this Security Target. This Security Target completes these operations in compliance with section 8.1 in CC Part 1 [1].

FCS_COP.1/TDES	**Cryptographic operation - TDES**
Hierarchical to:	No other components.
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.1.1/TDES	The TSF shall perform *encryption and decryption* [14] in accordance with a specified cryptographic algorithm *TDES in ECB mode and with support for CBC mode, CFB mode, OFB mode, CTR mode*[15] and cryptographic key sizes *112 bit, 168 bit* [16] that meet the following: *NIST SP 800-67* [8] *, NIST SP 800-38A* [9] [10] [17].
FCS_CKM.4/TDES	**Cryptographic key destruction - TDES**
Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with

11 [assignment: *list of security capabilities*]
12 [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*]
13 [assignment: *a defined quality metric*]
14 [assignment: *list of cryptographic operations*]
15 [assignment: *list of cryptographic algorithm*]
16 [assignment: *cryptographic key sizes*]
17 [assignment: *list of standards*]

	security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1/TDES	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting the internally stored key* [18] that meets the following: *none* [19] .
FCS_COP.1/AES	**Cryptographic operation - AES**
Hierarchical to:	No other components.
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.1.1/AES	The TSF shall perform *encryption and decryption* [20] in accordance with a specified cryptographic algorithm *AES in ECB mode and with support for CBC mode, CFB mode, OFB mode, CTR mode*[21] and cryptographic key sizes *128 bit, 196 bit, 256 bit* [22] that meet the following: *FIBS 197* [11] *, NIST SP 800-38A* [9] [10] [23].
FCS_CKM.4/AES	**Cryptographic key destruction - AES**
Hierarchical to:	No other components.
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.4.1/AES	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting the internally stored key* [24] that meets the following: *none* [25].

This Security Target performs the following iterations on FCS_COP.1, which are in addition to those already done in sections 7.4.1 and 7.4.2 of the Protection Profile [5].

FCS_COP.1/GCM	**Cryptographic operation - GCM support**
Hierarchical to:	No other components.
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.1.1/GCM	The TSF shall perform *multiplication operation on blocks and incrementing function* [26] in accordance with a specified cryptographic algorithm *Galois/Counter Mode*

18 [assignment: *cryptographic key destruction method*]
19 [assignment: *list of standards*]
20 [assignment: *list of cryptographic operations*]
21 [assignment: *list of cryptographic algorithm*]
22 [assignment: *cryptographic key sizes*]
23 [assignment: *list of standards*]
24 [assignment: *list of cryptographic key destruction method*]
25 [assignment: *list of standards*]
26 [assignment: *list of cryptographic operations*]

	(GCM) and GMAC [27] and cryptographic key sizes *none* [28] that meet the following: *NIST SP 800-38D* [12] [29].
FCS_COP.1/CRC	**Cryptographic operation - CRC**
Hierarchical to:	No other components.
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.1.1/CRC	The TSF shall perform *calculation of cyclic redundancy checks* [30] in accordance with a specified cryptographic algorithm *CRC-8 resp. CRC-16 resp. CRC-32* [31] and cryptographic key sizes *none* [32] that meet the following: *ITU-T I.432.1* [13], *resp. ITU-T V.42* [14], *ITU-T X.25* [15] *resp. ITU-T V.42* [14], *IEEE 802.3* [16] [33].

6.1.3 Security Functional Requirements added in this Security Target

Table 22 lists the security functional requirements for the TOE, which are added in this Security Target. These security functional requirements are taken from CC Part 2 [2] as denoted in the third column of the table. They are subject to refinement, selection, assignment and/or iteration operations in this Security Target as indicated in the fourth column of the table.

Table 22. Security functional requirements added in this Security Target

Name	Title	defined in	operations done in
FDP_ACC.1	Subset access control	CC	ST
FDP_ACF.1	Security attribute based access control	CC	ST
FMT_MSA.1	Management of security attributes	CC	ST
FMT_MSA.3	Static attribute initialisation	CC	ST
FMT_SMF.1	Management of TSF data	CC	ST

The security functional requirements in Table 22 address the Access Control Policy of the TOE. This Access Control Policy is applied to the memories and hardware components. It is enforced on the following access ports, which are:

- *CPU_ovBSY*: CPU access over the bus system
- *DMA_ovBSY*: DMA controller access over the bus system
- *PKC_ovBSY*: PKC coprocessor access over the bus system
- *PKC_ovDMA*: PKC coprocessor access over the DMA channel

by generic limitations as well as restrictions based on the following system operation modes (*SOMs*):

27 [assignment: *list of cryptographic algorithm*]
28 [assignment: *cryptographic key sizes*]
29 [assignment: *list of standards*]
30 [assignment: *list of cryptographic operations*]
31 [assignment: *list of cryptographic algorithm*]
32 [assignment: *cryptographic key sizes*]
33 [assignment: *list of standards*]

- *AP*: Application Mode
- *BL*: Bootloader Mode
- *SV*: Service Mode
- *SH*: Shared Mode
- *NXP*: NXP Mode

and the following CPU privilege levels:

- *P*: privileged
- *U*: unprivileged

The Access Control Policy controls access to two groups of objects, which are *objects for access control to memories* and *objects for access control to hardware components*. The objects of each group are detailed below.

Objects for access control to memories are as follows.

- *DWINs*: default address windows, which do not overlap in their address ranges with each other. All address ranges are fixed in hardware, except for one window, which can be configured by software as an option.
- *SWWINs*: software-controlled address windows, which must overlap with *DWINs*. They can be configured by software as an option.

Objects for access control to hardware components are as follows.

