TOSHIBA

T6ND1 series Integrated Circuit with Crypto Library Security Target

Version 2.16

28 December 2010

developed by

TOSHIBA CORPORATION

Change History

No	Version	Date	chapter	Content	name
1	0.3	23 July 08	All	First draft for CC	ECSEC
2	1.0	5 Aug. 2008		By BS meeting	Hironaka
3	1.1	14 Aug. 2008	All	Modifications after receiving version for review	Bakker
4	1.2	20.Aug.2008	All	Adopt BS Precheck Commercial name explanation added.Table1-1 ,Fig2 minor change	Hasebe
5	1.3	25 Aug. 2008	1.4.2	Revised explanation for different form factors	Bekkers
6	1.4	25.Aug.2008	All	For evaluation	Hasebe
7	1.5	6.Jan.2009	See right	Revision from 1st Round evaluation Chapter 1.1 Title revised. Chapter 1.4.2 Table 1-1 revised. Chapter 1.4.3 Fig2 and description Revised. Chapter 1.4.4 Logical scope description revised. Chapter 2.1,8.1 CC conformance revision number revised. Chapter 7 FRU_FLT.2 ,FPT_FLS.1, FCS_RNG.1 revised. For 2nd Round evaluation	Hasebe
8	1.51	17.Feb.2009		Chapter 6.1 RSA, DH description changed	Hasebe
9	1.52	6.Apr.2009		TOE table version adjusted	Hasebe
10	1.53	27.May.2009		TOE table adjusted.AGD,SSG version	Hasebe
11	2.00	30 July 2009		Add crypto extension algorithms SFRs (and matching security objectives, etc.) to the ST	Blonk
12	2.01	12 Aug 2009		Revised TOE identification	Izumisawa
13	2.02	31 Aug 2009		For CC evaluation	Hasebe
14	2.03	2 Sep 2009		For CC evaluation	Hasebe
15	2.04	2 Sep 2009	Chap7	FPT_FLS.1 revised. For CC evaluation	Hasebe

16	2.05	2 Sep 2009	Chap1.4.2	TOE Table revised	Hasebe
17	2.06	17 Sep 2009	Chap 6 and 7	Small correction	Izumisawa
18	2.07	18 Sep 2009	Chap 1.1	Correction of version and data	Izumisawa
19	2.08	16 December 2009	Chap 1.3 and 6.1	Refine scope SHA	Tettero
20	2.09	18 December 2009	Chap 1.1	Version , Date changed	Hasebe
21	2.10	29.March. 2010	Chap 1.1	Version ,Date changed	Hasebe
22	2.11	12 April 2010	Chap 7	Add SHA scope refinement	Tettero
23	2.12	22 OCT 2010		TOE #5.0	Izumisawa
24	2.13	30 Nov 2010		TOE #6.0	Hasebe
25	2.14	14 December 2010		SHA224 has been removed as an SFR	J.Blonk
26	2.15	15 December 2010		Update AGD version	Izumisawa
27	2.16	28 December 2010		Coorection of name of CryptoLibrary.lib	Izumisawa

Contents

1 ST Introduction

1.1 ST reference

Title: T6ND1 series Integrated Circuit with Crypto Library Security Target

Version: 2.16

Publication date: 28 Dec 2010

Authors: Wireless System LSI Group 4, Wireless System LSI Marketing & Engineering Department, System LSI Division, TOSHIBA CORPORATION

1.2 TOE reference

TOE: T6ND1 series Integrated Circuit with Crypto Library

Developer: TOSHIBA CORPORATION

Version: #6.0

Commercial Name [JEB]T6ND1

Characters in the parenthesis are chosen properly by the following rule.

J : chip , E: wafer , B: bump pad,.

For example:

JT6ND1 is aluminium pad and chip tray shipment.

JBT6ND1 is bump pad and chip tray shipment.

JET6ND1 is sawn wafer (but each chip is attached on a tape), aluminium pad product. and wafer case shipment

JEBT6ND1 is sawn wafer (but each chip is attached on a tape), bump pad and wafer case shipment

And rom version information etc will be followed to the above mentioned commercial name. In summary,TOE has different form of pad ,delivery and Commercial name.

1.3 TOE overview

The TOE - T6ND1 series Integrated Circuit with Crypto Library is a LSI chip designed for devices such as smartcard equipped with wireless communication interface. The TOE is capable to install user application programs and provides security functionality to protect stored data or executable code in the TOE.

Main components of the TOE are 16bit CPU (TLCS-900/L1), 60kB user ROM, 6kB RAM, 80kB non-volatile memory and co-processor for 2048-bit modular exponential operations. The TOE also has an RF external interface compliant to ISO/IEC 14443 Type B. An external antenna is attached to the TOE for wireless communication.

The TOE will be a platform for “the security IC Embedded software”. The primary purpose of the TOE is to provide safeguard for information stored in the TOE (e.g., personal data, secret number or user program). To protect the information, the TOE involves cryptographic functionality - triple DES, RSA, ECDSA signature

verification, EC-Diffie-Hellman key exchange, Diffie-Hellman, SHA-256/SHA-1. The TOE also prepares the other security components to protect data in the TOE and the TOE itself from physical attacks.

The SHA-1 can be used as a building block, e.g. for session key generation in an e-passport application. However the cryptographic strength of SHA-1 is not considered to be sufficient on level AVA_VAN.5.

Further, it is noted that the TOE does not support the generation of hashes from SHA-256/SHA-1 that are confidential in nature.

