TPG0214B

General Business Use

Security Target Lite

AT90SDC100

Table of Contents

TPG0214B_VIC_18Jul11

1 Introduction

1.1 Security target reference

Title: AT90SDC100 Security Target

Version number: B

Sponsor: Inside Secure

Evaluation Scheme: France (ANSSI)

Evaluator: SERMA Technologies France

Version	Date	Changes	Author
A	14 Jul 11	Initial released version	John Boggie
B	18 Jul 11	Fixed error on title page (wrong classification)	John Boggie

1.2 Purpose

1   This document defines the Security Target of the AT90SDC100 project, and is provided to satisfy the Assurance Class ASE Security Target Evaluation as defined in Part of the Common Criteria version 3.1

1.3 References

The table below lists only the documents that are referenced in this Security Target to give the user further information. Section 1.4 the TOE overview lists the User Guidance documents applicable to the Security IC Embedded Software Developer. Section 8.3 lists the Standards used to perform the certification of the TOE.

[COF]	Customer Option Form

1.4 TOE Overview

1.4.1 TOE Identification

2   The Target of Evaluation is a Secure Microcontroller with Cryptographic Software library. The TOE is identified as shown below:

		Identifier (FAU_SAS.1 where applicable)
Part Number	AT90SDC100	SN_0 = 0xC0 [TD]
Product Identification Number	59U06	
Hardware Revision	B	SN_1 = 0x01 [TD]
Applicable Inside Secure Toolbox	00.03.11.08	0x00031108 [a]

3   The TOE is a Dual Core Secure Microcontroller (Security IC) that may be used in a variety of security applications, including, PayTV and embedded systems.

4   The increase in the number and complexity of applications in the market of a Secure Microcontroller is reflected in the increase of the level of data security required. The security needs for the TOE can be summarised as being able to counter those who want to defraud, gain unauthorised access to data and control a system utilising the TOE. Therefore it is mandatory to:

-      maintain the integrity and the confidentiality of the content of the TOE memories as required by the end application(s)

-      maintain the correct execution of the software residing on the TOE

5   This requires that the TOE especially maintains the integrity and the confidentiality of its security functionality.

6   Protected information is in general secret or integrity sensitive data such as Personal Identification Numbers, Balance Value (Stored Value Cards), and Personal Data Files. Other protected information 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 Security IC.

7   The TOE can be used in smartcard application, a USB token or other devices. The intended environment is very large; and generally once issued the TOE may be stored and used anywhere, generally there is no control applied to the TOE and its operational environment.

---

[a] The toolbox identification is output by the TOE when the self test function of the toolbox is called

1.4.2 TOE Definition

1.4.2.1 TOE Definition Summary

General Features

- Dual core High-end secure microcontroller offering 2 secure Twincore $^{®}$ Master and Secure Core Enhanced RISC Architecture

    o 135 Powerful Instructions (Most Executed in a Single Clock Cycle)

- Operating Ranges: from 2.70v to 5.50v

- Compliant with EMV 2000 Specifications, PC industry Compatible

Memory

Master Core

- 128K Bytes of ROM Program Memory

- 36K Bytes of EEPROM, including 128 OTP Bytes and 384 Bit-addressable Bytes

    o 1 to 128-byte Program/Erase

    o 2ms Program, 2ms Erase

- 6K Bytes of RAM Memory

Secure Core

- 64K Bytes of ROM Program Memory including 32K bytes for Inside Secure Toolbox Library

- 18K Bytes of EEPROM, including 64 OTP Bytes and 384 Bit-addressable Bytes

    o 1 to 64-byte Program/Erase

    o 2ms Program, 2ms Erase

- 6K Bytes of RAM Memory (4K bytes of RISC CPU Core RAM, 2K bytes of Ad-X^{TM} RAM, shared with the RISC CPU core)

Peripherals

- Four I/O ports (can be configured to support ISO7816-3, TWI, General Purpose, DataFlash Control, etc.)

- One ISO 7816 Controller

    o Up to 625 kbps at 5 MHz

    o Compliant with T = 0 and T = 1 Protocols

TPG0214B_VIC_18Jul11

- Serial Peripheral Interface (SPI) controller (up to 15 MBps) with Flash power management

- Programmable Internal Oscillator (Up to 30 MHz for Ad-X^{TM} and 30MHz for both CPU clocks)

- Two 16-bit Timers in Master Core and one 16-bit Timer in Secure Core

- Random Number Generators: PRNG on Master Core and AIS31 TRNG on Secure Core

- 2-level Interrupt Controller

- Hardware DES and Triple DES with DPA Resistance

- Hardware AES

- Checksum Accelerator

- Code Signature Module

- CRC16 and 32 Engine (compliant with ISO/IEC 3309)

- 32-bit Cryptographic Accelerator (Ad-X for public key Operations): RSA, DSA, ECC, etc.

Security

- Dedicated Hardware Protection Against SPA/DPA/DEMA/SEMA attacks

- Advanced Protection Against Physical Attack, Glitch Attack, Side Channel Attack

- Environmental Protection Systems

- Voltage Monitor

- Frequency Monitor

- Temperature Monitor

- Light Protection

- Secure Memory Management / Access Protection

Security IC Embedded Software Developer Guidance Documents

REF	Title	Inside Secure Identifier	Version	Note
[TD]	AT90SDC100 Technical Datasheet	TPR0424	B	Hardware Datasheet details the FSP
[APP_SEC]	Security Recommendations for AT90SDC10x Family	TPR0461	B	General Security recommendations for the TOE
[APP_DES]	Secured Hardware DES/TDES for 0.13 µm Products	TPR0400	E	Hardware TDES Recommendations
[APP_AES]	Secured Hardware AES for 0.13 µm Products	TPR0428	C	Hardware AES Recommendations
[APP_CSM]	The Code Signature Module for 0.13 µm Products	TPR0409	C	Datasheet for the Code Signature Module
[APP_RNG]	Generating Random Numbers with a controlled entropy for 0.13 µm Products	TPR0468	C	RNG recommendations
[APP_AD-X]	Ad-X for AT90SC Family	TPR0116	F	Hardware Datasheet for Ad-X Accelerator
[APP_TBX]	Toolbox 00.03.1x.xx on AT90SCXXXXC	TPR0454	C	Toolbox 00.03.1x.xx family Datasheet, details the FSP for the Toolbox functions
[APP_TBX_SEC]	Secure use of Tbx 00.03.1x.xx on AT90SC	TPR0455	C	Toolbox 00.03.1x.xx family Security recommendations
[APP_CUST_TBX]	Efficient use of Ad-X for Implementing Cryptographic Operations	TPR0142	E	Guidance for customers who wish to use their own Cryptographic Toolbox
[ACT]	SmartACT User's Manual	TPR0134	D	Security IC developer Code entry user manual

inside
SECURE

TOE Life Cycle Addresses

Function	Company	Location
• IC Design • Dataprep • Cryptographic Support Software Development	Inside Secure	Inside Secure Rousset Zone Industrielle 13106 Rousset Cedex France
• IC Design	Inside Secure	Inside Secure Scottish Enterprise Technology Park East Kilbride G75 0QR Scotland
• Wafer Fab	Lfoundry	Lfoundry Rousset Zone Industrielle 13106 Rousset Cedex France
• Mask Shop	Toppan Europe	Toppan Photomasks Europe 01109 Dresden Germany 91105 Corbeil Essonnes Cedex France
• Mask Shop	Compugraphics	Compugraphics International Limited Newark Road North Eastfield Industrial Estate KY7 4NT Scotland
• Test Centre	Atmel	Atmel Test Centre (ACP) 102 Accuracy Drive Corner Excellence Avenue Carmetray Industrial Park 1 Canlubang City 4028 Laguna Philippines