- *GSFR_ALL*: The Special Function Registers (SFRs) of all hardware components as composed of
  - *GSFR_PCBUS*: All SFRs of the hardware components connected to the peripheral control bus as composed of
    - *GSFR_DMAC*: SFRs of the DMA controller
    - *GSFR_IOSM*: SFRs of the IO Switch Matrix
    - *GSFR_IOCC*: SFRs of the IO-CRC/LRC
    - *GSFR_SWPS*: SFRs of the SWP communication interface
    - *GSFR_GPIO*: SFRs of the Port IO communication interface
    - *GSFR_UART*: SFRs of the ISO7816 UART communication interface
    - *GSFR_I2C*: SFRs of the I2C communication interface
    - *GSFR_SPI0*: SFRs of the SPI communication interface
  - *GSFR_CBUS*: All SFRs of the hardware components connected to the control bus as composed of
    - *GSFR_GRD*: SFRs of the CPU Guard
    - *GSFR_PKC*: SFRs of the PKC coprocessor
    - *GSFR_SBC*: SFRs of the SBC interface to AES and DES coprocessors
    - *GSFR_PCR*: SFRs of the PCR
    - *GSFR_CRCi*: SFRs of CRC coprocessor i=0,1
    - *GSFR_TMRi*: SFRs of Timer i=0,1,2,3
    - *GSFR_WDG*: SFRs of the Watchdog Timer
    - *GSFR_PUF*: SFRs of the PUF
    - *GSFR_RNG*: SFRs of the Random Number Generator
    - *GSFR_OTHERS*: SFRs of all other hardware components on the control bus

The *objects for access control to memories* are controlled against access rights in read (*r*) and write (*w*) and for *CPU_ovBSY* access also against access rights in execute (*x*). The *objects for access control to hardware components* are controlled against access rights in read (*r*) and write (*w*).

The Access Control Policy is applied to the following *subjects of access control to memories and hardware components*.

Subjects of access control to memories and hardware components are these:

- *CPU_ovBSY*: accesses via 7 types of software component types as follows
  - *BOS_ovBSY*: Boot OS, stored to *DWIN_ROM*, executed in *NXP*
  - *FOS_ovBSY*: Factory OS , stored to *DWIN_ROM*, executed in *NXP*
    COS_ovBSY: Customer OS, stored to *DWIN_AP-FLH*, executed in AP or (AP and BL)
  - *BLOS_ovBSY*: Bootloader OS, stored to *DWIN_BL-FLH*, executed in *BL*
  - *FDSW_ovBSY*: Flash Driver Software, stored to *DWIN_ROM*, executed like *ssw_ovBSYS*
  - *ssw_ovBSY*: services software, stored to *DWIN_SV-FLH*, executed in
    - *SV* when called by software in *AP*, in *BL* or in *AP* + *BL*
    - *SV* + *AP* when called by software in *BL* or in *AP* + *BL*
    - *SV* + *BL* when called by software in *BL* or in *AP* + *BL*
    - *SV* + *AP* + *BL* when called by software in *AP* + *BL*
  - *LSW_ovBSY*: Library Software, stored to *DWIN_SH-FLH*, executed in *SH* and the *SOM(s)* of the software from which it is executed
- *DMA_ovBSY*: accesses in the *SOM(s)* in which the actual *CPU_ovBSY* access runs, but *SV* and *SH* are masked out
- *PKC_ovBSY*: accesses in the *SOM(s)* in which the PKC coprocessor was recently started
- *PKC_ovDMA*: accesses w/o *SOM(s)*

The Access Control Policy of the above subjects to the above objects is defined in the following security functional requirements. The rules there are given for each port accessing in a single *SOM*. In case a port accesses in more than one *SOM* the access rights of this port are the sum of its granted access rights in each single *SOM* except in cases where rules are explicitly stated for combinations of *SOM(s)*. This occurs to some extent for combinations with *SV+AP*, *SV+BL* and *BL+SH*.

This Security Target performs two iteration operations on FDP_ACC.1 and also two assignment operations on each iteration, which comply with section 8.1 of CC Part 1 [1].

FDP_ACC.1/MEM	**Subset access control - Memories**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/MEM	The TSF shall enforce the *Access Control Policy* [34] on *all subjects, all objects for access control to memories and all operations on the objects for access control to memories* [35].
FDP_ACC.1/SFR	**Subset access control - Hardware components**
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/SFR	The TSF shall enforce the *Access Control Policy* [36] on *all subjects, all objects for access control to Special*

34 [assignment: *access control SFP*]
35 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
36 [assignment: *access control SFP*]

Function Registers and all operations on the objects for access control to Special Function Registers [37].

This Security Target performs two iteration operations on FDP_ACF.1 and also five assignment operations on each iteration, which comply with section 8.1 in CC Part 1 [1].

