T6ND7 Integrated Circuit Security Target Lite Public

19 Mar. 2014

Version 1.0

TOSHIBA CORPORATION
Semiconductor & Storage Products Company

Change History

No	Version	Date	Chapter	Content	Name
1	1.0	19 Mar. 2014	-	Creation	Toshiba

Table of contents

1. ST Introduction

This Security Target (ST) is built upon the Security IC Platform Protection Profile [5]. Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035.

This chapter presents the ST reference and for the Target Of Evaluation (TOE) the reference, an overview and a description.

1.1. ST identifiers

ST reference: T6ND7 Integrated Circuit Security Target Lite, version 1.0, 19 Mar. 2014

TOE reference: T6ND7 Integrated Circuit

1.2. TOE overview

The T6ND7 Integrated Circuit (Target of Evaluation – TOE) is an Integrated Circuit with a DES and RSA accelerator. The TOE that is described in this ST is a single chip microcontroller (hardware, security IC dedicated support software (Boot Loader) and security IC dedicated test software) that is used in mobile equipment. The TOE combined with an IC for communication (which is not part of the TOE) realizes a platform for various applications running on the mobile phone. The TOE has two different communication interfaces:

1. an interface that receives data from or send data to the ISO7816 Host controller (= Application processor).
2. a SWP interface, a wired serial interface that communicates with the SWP host controller of the mobile equipment. SWP host controller is usually called CLF or Contactless Front End and used as wireless communication.

The objective of the TOE is to protect the security of the IC and embedded software that is intended to be used as applications on the phone. One of the applications is user can read the URL by this TOE and SWP host controller and search the actual information through application processor from Internet.

The intended usage of the operational TOE is by consumers (end-user), who own/use mobile equipment in which the TOE is embedded.

The TOE is delivered to a composite product manufacturer. Toshiba develops the IC dedicated test software and Boot loader. Toshiba implements the Boot Loader and the IC dedicated test software and implemented in T6ND7. After testing in Toshiba, the test software is made unavailable. User can download their own application software encrypted by Triple DES onto the TOE and decrypt it. The Boot Loader is used by the composite product manufacturer to download their Operating system and download softwares running on their Operating System and this is different from Boot Loader and other necessary programs. .

TOE is expected to be used for multiple applications in a multiple provider environment.

Therefore the TOE may store and process secrets of several systems that must be protected each other. So the TOE must meet the security requirements to be applied to security modules.

Protected information is in general secret data as Personal Identification Numbers, Balance Value (Stored Value Cards), and Personal Data Files. Other protected information is the data representing the access rights; these include any cryptographic algorithms and keys needed for accessing and using the services provided by the system through use of the TOE and its embedded software in mobile equipment.

The IC that is used in mobile equipment consists of the central processing unit (CPU), memory element (ROM, RAM, Flash memory), and circuit for the two defined external interfaces that have been integrated with consideration given to tamper resistance.

The increase in the number and complexity of applications in the market of these products is reflected in the increase of the level of data security required. The security needs for a this product can be summarised as being able to counter those who want to defraud, gain unauthorised access to data and control a system using the TOE and its embedded software. Therefore it is mandatory to:

- maintain the integrity and the confidentiality of the content of the memory as required by the security IC embedded software the product is built for
- maintain the correct execution of the security IC embedded software residing on the TOE.

This requires that the TOE's integrated circuit especially maintains the integrity and the confidentiality of its security enforcing and security relevant architectural components.

The intended environment is very large; and generally once issued the IC embedded in the mobile equipment can be stored and used and no control can be applied to the TOE and the mobile equipment operational environment. For example, a commuter ticket, electronic money or data (money information, user information etc) or even application programs are stored in the NOR-flash-non-volatile memory. By wired communication of ISO7816 compliant, the data that Application processor receives is communicated to T6ND7. T6ND7 manages the data securely, and returns the processed result to Application processor. This is one way of communication to this TOE.

There is another way of communication in this TOE. SWP (or Single Wire Protocol) host is attached outside of this TOE. SWP terminal of the TOE is used for wireless communication called NFC (=Near Field Communication). SWP host is out of scope of this security target.

Co-processor accelerates arithmetic operations such as modular exponentiation. As no cryptographic algorithm is provided by Toshiba for the TOE, the functionality of this co-processor is included in the TOE but its specific use in cryptographic algorithm is out of the scope.

1.3. TOE description

In this chapter, for the sake of providing deeper understanding of the security requirements and intended use of the TOE, overall information regarding the TOE will be provided.

1.3.1. Physical scope

The Target of Evaluation (TOE) is intended to be used in mobile equipment, independent of the physical interface and the way it is packaged. Generally, the product may include other optional elements (such as specific hardware components, batteries, capacitors, etc.) but these are not in the scope of this Security Target. In Table 1-1 the physical scope the TOE is presented.

Table 1-1, Physical scope of the TOE.

DELIVERY ITEM TYPE	IDENTIFIER	VERSION	MEDIUM	ADDITIONAL INFORMATION
Hardware	T6ND7	4.0	T6ND7 wafer	The T6ND7 TOE is delivered in Diced wafer.
Software	Boot Loader software	00.00.06	ROM of hardware (Boot Loader area)	
	TEST ROM software	02	ROM of hardware (test area)	
	API software	00.00.06	ROM of hardware (Boot Loader area)	
Manuals	T6ND7 User guidance overview	0.6	Electronic document	
	1MB SIM LSI (T6ND7) Data Sheet	1.10	Electronic document	
	T6ND7 User Guidance manual	1.10	Electronic document	User Guidance Manual describes about Register setting securely.
	T6ND7 Bootloader User Manual	1.12	Electronic document	
	T6ND7 API User Manual	1.00	Electronic document	

The software (i.e. Boot Loader and TEST ROM software) is part of the TOE, because it includes some security mechanisms after TOE Delivery.