1.4.2.2 TOE Detailed Description

8   The TOE (AT90SDC100) microcontroller contains 2 physical domains contained on a single chip. Each domain features one independent 8/16-bit core running concurrently to each other. These cores are named Master Core (Black Domain) and Secure Core (Red Domain).

9   Figure 1 gives an overview of the two cores. The two cores are shown with a black line around the Master Core boundary and a red line around the Secure Core boundary.
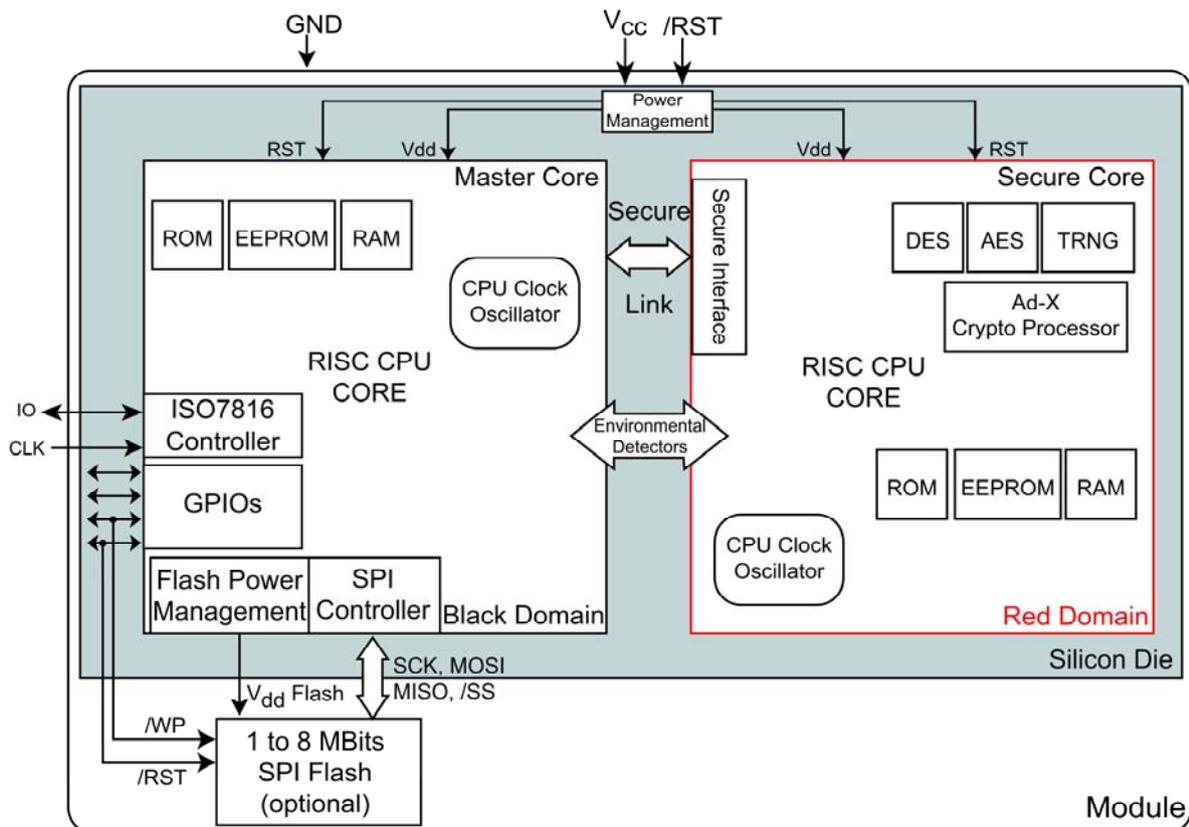
Figure 1: Overview of the 2 cores and how they are connected

10   Each core contains a 8/16-bit microcontroller, with ROM, EEPROM, and RAM memories.

11   In order to prevent sensitive data leakage, each core can only communicate to each other using a SecureLink where only certified data can move from the Red Domain (Secure) to the Black Domain (Master).