FDP_ACF.1/MEM	**Security attribute based access control - Memories**
Hierarchical to:	No other components
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/MEM	The TSF shall enforce the *Access Control Policy* [38] to objects based on the following: *all subjects and all objects for access control to memories and security attributes for memories.* [39].
Application Note:	List of all subjects and all objects for access control to memories and security attributes for memories is given in the full Security Target.
FDP_ACF1.2/MEM	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed *for CPU_ovBSY access to DWINs, DMA_ovBSY access to DWINs, PKC_ovBSY access to DWINs and PKC_ovDMA access to DWINs* [40].
Application Note:	List of rules to determine if an operation among controlled subjects and controlled objects is allowed for CPU_ovBSY access to DWINs, DMA_ovBSY access to DWINs, PKC_ovBSY access to DWINs and PKC_ovDMA access to DWINs is given in the full Security Target.
FDP_ACF1.3/MEM	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *rules to explicitly authorise DMA_ovBSY access to DMAWIN, PKC_ovBSY access to PKCWIN0 and PKC_ovBSY access to PKCWIN1* [41].
Application Note:	List of rules to explicitly authorise DMA_ovBSY access to DMAWIN, PKC_ovBSY access to PKCWIN0 and PKC_ovBSY access to PKCWIN1 is given in the full Security Target.
FDP_ACF1.4/MEM	The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

37 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
38 [assignment: *access control SFP*]
39 [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
40 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
41 [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

	CPU_ovBSY access to DWINs, CPU_ovBSY access to IDWINn and CPU_ovBSY access to SWINn [42].
Application Note:	List of rules to explicitly deny CPU_ovBSY access to DWINs, CPU_ovBSY access to IDWINn and CPU_ovBSY access to SWINn is given in the full Security Target.
FDP_ACF.1/SFR	**Security attribute based access control - Hardware components**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/SFR	The TSF shall enforce the *Access Control Policy* [43] to objects based on the following: *all subjects and all objects for access control to Special Function Registers and security attributes S2A_APACTRL, S2A_SVACTRL, S2S_APACTRL, S2S_SVACTRL* [44].
FDP_ACF1.2/SFR	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *rules for CPU_ovBSY, DMA_ovBSY, PKC_ovBSY and PKC_ovDMA access to SFR_PCBUS and SFR_CBUS.* [45].
Application Note:	List of rules for CPU_ovBSY, DMA_ovBSY, PKC_ovBSY and PKC_ovDMA access to SFR_PCBUS and SFR_CBUS is given in the full Security Target.
FDP_ACF1.3/SFR	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: • *CPU_ovBSY, DMA_ovBSY access to each group out of GSFR_DMAC, GSFR_IOSM, GSFR_IOCC, GSFR_SWPS, GSFR_GPIO, GSFR_UART, GSFR_I2C, GSFR_SPI0 can be:* – *in AP for U: allowed in rw acc. to the rules for each bit in GSFR_ALL for a group by setting its corresponding bit in S2A_APUCTRL* – *in SV for U: allowed in rw acc. to the rules for each bit in GSFR_ALL for a group by setting its corresponding bit in S2A_SVUCTRL* • *CPU_ovBSY access to each group out of GSFR_GRD, GSFR_PKC, GSFR_SBC, GSFR_PCR, GSFR_CRCi, GSFR_TMRi, GSFR_WDG, GSFR_PUF, GSFR_RNG can be:*

42 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
43 [assignment: *access control SFP*]
44 [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant securtiy attributes, or named groups of SFP-relevant security attributes*]
45 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

– *in AP for U: allowed acc. to the rules for each bit in GSFR_ALL in for a group by setting its corresponding bit in S2S_APUCTRL*
– *in SV for U: allowed acc. to the rules for each bit in GSFR_ALL in for a group by setting its corresponding bit in S2S_SVUCTRL*[46].

FDP_ACF1.4/SFR The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- *CPU_ovBSY, DMA_ovBSY access to each group out of GSFR_DMAC, GSFR_IOSM, GSFR_IOCC, GSFR_SWPS, GSFR_GPIO, GSFR_UART, GSFR_I2C, GSFR_SPI0 can be:*
  – *in AP for P: denied in rw for a group by clearing its corresponding bit in S2A_APACTRL*
  – *in SV for P: denied in rw for a group by clearing its corresponding bit in S2A_SVACTRL*
- *CPU_ovBSY access to each group out of GSFR_GRD, GSFR_PKC, GSFR_SBC, GSFR_PCR, GSFR_CRCi, GSFR_TMRi, GSFR_WDG, GSFR_PUF, GSFR_RNG can be:*
  – *in AP for P: denied in rw for a group by clearing its corresponding bit in S2S_APACTRL*
  – *in SV for P: denied in rw for a group by clearing its corresponding bit in S2S_SVACTRL* [47].

This Security Target performs two iteration operations on FMT_MSA.1 and also one selection and four assignment operations on each iteration, which comply with section 8.1 of CC Part 1.

FMT_MSA.1/MEM	**Management of security attributes - Memories**
Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1/MEM	The TSF shall enforce the *Access Control Policy* [48] to restrict the ability to *modify* [49] *security attributes for memories*[50] to the authorised identified roles. [51]
Application Note:	List of security attributes for memories and authorised identified roles is given in the full Security Target.

46 [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
47 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
48 [assignment: *access control SFP(s), information flow control SFP(s)*]
49 [selection: *change_default, query, modify, delete [assignment: other operations]*]
50 [assignment: *list of security attributes*]
51 [assignment: *the authorised identified roles*]

FMT_MSA.1/SFR	**Management of security attributes - Hardware components**
Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
	FMT_SMR.1 Security roles
	FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1/SFR	The TSF shall enforce the *Access control Policy* [52] to restrict the ability to *modify* [53] *the security attributes S2S_APACTRL, S2S_APUCTRL, S2S_SVACTRL, S2S_SVUCTRL*[54] to the authorised identified roles.' [55]

This Security Target performs two iteration operations on FMT_MSA.3 and also one selection and two assignment operations on each iteration, which comply with section 8.1 of CC Part 1.