1.4 TOE description

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

1.4.1 TOE life cycle

Life cycle of a typical security IC is represented in Fig 1 (excerpted from the PP). The TOE corresponds to a product on “Phase 2 and 3”. The TOE is delivered to a composite product manufacturer after being configured and tested by the TOE manufacturer. Therefore, the user guidance documentation, which is a part of the TOE, is not for end consumers of the TOE but for a composite product manufacturer.

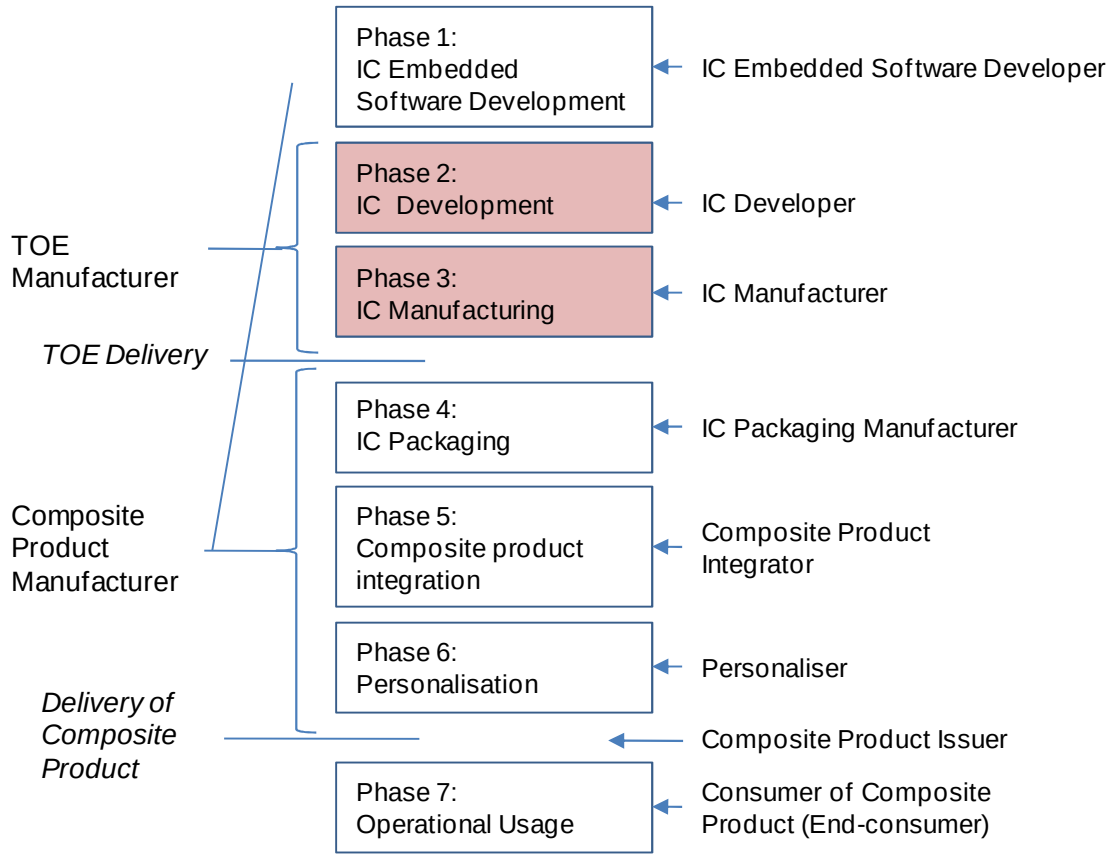

Fig 1: Life cycle of the TOE

1.4.2 Components of the TOE

TOE identification

The TOE comprises components specified below.

Table 1-1 ,TOE components.

TOE				
Delivery item type	**Identifier**	**Version**	**Medium**	**additional information**
Hardware	T6ND1	#5.0	Chip (bump or aluminium pad) / Wafer (bump or aluminium pad)	Aluminium pad samples contains33pF and Bump pad samples contains 0pF tuning Capacitors.
Software	Hardware configuration (CODE)	0.94	Electrical data	T6ND1_HWconfig.lib SHA-256 = d728e6bb93d57daa606c8ae9f391b824118dab2841d046bb2a36363c89c1fee5 Note that the source code is provided in the T6ND1 software security guidance manual.
	Boot ROM	0.93	Electrical data	Boot program is provided as source file from The T6ND1 software security guidance manual
	Hardware configuration (Data)	0.94	EEPROM in delivered T6ND1 hardware	
	Co-Processor control library	1.04	Electrical data	CryptoLibrary.lib. SHA-256 value = a229e515d7578ca268bc791d356c6d20ed7ac8a2ce146f79645422e2bda1474b Crypto_global.h SHA-256 value = 3ae2868ecc3fc8c5fc26e701e3dcaf6d38f83d4bb963348c6a82f03c51d5e0e0 RSA, DH, SHA, DES libraries are included.
	Ecc Library	1.01	Electrical data	EccLibrary.lib SHA-256 value= a492bf2d41710bb99d7a2e4275001d986ba4fe674655a9f22a96545ed0e7442e
	TEST ROM software	1.3	ROM of hardware (test area)	
Manuals	T6ND1 User guidance overview	0.21	Electronic document	
	T6ND1 User Specification	0.962	Electronic document	
	T6ND1 Software Security Guidance	0.953	Electronic document	
	Next-generation IC Sheet Crypt Library Interface Specification	1.0.4	Electronic document	

The only difference between the form factors is the way the chip dies are prepared for further processing. They will be delivered as complete wafer or as single chips, with aluminium pads for bonding or bump pad for flip-

chip assembly. Because the functional and electrical characteristics of the pads and bumps are the same the different form factors are security irrelevant.