12   Figure 2 shows a block diagram of the Master Core (Black Domain).

TPG0214B_VIC_18Jul11
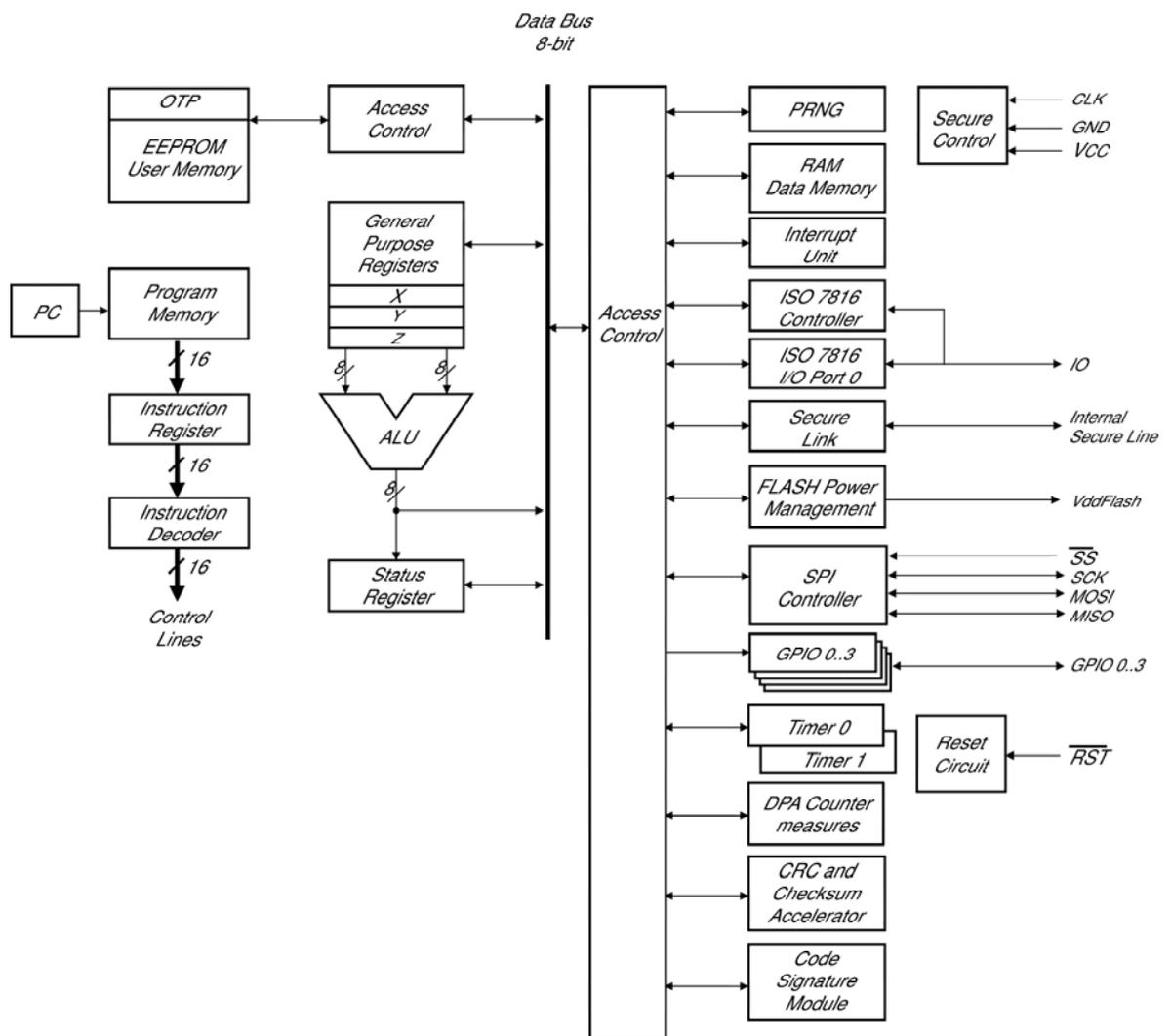
Figure 2: Block Diagram of the Master Core

13   Figure 3 shows a block diagram of the Secure Core (Red Domain).

GENERAL BUSINESS USE

TPG0214B_VIC_18Jul11
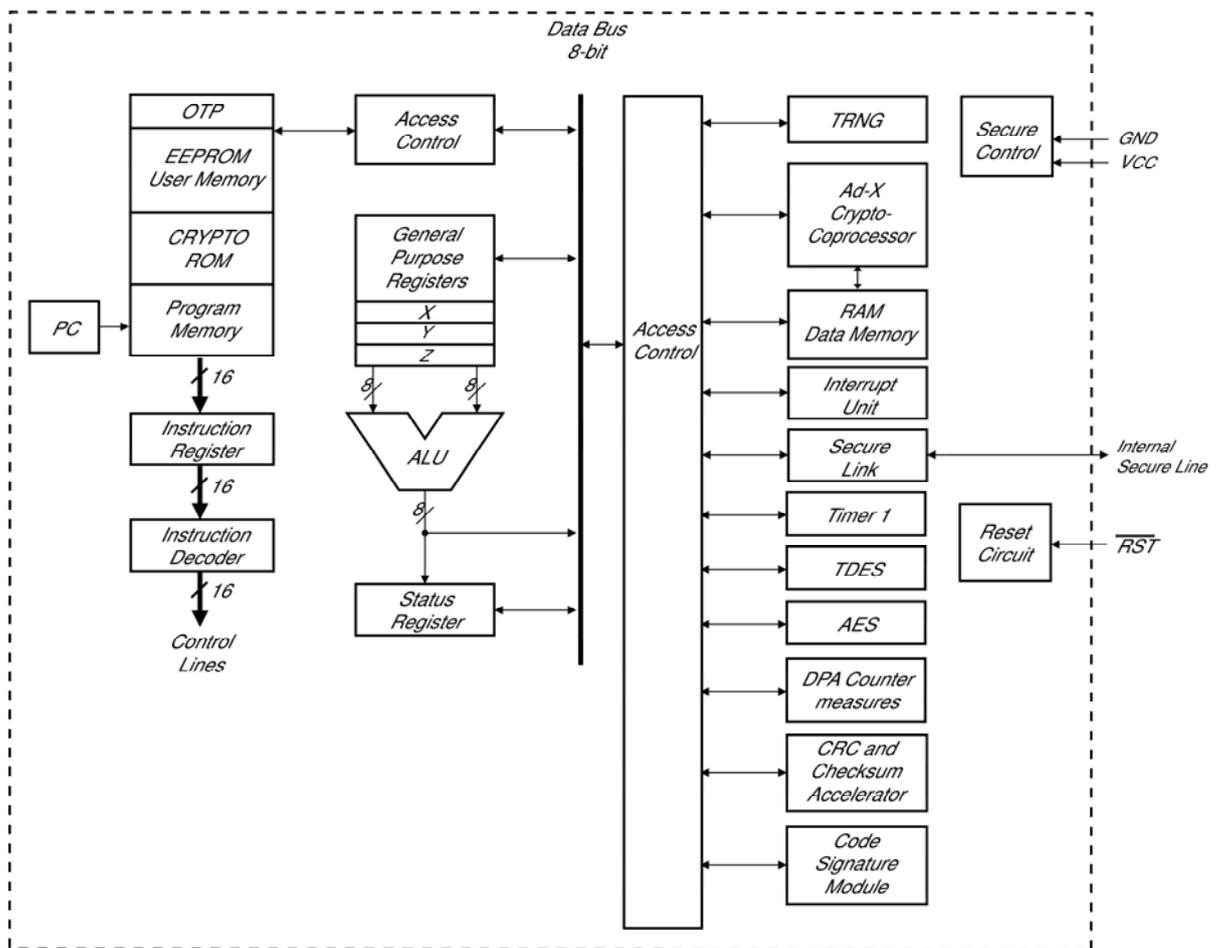
Figure 3: Block Diagram of the Secure Core

14   The Target of Evaluation (TOE) is a Dual Core Secure Microcontroller (Security IC) each core comprises, processing unit, security components, ROM, EEPROM, and RAM memories, the Master core also contains I/O ports. The Secure Core contains a crypto-accelerator. The TOE will contain software elements during its life cycle. This software falls into 3 distinct categories:

- Test Software

- Cryptographic Support Software (Secure Core only)

- Security IC Embedded Software

15   **Test Software:** Test software includes the test programs that are produced as evidence to support the ATE class for the evaluation of the TOE. Inside Engineering ROM is provided to facilitate testing of the device, this Engineering ROM is applicable to Phases 2 and 3 of the TOE life Cycle. To further aid testing of the TOE, additional test programs may be loaded into the EEPROM. In addition to the Test software the TOE also includes dedicated hardware to perform testing. To allow the ITSEF to perform testing of the TOE a version of the TOE is delivered with an Inside Engineering ROM, and some simple test routines stored in the EEPROM. It must be noted that this **Engineering ROM and associated test software is not part of the**

TOE. The entry and abuse of test modes (hardware) must be verified after TOE Delivery: this is evaluated according to the Common Criteria assurance family AVA_VAN. Refer to TOE Summary Specification for further information.