FMT_MSA.3/MEM	**Static attribute initialisation - Memories**
Hierarchical to:	No other components
Dependencies:	FMT_MSA.1 Management of security attributes
	FMT_SMR.1 Security roles
FMT_MSA.3.1/MEM	The TSF shall enforce the *Access Control Policy* [56] to provide *restrictive* [57] default values for security attributes that are used to enforce the SFP.
Application Note:	Restrictive default values of security attributes for memories are given in the full Security Target.
FMT_MSA.3.2/MEM	The TSF shall allow the *no subject* [58] to specify alternative initial values to override the default values when an object or information is created.
FMT_MSA.3/SFR	**Static attribute initialisation - Hardware components**
Hierarchical to:	No other components
Dependencies:	FMT_MSA.1 Management of security attributes
	FMT_SMR.1 Security roles
FMT_MSA.3.1/SFR	The TSF shall enforce the *Access Control Policy* [59] to provide *restrictive* [60] default values for security attributes that are used to enforce the SFP.
Application Note:	Restrictive default values of security attributes S2S_APACTRL, S2S_APUCTRL, S2S_SVACTRL, S2S_SVUCTRL are given in the full Security Target.

52 [assignment: *access control SFP(s), information flow control SFP(s)*]
53 [selection: *change_default, query, modify, delete [assignment: other operations]*]
54 [assignment: *list of security attributes*]
55 [assignment: *the authorised identified roles*]
56 [assignment: *access control SFP, information flow control SFP*]
57 [selection, choose one of: *restrictive, permissive, [assignment: other property]*]
58 [assignment: *the authorised identified roles*]
59 [assignment: *access control SFP, information flow control SFP*]
60 [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

FMT_MSA.3.2/SFR	The TSF shall allow the *no subject* [61] to specify alternative initial values to override the default values when an object or information is created.

This Security Target performs two assignment operations on FMT_SMF.1, which comply with section 8.1 of CC Part 1 [1].

FMT_SMF.1	**Specification of Management Functions**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: • *Transformations in system operation modes for subjects CPU_ovBSY, DMA_ovBSY and PKC_ovBSY* • *Change in the CPU privilege level for subject(s) CPU_ovBSY* [62]
Application Note:	The conditions for the management functions are given in the full Security Target.

6.2 Security Assurance Requirements for the TOE

Table 23 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 23. 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
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+

61 [assignment: *the authorised identified roles*]
62 [assignment: *list of management functions to be provided by the TSF*]

Name	Title	compared to PP
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 23, 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 23, 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 P73N2M0B0.202 and also with a readout of the identification flags of P73N2M0B0.202 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

Table 24 maps the security objectives for the TOE to the security functional requirements for the TOE.

Table 24. Mapping of the security objectives for the TOE to the security functional requirements for the TOE

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

Security objective for the TOE	Security functional requirement of the TOE
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

The green and blue colored cells in Table 24 show how the Protection Profile [5] maps its security objectives for the TOE to the security functional requirements for the TOE, see section 6.3.1 and section 7.4.2. of the Protection Profile [5]. Green marks this for the mandatory security requirements of the protection profile, blue marks this for the augmentations. Section 6.3.1 of the Protection Profile [5] also gives the rationale for the mappings colored in green.

The justification related to security objective O.TDES is as follows:

O.TDES is met by FCS_COP.1/TDES and FCS_CKM.4/TDES since FCS_COP.1/TDES requests the TOE to implement the cryptographic service targeted in O.TDES according to approved public standards and FCS_CKM.4/TDES requests the TOE to implement a secure destruction method for its cryptographic key.

The justification related to security objective O.AES is as follows:

O.AES is met by FCS_COP.1/AES and FCS_CKM.4/AES since FCS_COP.1/AES requests the TOE to implement the cryptographic service targeted in O.AES according to approved public standards and FCS_CKM.4/AES requests the TOE to implement a secure destruction method for its cryptographic key.

The justification related to security objective O.MEM-ACCESS is as follows:

O.MEM-ACCESS is met by FDP_ACC.1/MEM, FDP_ACF.1/MEM, FDP_MSA.1/MEM, FDP_MSA.3/MEM and FDP_SMF.1 together.

FDP_ACC.1/MEM requests the TOE to enforce the Access Control Policy to its memories. FDP_ACF.1/MEM gives the rules for all access ports of the TOE versus system operation modes and CPU privilege levels, which must be applied to the objects, and also the dependencies of these rules on security attributes. FDP_MSA.1/MEM and FDP_MSA.3/MEM give the restrictions required on these security attributes. FDP_SMF.1 finally lists the rules for all access ports that make the TOE changing their system operation modes and CPU privilege levels.

The justification related to security objective O.SFR-ACCESS is as follows:

O.SFR-ACCESS is met by FDP_ACC.1/SFR, FDP_ACF.1/SFR, FDP_MSA.1/SFR, FDP_MSA.3/SFR and FDP_SMF.1 together.

FDP_ACC.1/SFR requests the TOE to enforce the Access Control Policy to its hardware components. FDP_ACF.1/SFR gives the rules for all access ports of the TOE versus system operation modes and CPU privilege levels, which must be applied to the objects, and also the dependencies of these rules on security attributes. FDP_MSA.1/MEM and FDP_MSA.3/MEM give the restrictions required on these security attributes. FDP_SMF.1 finally lists the rules for all access ports that make the TOE changing their system operation modes and CPU privilege levels.

The justification related to security objective O.FLASH-INTEGRITY is as follows:

O.FLASH-INTEGRITY is met by FDP_SDI.2/AGE for the following reason. O.FLASH-INTEGRITY targets to preserve integrity over life-time and FDP_SDI.2/AGE addresses this with a request to monitor integrity and either correct violations or indicate a wearout failure.

