T6ND4 Integrated Circuit

Security Target

30 Nov. 2010

Version 0.01

TOSHIBA CORPORATION

Analog Device Design Department
System LSI Division

Change History

No	Version	Date	Chapter	Content	Name
1	0.01	30/Nov/2010		ST Lite	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: T6ND4 Integrated Circuit Security Target, version 0.01, 30 Nov 2010
ST Status: evaluation.
TOE reference: T6ND4 Integrated Circuit

1.2. TOE overview

The T6ND4 Integrated Circuit (Target of Evaluation – TOE) is an Integrated Circuit (41 pin BGA package) with a DES accelerator. The TOE that is described in this ST is a single chip microcontroller (hardware, security IC dedicated software to initialise a number of settings for sensor levels and countermeasures at start-up 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 electric purse. The TOE has three different communication interfaces:

1. an interface, a wireless interface that receives modulation data from the IC for communication
2. a mobile host interface, a wired serial interface that communicates with the host controller of the mobile equipment
3. a RFChip interface, a local serial bus that monitors the IC for communication

.The objective of the TOE is to protect the IT security of the IC and embedded software that is intended to be used as an electronic purse (people can pay with the TOE embedded in mobile equipment).

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. The security IC embedded software is developed by the composite product manufacturer. This software is sent to Toshiba. Toshiba develops the IC dedicated test software. Toshiba merges the security IC embedded software and the IC dedicated test software and implemented in T6ND4. After testing in Toshiba,the test software is made unavailable.
and the TOE becomes inaccessible when it is delivered to the composite product manufacturer or . used by the end-user.

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, NV memory), and circuit for the three 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.

Other security features of the TOE are:

- Bus and memory encryption
- Clock filter
- Detection of abnormal power supply voltage, detection of abnormal Temperature, detection of abnormal Input clock frequency, Power supply glitch, Metal cover removal, detection of Light.
- Duplicated signals
- EEPROM error correction
- Memory firewall
- Shield cover

- Random number generator
- Timing and power noise generation
- Undefined CPU instruction monitoring
- Undefined address access monitoring
- Memory address scrambling
- Bus and memory parity checking
- DES accelerator
- Complicated test mode control

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) are stored in the EEPROM. By wireless communication, the data that I-chip receives is communicated to T6ND4. T6ND4 manages the data securely, and returns the processed result through I-chip to the Reader/writer (R/W).
There is a package derivative of 64 pin BGA called T6ND5. The same chip is included with RF chip in 64 pin BGA package.

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, antennae,...) 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	T6ND4	5.0	Package T6ND4: 41 PIN BGA package Package T6ND5: 64 PIN BGA package	The T6ND4 TOE is delivered in two different plastic packages. A 41 PIN BGA package named T6ND4, and a 64 PIN BGA package named T6ND5.
Sftoware	Hardware configuration (CODE)	0.97	Library file (hwcfg.s)	

			MD5 value = 9dac6158b77f378ebfd 5b31927d28a6d	
	Hardware configuration (Data)	0.97	EEPROM in delivered T6ND4 hardware	
	TEST ROM software	0.02	ROM of hardware (test area)	
Manuals	T6ND4 User guidance overview	0.18	Electronic document	
	T6ND4 Customer specification	1.00	Electronic document	
	T6ND4 User Guidance manual	0.94	Electronic document	User Guidance Manual describes about Register setting securely.
	T6ND4 HW Configuration	0.97	Electrical document	

The software (i.e. Hardware configuration and TEST ROM software) is part of the TOE, because it exists in the IC memory after TOE Delivery to a composite product manufacturer[1]. The hardware configuration software 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 configuration of the T6ND4 is defined by the hardware configuration settings. For secure operation the security IC embedded software must use the mandated settings. These settings are defined in the T6ND4 User Specification.

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 software together with security IC embedded software in the ROM from the composite product manufacturer.

The TOE in its environment is depicted in Figure 2-1. The T6ND4 TOE is an LSI which has been designed to realize card functionality in combination with an RF LSI chip (I-chip) for an electronic purse function (e–payment. This is an example) in mobile phone. In such a function there can be a user OS in the ROM and service data in the EEPROM. For example, a commuter ticket, electronic money or data (money information, user information etc) are stored in the EEPROM. By wireless communication, the data that I-chip receives is communicated to the TOE. The TOE manages the data securely, and returns the processed result through I-chip to the Reader/writer (R/W).

[1] In terms of the protection profile the TOE is delivered at the end of Phase 3 IC Manufacturing.