The Boot Loader is usable after TOE Delivery. Exception is the “IC dedicated test software (TEST ROM software)” that is not usable after TOE Delivery to a composite product manufacturer and is only used to support production of the TOE.

The manuals are delivered to the composite product manufacturer. The end user does not receive these manuals. The delivery to the end user contains the operational TOE consisting of the IC Hardware and IC embedded application software downloaded in Nor-flash by composite product manufacturer.

The TOE in its environment is depicted in Figure 2-1. The T6ND7 TOE is an LSI which has been designed to realize card functionality in combination with an SWP Host Controller (CLF) for applications in mobile phone. In such a function there can be a user OS and service data in the NOR-flash non-volatile memory. For example, a commuter ticket, electronic money or data (money information, user information etc) are stored in the NOR-flash non-volatile memory. By wireless communication, the data that SWP host controller receives is communicated to the TOE. The TOE manages the data securely, and returns the processed result through SWP host controller to the

Reader/writer (R/W).

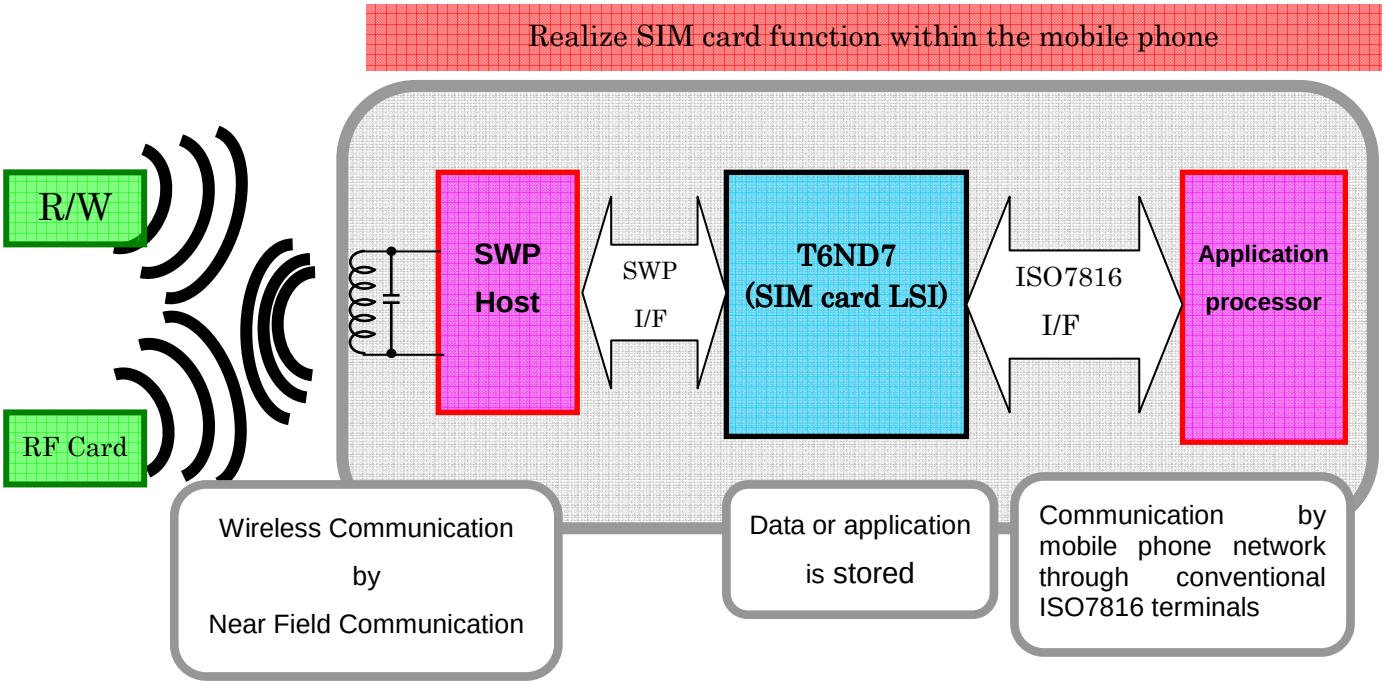

Figure 2-1 TOE in its environment

The components of the TOE are depicted in Figure2-2 as block diagram. The basic configuration elements of the TOE are the CPU, the CPU peripheral circuits (MEMC, Control Logic), the various memory elements (NOR-flash, ROM, RAM), security function circuit (CRC, RNG, Triple-DES, Coprocessor), various types of detection circuits (SECURITY DETECTORS), and others (TEST CIRCUIT, etc.).