The justification related to security objective O.GCM-SUPPORT is as follows:

O.GCM-SUPPORT is met by FCS_COP.1/GCM since FCS_COP.1/GCM requests the TOE to implement the support for cryptographic services targeted in O.GCM-SUPPORT according to an approved public standard. No keys are used by the support for the cryptographic services.

The justification related to security objective O.CRC is as follows:

O.CRC is met by FCS_COP.1/CRC since FCS_COP.1/CRC requests the TOE to implement the cryptographic service targeted in O.CRC according approved public standards. No keys are used by the cryptographic service.

6.3.2 Dependencies of Security Functional Requirements

Table 25 shows all dependencies of the security functional requirements for the TOE.

Table 25. Dependencies of the security functional requirements for the TOE

SFR of the TOE	Dependencies	Fullfilled by SFRs
FRU_FLT.2	FPT_FLS.1	FPT_FLS.1

SFR of the TOE	Dependencies	Fullfilled by SFRs
FPT_FLS.1	none	N/A
FMT_LIM.1	FMT_LIM.2	FMT_LIM.2
FMT_LIM.2	FMT_LIM.1	FMT_LIM.1
FPT_PHP.3	none	N/A
FDP_SDC.1	none	N/A
FDP_SDI.2/FLT	none	N/A
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1
FPT_ITT.1	none	N/A
FDP_IFC.1	FDP_IFF.1	N/R, see sec. 6.3.2 in PP [5]
FCS_RNG.1/PTG.2	none	N/A
FAU_SAS.1	none	N/A
FCS_COP.1/TDES	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	see item 1 below
	FCS_CKM.4	FCS_CKM.4/TDES
FCS_CKM.4/TDES	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	see item 1 below
FCS_COP.1/AES	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	see item 1 below
	FCS_CKM.4	FCS_CKM.4/AES
FCS_CKM.4/AES	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	see item 1 below
FDP_SDI.2/AGE	none	N/A
FCS_COP.1/CRC	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	see item 1 below
	FCS_CKM.4	N/R, see item 2 below
FCS_COP.1/GCM	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	see item 1 below
	FCS_CKM.4	N/R, see item 2 below
FDP_ACC.1/MEM	FDP_ACF.1	FDP_ACF.1/MEM
FDP_ACF.1/MEM	FDP_ACC.1	FDP_ACC.1/MEM
	FMT_MSA.3	FMT_MSA.3/MEM
FMT_MSA.1/MEM	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1/MEM
	FMT_SMR.1	see item 3 below
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3/MEM	FMT_MSA.1	FMT_MSA.1/MEM
	FMT_SMR.1	see item 3 below
FDP_ACC.1/SFR	FDP_ACF.1	FDP_ACF.1/SFR
FDP_ACF.1/SFR	FDP_ACC.1	FDP_ACC.1/SFR
	FMT_MSA.3	FMT_MSA.3/SFR
FMT_MSA.1/SFR	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1/SFR
	FMT_SMR.1	see item 3 below
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3/SFR	FMT_MSA.1	FMT_MSA.1/SFR

SFR of the TOE	Dependencies	Fullfilled by SFRs
	FMT_SMR.1	see item 3 below
FMT_SMF.1	none	N/A

1. The dependencies of security functional requirements FCS_COP.1/TDES, FCS_COP.1/AES, FCS_COP.1/CRC and FCS_COP.1/GCM on FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 are not considered in this Security Target. This is because the decision on how to import user data and how to generate the keys shall be left to the Security IC Embedded Software.
2. The dependencies of security functional requirements FCS_COP.1/CRC and FCS_COP.1/GCM on FCS_CKM.4 don't have to be considered in this Security Target since their operations do not need any cryptographic keys.
3. The dependencies of security functional requirements FMT_MSA.1/MEM, FMT_MSA.3/MEM, FMT_MSA.1/SFR and FMT_MSA.3/SFR on FMT_SMR.1 are not considered in this Security Target. This is because the security attributes shall be managed by Security IC Embedded Software based on which the Security IC Embedded Software shall be capable to maintain roles and assign users to roles appropriate to its needs.

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.

6.3.4 Security Requirements are Internally Consistent

The statement on internal consistency of security requirements in section 6.3.4 of the Protection Profile [5] entirely applies to this Security Target.

Security functional requirements FRU_FLT.2, FPT_FLS.1, FPT_PHP.3, FDP_SDC.1, FDP_SDI.2/FLT, FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, which meet security objectives O.Malfunction, O.Phys-Probing, O.Phys-Manipulation, O.Leak- Inherent and O.Leak-Forced, protect the whole security functionality of the TOE and with this also the cryptographic operations requested in all iterations on FCS_COP.1, related operations on keys as requested in the iterations on FCS_CKM.4 as well as the access control policy according to FMT_SMF.1 and both iterations on each of FDP_ACC.1, FDP_ACF.1, FMT_MAS.1 and FMT_MSA.3.

The iterations FDP_SDI.2/FLT and FDP_SDI.2/AGE on FCS_SDI.2 complement each other in protecting integrity since they both request security functionality that detects integrity violations. Therefore FDP_SDI.2/AGE also adds to O.Phys-Manipulation.

The iterations on FCS_COP and FCS_CKM do not conflict since they address different operations with different keys.

The two iterations on each FDP_ACC.1, FDP_ACF.1, FMT_MSA.1 and FMT_MSA.3 do not contradict as they are related to different objects and their requests on shared security attributes fit together.