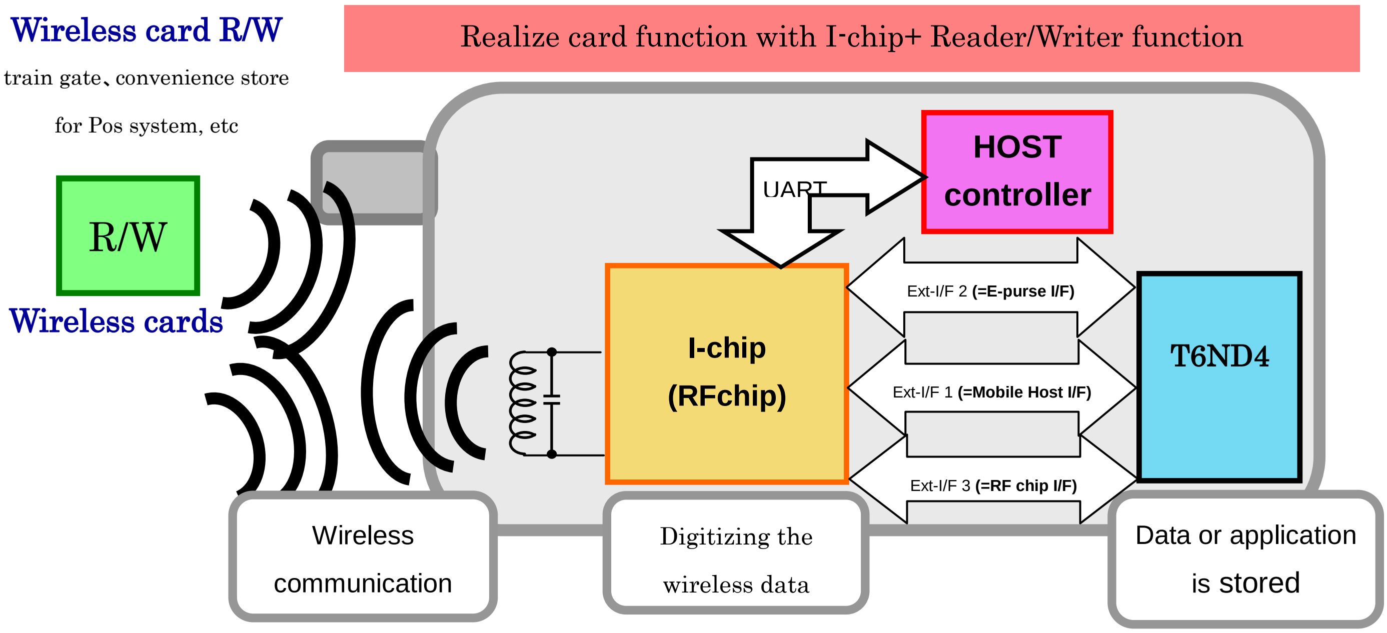
Wireless card R/W
train gate、convenience store
for Pos system, etc
R/W
Wireless cards
Realize card function with I-chip+ Reader/Writer function
HOST controller
UART
I-chip (RFchip)
Ext-I/F 2 (=E-purse I/F)
Ext-I/F 1 (=Mobile Host I/F)
Ext-I/F 3 (=RF chip I/F)
T6ND4
Wireless communication
Digitizing the wireless data
Data or application is stored

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 (MFW, MEMC, EXT－I/F 1, EXT－I/F 2, EXT－I/F 3, Control Logic), the various memory elements (EEP, ROM, RAM), security function circuit (CRC, RNG, Triple-DES), various types of detection circuits (SECURITY DETECTORS), and others (TEST CIRCUIT, etc.).