16   **Cryptographic Support Software (Toolbox):** The TOE where applicable also consists of a Cryptographic Toolbox provided by Inside Secure. This Toolbox is part of the ROM embedded on the TOE within the Secure Core. The user of this document should refer to the TOE Summary specification of this document for the full details. **The Inside Secure Toolbox is considered part of the TOE.**

17   **Security IC Embedded Software:** The final version of the AT90SDC100 device also includes embedded software, this final version of the product is referred to as a Composite Product. The Security IC Embedded Software can be stored in non-volatile non-programmable memories (ROM). But some parts of it (called supplements for the Security IC Embedded Software, refer to [PP]) may also be stored in non-volatile programmable memories (for instance EEPROM). All data managed by the Security IC Embedded Software is called User Data. In addition, Pre-personalisation Data [PP] belongs to the User Data.

18   The Composite Product comprises

   -   the TOE

   -   the Security IC Embedded Software comprising

       -   Hard-coded Security IC Embedded Software (normally stored in ROM)

       -   Soft-coded Security IC Embedded Software (normally stored in EEPROM) and

   -   User Data (especially personalisation data and other data generated and used by the Security IC Embedded Software)

19   The **Security IC Embedded Software** and the User Data are developed separately to the hardware TOE by the Inside Secure Customers. Therefore **the Security IC Embedded Software is not part of the TOE**.

   Note: even though the Security IC Embedded Software is not part of the TOE, the documentations delivered as evidence for the AGD Class (**Guidance Documentation**) aid the developer to ensure the correct operation of the device and more importantly the security functionality of the device and **is therefore part of the TOE**.

20   Therefore, the TOE comprises

   -   the circuitry of the IC (hardware including the physical memories)

   -   configuration data, initialisation data related to the IC Dedicated Software and the behaviour of the security functionality [b]

   -   the associated guidance documentation

   -   Cryptographic Support Software

_____

[b]   which may also be coded in specific circuitry of the IC; for a definition refer to [PP]

TPG0214B_VIC_18Jul11

The TOE is designed, and generated by the TOE Manufacturer

21   The TOE is intended to be used for a Secure Microcontroller product (Security IC), independent of the physical interface and the way it is packaged. Generally, a Security IC 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.

22   Note that the Security IC is usually packaged. However the way it is packaged is not specified here.

1.4.3 TOE life cycle

23   This security Target is fully conformant to the claimed PP, the full details of the Security IC life cycle is shown in the PP. This Security Target gives a short summary of the information given in the PP. Information is also given within this Security Target to expand on the applicable phases of the life cycle of the TOE.

1.4.3.1 Overview of the Composite Product Life Cycle

24   The complex development and manufacturing processes of a Composite Product can be separated into seven distinct phases. The phases 2 and 3 of the Composite Product life cycle cover the TOE (IC) development and production:

-    The IC Development (Phase 2):

    -    IC design

    -    IC Dedicated Software development

-    The IC Manufacturing (Phase 3):

    -    integration and photomask fabrication

    -    IC production

    -    IC testing

    -    preparation

    -    Pre-personalisation if necessary

25   In addition, five important stages have to be considered in the Composite Product life cycle:

-    Security IC Embedded Software Development (Phase 1)

-    the IC Packaging (Phase 4)

-    the Composite Product finishing process, preparation and shipping to the personalisation line for the Composite Product (Composite Product Integration Phase 5)

-    the Composite Product personalisation and testing stage where the User Data is loaded into the Security IC's memory (Personalisation Phase 6)

TPG0214B_VIC_18Jul11

- the Composite Product usage by its issuers and consumers (Operational Usage Phase 7) which may include loading and other management of applications in the field
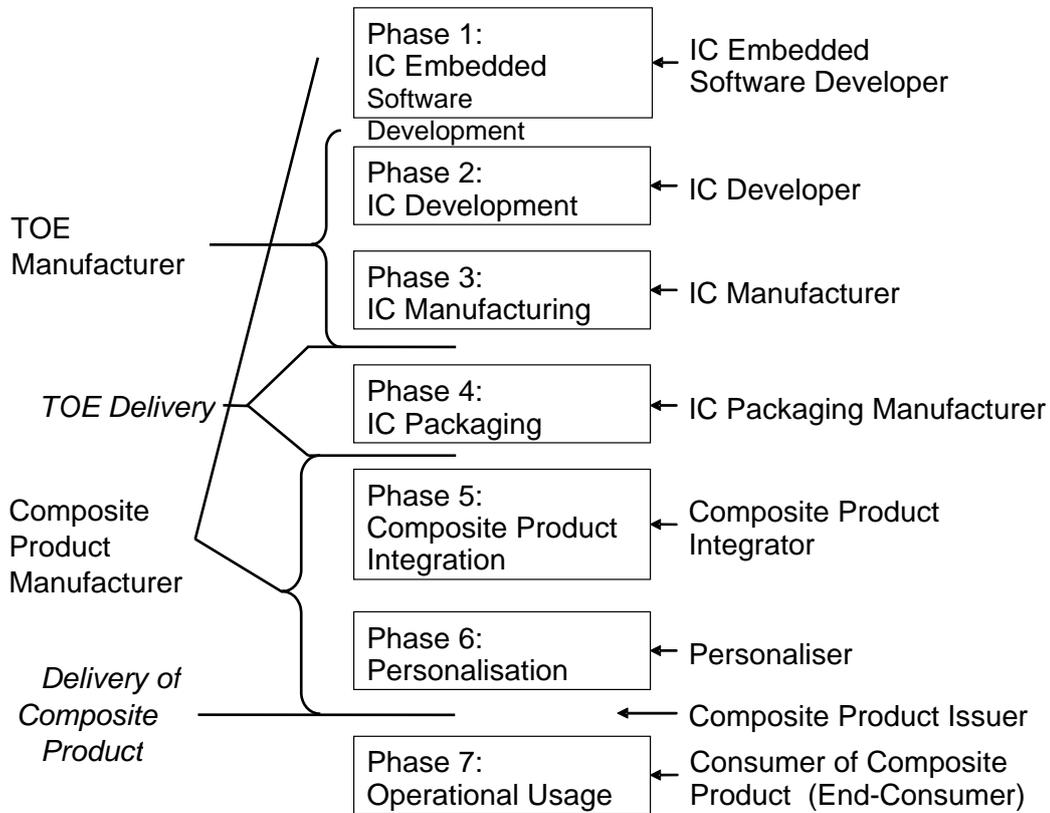
```
                                    ┌──────────────────┐
                                    │ Phase 1:         │     IC Embedded
                                    │ IC Embedded      │◄─── Software Developer
                                    │ Software         │
                                    │ Development      │
                                    ├──────────────────┤
                                    │ Phase 2:         │◄─── IC Developer
              TOE                   │ IC Development   │
              Manufacturer          ├──────────────────┤
                                    │ Phase 3:         │◄─── IC Manufacturer
                                    │ IC Manufacturing │
                                    ├──────────────────┤
              TOE Delivery          │ Phase 4:         │◄─── IC Packaging Manufacturer
                                    │ IC Packaging     │
                                    ├──────────────────┤
                                    │ Phase 5:         │     Composite Product
              Composite             │ Composite Product│◄─── Integrator
              Product               │ Integration      │
              Manufacturer          ├──────────────────┤
                                    │ Phase 6:         │◄─── Personaliser
                                    │ Personalisation  │
              Delivery of           ├──────────────────┤◄─── Composite Product Issuer
              Composite             │ Phase 7:         │     Consumer of Composite
              Product               │ Operational Usage│◄─── Product (End-Consumer)
                                    └──────────────────┘
```