7 TOE Summary Specification

7.1 Portions of the TOE Security Functionality

7.1.1 Security Functionality of the TOE

The TOE Security Functionality (TSF) is composed of Security Services (SS) and Security Features (SF). They together fulfill the security functional requirements for the TOE, which are identified in Section 6.1. The TOE also implements security functionality, which is not part of its Security Services and Security Features like the PKC coprocessor. Such security functionality isn't required to meet the security functional requirements for the TOE. Instead, it can be used by Security IC Embedded Software to implement further Security Services and Security Features.

7.1.2 Security Services of the TOE

SS.RNG: Random Number Generator

SS.RNG serves Security IC Embedded Software with random numbers.

For this purpose SS.RNG implements a physical hardware Random Number Generator, which claims functionality class PTG2 of the pre-defined RNG classes in [7]. With this it is suitable for generation of signature key pairs, generation of session keys for symmetric encryption mechanisms, random padding bits, zero-knowledge proofs, generation of seeds for Digital Random Number Generation (DRNG).

The Random Number Generator fulfills the online test requirements defined in [7] and embeds hardware test functionality to detect hardware defects and quality issues of the random numbers.

SS.TDES: Triple-DES coprocessor

SS.TDES serves Security IC Embedded Software with calculation of the Triple Data Encryption Algorithm (TDEA) based on the Data Encryption Standard (DES) as defined in [8].

For this purpose SS.TDES implements a Triple-DES coprocessor in hardware, which can be configured by the Security IC Embedded Software to calculate the Triple DES algorithm or the Triple DES inverse algorithm on blocks of 64 bits with selectable keying option 1 of two 56-bit keys or keying option 2 of three 56-bit keys according to [8]. The keys shall be provided by the Security IC Embedded Software.

SS.AES: AES coprocessor

SS.AES serves Security IC Embedded Software with calculation of the Advanced Encryption Standard (AES) algorithm as defined in [11].

For this purpose SS.AES implements an AES coprocessor in hardware, which can be configured by the Security IC Embedded Software to calculate the AES algorithm or the inverse AES algorithm on blocks of 128 bits with a selectable key length of 128, 192 or 256 bits. The keys shall be provided by the Security IC Embedded Software.

SS.GCM: GCM coprocessor

SS.GCM serves Security IC Embedded Software with support of Galois/Counter Mode (GCM) of operation for symmetric-key cryptographic block ciphers and Galois Message Authentication Code (GMAC) as defined in [12].

For this purpose SS.GCM implements a GCM coprocessor in hardware, which can be configured by the Security IC Embedded Software to perform Galois field multiplication of two 128-bits input values according to section 6.3 of [12].

SS.SBC: SBC interface functions

SS.SBC serves the Security IC Embedded Software with support of Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR) modes of operation for symmetric block ciphers as defined in [9], [10] and with support of Galois/Counter Mode (GCM) of operation for symmetric block ciphers and Galois Message Authentication Code (GMAC) as defined in [12].

For this purpose SS.SBC implements XOR operations in hardware and also implements an increment function in hardware according to section 6.2 of [12] with $s = 32$. In addition, the TOE implements a register bank that handles input and output data of SS.TDES, SS.AES, SS.GCM as well as their pre- and post-processing with XOR operations and increment function.

SS.CRC: CRC coprocessor

SS.CRC serves the Security IC Embedded Software with calculation of of cyclic redundancy checks as defined in [13] for 8 bits, in [15] for 16 bits and in [16] for 32 bits.

For this purpose SS.CRC implements two CRC coprocessors in hardware. Each CRC coprocessor can be configured by Security IC Embedded software to calculate a cyclic redundancy check over a data stream of selectable number of one, two, three or four input bytes. The Security IC embedded Software can choose the cyclic redundancy check out of an 8-bits value based on the polynomial in [13], a 16-bits value based on the polynomial in [15] and a 32-bits value based on the polynomial in [16].

7.1.3 Security Features of the TOE

SF.OPC: Control of Operating Conditions

SF.OPC controls operating conditions of the TOE. These are explicitly controlled by security functionality that simply hampers feeding certain electrical stimulations into the device. Such security functionality is composed of frequency filters and voltage limiters. Operating conditions of the device are explicitly controlled also by security functionality that actively monitors certain electrical parameters. These parameters are voltage levels of external supply from pad and internal supplies, frequencies of internal clocks and on-chip temperature. Such security functionality raises an error message whenever a monitored parameter drops out of its valid range. In addition, exposure of the device to light is explicitly controlled by security functionality that senses abnormal light over its whole surface, raising an error message when detected.

SF.OPC also controls operating conditions implicitly. This is done by security functionality that detects faults in code and data stored to memories and while processed in the device. Such faults might be inserted by electrical stimulations or by exposure of the device to energy or particles. Error detection codes are used to protect the memories as well as the access channels over the bus system to memories and to hardware peripherals on the control bus, the direct access channel to PKC RAM and security-relevant storage and processing in CPU coprocessor and hardware peripherals on the control bus including SBC interface with Triple-DES, AES, GCM coprocessors and CRC

coprocessor. Watchdogs on error detection codes run over code and data stored to System RAM and PKC RAM, and the Secure Fetch Plus on code and data read from Flash memory can be configured and enabled by Security IC Embedded Software.

Further on, Security IC Embedded Software can configure and enable a Secure Fetch on CPU code and/or data accesses over the bus system and also range checks on values in general purpose, stack pointers and link registers of the CPU as well as checks on predefined CPU instructions for zero values in their operands or in the addresses of their resulting data accesses to memory. In addition, Security IC Embedded Software may protect its program flow by use of a signature watchdog on CPU code accesses over the bus system, by use of a secure counter and by use of a watchdog timer.