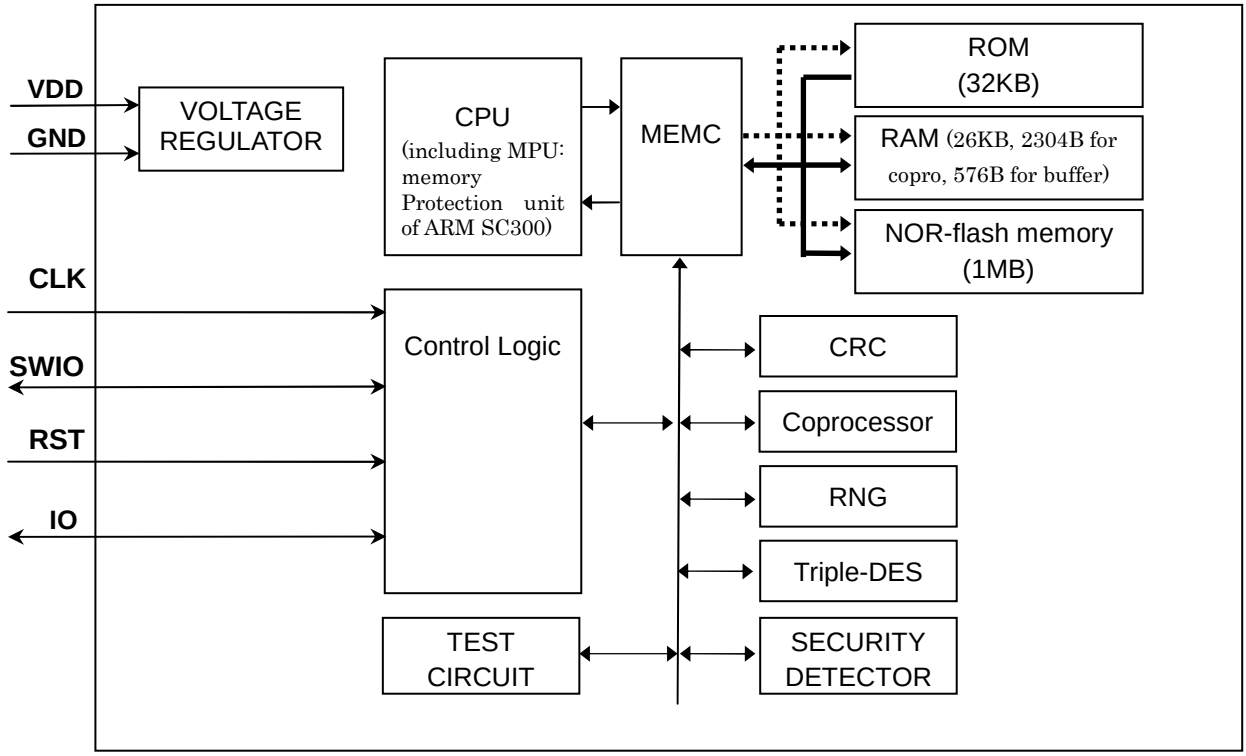

Figure 2-2 Basic Configuration Elements of the Hardware

The following components are used.

- CPU — ARM SC300
- MPU — Memory Protection Unit in SC300
- MEMC — Memory Crypto Circuit
- RAM, ROM, NOR-flash memory
  - RAM: 26KB RAM (SYSTEM RAM) + 2304B (CRYPTO RAM) + 576B (COMMUNICATION BUFFER RAM)
  - ROM 32KB (TEST ROM and Boot Loader ROM)
  - NOR-flash memory 1MB
- Control Logic
- Triple-DES — Single-DES is used 3 times for Triple-DES operation
- Coprocessor — Arithmetic accelerator (accelerates arithmetic operations such as modular exponentiation). As no cryptographic algorithm is provided by Toshiba for the TOE, the functionality of this co-processor is included in the TOE but its specific use in cryptographic algorithm is out of the scope.
- CRC — CRC-32, CRC-CCITT (16 bit CRC)
- RNG — Random number generator
- VOLTAGE REGULATOR
- SECURITY DETECTORS
- TEST CIRCUIT
- ISO7816 serial Input Output terminals (IO =input output)

- SWP (= Single wire protocol.) SWP is not included in the evaluation.

  RST is external reset input.

  CLK is external clock input.

  IO is connected to HOST controller (=Application processor) directly. SWIO is connected to SWP Host controller. SWP Host Controller is called CLF in NFC technology.

  VDD and GND are power supply terminal and ground terminal respectively. VDD can be controlled by External power management unit.

1.3.2. Logical scope

The logical security features offered by the TOE are the following:

1. Triple-DES:
   a. ECB mode, Triple DES 2KEY,Encryption/Decryption
   b. ECB mode, Triple DES 3KEY,Encryption/Decryption
2. Physically seeded random number generator:

   A physical noise source provides seeding for deterministic random number generator built from recursive calls to Triple DES, conformant to AIS20 Class K3.
3. Memory access control

   TOE has “Memory Protection Unit (MPU)” as a unit for memory access control function.
4. Boot Loader

   Boot Loader downloads user code to Flash memory.

1.3.3. TOE Life cycle

The Security IC product life-cycle is scheduled in phases as introduced in the PP [5]. IC Development as well as IC Manufacturing and Testing, which are phases 2 and 3 of the life-cycle, are scope of the evaluation.

Because the TOE is delivered in diced wafer, phase 4 is not scope of evaluation. Phase 1 and 5 to 7 are also out of evaluation scope.

2. Conformance claim

This chapter presents conformance claim and the conformance claim rationale.

2.1. CC Conformance

This Security Target claims to be conformant to the Common Criteria "version 3.1 revision 4" September 2012.

- The conformance of the ST to CC Part 2 is CC Part 2 extended
- The conformance of the ST to CC Part 3 is CC Part 3 conformant

The extended Security Functional Requirements are defined in chapter 5.

This TOE claims to be conformant to the Common Criteria "version 3.1 revision 4" September 2012.

The attack potential quotation as part of the vulnerability analysis shall use the Mandatory Technical Document "Application of Attack Potential to Smartcards", which current version is [8].

2.2. PP Claim

The ST and the TOE claim conformance to the following Protection Profile (PP):

- Security IC Platform Protection Profile. Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035 [5].

2.3. Package claim

The assurance level for this Security Target is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2. This assurance level is in line with the Security IC Platform Protection Profile [5].

2.4. Conformance claim rationale

This TOE is equivalent to the conformance claim stated in a Security IC Platform Protection Profile.

3. Security problem definition

This chapter presents the threats, organisational security policies and assumptions for the TOE.

The Assets, Assumptions, Threats and Organisational Security Policies are completely taken from the Security IC Platform Protection Profile [5].

3.1. Description of Assets

Since this Security Target claims conformance to the Security IC Platform Protection Profile [5], the assets defined in section 3.1 of the Protection Profile are applied.

3.2. Threats

Since this Security Target claims conformance to the Security IC Platform Protection Profile [5], the threats defined in section 3.2 of the Protection Profile are valid for this Security Target. The following table lists the threats of the Protection Profile.

Table 3-1, Threats defined in the Security IC Platform Protection Profile.