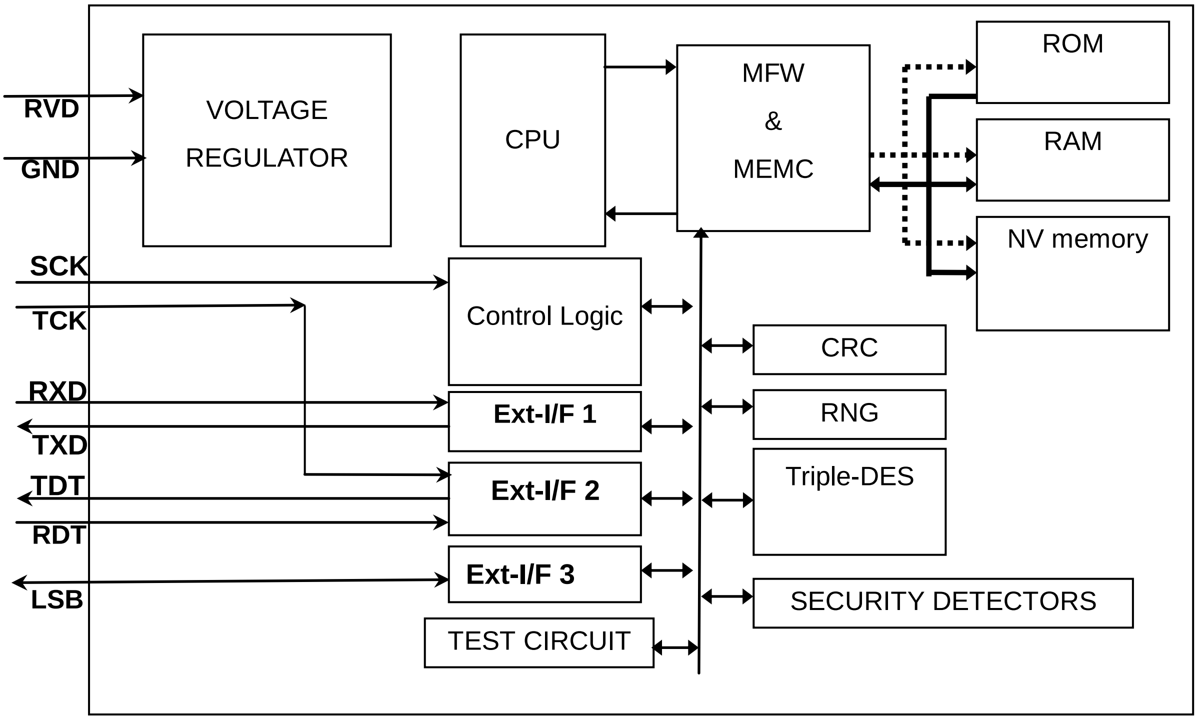

Figure 2-2 Basic Configuration Elements of the Hardware

The following components are used.

-	CPU	ARM SC100
-	MFW	Memory Fire Wall
-	MEMC	Memory Cipher Circuit
-	RAM, ROM,NV mem.	transmitting or receiving buffer RAM, (test rom included) ROM, EEPROM
-	Control Logic	
-	Triple-DES	
-	CRC	CRC-CCITT (16 bit CRC)
-	RNG	Random number generator
-	VOLTAGE REGULATOR	
-	SECURITY DETECTOR	
-	TEST CIRCUIT	

- EXT－I/F 2(=Local NRz Receive /Transmit. E-purse I/F) (Through the external interfaces RDT/TDT and TCK)
- EXT－I/F 1(=Local UART.) (Through the external interfaces RXD/TXD)
- EXT－I/F 3(=Local SERial Bus. RFChip I/F) (through the external interface LSB)

TCK,TDT,RDT,TXD,RXD,SCK and LSB are connected to I-Chip and not connected to HOST controller directly. (LSB belongs to the RF chip I/F and TDT,RDT,TCK belong to E-purse interface in Figure 2-1. TXD and RXD are connected HOST controller via I-Chip. SCK is the external clock terminal.)

RVD and GND are power supply terminal and ground terminal respectively and can be connected to RF chip power supply terminal and ground line respectively.

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
    c. CBC mode, initial value: arbitrary, Triple DES 2KEY,Encryption/Decryption
    d. CBC mode, initial value: arbitrary, Triple DES 3KEY,Encryption/Decryption

2. Physically seeded random number generator:

    A physical noise source provides seeding for a deterministic random number generator built from recursive calls to Triple DES, conformant to AIS20 Class K3. The seeding must be performed before use. random number seeding is activated by hardware configuration(not at reset).If seed once set, seed can not be changed until the next reset. The quality of the noise source is monitored during this seeding process for total failure of the noise source. The whole construction (physical noise source, total failure tests, Triple DES in recursive mode) is completely implemented in hardware, and the actual entropy is provided by physical random processes.

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 3" d.d. July 2009.

- 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 3" d.d. July 2009.

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 [7].

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.

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 3.3 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.RNG	Deficiency of Random Numbers

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 following the Organisational Security Policy considers the Application Note 12 of the Security IC Platform Protection Profile [5] related to the specialised functions of the TOE.