SF.OPC also provides the Security IC Embedded Software with multiple calculation modes for the Triple-DES, AES and GCM coprocessors. Triple-DES and AES coprocessors each is equipped with a fault detection mechanism on its key schedule that must be enabled by Security IC Embedded Software.

In case an error message is raised the TOE either (i) aborts code execution and forces a reset or (ii) raises an exception, which interrupts code execution and jumps to an exception vector on which the Security IC Embedded Software can react with an appropriate exception handler. In case of reset the TOE returns to its initial state and provides information on the reset source to the Security IC Embedded Software. In case of an exception the TOE provides information on the exception source to the Security IC Embedded Software.

SF.OPC also implements security functionality that corrects errors in Flash memory.

SF.PHY: Protection against Physical Manipulation

SF.PHY protects the TOE from physical probing and physical manipulation of its hardware, its IC Dedicated Software, its TSF data and Security IC Embedded Software stored to its Flash memory including user data of the Composite TOE. This is achieved by appropriate shielding techniques for all elements in the physical design of the TOE, as well as redundant routing of sensitive signals and layout constraints on particular placements and routings.

Selected security functionality in analog design parts of the TOE is additionally checked for its basic operability by a built-in selftests that run during startup of the device.

Memories and their interfaces are additionally protected against probing by appropriate encryption of stored content and address scrambling mechanisms.

SF.LOG: Logical Protection

SF.LOG provides logical protection of the TOE that fights disclosure of confidential data stored to and processed in the TOE through tracing of power consumption or emanation and subsequent complex signal analysis.

Triple-DES, AES, GCM and CRC coprocessors each implements security functionality that eliminates exploitable side channel leakage. Such security functionality in Triple-DES and AES coprocessors uses masking techniques in data processing, inserts diverse dummy activity that can partly be configured by Security Embedded Software, and randomizations. GCM coprocessor and CRC coprocessor implement masking schemes on their data processing.

Input and output data of Triple-DES, AES and GCM coprocessors are handled via the register bank in the SBC interface that implements masking. XOR operations in the SBC interface are embedded in this masking.

The PKC coprocessor implements security functionality that effectively reduces side channel leakage by adding noise, inserting dummy activity and randomizations.

Code and data are masked on their transfer via the access channels over the bus system to memories and hardware peripherals on the control bus like SBC interface, CRC coprocessor and PKC coprocessor. The CPU embeds masking schemes for storage and processing of data and code.

SF.LOG also serves the Security IC Embedded Software with security functionality for additional protection for loading of data into the register bank of the SBC interface and into the input register of the CRC coprocessor.

SF.FOS-USE: Factory OS use restrictions

SF.FOS-USE restricts use of the Factory OS among three levels of testing capabilities of the TOE. Access to the lower level of testing capabilities is not blocked. Instead, its testing capabilities are very limited so that they cannot be exploited. The medium level of testing capabilities is blocked by an authentication procedure. After successful authentication to this level the TOE serves with testing capabilities to the extent that confidentiality of content stored to its memories cannot be compromised.

The upper level of testing capabilities is blocked by two authentication checks, of which the latter one also forces an erase of AP-Flash, BL-Flash, SH-Flash and SV-Flash windows as well as System Page Application, System Page Bootloader and System Page Common before full testing capabilities are provided.

Commands of the Factory OS are conditionally installed in stages and commands with test functionality are cut to tests of basic functionality only.

SF.MEM-ACC: Memory Access Control

SF.MEM-ACC controls access to the memories of the TOE. This is done based on physical restrictions in the bus system that block certain access ports for particular memories, and also direct memory access to PKC RAM is physically restricted to the PKC coprocessor.

In addition, security functionality is implemented that checks every single access over the bus system to the memories against predefined and/or configurable access rights for each of the following combinations of system operations modes and CPU privilege levels:

- NXP Mode
- Service Mode privileged
- Service Mode unprivileged
- Shared Mode
- Bootloader Mode privileged
- Bootloader Mode unprivileged
- Application Mode privileged
- Application Mode unprivileged

Every access over the bus system to a memory address is checked against access rights in read, write and execute. Access rights are set for predefined default address windows in ROM, Flash memory, System RAM and PKC RAM and also for configurable software-controlled address windows within these default address windows. Configurations are accessible to Security IC Embedded Software.

System operation modes and CPU privilege levels are assigned to each access port on the bus system and are transmitted over the bus system into the memory controllers. System operation modes and CPU privilege levels are also transmitted into the mode

controller, which implements appropriate rules for transformations in system operation modes that dynamically update those assigned to CPU and DMA controller access ports, whereat Service Mode is permanently masked out for the DMA controller access port. CPU privilege levels are updated by the CPU. The PKC controller access port is assigned with system operation modes that are dynamically updated to the access rights actually valid for direct memory access to PKC RAM.

SF.SFR-ACC: Special Function Register Access Control

SF.SFR-ACC controls access to the Special Function Registers of the TOE. This is done based on physical restrictions in the bus system that block DMA controller access to hardware components on the control bus and also PKC coprocessor access to hardware components on both, control bus and peripheral control bus.

In addition, security functionality is implemented that checks every single access over the bus system on the control bus and on the peripheral control bus to a Special Function Register against predefined and/or configurable access rights for the following combinations of system operation modes and CPU privilege levels:

- NXP Mode
- Service Mode privileged
- Service Mode unprivileged
- Bootloader Mode privileged or Application Mode privileged
- Bootloader Mode unprivileged or Application Mode unprivileged

Control of access to the Special Function Registers is done in two layers of security functionality. The first layer of security functionality is implemented in every hardware component that is connected to the control bus or to the peripheral control bus and checks each access to a Special Function Register per bit against predefined and partly configurable access rights in read and write. Such access rights cannot be enlarged in the second layer but only be further restricted. The second layer of security functionality is implemented in the bus system and can be configured to either completely block access to the group of Special Function Registers belonging to a hardware component or completely unblock it to the extent provided in the first layer. Configurations of access rights are accessible to Security IC Embedded Software.