Threats	Titles
T.Phys-Manipulation	Physical Manipulation
T.Phys-Probing	Physical Probing
T.Malfunction	Malfunction due to Environmental Stress
T.Leak-Inherent	Inherent Information Leakage
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

The TOE shall avert the additional threat “Memory Access Violation (T.Mem-Access)” as specified below.

T.Mem-Access Memory Access Violation

Parts of the Smartcard Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). Any restrictions are defined by the security policy of the specific application context and must be implemented by the Smartcard Embedded Software.

3.3. Organisational security policies

Since this Security Target claims conformance to the Security IC Platform Protection Profile [5], the Organisational Security Policies defined in section 3.3 of the Protection Profile are valid for this Security Target. The following table lists the Organisational Security Policies of the Protection Profile.

Table 3-2, Organisational Security Policies defined in the Security IC Platform Protection Profile.

Organisational Security Policies	Titles
P.Process-TOE	Protection during TOE Development and Production

The TOE provides specific security functionality, which can be used by the security IC embedded software. In the following specific security functionality is listed which is not derived from threats identified for the TOE's environment because it can only be decided in the context of the security IC application, against which threats the security IC embedded software will use the specific security functionality.

The IC Developer / Manufacturer must apply the policy "Additional Specific Security Functionality (P.Add-Functions)" as specified below.

P.Add-Functions Additional Specific Security Functionality

The TOE shall provide the following specific security functionality to the security IC embedded software:

- Triple Data Encryption Standard (TDES),
- Secure Boot Loader

3.4. Assumptions

Since this Security Target claims conformance to the Security IC Platform Protection Profile [5], the assumptions defined in section 3.4 of the Protection Profile are valid for this Security Target. No additional assumptions are added. The following table lists the assumptions of the Protection Profile.

Table 3-3, Assumptions defined in the Security IC Platform Protection Profile.

Assumptions	Titles
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
A.Plat-Appl	Usage of Hardware Platform
A.Resp-Appl	Treatment of User Data

The developer of the Security IC Embedded Software must ensure the appropriate "Treatment of User Data (A.Resp-Appl)" while developing this software in Phase 1 as specified below.

4. Security objectives

This chapter provides the statement of security objectives and the security objective rationale. For this chapter the Security IC Platform Protection Profile [5] can be applied completely. Only a short overview is given in the following.

4.1. Security objectives for the TOE

The TOE shall provide the following security objectives, taken from the Security IC Platform Protection Profile [5]. The following table lists the security objectives for the TOE of the Protection Profile.

Table 4-1, Security objectives for the TOE defined in the Security IC Platform Protection Profile.

Security objectives for the TOE	Titles
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunctions
O.Phys-Manipulation	Protection against Physical Manipulation
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality
O.Identification	TOE Identification
O.RND	Random Numbers

Regarding Application Notes 9 and 10 of the Security IC Platform Protection Profile [5] the following additional security objectives are defined based on additional functionality provided by the TOE as specified below.

O.HW_TDES DES Functionality

The TOE shall provide the cryptographic functionality to calculate a TDES encryption and decryption to the security IC embedded software. The TOE supports directly the calculation of Triple-DES.

O.Mem-Access Area based Memory Access Control

The TOE must provide the Security IC Embedded Software with the capability to define memory segmentation and protection. The TOE must then enforce the defined access rules so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

O. Boot-Loader	Boot load Functionality Controlled loading of the Security IC Embedded Software: The TOE must provide the capability to load the Security IC Embedded Software into the FLASH memory, either before TOE delivery, under Toshiba authority, either after TOE delivery, under the composite product manufacturer authority. The TOE must ensure confidentiality and integrity of loaded Security IC Embedded Software as well as restrict the access to these features. This capability is not available in User configuration.

4.2. Security objectives for the security IC embedded software development environment

According to the Security IC Platform Protection Profile [5], the following security objectives for the environment are specified:

Table 4-2, Security objectives for the security IC embedded software development environment defined in the Security IC Platform Protection Profile.

Security objectives for the Environment	Titles
OE.Plat-Appl	Usage of Hardware Platform
OE.Resp-Appl	Treatment of User Data

Clarification of "Usage of Hardware Platform (OE.Plat-Appl)"

The TOE supports cipher schemes as additional specific security functionality. If required the security IC embedded software shall use these cryptographic services of the TOE and their interface as specified. When key-dependent functions implemented in the security IC embedded software are just being executed, the security IC embedded software must provide protection against disclosure of confidential data (User Data) stored and/or processed in the TOE by using the methods described under "Inherent Information Leakage (T.Leak-Inherent)" and "Forced Information Leakage (T.Leak-Forced)".

Clarification of "Treatment of User Data (OE.Resp-Appl)"

By definition cipher or plain text data and cryptographic keys are User Data. The security IC embedded software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the TOE and use keys and functions appropriately in order to ensure the strength of cryptographic operation.

This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong.

For example, if keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained.

This implies that appropriate key management has to be realised in the environment.

4.3. Security objectives for the operational environment

According to the Security IC Platform Protection Profile [5], the following security objectives for the environment are specified.

Table 4-3, Security objectives for the Environment defined in the Security IC Platform Protection Profile.

Security objectives for the Environment	Titles
OE.Process-Sec-IC	Protection during composite product manufacturing

4.4. Security objectives rationale

In Table 4-4 each security objective for the TOE is traced back to threats countered by that security objective and OSPs enforced by that security objective.

Table 4-4, Tracing between objectives and Threat, Organisational Security Policy or Assumption.