Figure 4: Definition of "TOE Delivery" and responsible Parties

26   The Security IC Embedded Software is developed outside the TOE development in Phase 1. The TOE is developed in Phase 2 and produced in Phase 3. Then the TOE can be delivered in form of wafers or sawn wafers (dice).

27   In the following the term "TOE Delivery" (refer to Figure 4) is uniquely used to indicate

-    after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice).

-The Protection Profile uniquely uses the term "TOE Manufacturer" (refer to Figure 4) which includes the following roles:

-    the IC Developer (Phase 2) and
     the IC Manufacturer (Phase 3)

     The TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice).

28   Hence the "TOE Manufacturer" comprises all roles beginning with Phase 2 and before "TOE Delivery". Starting with "TOE Delivery" another party takes over the control of the TOE.

29   The Protection Profile uniquely uses the term "Composite Product Manufacturer" which includes all roles (outside TOE development and manufacturing) except the End-consumer as user of the Composite Product (refer to Figure 4) which are the following:

- Security IC Embedded Software development (Phase 1)

- the IC Packaging Manufacturer (Phase 4)
  if the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice)

- the Composite Product Manufacturer (Phase 5) and
  the Personaliser (Phase 6).

1.4.3.2 Phases 2 and 3 of the TOE Life Cycle

1.4.3.3 Phase 2 IC Development

30   The development of the TOE is applicable to phase 2 of the life cycle and can be split into two sections:

- IC design

- Cryptographic Support Software Development

31   **IC design:** IC design takes place across two locations, the Inside Secure Design Centre in East Kilbride Scotland (EKB), and the design centre in Rousset France (RFO). The main project design team is located in RFO but some modules or libraries may originate in EKB.

32   **Cryptographic Support Software Development:** The Toolbox development takes place within the Inside Secure Design Centre in Rousset France.

33   To ensure security of both EKB and RFO, IC design takes place within a secure environment, access is controlled with full traceability. A dedicated security person is on site at all times. The IC and Toolbox development is achieved using appropriate development tools running on a secure network, all access to tools and data are controlled using appropriate restrictions and passwords, the full details are shown within the evidence provided for the ALC class. On completion of the design database, the data is transferred from RFO Design to RFO Dataprep to allow for generation of the Photomasks used to manufacture the TOE.

1.4.3.4   Phase 3 IC Manufacturing

34   The IC manufacturing falls into three sections

- Dataprep and Mask Shop

- Wafer Fab

- Testing

35   **Dataprep and Mask Shop:** The design database is delivered from the design centre to the Dataprep team within Rousset France (RFO). This delivery and acceptance process and associated outputs are delivered as part of the evidence provided for the

TPG0214B_VIC_18Jul11

ALC class. The Photomasks used to manufacture the TOE are created by the Mask Shop. Data is transferred from RFO to the Mask Shop. Once created the Photomasks are transferred to the Wafer Fab by a secure approved carrier. This transfer includes tamper evidence and full traceability.

36   **Wafer Fab:** The TOE is manufactured within the Wafer Fabrication facility. The fabrication process occurs within the secure facility, as with the protection mechanisms in place in Phase 2 access to the fabrication facility is restricted. The batches are controlled using a tracking database to ensure that there is traceability of wafers at all times (including rejected wafers/dies). On completion of the fabrication process the wafers are transferred to the Atmel test facility for test and pre-personalisation. Transfer is by a secure carrier, includes tamper evidence, and has full traceability.

37   **Testing:** The Atmel Test Centre is located in Laguna Philippines (ACP). This stage of the process includes production testing (refer to ATE evidence), pre-personalisation, configuration of the security functionality, wafer thinning and saw. The ACP facility has a controlled environment, access is restricted with full traceability, and dedicated security personnel are on site at all times.

1.4.3.5 Composite Product Manufacturer Phases of the Life Cycle

38   Although the pertinent phases of the Life cycle associated with the TOE and this Security Target are Phases 2 and 3; It should be noted that parts of the TOE and this Security Target relate to Phase 1 of the TOE life Cycle. The user of this document should note the following:

- Tools and Emulator

- Guidance Documents

- Code Entry (Security IC Embedded Software Delivery)

39   **Tools and Emulator:** To aid with the development of the Security IC Embedded Software, specific tools and an emulator configured to simulate the AT90SDC100 and Toolbox can be delivered by Inside Secure. The emulator and tools are treated with the same level of protection by Inside as the final IC.

40   **Guidance Documents:** To ensure that the end Composite Product is fully protected and that the SFR enforcing mechanisms can not be tampered with or bypassed, user guidance is delivered in Phase 1 to the Security IC Embedded Software Developer. Delivery procedures are in place to ensure the confidentiality of the sensitive information contained in this documentation set, including secure courier delivery with traceability is followed. Also all parties are covered with NDA before any information is delivered (this also is applicable to Tools and Emulator).

41   **Code Entry:** Guidance documents and a delivery tool (smartACT) are delivered to the Security IC Embedded Software Developer. The guidance documents describe how to use the smartACT tool and also how to securely transmit the final code to Inside Secure for embedding on the final device. As part of the code delivery a Customer Option Form is also delivered to the Code entry team in EKB, this gives details of the options that the customer may choose for the AT90SDC100 device.

42   Guidance Documents and Code Entry are also delivered as evidence for the AGD class, to allow the ITSEF to use these as part of the search for vulnerabilities during the Vulnerability Assessment part of the evaluation.