Features of the TOE

There are two types of security features for the TOE:

- Safeguarding user data stored in the TOE and protecting the TOE itself from attacks to compromise the security functionality of the TOE. (Physical scope)
- providing security services for the security IC Embedded software running on the TOE (Logical scope)

1.4.3 Physical scope

The first group of security features are functions to protect the TOE itself, as well as data in the TOE, from physical attacks. Those security functions listed below are implemented by hardware circuitry. Fig 2 represents the construction of hardware blocks of the TOE (includes non-security parts and not consistent to the contents of the security function list below by name). The basic configuration elements of the TOE are the CPUT, peripheral circuits (MFW, RFUART, INTC, MEMIF, DMAC, TIMER, CLKGEN, ACTSLD, TRAPL, ANAIF, WDT, ALMC, BUSBRIDGE), various memory elements(EEPROM, ROM, RAM), security function circuits (CRC, RNG, DES, COPRO, SHA) ,various types of detection circuits(ANALOG) and others (TESTC).

Detection for:

- trap latch (light sensor)
- power supply glitch
- clock frequency, out of the range
- internal/rectified supply and current, out of the range
- temperature, out of the range
- signal line error
- illegal access to the memories
- illegal configuration on test mode
- undefined instruction to CPU or co-processor
- access to vacant addresses
- active shield error

Countermeasures for physical probing to the TSF:

- bus scrambling
- memory address scrambling
- memory ciphering
- active shield

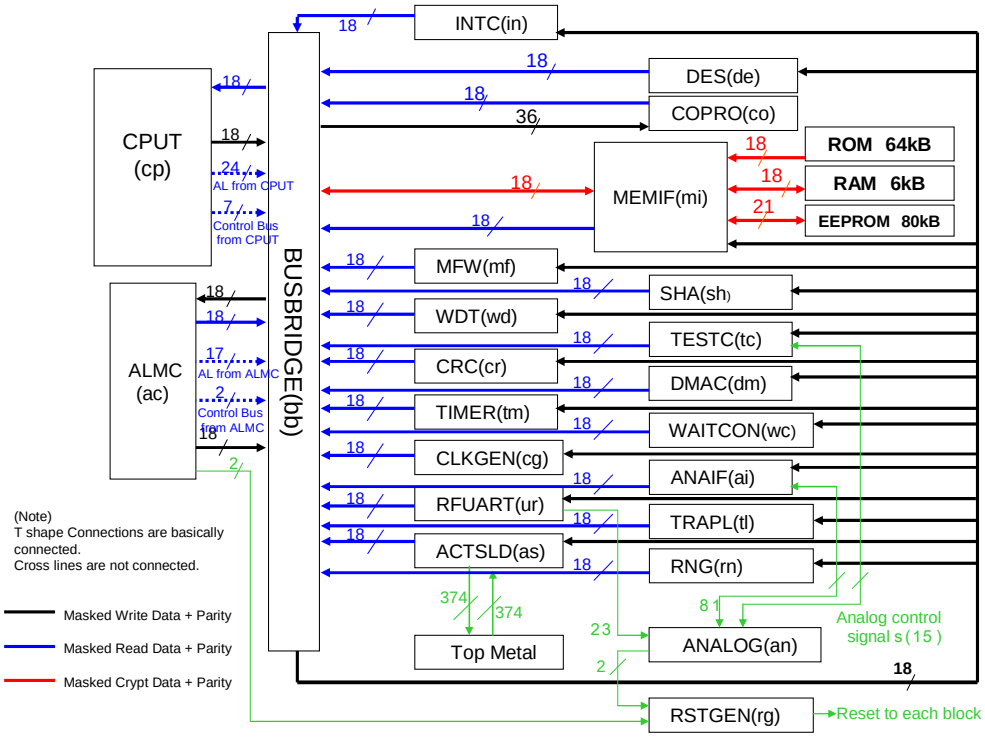

Fig 2: The TOE hardware components

Supplementary information about Fig2

Connection from COPRO to BUSBRIDGE line number has 18 lines.

And the lines to BUSBRIDGE to COPRO are 36 lines.

DMAC controls memories by BUSBRIDGE.

The green 2bit signal between ALMC and RSTGEN are reset signals of ALMC when alarm happens. One of these reset signals is a reset signal for RFUART and COPRO. The other is a reset signal for CPUT.

The green signal between ANALOG and RFUART are 23 lines as input signals to ANALOG.

The green signal between ANALOG and RSTGEN are 2 signals.

The green “Analog control signal” are control signals of 15 lines.

The red 18bit “Crypt data” bus between MEMIF and BUSBRIDGE is the crypt data. That is common for both EEPROM ,RAM and ROM.

The following components are used. Components of TSF subsystem are described as TSF subsystem.

- CPUT: TLCS900-L1 Toshiba original 16bit CPU, TSF subsystem
- MFW: Memory firewall, TSF subsystem
- RAM, ROM, EEPROM: 6kbyte RAM, 64kbyte (User 60kbyte) ROM, 80kbyte non-volatile memory.
- DES: triple des (single des circuit and cyclically used) , TSF subsystem
- COPRO: coprocessor for RSA, Diffie-Hellman, ECDSA signature verification and ECDH key exchange TSF subsystem

- CRC: cyclic redundancy check, TSF subsystem
- RNG: Random number generator. True random number generator, LFSR random number generator, Triple des type random number generator, TSF subsystem
- ANALOG: Analog circuit for RFUART,.shunt regulator, sensors
  See the upper detections for part, TSF subsystem
- TESTC: test circuit, TSF subsystem
- RFUART: RF external interface with compliant to ISO/IEC 14443 type B
- DMAC: DMA controller
- MEMIF: Memory interface , TSF subsystem
- ANAIF: analog interface, TSF subsystem
- INTC: interrupt controller, TSF subsystem
- TIMER: timer
- WDT: watch dog timer
- SHA: secure hash , TSF subsystem
- TRAPL: trap latch , TSF subsystem
- ACTSLD: active shield, TSF subsystem
- CLKGEN: clock generator, TSF subsystem