Threat, Organisational Security Policy or Assumption	Security Objective	Sufficiency of countering
T.Phys-Manipulation	O.Phys-Manipulation	See [5]
T.Phys-Probing	O.Phys-Probing	See [5]
T.Malfunction	O.Malfunction	See [5]
T.Leak-Inherent	O.Leak-Inherent	See [5]
T.Leak-Forced	O.Leak-Forced	See [5]
T.Abuse-Func	O.Abuse-Func	See [5]
T.RND	O.RND	See [5]
P.Process-TOE	O.Identification	See [5]
P.Add-Functions	O.HW_TDES	See below
P.Add-Functions	O.Boot-Loader	See below
T.Mem-Access	O.Mem-Access	See [7] and below
	OE.Plat-Appl	See [7] and below
	OE.Resp-Appl	See [7] and below
A.Process-Sec-IC	OE.Process-Sec-IC	See [5]
A.Plat-Appl	OE.Plat-Appl	See [5]
A.Resp-Appl	OE.Resp-Appl	See [5]

The justification related to the organisational security policy “Additional Specific Security

Functionality (P.Add-Functions) is as follows:

Since these objectives require the TOE to implement exactly the same specific security functionality as required by P.Add-Functions, the organisational security policy is covered by the objectives.

The justification related to the threat “Memory Access Violation (T.Mem-Access)” is as follows:

According to O.Mem-Access the TOE must enforce the partitioning of memory areas so that access of software to memory areas is controlled. Any restrictions are to be defined by the Smartcard Embedded Software. Thereby security violations caused by accidental or deliberate access to restricted data (which may include code) can be prevented (refer to T.Mem-Access). The threat T.Mem-Access is therefore removed if the objective is met.

The clarification of “Usage of Hardware Platform (OE.Plat-Appl)” makes clear that it is up to the Smartcard Embedded Software to implement the memory management scheme by appropriately administrating the TSF. This is also expressed both in T.Mem-Access and O.Mem-Access. The TOE shall provide access control functions as a means to be used by the Smartcard Embedded Software. This is further emphasised by the clarification of “Treatment of User Data (OE.Resp-Appl)” which reminds that the Smartcard Embedded Software must not undermine the restrictions it defines. Therefore, the clarifications contribute to the coverage of the threat T.Mem-Access.

5. Security requirements

This chapter presents the statement of security requirements for the TOE and the security requirements rationale. This chapter applies the Security IC Platform Protection Profile [5].

5.1. Definitions

In the next sections the following the notation used

- Whenever iteration is denoted, the component has an additional identification [XXX].
- When the refinement, selection or assignment operation is used these cases are indicated by *italic text* and explained in footnotes.

5.2. Security Functional Requirements (SFR)

To support a better understanding of the combination Security IC Platform Protection Profile vs. Security Target, the TOE Security Functional Requirements are presented in the following several different sections.

5.2.1. SFRs derived from the Security IC Platform Protection Profile

Table 5-1, Security Functional Requirements taken from the Security IC Platform Protection Profile.

Security functional requirements	Titles
FRU_FLT.2	“Limited fault tolerance“
FPT_FLS.1	“Failure with preservation of secure state”
FMT_LIM.1	“Limited capabilities”
FMT_LIM.2	“Limited availability”
FAU_SAS.1	“Audit storage”
FPT_PHP.3	“Resistance to physical attack”
FDP_ITT.1	“Basic internal transfer protection”
FDP_IFC.1	“Subset information flow control”
FPT_ITT.1	“Basic internal TSF data transfer protection”
FCS_RNG.1	“Quality metric for random numbers”

Table 5-1 lists the Security Functional Requirements that are directly taken from the Security IC Platform Protection Profile. With two exceptions, all assignment and selection operations are performed on these SFRs. The fist exception is the left open assignment of type of persistent memory by FAU_SAS.1. The second exception is the left open definition of a quality metric for the

random numbers required by FCS_RNG.1. The following statements define these SFRs. The SFRs FMT_LIM, FAU_SAS and FCS_RNG are extended security requirements, completely defined in the PP.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide *the test process before TOE Delivery*[1] with the capability to store *the Initialisation Data and/or Pre-personalisation Data in the NOR-flash and/or supplements of the security IC embedded software*[2] in the *NOR-flash*[3].

Dependencies: No dependencies.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

FCS_RNG.1.1 The TSF shall provide a *physical*[4] random number generator that implements *total failure test of the random source*[5].

FCS_RNG.1.2 The TSF shall provide random numbers that meet independent bits with *Shannon entropy of 7.976 bits per octet.*[6] [7]

Dependencies: No dependencies.

FCS_RNG.1 [DRNG] Random number generation

Hierarchical to: No other components.

---

[1] [assignment: *list of subjects*]

[2] [assignment: *list of audit information*]

[3] [assignment: *type of persistent memory*]

[4] [selection: physical, non-physical true, deterministic, hybrid]

[5] [assignment: *list of additional security capabilities*] refined with "none" in accordance with application note 20 of [5]. The results of the total failure test are provided to the Security IC Embedded Software by a seeding error warning.

[6] [selection: independent bits with Shannon entropy of 7.976 bits per octet, Min-entropy of 7.95 bit per octet, [assignment: other comparable quality metric]].

[7] [assignment: other comparable quality metric]

FCS_RNG.1.1 [DRNG] The TSF shall provide a *deterministic*[8] random number generator that implements *none*[9].

FCS_RNG.1.2 [DRNG] The TSF shall provide random numbers that meet Class K3 of [6][10].

Dependencies: No dependencies.

5.2.2. SFRs regarding cryptographic functionality

For the security IC embedded software the following cryptographic functionality is defined related to DES operation.

5.2.2.1. DES Operation

The DES Operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)".

FCS_COP.1 [TDES] Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 [TDES] The TSF shall perform *encryption and decryption*[11] in accordance with a specified cryptographic algorithm *Triple Data Encryption Standard (3DES – supporting ECB mode)*[12] and cryptographic key sizes of *112 bit and 168 bit keys*[13] that meet the following standards[14]:

U.S. Department of Commerce / National Bureau of Standards, Data Encryption Standard (DES), FIPS PUB 46-3, 1999, October 25, TDEA keying option 1 and 2.