TPG0214B_VIC_18Jul11

2 Conformance Claims

43 This chapter contains details the conformance claims for the TOE.

2.1 CC Conformance Claim

44 This Security Target claims to be conformant to the Common Criteria Version 3.1, Revision 3, July 2009.

45 Furthermore it claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in the Protection Profile.

2.2 Package Claim

46 The TOE is evaluated to EAL5 level augmented with AVA_VAN.5 and ALC_DVS.2.

2.3 PP Claim

47 This Security Target is strictly conformant to the Protection Profile BSI-PP-0035 "Security IC Platform Protection Profile"

2.4 PP Refinements

48 The refinements to the PP within this security target relate to the Cryptographic Operations. The refinements and additions are taken from "Smartcard Integrated Circuit Augmentations" Version 1.0, March 2002, registered under the German Certification Scheme BSI-AUG-2002 [AUG].

49 Refinements are made to the following Security objectives for the environment:

- OE.Plat-Appl

- OE.Resp-Appl

2.5 PP Additions

50 The following organisational security policies, security objectives, and security functional requirements have been added.

- P.Add-Functions

- A.Key-Function

- O.Add-Functions

- FCS_COP.1

2.6 PP Claims Rationale

51 The differences between this Security Target and the BSI-PP-0035, that is the addition of:

- Organisational Security Policy

TPG0214B_VIC_18Jul11

- Assumptions

- Security Objectives for the TOE

- Security Functional Requirements for the TOE

52   Do not affect the conformance claim of this Security Target. The Rationale for the additions is given in section 6 and section 7 of the full Security Target.

53   For each addition the appropriate section clearly shows the addition, that is, section 3, Section 4 and section 6.

54   Although the PP recommends a EAL4 certification level with augmentations, the TOE claims an EAL5 plus certification level. This ST maintains the conformance to BSI-PP-0035, the rationale for this is given in section 6.2.1.

55   All the Protection Profile requirements have been shown to be satisfied.

3 Security Problem Definition

56   This chapter describes the security aspects of the environment in which the TOE is intended to be used. As this security target is conformant to BSI-PP-0035, this section contains only the relevant details and a summary where applicable. For complete details refer to the Protection Profile.

3.1 Description of Assets

Assets regarding the Threats

57   The assets (related to standard functionality) to be protected are

- the User Data
- the Security IC Embedded Software, stored and in operation
- the security services provided by the TOE for the Security IC Embedded Software

58   The user (consumer) of the TOE places value upon the assets related to high-level security concerns:

SC1   integrity of User Data and of the Security IC Embedded Software (while being executed/processed and while being stored in the TOE's memories)

SC2   confidentiality of User Data and of the Security IC Embedded Software (while being processed and while being stored in the TOE's memories)

SC3   correct operation of the security services provided by the TOE for the Security IC Embedded Software

59   According to this Protection Profile there is the following high-level security concern related to security service:

SC4   deficiency of random numbers.

60   To be able to protect these assets the TOE shall protect its security functionality. Therefore critical information about the TOE shall be protected. Critical information includes:

- logical design data, physical design data, IC Dedicated Software, and configuration data

- Initialisation Data and Pre-personalisation Data, specific development aids, test and characterisation related data, material for software development support, and photomasks

Such information and the ability to perform manipulations assist in threatening the above assets.

3.2 Threats

61   The threats are listed in PP-BSI-0035, only a summary is provided in this Security target.

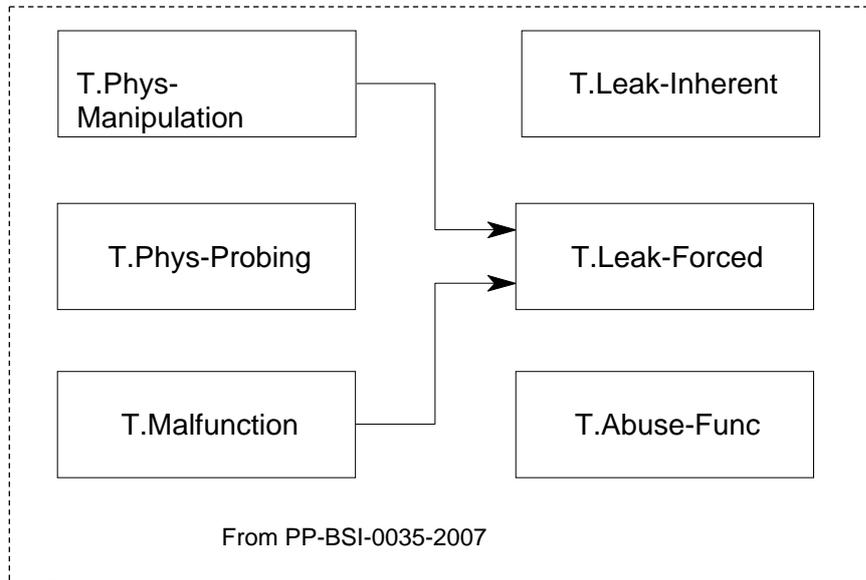62   The standard threats to the TOE are shown in Figure 5.

Figure 5: Standard Threats

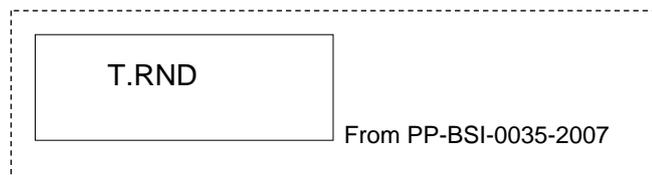63   The threats relating to specific security services are shown in Figure 6.

Figure 6: Threats related to security service

64   The Security IC Embedded Software may be required to contribute to preventing the threats. At least it must not undermine the security provided by the TOE. For detail refer to the assumptions regarding the Security IC Embedded Software specified in Section 3.4

65   The above security concerns are derived from considering the operational usage by the end-consumer (Phase 7) since

-    Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by assumptions and

TPG0214B_VIC_18Jul11

- the development and production environment starting with Phase 2 up to TOE Delivery are covered by an organisational security policy.

3.3 Organisational Security Policies

66   The following Figure 7 shows the policies applied in this Security Target.

<div style="text-align:center">

┌ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┐
│   │
│   ┌──────────────┐   │   ┌──────────────┐
│   │   │   │   │   │
│   │ P.Process-TOE│   │   │ P.Add-Functions│
│   │   │   │   │   │
│   └──────────────┘   │   └──────────────┘
│   │
│ From PP-BSI-0035-2007   │   From [AUG]
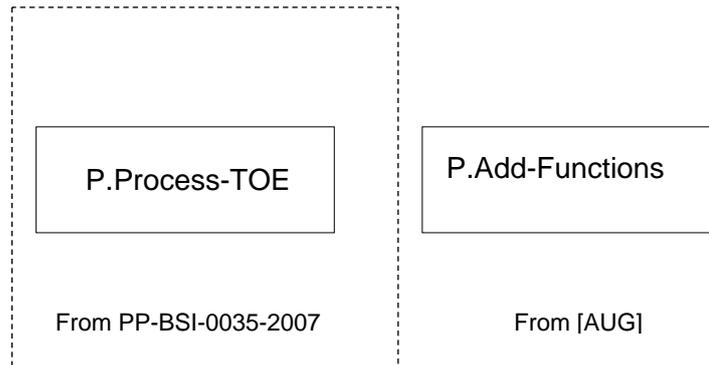└ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┘

</div>

Figure 7: Policies

67   The IC Developer / Manufacturer must apply the policy "Protection during TOE Development and Production (P.Process-TOE)" as specified below.