- ALMC : alarm controller , TSF subsystem
- BUSBRIDGE: bus controller, TSF subsystem
- RSTGEN: reset generator
- WAITCON: random wait controller, TSF subsystem

1.4.4 Logical scope

The second group of the security features are cryptographic functions listed below. They will be invoked by an application program “the security IC Embedded software” installed on the non-volatile memory of the TOE. For cryptographic functions, the TOE provides only cryptographic operational mechanisms. Key management shall be performed by “the security IC Embedded software” (an application program on the TOE).

- Triple DES
- RSA
- Diffie-Hellman
- ECDSA signature verification
- ECDH key exchange
- SHA-256/ SHA-1

Test software is used to test the TOE before delivery but which does not give any functionality there after.

The SHA-1 can be used as a building block, e.g. session key generation in the e-passport. However the cryptographic strength of SHA-1 is not considered to be sufficient on level AVA_VAN.5 and therefor SHA-1 is not part of the evaluated logical scope.

1.4.5 Physical interfaces of the TOE

After phase 4 (IC packaging), the TOE is concealed under a IC package and communicates via the contactless interface (using an external antenna) with external entities.

2 Conformance claims

2.1 CC conformance claim

This ST and the TOE claims to be conformant to the Common Criteria version 3.1 Rev 1[1],Rev2 [2], Rev2[3]
This ST claims to be CC part 2 extended.
The extended components are FCS_RNG.1, FMT_LIM.1, FMT_LIM2, FAU_SAS.1
This ST claims to be CC part 3 conformant

2.2 Package conformance claim

This ST claims to be EAL4 augmented with AVA_VAN.5 and ALC_DVS.2

2.3 PP conformance claim

This ST claims to be conformant to:
Security IC Platform Protection Profile version 1.0 15.06.2007; BSI-PP-0035[4]

2.4 Conformance claim rationale

2.4.1 TOE type

This ST claims to be conformant to a PP. The TOE type in the PP is described such as “The TOE is a security integrated circuit which is composed of a processing unit, security components, I/O ports and volatile and non-volatile memories.” in paragraph 8. The TOE type described in this ST [1.3. TOE overview] covers all contents quoted above. Therefore, the TOE type in the ST is consistent with the TOE type in the PP.

2.4.2 SPD

The PP to which the ST claims conformance requires “strict conformance”.

- The threats in the ST are identical to the threats in the PP.
- The organisational security policies in the ST are superset of the organisational security policies in the PP. An organisational security policy was added.
- The assumptions in the ST are identical to the assumptions in the PP.

2.4.3 Security objectives

The PP to which the ST claims conformance requires strict conformance. The ST contains all security objectives for the TOE and operational environment in the PP. The ST also includes an additional security objective for the TOE related to the additional organisational security policy.

2.4.4 Security requirements

The PP to which the ST claims conformance requires strict conformance. The security functional requirements in the ST are superset of the security functional requirements in the PP. The security assurance requirements in the ST is identical to the security assurance requirements in the PP.

3 Security problem definitions

Most of the security problem definitions here are derived from the PP to which this ST claims conformance. Threats, organisational security policies, assumptions from the PP are reproduced in the ST. An organisational security policy concerning with cryptographic functionality was added.

3.1 Threats

T.Leak-Inherent Inherent Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential User Data as part of the assets.

T.Phys-Probing Physical Probing

An attacker may perform physical probing of the TOE in order (i) to disclose User Data, (ii) to disclose/reconstruct the Security IC Embedded Software or (iii) to disclose other critical information about the operation of the TOE to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software.

T.Malfunction Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of the Security IC Embedded Software by applying environmental stress in order to (i) modify security services of the TOE or (ii) modify functions of the Security IC Embedded Software (iii) deactivate or affect security mechanisms of the TOE to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software. This may be achieved by operating the Security IC outside the normal operating conditions (Electrical stimulation or Energy and Particle Exposure on chip surface, or Electrical stimulation via contactless interface).

T.Phys-Manipulation Physical Manipulation

An attacker may physically modify the Security IC in order to (i) modify User Data, (ii) modify the Security IC Embedded Software, (iii) modify or deactivate security services of the TOE, or (iv) modify security mechanisms of the TOE to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software.

T.Leak-Forced Forced Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential User Data as part of the assets even if the information leakage is not inherent but caused by the attacker.

T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which may not be used after TOE Delivery in order to (i) disclose or manipulate User Data, (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE or (iii) manipulate (explore, bypass, deactivate or change) functions of the Security IC Embedded Software or (iv) enable an attack disclosing or manipulating the User Data or the Security IC Embedded Software.

T.RND Deficiency of Random Numbers

An attacker may predict or obtain information about random numbers generated by the TOE security service for instance because of a lack of entropy of the random numbers provided.

3.2 Organisational security policies

P.Process-TOE Protection during TOE Development and Production

An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

[Additional organisational security policy]

One organisational security policy was added to the organisational security policies in the PP. This is concerned with cryptographic functions invoked by the Security IC Embedded Software. Three cryptographic algorithms are specified.