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

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

5.2.3. SFRs regarding Memory Access control

FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

---

8 [selection: physical, non-physical true, deterministic, hybrid]

9 [assignment: *list of security capabilities*]

10 [assignment: *a defined quality metric*]

11 [assignment: list of crypto-graphic operations]

12 [assignment: cryptographic algorithm], change due to different standard

13 [assignment: cryptographic key sizes], change due to different part of standard

14 [assignment: list of standards], change of referred standard

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 The TSF shall enforce the *Memory Access Control Policy*[15] on *all subjects (software), all objects (data including code stored in memories)*[16] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operation between any subject controlled by the TSF and any object controlled by TSF are covered by an access control SFP.

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the *Memory Access Control Policy*[17] to objects based on the *memory region and the current set of access rights.*[18]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *the operation is allowed if and only if the software mode, the memory region and the operation matches an entry in the current set of access rights.* [19]

FDP_ACF1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *None*[20]

FDP_ACF1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *None*. [21]

Memory Access Control Policy

---

[15] [assignment: access control SFP]

[16] [assignment: list of subjects and objects]

[17] [assignment: access control SFP]

[18] [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].

[19] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].

[20] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

[21] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

The TSF must control read, write, execute accesses of software to data, based on the software mode and on the security attributes.

The software mode is operating mode of the TOE. It consists of privileged mode and unprivileged mode.

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the *Memory Access Control Policy*[22] to provide *minimally protective(*)*[23][24] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow *none*[25] to specify alternative initial values to override the default values when an object or information is created.

(*) The actual values are shown in T6ND7 Data Sheet referred in Table 1-1.

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control or FMT_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management Functions

FMT_MSA.1.1 The TSF shall enforce the *Memory Access Control Policy*[26] to restrict the ability to *modify*, [27] the security attributes *memory region and current set of access rights*[28] to *software running in privileged mode*.[29]

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:

---

[22] [assignment: access control SFP, information flow control SFP]

[23] [selection, choose one of: restrictive, permissive, [assignment: other property]]

[24] [assignment: other property]

[25] [assignment: the authorised identified roles]

[26] [assignment: access control SFP(s), information flow control SFP(s)]

[27] [selection: change_default, query, modify, delete, [assignment: other operations]]

[28] [assignment: list of security attributes]

[29] [assignment: the authorised identified roles]

modification of the memory region and the current set of access rights.[30]

5.2.4. SFRs regarding Boot loader

FDP_ITC.1 [Loader] Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 [Loader] Subset access control

FMT_MSA.3 [Loader] Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the *Loading Access Control Policy*[31] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the User data when imported from outside of the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside of the TOE:
・The TSF shall be able to check the integrity of the loaded user data,
・The TSF shall decrypt the loaded user data internally, then stored into the Flash memory. [32]

FDP_ACC.1 [Loader] Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 [Loader] Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the *Loading Access Control Policy*[33] on *loading user data (including code) to the Flash memory via boot loader*[34]

Loading Access Control Policy

The TSF grants to import user data if user authentication has been successfully completed. The user data is imported without any security attributes and is not associated any security attributes after importing.

FMT_SMF.1 [Loader] Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF will be able to perform the following management functions: below list[35].

- load the Security IC Embedded Software to FLASH memory

[30] [assignment: list of management functions to be provided by the TSF].

[31] [assignment: access control SFP(s) and/or information flow control SFP(s)]

[32] [assignment: additional importation control rules]

[33] [assignment: access control SFP]

[34] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP].

[35] [assignment: list of management functions to be provided by the TSF]

- disable the boot loader

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow *below commands*[36] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

- Read chip ID
- Internal Authentication
- Get Challenge
- External Authentication
- Set Challenge
- Get Internal State

Application Note : This SFR assumes only one user, the composite product manufacturer.

Application Note 2: The authentication is carried out based on individual TOE specific authentication key during mutual authentication.

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to disable[37] the functions boot loader[38] to the composite product manufacturer[39].

Application Note : This SFR assumes only one user, the composite product manufacturer.

5.3. Security Assurance Requirements (SAR)

The Security Target will be evaluated according to

Security Target evaluation (Class ASE)

---

[36] [assignment: list of TSF mediated actions]

[37] [selection: determine the behaviour of, disable, enable, modify the behaviour of]

[38] [assignment: list of functions]

[39] [assignment: the authorised identified roles]

The Security Assurance Requirements for the TOE for the evaluation of the TOE are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following components:

ALC_DVS.2, and AVA_VAN.5.

The assurance requirements are:

- Class ADV: Development
  - Architectural design (ADV_ARC.1)
  - Functional specification (ADV_FSP.4)
  - Implementation representation (ADV_IMP.1)
  - TOE design (ADV_TDS.3)
- Class AGD: Guidance documents
  - Operational user guidance (AGD_OPE.1)
  - Preparative user guidance (AGD_PRE.1)
- Class ALC: Life-cycle support
  - CM capabilities (ALC_CMC.4)
  - CM scope (ALC_CMS.4)
  - Delivery (ALC_DEL.1)
  - Development security (ALC_DVS.2)
  - Life-cycle definition (ALC_LCD.1)
  - Tools and techniques (ALC_TAT.1)
- Class ASE: Security Target evaluation
  - Conformance claims (ASE_CCL.1)
  - Extended components definition (ASE_ECD.1)
  - ST introduction (ASE_INT.1)
  - Security objectives (ASE_OBJ.2)
  - Derived security requirements (ASE_REQ.2)
  - Security problem definition (ASE_SPD.1)
  - TOE summary specification (ASE_TSS.1)
- Class ATE: Tests
  - Coverage (ATE_COV.2)
  - Depth (ATE_DPT.1)
  - Functional tests (ATE_FUN.1)
  - Independent testing (ATE_IND.2)
- Class AVA: Vulnerability assessment
  - Vulnerability analysis (AVA_VAN.5)

5.4. Security requirements rationale

5.4.1. Security Functional Requirements (SFR)

Table 5-2, Tracing between SFRs and objectives for the TOE.