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.

68   The accurate identification is introduced at the end of the production test in phase 3. Therefore the production environment must support this unique identification.

69   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:

- TDES

- AES

- RSA without CRT

- RSA with CRT

- Miller Rabin algorithm

- EC-DSA

- ECDH

3.4 Assumptions

70   Full details of the assumptions are listed in PP-BSI-0035, only a summary is provided in this Security Target. Full details are given for the additional assumption taken from [AUG].

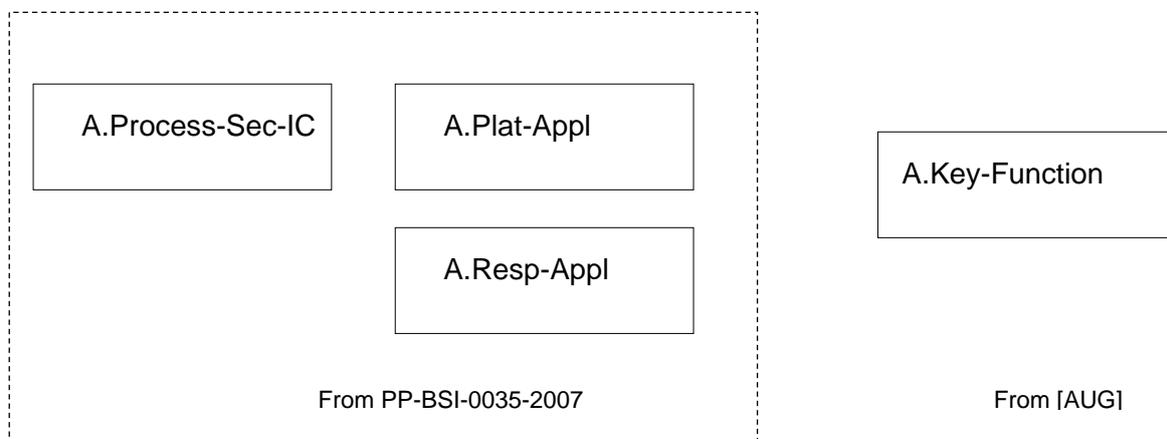71   The following Figure 8 shows the assumptions applied in this Security Target.

Figure 8: Assumptions

72   Appropriate "Protection during Packaging, Finishing and Personalisation (A.Process-Sec-IC)" must be ensured after TOE Delivery up to the end of Phase 6, as well as during the delivery to Phase 7 as specified below.

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 Section 1.4.3) are assumed to be protected appropriately. For a list of assets to be protected see below.

73   The information and material produced and/or processed by the Security IC Embedded Software Developer in Phase 1 and by the Composite Product Manufacturer can be grouped as follows:

- the Security IC Embedded Software including specifications, implementation and related documentation

TPG0214B_VIC_18Jul11

- pre-personalisation and personalisation data including specifications of formats and memory areas, test related data

- the User Data and related documentation

- material for software development support

74   The developer of the Security IC Embedded Software must ensure the appropriate "Usage of Hardware Platform (A.Plat-Appl)" while developing this software in Phase 1 as specified below.

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.

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

A.Resp-Appl   Treatment of User Data

All User Data is owned by the 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.

76   The developer of the Security IC Embedded Software must ensure the appropriate "Usage of key-dependent Functions (A.Key-Function)" while developing this software in Phase 1 as specified below.

A.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.

4 Security Objectives

77   The full details of the Security Objectives are listed in PP-BSI-0035, only a summary is provided in this Security target.

4.1 Security Objectives for the TOE

78   The user has the following standard high-level security goals related to the assets:

SG1   maintain the integrity of User Data and of the Security IC Embedded Software (when being executed/processed and when being stored in the TOE's memories) as well as

SG2   maintain the confidentiality of User Data and of the Security IC Embedded Software (when being processed and when being stored in the TOE's memories).

The Security IC may not distinguish between User Data which are public known or kept confidential. Therefore the security IC shall protect the confidentiality and integrity of the User Data, unless the Security IC Embedded Software chooses to disclose or modify it.

In particular, integrity of the Security IC Embedded Software means that it is correctly being executed which includes the correct operation of the TOE's functionality. Though the Security IC Embedded Software (normally stored in the ROM) will in many cases not contain secret data or algorithms, it must be protected from being disclosed, since for instance knowledge of specific implementation details may assist an attacker.

SG3   maintain the correct operation of the security services provided by the TOE for the Security IC Embedded Software.

79   These standard high-level security goals in the context of the security problem definition build the starting point for the definition of security objectives as required by the Common Criteria (refer to Figure 9). Note that the integrity of the TOE is a means to reach these objectives.

TPG0214B_VIC_18Jul11

```
O.Phys-
Manipulation          O.Leak-Inherent

O.Phys-Probing        O.Leak-Forced

O.Malfunction         O.Abuse-Func

                      O.Identification

From PP-BSI-0035-2007
```
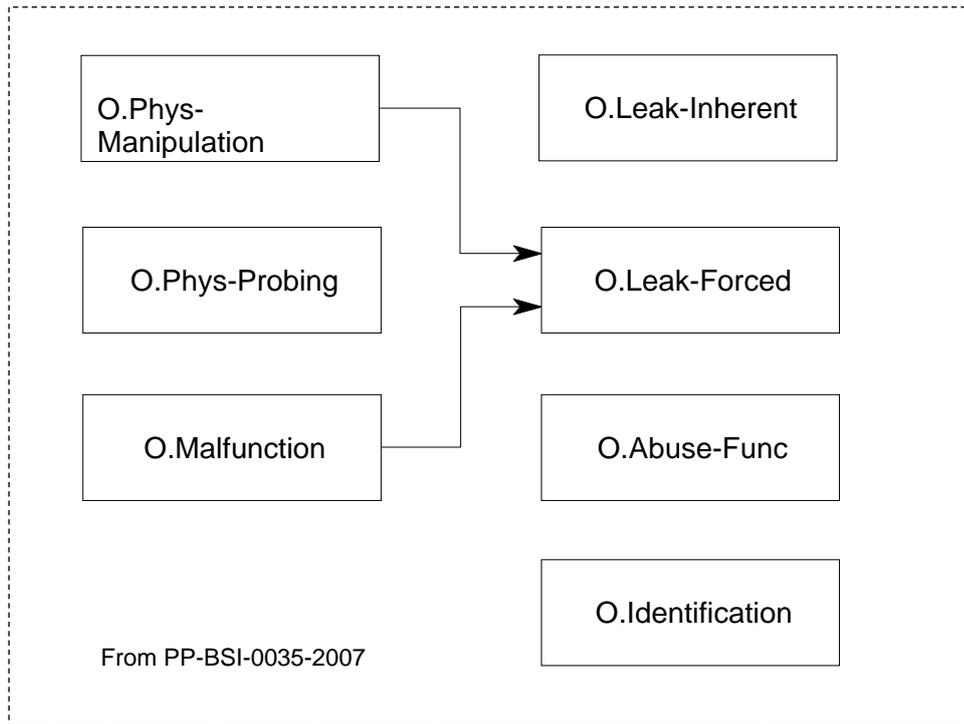
Figure 9: Standard Security Objectives