P.HW-Crypto Hardware cryptographic functions

Cryptographic operational functions specified below are provided to the Security IC Embedded Software:

- Triple DES,
- RSA,
- Diffie-Hellman
- ECDSA signature verification
- ECDH key exchange and
- SHA-256;

3.3 Assumptions

A.Process-Sec-IC Protection during Packaging, Finishing and Personalisation

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Phases after TOE Delivery (refer to Sections 1.2.2 and 7.1 in the PP) are assumed to be protected appropriately. For a preliminary list of assets to be protected refer to paragraph92 (page30) in the PP.

A.Plat-Appl Usage of Hardware Platform

The Security IC Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as documented in the certification report.

A.Resp-Appl Treatment of User Data

All User Data are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.

4 Security objectives

Security objectives for the TOE and its operational environment will be defined in this chapter. All security objectives except an additional objectives (O.HW_Crypto) are identical to the security objectives defined in the PP.

4.1 Security objectives for the TOE

O.Leak-Inherent Protection against Inherent Information Leakage

The TOE must provide protection against disclosure of confidential data stored and/or processed in the Security IC

- by measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and
- by measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or I/O lines).

This objective pertains to measurements with subsequent complex signal processing whereas O.Phys-Probing is about direct measurements on elements on the chip surface. Details correspond to an analysis of attack scenarios which is not given here.

O.Phys-Probing Protection against Physical Probing

The TOE must provide protection against disclosure of User Data, against the disclosure/reconstruction of the Security IC Embedded Software or against the disclosure of other critical information about the operation of the TOE. This includes protection against

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)

with a prior

- reverse-engineering to understand the design and its properties and functions. The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

O.Malfunction Protection against Malfunctions

The TOE must ensure its correct operation.

The TOE must indicate or prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent malfunctions. Examples of environmental conditions are voltage, clock frequency, temperature, or external energy fields.

O.Phys-Manipulation Protection against Physical Manipulation

The TOE must provide protection against manipulation of the TOE (including its software and Data), the Security IC Embedded Software and the User Data. This includes protection against

- reverse-engineering (understanding the design and its properties and functions),
- manipulation of the hardware and any data, as well as
- controlled manipulation of memory contents (Application Data).

The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

O.Leak-Forced Protection against Forced Information Leakage

The Security IC must be protected against disclosure of confidential data processed in the Security IC (using methods as described under O.Leak-Inherent) even if the information leakage is not inherent but caused by the attacker

- by forcing a malfunction (refer to “Protection against Malfunction due to Environmental Stress (O.Malfunction)” and/or
- by a physical manipulation (refer to “Protection against Physical Manipulation (O.Phys-Manipulation)”.

If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.

O.Abuse-Func Protection against Abuse of Functionality

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical User Data, (ii) manipulate critical User Data of the Security IC Embedded Software, (iii) manipulate Soft-coded Security IC Embedded Software or (iv) bypass, deactivate, change or explore security features or security services of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

O.Identification TOE Identification

The TOE must provide means to store Initialisation Data and Pre-personalisation Data in its non-volatile memory. The Initialisation Data (or parts of them) are used for TOE identification.

O.RND Random Numbers

The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a sufficient entropy.

The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.

[Additional security objective for the TOE]

One security objective was added to the security objectives in the PP. It is concerned with cryptographic functions to be invoked by the security IC Embedded Software.

O.HW-Crypto Hardware cryptographic functions

The TOE provides triple-DES, RSA, Diffie-Hellman, ECDSA signature verification, ECDH key exchange and SHA-256 cryptographic operational functions in order that the security IC Embedded Software can invoke them as libraries.

4.2 Security objectives for the Security IC Embedded Software development environment

OE.Plat-Appl Usage of Hardware Platform

To ensure that the TOE is used in a secure manner the Security IC Embedded Software shall be designed so that the requirements from the following documents are met: (i) hardware data sheet for the TOE, (ii) data sheet of the IC Dedicated Software of the TOE, (iii) TOE application notes, other guidance documents, and (iv) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as referenced in the certification report.

OE.Resp-Appl Treatment of User Data

Security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context.

4.3 Security objectives for the operational environment

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

Security procedures shall be used after TOE Delivery up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 1.2.3) must be protected appropriately. For a preliminary list of assets to be protected refer to paragraph 92 (page 30 in the PP).

4.4 Security objectives rationale

All security objectives in this ST, except O.HW-Crypto, were derived from the security objectives in the PP. Those security objectives trace back to security problem definition as shown Table 1. The security objectives rationale about Table 1, except P.HW-Crypto/O.HW-Crypto, can be referred to the PP.

Security problem definition	Security objectives
T.Leak-Inherent	O.Leak-Inherent
T.Phys-Probing	O.Phys-Probing
T.Malfunction	O.Malfunction
T.Phys-Manipulation	O.Phys-Manupilation
T.Leak-Forced	O.Leak-Forced
T.Abuse-Func	O.Abuse-Func
T.RND	O.RND
P.Process-TOE	O.Identification

P.HW-Crypto	O.HW-Crypto
A.Plat-Appl	OE.Plat-Appl
A.Resp-Appl	OE.Resp-Appl
A.Process-Sec-IC	OE.Process-Sec-IC

Table 1: Security objectives versus security problem definition

Rationale for O.HW-Crypto:

The additional security objective O.HW-Crypto very resembles P.HW-Crypto (semantically identical). Then, security objective O.HW-Crypto directly enforces organisational security policy P.HW-Crypto.

5 Extended components definition

The PP defined three new security functional families and four new security functional components associating with those new families. They are referred to as shown in Table 2. There is no additional extended component newly defined in the ST.