Relevant combinations of system operation modes and CPU privilege levels are assigned to every access port on the bus system and are transmitted over the bus system into the hardware components on the control bus and on the peripheral control bus. System operation modes and CPU privilege levels are also transmitted into the mode controller, which implements appropriate rules for transformations in system operation modes that dynamically update those assigned to CPU and DMA controller access ports, whereat Service Mode is permanently masked out for the DMA controller access port. CPU privilege levels are updated by the CPU.

SF.FLSV-SUP: Flash Services Software support

SF.FLSV-SUP implements security functionality, which enables Services Software to implement an application programming interface (API) serving other Security IC Embedded Software with tearing-save operations to update content in Flash memory with verification of updated content.

SF.FLSV-SUP provides Service Software with security functionality to check the rate of wear per page in the Flash memory. Based on this Service Software can implement dynamic wear-leveling as well as static wear-leveling and refreshing of Flash pages to optimize life-time of the Flash memory and to provide wearout indication to other Security IC Embedded Software or enforce a wearout failure on its own.

7.2 TOE Summary Specification Rationale

7.2.1 Mapping of Security Functional Requirements and TOE Security Functionality

Table 26 maps the security functional requirements for the TOE to the TOE security functionality.

Table 26. Dependencies of the security functional requirements for the TOE

SFR of the TOE	SS.RNG	SS.TDES	SS.AES	SS.GCM	SS.SBC	SS.CRC	SF.OPC	SF.PHY	SF.LOG	SF.FOS-USE	SF.MEM-ACC	SF.SFR-ACC	SF.FLSV-SUP
FRU_FLT.2							X	X					X
FPT_FLS.1							X	X					X
FMT_LIM.1										X			
FMT_LIM.2										X	X	X	
FPT_PHP.3	X						X	X					
FDP_SDC.1								X					
FDP_SDI.2/FLT							X						
FDP_ITT.1								X	X				
FPT_ITT.1								X	X				
FDP_IFC.1								X	X				
FCS_RNG.1/PTG.2	X												
FAU_SAS.1										X			
FCS_COP.1/TDES		X			X								
FCS_CKM.4/TDES					X								
FCS_COP.1/AES			X		X								
FCS_CKM.4/AES					X								
FDP_SDI.2/AGE													X
FCS_COP.1/CRC						X							
FCS_COP.1/GCM				X	X								
FDP_ACC.1/MEM											X		
FDP_ACF.1/MEM											X		
FMT_MSA.1/MEM											X		

SFR of the TOE	SS.RNG	SS.TDES	SS.AES	SS.GCM	SS.SBC	SS.CRC	SF.OPC	SF.PHY	SF.LOG	SF.FOS-USE	SF.MEM-ACC	SF.SFR-ACC	SF.FLSV-SUP
FMT_MSA.3/MEM											X		
FDP_ACC.1/SFR												X	
FDP_ACF.1/SFR												X	
FMT_MSA.1/SFR												X	
FMT_MSA.3/SFR												X	
FMT_SMF.1											X	X	

7.2.2 Rationale for the Portions of the TOE Security Functionality

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

7.2.3 Security Architectural Information

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

8 Bibliography

8.1 Evaluation documents

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004

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

[6] Evaluation of random number generators, Bundesamt für Sicherheit in der Informationstechnik, Version 0.10

[7] A proposal for: Functionality classes for random number generators, Bundesamt für Sicherheit in der Informationstechnik/T-Systems GEI GmbH, Version 2.0, 18 September 2011

8.2 Standards

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

[9] NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation, National Nationale Institute of Standards and Technology, Edition 2001

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

[11] Federal Information Processing Standrads Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

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

[13] "SERIES I: INTEGRATED SERVICES DIGITAL NETWORK, ISDN user-network interfaces – Layer 1 Recommendations", International Telecommunication Union, ITU-T Recommendation I.432.1, Februar 1999

[14] "SERIES V: DATA COMMUNICATION OVER THE TELEPHONE NETWORK, Error control", International Telecommunication Union, ITU-T Recommendation V.42, March 2002

[15] "SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATION, Public data networks – Interfaces", International Telecommunication Union, ITU-T Recommendation X.25, October 1996

[16] "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

8.3 Developer documents

[17] P73N2M0B0.20n, Information on User Guidance and Operation, User manual, NXP Semiconductors, Version 1.01, 18 April 2017

[18] P73N2M0, High-performance secure controller, Product data sheet, NXP Semiconductors, DocID: 297431

[19] P73N2M0B, Wafer and Delivery Specification, Product data sheet addendum, NXP Semiconductors, DocID 328231

[20] P73 Family, SC300 User Manual, Product Data sheet addendum, NXP Semiconductors, DocID: 341410

[21] ARM®v7-M Architecture Reference Manual, ARM, DDI 0403E.b (ID120114)

[22] P73 Family, DMA Controller PL080 User Manual, Product data sheet addendum, NXP Semiconductors, DocID: 341510

[23] FLASH Services Architecture Overview ROM-resident Firmware, NXP Semiconductors, Revision 0.2, 29.03.2016 (internal document)

[24] Electronic Order Entry Form, online document, NXP Semiconductors, https://www.eoef.nxp.com

9 Legal information

9.1 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.

9.2 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

Figures

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 2 November 2018