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:

- Data Encryption Standard (DES),

The following Organisational Security Policy considers the Application Note 8 of the Security IC Platform Protection Profile [5] related to the specialised encryption hardware of the TOE. The developer of the security IC embedded software must ensure the appropriate "Usage of Key dependent Functions (P.Key-Function)" while developing this software in Phase 1 IC embedded software developer (see Security IC Platform Protection Profile [5]) as specified below.

P.Key-Function — Usage of Key-dependent Functions

Key-dependent functions (if any) shall be implemented in the security IC embedded software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced).

Note that here the routines which may compromise keys when being executed are part of the security IC embedded software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE and (ii) the processing of User Data including cryptographic keys.

3.4. Assumptions

Since this Security Target claims conformance to the Security IC Platform Protection Profile [5], the assumptions defined in section 3.2 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

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.RNG	Random Numbers

Regarding Application Notes 13 and 14 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_DES DES Functionality

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

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 PP
T.Phys-Probing	O.Phys-Probing	See PP
T.Malfunction	O.Malfunction	See PP
T.Leak-Inherent	O.Leak-Inherent	See PP
T.Leak-Forced	O.Leak-Forced	See PP
T.Abuse-Func	O.Abuse-Func	See PP
T.RNG	O.RNG	See PP
P.Process-TOE	O.Identification	See PP
P.Add-Functions	O.HW_DES	See below
P.Key-Functions	OE.Plat-Appl	See PP
A.Process-Sec-IC	OE.Process-Sec-IC	See PP
A.Plat-Appl	OE.Plat-Appl	See PP
A.Resp-Appl	OE.Resp-Appl	See PP

The justification related to the organisational security policy “Protection during TOE Development and Production (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

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*[2] with the capability to store *the Initialisation Data and/or Pre-personalisation Data in the EEPROM and/or supplements of the security IC embedded software*[3] in the *ROM*[4].

Dependencies: No dependencies.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

FCS_RNG.1.1 The TSF shall provide a physical 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 Class K3 of [6][6].

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

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

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

[5] [assignment: *list of 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] [assignment: *a defined quality metric*] – refined in the PP as [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]]*. The TOE uses the physical random processes for its entropy and post-processes this with a Triple DES deterministic random number generator for additional security. AIS20 describes this construction exactly, therefore AIS20 is chosen as quality metric and evaluation methodology.

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 [DES] Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 [DES] The TSF shall perform *encryption and decryption*[7] in accordance with a specified cryptographic algorithm *Triple Data Encryption Standard (3DES – supporting both ECB and CBC mode)*[8] and cryptographic key sizes of *112 bit and 168 bit keys*[9] that meet the following standards[10]:

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

5.3. Security Assurance Requirements (SAR)

[7] [assignment: list of crypto-graphic operations]

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

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

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

The Security Target will be evaluated according to

Security Target evaluation (Class ASE)

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 ATE: Tests
  Coverage (ATE_COV.2)
  Depth (ATE_DPT.2)
  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	Dependencies	Fulfillment of dependencies
O.Leak-Inherent	FDP_ITT.1 FDP_IFC.1 FPT_ITT.1	See PP
O.Phys-Probing	FPT_PHP.3	See PP
O.Malfunction	FRU_FLT.2 FPT_FLS.1	See PP
O.Phys-Manipulation	FPT_PHP.3	See PP
O.Leak-Forced	FDP_ITT.1 FDP_IFC.1 FPT_ITT.1 FRU_FLT.2 FPT_FLS.1 FPT_PHP.3	See PP
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 PP
O.Identification	FAU_SAS.1	See PP
O.RNG	FCS_RNG.1 FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1	See PP
O.HW_DES	FCS_COP.1 [DES]	See below.
OE.Process-Sec-IC		
OE.Plat-Appl		
OE.Resp-Appl		

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

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

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	Fulfillment of dependencies
FRU_FLT.2	FPT_FLS.1	Covered by PP
FPT_FLS.1	none	-
FMT_LIM.1	FMT_LIM.2	Covered by PP
FMT_LIM.2	FMT_LIM.1	Covered by PP
FAU_SAS.1	none	-
FPT_PHP.3	none	-
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1 covered by PP
FDP_IFC.1	FDP_IFF.1	The PP states in the Data Processing Policy (referred to in FDP_IFC.1) that there are no attributes necessary and therefore this dependency is met.
FPT_ITT.1	none	-
FCS_RNG.1	none	-
FCS_COP.1 [DES]	FDP_ITC.1 or FCS_CKM.1	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 T6ND4 User Guidance manual, User guidance overview have to be followed by the security IC embedded software developer to realise this SFR.
	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 T6ND4 User Guidance manual , User guidance overview have to be followed by the security IC embedded software developer to realise this SFR.
	FMT_MSA.2	The PP states in the Data Processing Policy (referred to in

		FDP_IFC.1) that there are no attributes necessary and therefore this dependency is met. T6ND4 User Guidance manual describes not weak key coming from DES and User guidance overview describes about the treat ment of user data.