Extended family	Extended component
FCS_RNG Generation of random numbers	FCS_RNG.1 Random number generation
FMT_LIM Limited capabilities and availability	FMT_LIM.1 Limited capabilities
	FMT_LIM.2 Limited availability
FAU_SAS Audit data storage	FAU_SAS.1 Audit storage

Table 2: Extended families and components

6 Security requirements

6.1 Security functional requirements

Security functional requirements for the TOE are specified below. All security functional requirements in the PP are covered and an additional requirement for specific cryptographic operational functions is described in FCS_COP.1.

Operations in the requirements are identified in accordance with the conventions below.

- **Selection and assignment: identified in *italics* in each element (*underlined part* are operations by the ST author)**
- **Refinement: identified as "Refinement" after each element (all refinements in the requirements are identical to the PP)**

Furthermore, there added a description of "Definition" to one component. This is not a part of the component but gives explanation and definition of key words for the component.

FRU_FLT.2 Limited fault tolerance

Hierarchical to: FRU_FLT.1 Degraded fault tolerance

Dependencies: FPT_FLS.1 Failure with preservation of secure state.

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: *exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1)*.

Refinement: The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur*.

Refinement: The term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.

Definition: The term "a secure state" in FPT_FLS.1.1 refers to the state in which the integrity of contents of the non-volatile memory is preserved and the TOE suspends any services for external entities. This will prevent exposure or tampering of the assets of the TOE through compromised security functionality of the TOE.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 **The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced:** ***Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks*****.**

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 **The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced:** ***Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks*****.**

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 and/or Prepersonalisation Data and/or supplements of the Security IC Embedded Software*** **in the** ***non-volatile memory*****.**

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 **The TSF shall resist** ***physical manipulation and physical probing*** **to the** ***TSF*** **by responding automatically such that the SFRs are always enforced.**

Refinement: **The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.**

FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control].

FDP_ITT.1.1 **The TSF shall enforce the *Data Processing Policy* to prevent the *disclosure* of user data when it is transmitted between physically-separated parts of the TOE.**

Refinement: **The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.**

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 **The TSF shall protect TSF data from *disclosure* when it is transmitted between separate parts of the TOE.**

Refinement: **The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE.**

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 **The TSF shall enforce the *Data Processing Policy* on *all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software*.**

Application Note: Input/internal/output data of the SHA-256/SHA-1 algorithms shall not be considered confidential data.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

FCS_COP.1[DES] Cryptographic operation

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
FMT_MSA.2 Secure security attributes

FCS_COP.1.1[DES] **The TSF shall perform Encryption and decryption in accordance with a specified cryptographic algorithm Triple DES (3DES-CBC mode) and key size of 112-bit key that meet the following standards: 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**

FCS_COP.1[RSA] Cryptographic operation

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
FMT_MSA.2 Secure security attributes

FCS_COP.1.1[RSA] The TSF shall perform signature generation in accordance with a specified cryptographic algorithm RSA(Active authentication ISO9796) and key sizes of *512,768,1024,1280,1536,1792 or 2048bits* and signature verification in accordance with a specified cryptographic algorithm RSA(extended access control RSA-PSS and RSA-PKCS) and key sizes of *1024,1280,1536,2048,3072 or 4096bits* that meet the following standards: *PKCS#1: RSA Encryption Standard, version 2.1, RSA Laboratories*

FCS_COP.1[DH] Cryptographic operation

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
FMT_MSA.2 Secure security attributes

FCS_COP.1.1[DH]The TSF shall perform key sharing in accordance with a specified algorithm DH and key sizes of *1024,1280,1536 or 2048 bits* that meet the following standards: *PKCS#3:Diffie-Hellman Key-Agreement Standard, RFC2631*

FCS_COP.1[SHA] Cryptographic operation

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
FMT_MSA.2 Secure security attributes

FCS_COP.1.1[SHA]The TSF shall perform a *cryptographic checksum* in accordance with a specified cryptographic algorithm *SHA-256* and key sizes of *none* that meet the following standards: *FIPS PUB 180-2 with Change Notice 1.*

Application Notes: The TOE also supports SHA-1, but the cryptographic strength of SHA-1 is not

considered sufficient to meet the level of AVA_VAN.5; therefore only SHA.256 is listed here.

FCS_COP.1[ECDSA] Cryptographic operation

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
FMT_MSA.2 Secure security attributes

FCS_COP.1.1[ECDSA]The TSF shall perform *signature verification* in accordance with a specified cryptographic algorithm *ECDSA* and cryptographic key sizes *160 bits, 192 bits, 224 bits, 256 bits and 384 bits* that meet the following: *ECDSA Technical guideline TR-03111 Elliptic Curve cryptography v1.00.*

Application note: The ECDSA internally uses SHA224 according to *FIPS PUB 180-2 with Change Notice 1*.

FCS_COP.1[ECDH] Cryptographic operation

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
FMT_MSA.2 Secure security attributes

FCS_COP.1.1[ECDH]The TSF shall perform *key sharing* in accordance with a specified cryptographic algorithm *ECDH* and cryptographic key sizes *160 bits, 192 bits, 224 bits, 256 bits and 384 bits* that meet the following: *ECDH (ISO15946), Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents TR-03110- Extended Access control (EAC) v1.1, Annex A.1, ISO/IEC 15946-1. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part1: General 2002-12-01, ISO/IEC 15946-3. Information technology – Security techniques – Cryptographic techniques based on elliptic curves –Part3: Key establishment 2002-12-01 and Technical guideline TR-03111 Elliptic Curve cryptography v1.00.*

6.2 Security assurance requirements

The security assurance requirements of this ST are identical to the security assurance requirements in the PP with which the ST claims to be conformant.