Security Objectives for the TOE	TOE Security Functional Requirements	Fulfilment of dependencies
O.Leak-Inherent	FDP_ITT.1 FPT_ITT.1 FDP_IFC.1	See [5]
O.Phys-Probing	FPT_PHP.3	See [5]
O.Malfunction	FRU_FLT.2 FPT_FLS.1	See [5]
O.Phys-Manipulation	FPT_PHP.3	See [5]
O.Leak-Forced	FDP_ITT.1 FDP_IFC.1 FPT_ITT.1 FRU_FLT.2 FPT_FLS.1 FPT_PHP.3	See [5]
O.Abuse-Func	FMT_LIM.1 FMT_LIM.2 FDP_ITT.1 FDP_IFC.1 FPT_ITT.1 FRU_FLT.2 FPT_FLS.1 FPT_PHP.3	See [5]
O.Identification	FAU_SAS.1	See [5]
O.RND	FCS_RNG.1 FCS_RNG.1 [DRNG] FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1	See [5]
O.HW_DES	FCS_COP.1 [TDES]	See below and [7]
OE.Process-Sec-IC		

OE.Plat-Appl		
OE.Resp-Appl		
O.Mem-Access	FDP_ACC.2 FDP_ACF.1 FMT_MSA.3 FMT_MSA.1 FMT_SMF.1	See [7] and below
O.Boot-Loader	FDP_ITC.1 [Loader] FDP_ACC.1 [Loader] FMT_SMF.1 [Loader] FIA_UAU.1 FMT_MOF.1	See below

The justification related to the security objective “TDES Functionality (O.HW_TDES)” is as follows:

The SFR define the DES standard implemented with its specific characteristics regarding bit size.

The justification related to the security objective “Area based Memory Access Control (O.Mem-Access)” is as follows:

The security functional requirement “Subset access control (FDP_ACC.2)” with the related Security Function Policy (SFP) “Memory Access Control Policy” exactly require to implement an area based memory access control as demanded by O.Mem-Access. Therefore, FDP_ACC.2 with its SFP is suitable to meet the security objective.

The security functional requirement “Static attribute initialisation (FMT_MSA.3)” requires that the TOE provides default values for security attributes. These default values can be overwritten by any subject (software) provided that the necessary access is allowed what is further detailed in the security functional requirement “Management of security attributes (FMT_MSA.1)”: The ability to update the security attributes is restricted to privileged subject(s). These management functions ensure that the required access control can be realised using the functions provided by the TOE.

The justification related to the security objective “Controlled loading of the Security IC Embedded Software (O.Boot-Loader)” is as follows:

The security functional requirements "Import of user data without security attributes (FDP_ITC.1) [Loader]" and "Subset access control (FDP_ACC.1) [Loader]", with the related Security Function Policy (SFP) “Loading Access Control Policy” exactly require to implement a controlled loading of the Security IC Embedded Software as demanded by O.Boot-Loader. Therefore, FDP_ITC.1 [Loader] and FDP_ACC.1 [Loader] with their SFP are suitable to meet the security objective.

The security functional requirement "Specification of management functions (FMT_SMF.1) [Loader]" provides additional controlled facility for adapting the loader behaviour to the user’s needs. These management functions ensure that the required access control, associated to the loading feature, can be realised using the functions provided by the TOE. These management functions are also protected by user authentication mechanism based on customer specific password. FIA_UAU.1 and FMT_MOF.1 provide the protection mechanism.

5.4.2. Dependencies of the SFRs

In the following table the satisfaction of the dependencies is indicated.

Table 5-3, Dependencies of SFRs.

SFR	Dependencies	Fulfilment of dependencies
FRU_FLT.2	FPT_FLS.1	Covered by [5]
FPT_FLS.1	none	-
FMT_LIM.1	FMT_LIM.2	Covered by [5]
FMT_LIM.2	FMT_LIM.1	Covered by [5]
FAU_SAS.1	none	-
FPT_PHP.3	none	-
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Covered by [5]
FDP_IFC.1	FDP_IFF.1	Covered by [5]
FDP_ACC.2	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes. FDP_ACC.2 Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes See below
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes. FDP_ACC.2 See below Yes
FMT_SMF.1	none	-
FPT_ITT.1	none	-
FCS_RNG.1	none	-
FCS_RNG.1 [DRNG]	none	
FCS_COP.1 [TDES]	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	The security IC embedded software using this TOE is responsible to cover this. This is arranged by OE.Plat-Appl and OE.Resp-Appl. Instructions of T6ND7 User Guidance manual, User guidance overview have to be followed by the security IC embedded software developer to realise this SFR. The security IC embedded software using this TOE is responsible to cover this. This is arranged by OE.Plat-Appl and OE.Resp-Appl. Instructions of T6ND7 User Guidance manual, User guidance overview have to be followed by the security IC embedded software developer to realise this SFR.

FDP_ITC.1[Loader]	[FDP_ACC.1 [Loader]	Yes
	FMT_MSA.3 [Loader]	Because the TSF does not associate any security attribute according to *Loading Access Control Policy*, static attribute initialisation is not necessary.
FDP_ACC.1 [Loader]	FDP_ACF.1 [Loader]	Because the *Loading Access Control Policy* depends only user authentication (i.e. FIA_UAU.1) and does not use any security attributes, security attribute based access control is not necessary.
FMT_SMF.1 [Loader]	none	-
FIA_UAU.1	FIA_UID.1	Because the SFR assumes only one user, user identification is not necessary.
FMT_MOF.1	FMT_SMR.1	Because the SFR assumes only one user, user role is not necessary.
	FMT_SMF.1 [Loader]	Yes

The dependency FMT_SMR.1 introduced by the two components FMT_MSA.1 and FMT_MSA.3 is considered to be satisfied because the access control specified for the intended TOE is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of a security functional requirement FMT_SMR.1.