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.

This is achieved through an appropriate design of the TOE and the implementation of filters, sensors/detectors and integrity monitoring components. The filter eliminates high-frequency pulse (more than 10.5MHz. 10.5MHz is an adjusted value by trimming. 15.3MHz is the value before the trimming) in order to ensure the correct operation of the TOE. The sensors/detectors measure the supplied voltage, frequency, temperature, exposure to light, and glitch signals in supplied voltage. In addition, the target address range, the accessible segments of each memory and the operation of CPU are monitored. Furthermore, is a mechanism implemented that detects the removing the shield cover. In case that any malfunction occurred or may likely occur, operation is stopped. The integrity monitoring components involves Error Correct Circuit (ECC) for ensuring EEPROM data integrity, parity check for data transfer and parity checks for the different memories.

“stopped”
If one of the monitored parameters is out of the specified range, operation is stopped. ”stopped” means that reset signal is impressed to CPU, nop instruction is executed and I/O disabled. If Operation is “stopped”, all components of the TOE are initialised with their reset values.

“ECC”

If 2 bit or more bit errors of ECC for EEPROM are occurred, an exception is raised which interrupts the program flow and allows a reaction of the security IC embedded software. In the case of an exception raised, the security IC embedded software can select one of several operations. In case of 1 bit errors the memory content is automatically corrected by the ECC. In RF system, there is a possibility that the power is off. So ECC is sometimes not correct if the power is off during data writing. The program in EEPROM has only interrupt mechanism as there is a runaway and can not read ECC abnormal flag. For the data reading, software checking is more convenient than interupt processing so flag is prepared. The flag is checked by the embedded IC software.

“accessible segments of each memory”

This security mechanism restricts the ability of security IC embedded software to access segmented memory areas by implementing a memory firewall. The decision whether the access operation is granted or denied is based upon the address. The ability to define the access rights and memory segmentation is permitted to user by setting data on specific registers.

6.2. Leakage

Leakages relates 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.

The TOE implements additional features introducing timing noise and amplitude power noise. These features are partly configurable by the embedded software developer. Timing noise is effective not only for SPA/DPA but also EMA analysis.

For more information about the settings preventing SPA/DPA etc is referred to User guidance manual for software developers.

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 EEPROM,

(iii) the application data in the EEPROM 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.

The protection of the TOE comprises different features within the design and construction, which make reverse-engineering and tamper attacks more difficult. These features comprise dedicated shielding techniques for different components, specific encryption features for the memory blocks and scrambling the transport between the different blocks in 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.

The test functionality is not available to the user after Phase 3 IC Manufacturing as defined in Security IC Platform Protection Profile [5]. The TOE has complicated access control mechanisms in place to prevent using this functionality.

6.5. Random numbers

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

The random number generator contains a physical noise source, total failure tests on this noise source and a Triple-DES deterministic random number generator post-processing construction seeded by the physical noise source output. Thus the random number generator produces the random number by a noise source based on physical random processes. Seeding must be performed after each power-on at a minimum. This seed generation is done once by Hardware Config after power is supplied.The total failure tests are automatically performed on the seeding data. 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. DES

The TOE provides the Triple Data Encryption Standard (Triple-DES) algorithm according to the Data Encryption Standard to meet the security requirement FCS_COP.1[DES]. 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 both CBC and 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

Furthermore, the DES hardware co-processor implements a number of countermeasures that prevent side-channel leakage and malfunctioning.

7. Reference

No	Title	Date	Version	publisher	Document number
[1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model	July 2009	3.1 Revision 3		
[2]	Common Criteria for	July 2009	3.1		

	Information Technology Security Evaluation, Part 2: Security Functional Requirements		Revision 3		
[3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements	July 2009	3.1 Revision 3		
[4]	Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology	July 2009	3.1 Revision 3		
[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		
[7]	Supporting Document, Mandatory Technical Document: Application of Attack Potential to Smartcards	March 2009	2.7Revision 1		CCDB-2009-03-001

※ End of Document※※