The PP requires the ST writer to indicate the version of the Mandatory Technical Document "Application of Attack Potential to Smartcards" at "*Application Note 30*" in the PP. The current version of the document is "Version 2.5" [5].

6.3 Security requirements rationale

6.3.1 Rationale for the security functional requirements

The rationale described in the PP can be totally applied to this ST, since the ST is strictly conformant to the PP. Table 4 below is excerpted from the PP except FCS_COP.1[DES], FCS_COP.1[RSA], FCS_COP.1[DH], FCS_COP.1[SHA], FCS_COP.1[ECDSA], FCS_COP.1[ECDH] , and O.HW-Crypto which is a cryptographic requirement from an additional objective for the specific cryptographic functions. The rationale for FCS_COP.1[DES], FCS_COP.1[RSA], FCS_COP.1[DH], FCS_COP.1[SHA], FCS_COP.1[ECDSA], and FCS_COP.1[ECDHA] is described after Table 4.

Security objectives	Security functional requirements
O.Leak-Inherent	- FDP_ITT.1 - FPT_ITT.1 - FDP_IFC.1
O.Phys-Probing	- FPT_PHP.3
O.Malfunction	- FRU_FLT.2 - FPT_FLS.1
O.Phys-Manipulation	- FPT_PHP.3
O.Leak-Forced	All requirements listed for O.Leak-Inherent - FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 plus those listed for O.Malfunction and O.Phys-Manipulation - FRU_FLT.2, FPT_FLS.1, FPT_PHP.3
O.Abuse-Func	- FMT_LIM.1 - FMT_LIM.2 plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced - FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1
O.Identification	- FAU_SAS.1
O.RND	- FCS_RNG.1 plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced - FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1
O.HW-Crypto	- FCS_COP.1[DES], FCS_COP.1[RSA], FCS_COP.1[DH], FCS_COP.1[SHA], FCS_COP.1[ECDSA], and FCS_COP.1[ECDH]
OE.Plat-Appl	not applicable
OE.Resp-Appl	not applicable
OE.Process-Sec-IC	not applicable

Table 4: Security requirements versus security objectives

The justification for the security requirement FCS_COP.1[DES], FCS_COP.1[RSA], FCS_COP.1[DH] FCS_COP.1[SHA], FCS_COP.1[ECDSA] and FCS_COP.1[ECDH] is as follows:

This objective O.HW-Crypto describes the TOE must provide the specific cryptographic operation functions to be invoked by the security IC Embedded Software. FCS_COP.1[DES], FCS_COP.1[RSA], FCS_COP.1[DH], FCS_COP.1[SHA], FCS_COP.1[ECDSA] and FCS_COP.1[ECDH] requires that the cryptographic operation functions specified in the objective shall be performed by the TOE. The cryptographic operation functions in FCS_COP.1[DES], FCS_COP.1[RSA], FCS_COP.1[DH], FCS_COP.1[SHA], FCS_COP.1[ECDSA] and FCS_COP.1[ECDH] correspond to and satisfy whole O.HW-Crypto. There are no cryptographic key management requirements, which are usually involved together with cryptographic operation, since key management will be performed by the security IC Embedded Software (outside of the TOE).

6.3.2 Dependencies of security functional requirements

All security functional requirements in this ST except FCS_COP.1[DES], FCS_COP.1[RSA], FCS_COP.1[DH], FCS_COP.1[SHA], FCS_COP.1[ECDSA] and FCS_COP.1[ECDH] are identical to the PP. Dependencies described in each security functional requirement are explained in the PP (except FCS_COP.1[DES], FCS_COP.1[RSA], FCS_COP.1[DH], FCS_COP.1[SHA], FCS_COP.1[ECDSA] and FCS_COP.1[ECDH]).

FCS_COP.1[DES], FCS_COP.1[RSA], FCS_COP.1[DH] FCS_COP.1[SHA], FCS_COP.1[ECDSA] and FCS_COP.1[ECDH] have dependencies to the components concerning key management (for key introduction; FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, for key destruction; FCS_CKM.4, and for security attributes of keys; FMT_MSA.2), which are usually involved together with cryptographic operation. However, in this ST, the requirements FCS_COP.1[DES], FCS_COP.1[RSA], FCS_COP.1[DH], FCS_COP.1[SHA], FCS_COP.1[ECDSA] and FCS_COP.1[ECDH] are employed to require mechanisms for the specific cryptographic operations to satisfy O.HW-Crypto. Key management functionality is not required for the TOE because it will be served to the security IC Embedded Software (outside of the TOE). Therefore, these dependencies are not applicable in this ST.

6.3.3 Rationale for the security assurance requirements

All security assurance requirements in this ST are identical to the PP. There is no additional description to the rationale for the security assurance requirements of the PP.

7 TOE summary specification

The technical mechanisms to satisfy the SFRs are described in this chapter. Each SFR defined in the ST will be implemented as follows:

FRU_FLT.2

The TOE ensures its correct operation and preserves integrity of contents of the memories in circumstances.

Temperature , the internal clock frequency and internal voltage are within the defined operating range and by having a one bit error correction by ECC on the EEprom.

FPT_FLS.1

The TOE halts its operation when it detects circumstances below(excluding case2 signal error monitoring). The TOE resumes its normal operation by “power-on reset” or disposition of the failure by the security IC Embedded software. Contents of the non-volatile memory keep its integrity.