In this particular ST, the specification of FMT_SMF.1 is useless. There is no specific function for the management of the memory access rights, it is just part of the Management of the security attributes.

5.4.3. Security Assurance Requirements (SAR)

The SARs as defined in section 5.3 are in line with the SARs in the Security IC Platform Protection Profile. The context of this ST is equivalent to the context described in the Protection Profile and therefore these SARs are also applicable for this ST.

6. TOE summary specification

This chapter presents the TOE summary specification to gain a general understanding of how the TOE is implemented. The TOE summary specification describes how the TOE meets each SFR.

The TOE implements security functionality, which is also active just before the Phase 3 to Phase 4 and remains active thereafter as defined in Security IC Platform Protection Profile [5].

In the next paragraphs the grouping of the security requirements of the Security IC Platform Protection Profile is used.

6.1. Malfunction

Malfunctioning relates to the security requirements FRU_FLT.2 and FPT_FLS.1. The TOE meets these SFRs by a group of security measures that guarantee correct operation of the TOE.

The TOE ensures its correct operation and prevents any malfunction while the security IC embedded software is executed and utilises standard functions offered by the micro-controller (standard CPU instruction set including usage of standard peripherals such as memories, registers, I/O interfaces, timers etc.) and of all other Specific Security Functionality.

6.2. Leakage

Leakages relate to the security requirements FDP_ITT.1, FDP_IFC.1 and FPT_ITT.1. The TOE meets these SFRs by implementing several measures that provides logical protection against leakage.

The TOE implements measures to limit or eliminate the information that might be contained in the shape and amplitude of signals or in the time between events found by measuring such signals. This comprises the power consumption, electric magnetic emanation (=EMA) and signals on the other pads that are not intended by the terminal or the security IC embedded software. The TOE is implemented in small space by advanced CMOS process to protect as EMA measure.

Thereby this security function prevents the disclosure of User Data or TSF data stored and/or processed in the IC through the measurement of the power consumption and subsequent complex signal processing. The protection of the TOE comprises different features within the design that support the other security functions.

6.3. Physical manipulation and probing

Physical manipulation and probing relates to the security requirement FPT_PHP.3. The TOE meets this SFR by implementing security measures that provides physical protection against physical

probing and manipulation.

The security measures protect the TOE against manipulation of

(i) the hardware,

(ii) the security IC embedded software in the ROM and the NOR-flash memory,

(iii) the application data in the NOR-flash memory and RAM including the configuration data.

It also protects User Data or TSF data against disclosure by physical probing when stored or while being processed by the TOE.

6.4. Abuse of functionality and Identification

Abuse of functionality and Identification relates to the security requirements FMT_LIM.1, FMT_LIM.2 and FAU_SAS.1. The TOE meets these SFRs implementation of a complicated test mode control mechanism that prevents abuse of test functionality delivered as part of the TOE.

6.5. Random numbers

Random numbers relate to the security requirement FCS_RNG.1 and FCS_RNG.1 [DRNG]. The TOE meets this SFR by providing a random number generator.

The whole construction is implemented entirely in the hardware component and operates within the limits guaranteed by the implementation of measures to meet the security requirements FRU_FLT.2 and FPT_FLS.1.

The random number generator fulfils the requirements of functionality class K3 of [6].

6.6. TDES

The TOE provides the hardware DES processor for the Triple Data Encryption Standard (Triple-DES) algorithm according to the Data Encryption Standard to meet the security requirement FCS_COP.1 [TDES]. The TOE implements a modular basic cryptographic function, which provides the Triple-DES algorithm as defined by FIPS PUB 46-3 by means of a hardware co-processor. It supports the Triple-DES algorithm with three 56bit keys (168 bit) for the 3-key or 2-key Triple DES supporting ECB mode. The keys for the Triple-DES algorithm shall be provided by the security IC embedded software.

FIPS PUB 46-3

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

DATA ENCRYPTION STANDARD (DES)

Reaffirmed 1999 October 25

6.7. Memory Access control

Memory Access control relate to the security requirement FDP_ACC.2, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1 and FMT_SMF.1. The TOE meets this SFR by providing a Memory protection unit (MPU).

The TOE has memory protection unit in order to ensure the correct operation and separates applications or data in all kinds of memories processed by embedded software.

The TOE has the Protected Memory System Architecture in CPU.

If address besides the setting range is accessed, memory protection unit detects it. TOE reacts like reset itself.

6.8. Boot Loader

Boot Loader relate to the security requirement FDP_ITC.1 [Loader], FDP_ACC.1 [Loader], FMT_SMF.1 [Loader] , FIA_UAU.1 and FMT_MOF.1. The TOE meets this SFR by providing a Boot loader.

The TOE has Boot Loader software in order to download user code to Flash memory.

7. Reference

No	Title	Date	Version	publisher	Document number
[1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model	September 2012	3.1 Revision 4		CCMB-2012-09-001
[2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components	September 2012	3.1 Revision 4		CCMB-2012-09-002
[3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components	September 2012	3.1 Revision 4		CCMB-2012-09-003
[4]	Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology	September 2012	3.1 Revision 4		CCMB-2012-09-004
[5]	Security IC Platform Protection Profile	15.06.2007	1.0	Bundesamt für Sicherheit in der Informationstechnik (BSI)	BSI-PP-0035
[6]	Application Notes and Interpretation of the Scheme (AIS), AIS 20: Functionality classes and evaluation methodology for deterministic random number generators	2 December 1999	1		AIS 20
[7]	Smartcard Integrated Circuit Platform Augmentations	March 8, 2002	1.00		AUG
[8]	Application of Attack Potential to Smartcards	January 2013	Version 2.9		

** End of Document **