Case1: resumes by the external reset (power-on reset)

- Temperature monitoring, out of range
- clock frequency monitoring, out of range
- power supply monitoring, out of range
- glitch monitoring
- light attack monitoring
- address area monitoring
- duplicated signals
- signal error monitoring (Parity error for RAM is one of this)
- memory fire wall
- undefined instruction monitoring(some of them are dealt with in Case2 below)
- active shield error

Case2: disposition by the security IC Embedded software

- signal error monitoring(EEPROM error: for 2-bit or more error detected by ECC is one of this. If this happens, TOE jumps interrupt process(INT5) and user can execute what should be done.)
- Undefined instruction monitoring(SWI2 non-maskable interrupt)

FMT_LIM.1, FMT_LIM.2

There are testing interfaces (test pads) on the surface of the IC chip. Those interfaces remain on the chip, but will be disabled at the end of the phase 3. After delivery from the TOE manufacturer, the test features of the TOE will not be available through the testing interfaces by the mechanism explained below. Besides, after phase 4 (IC packaging), those test pads are concealed under IC packaging, so that physical access to the test pads becomes difficult.

The TOE requires password check to invoke the testing functionality of the TOE. A default password written in advance on the EEPROM will be initialised before delivery of the TOE. The TOE creates that initialisation value from random number and no one knows the value. The TOE will lock its password check process permanently if a password check failure occurs, so that the testing functionality will be virtually not available after delivery of the TOE.

FAU_SAS.1

For unique identification of the TOE, the following data is stored in the EEPROM before delivery.

- IC chip identification data

FPT_PHP.3

The TOE provides measures to resist physical manipulation and probing to the TSF as follows:

- Data bus and Address bus masking
- address bus scrambling
- memory ciphering
- active shielding
- passive shielding

FDP_ITT.1, FTP_ITT.1, FDP_IFC.1

Those requirements provide that confidentiality of user data and TSF data in the TOE must not be violated with illegal measures such as electromagnetic emission or physical probing. FDP_ITT.1 provides protection of user data, FPT_ITT.1 provides protection of TSF data and FDP_IFC.1 provides the policy to protect those data. Internal data of the TOE are transmitted between separated parts of the TOE such as different memories, CPU, co-processor etc. The measures to protect those data are almost identical to the measures described in FPT_PHP.3. Furthermore, random wait insertion makes observation difficult.

It is noted that the TOE does not support the generation of SHA hashes (SHA-256/SHA-1) for data that is confidential in nature.

FCS_RNG.1

The TOE implements a physical random number generator (RNG). A seed data is created with ring oscillator (logical oscillator) of the TOE. Phase noise inherent in the ring oscillator gives randomness to seed data. Based on this seed data, a triple DES RNG (TDES-RNG), is applied. Random number generator claims the fulfilment of functionality of K3 of [AIS20] for the strength Claim high.

The TSF monitors degree of randomness of seed data and indicates its status. When the status indicates valid, the RNG circuitry is allowed to use the seed data.

FCS_COP.1[DES], FCS_COP.1[RSA], FCS_COP.1[DH], FCS_COP.1[SHA], FCS_COP.1[ECDSA] and FCS_COP.1[ECDH]

The TOE provides cryptographic mechanism of triple DES, RSA Diffie-Hellman, ECDSA signature verification and ECDH key exchange. Triple DES operation is performed by a hardware circuitry of the TOE (“hardware triple DES” in Fig.2). RSA Diffie-Hellman, ECDSA signature verification and ECDH key exchange operation operations are performed by the co-processor of the TOE. Each cryptographic function can be invoked as a “cryptographic library” or ‘cryptographic library extension’ from the security IC Embedded Software.

The TOE provides a hash mechanism of SHA-256. It is implemented using the hardware accelerator for SHA in software functions that are part of the cryptographic library (see in Fig2). The TOE also implements a SHA-224 function as part of the ECDSA that also uses the hardware accellerator for SHA. The TOE also supports SHA-1 in a cryptographic library function, but the cryptographic strength of the SHA-1 is not considered sufficient to meet the level of AVA_VAN.5.

It is noted that the ECDSA signature verification and ECDH key exchange are part of the cryptographic library extension. The other algorithms are part of the cryptographic library.

8 Reference

8.1 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 1, September 2006

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 2, September 2007

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 2, September 2007

[4] Security IC Platform Protection Profile, Version 1.0 15.06.2007; BSI-PP-0035

[5] Supporting document, Mandatory Technical Document: Application of Attack Potential to Smartcards, April 2008, Version 2.5 Revision 1, CCDB-2008-04-001

[6] Application Notes and Interpretation of the Scheme (AIS), AIS 20: Functionality classes and evaluation methodology for deterministic random number generators, Version 1

8.2 Glossary of vocabulary

IC Dedicated Software — IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).

Initialisation Data — Initialisation Data defined by the TOE Manufacturer to identify the TOE and to keep track of the Security IC's production and further life-cycle phases are considered as belonging to the TSF data. These data are for instance used for traceability and for TOE identification (identification data).

Pre-personalisation Data — Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases.

Security IC Embedded Software — Software embedded in a Security IC and normally not being developed by the IC Designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3 or in later phases of the Security IC product life-cycle. Some part of that software may actually implement a Security IC application others may provide standard services. Nevertheless, this distinction doesn't matter here so that the Security IC Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.

Test Features — All features and functions (implemented by the IC Dedicated Test Software and/or hardware) which are designed to be used before TOE Delivery only and delivered as part of the TOE.

TOE Delivery — The period when the TOE is delivered which is (refer to Figure 2 on page 10) either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is

	delivered in form of packaged products.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE. This includes information about the TOE's configuration, if any is coded in non-volatile non-programmable memories (ROM), in specific circuitry, in non-volatile programmable memories (for instance EEPROM) or a combination thereof.
User Data	All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.

8.3 Abbreviations

CC	Common Criteria
IC	Integrated Circuit
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

- End of document -