80   According to this Security Target there is the following high-level security goal related to specific functionality:

SG4   provide true random numbers.

81   The additional high-level security considerations are refined below by defining security objectives as required by the Common Criteria (refer to Figure 10).
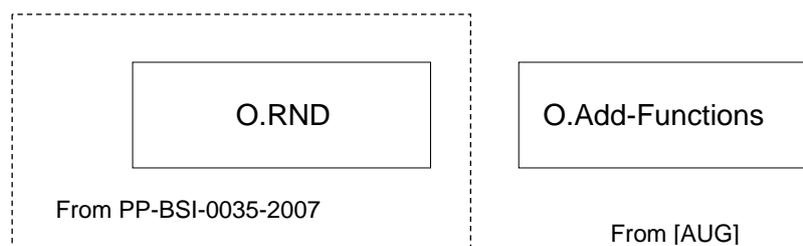


```
O.RND                 O.Add-Functions

From PP-BSI-0035-2007    From [AUG]
```

Figure 10: Security Objectives related to Specific Functionality

TPG0214B_VIC_18Jul11

Security Objectives related to Specific Functionality (referring to SG4)

82   The TOE shall provide "Additional Specific Security Functionality (O.Add-Functions)" [AUG] as specified below.

O.Add-Functions   Additional Specific Security Functionality

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

- TDES

- AES

- RSA without CRT

- RSA with CRT

- Miller Rabin algorithm

- EC-DSA

- ECDH

4.2 Security Objectives for the Security IC Embedded Software development Environment

83   The development of the Security IC Embedded Software is outside the development and manufacturing of the TOE (cf. section 1.4.3). The Security IC Embedded Software defines the operational use of the TOE. This section describes the security objectives for the operational environment enforced by the Security IC Embedded Software.

Phase 1

84   The Security IC Embedded Software shall provide "Usage of Hardware Platform (OE.Plat-Appl)" as specified below.

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.

The TOE supports cipher schemes as additional specific security functionality. If required the Security IC Embedded Software shall use the 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
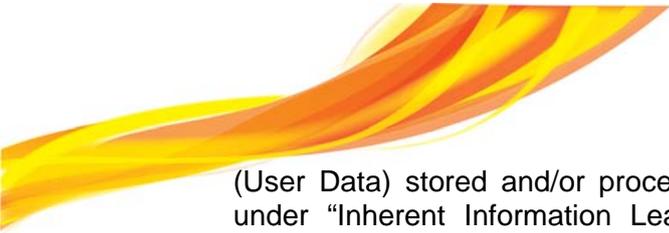
(User Data) stored and/or processed in the TOE by using the methods described under "Inherent Information Leakage (T.Leak-Inherent)" and "Forced Information Leakage (T.Leak-Forced)" [AUG].

85   The Security IC Embedded Software shall provide "Treatment of User Data (OE.Resp-Appl)" as specified below.

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.

For example the Security IC Embedded Software will not disclose security relevant User Data to unauthorised users or processes when communicating with a terminal.

By definition, cipher or plain text data and cryptographic keys are User Data. The Security IC Embedded Software shall treat this 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 the 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, it must be ensured that it is not practical to derive the private key from a public key if asymmetric algorithms are used. 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 [AUG].

4.3 Security Objectives for the operational Environment

TOE Delivery up to the end of Phase 6

86   Appropriate "Protection during Packaging, Finishing and Personalisation (OE.Process-Sec-IC)" must be ensured after TOE Delivery up to the end of Phases 6, as well as during the delivery to Phase 7 as specified below.

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 1.4.3) must be protected appropriately. For a preliminary list of assets to be protected refer to (Section 3.4, A.Process-Sec-IC).

4.4 Security Objectives Rationale

87   Table 1 below shows how the assumptions, threats, and organisational security policies are addressed by the objectives. The text following after the table justifies this in detail.

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
A.Plat-Appl	OE.Plat-Appl	Phase 1
A.Resp-Appl	OE.Resp-Appl	Phase 1
A.Key-Function	OE.Resp-Appl	Phase 1
P.Process-TOE	O.Identification	Phase 2 – 3 optional Phase 4
A.Process-Sec-IC	OE.Process-Sec-IC	Phase 5 – 6 optional Phase 4
T.Leak-Inherent	O.Leak-Inherent	
T.Phys-Probing	O.Phys-Probing	
T.Malfunction	O.Malfunction	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Forced	O.Leak-Forced	
T.Abuse-Func	O.Abuse-Func	
T.RND	O.RND	
P.Add-Functions	O.Add-Functions	

Table 1: Security Objectives versus Assumptions, Threats or Policies

88   The justification related to the assumption "Usage of Hardware Platform (A.Plat-Appl)" is as follows:

89   Since OE.Plat-Appl requires the Security IC Embedded Software developer to implement those measures assumed in A.Plat-Appl, the assumption is covered by the objective.

90   The justification related to the assumption "Usage of Key-dependent Functions (A.Key-Function)" is as follows:

91   Since OE.Plat-Appl requires the Security IC Embedded Software developer to implement those measures assumed in A.Key-Function, the assumption is covered by the objective.

92   The justification related to the assumption "Treatment of User Data (A.Resp-Appl)" is as follows:

93   Since OE.Resp-Appl requires the developer of the Security IC Embedded Software to implement measures as assumed in A.Resp-Appl, the assumption is covered by the objective.

94   The justification related to the organisational security policy "Protection during TOE Development and Production (P.Process-TOE)" is as follows:

95   O.Identification requires that the TOE has to support the possibility of a unique identification. The unique identification can be stored on the TOE. Since the unique identification is generated by the production environment, it must support the integrity of the generated unique identification. The technical and organisational security measures that ensure the security of the development environment and production environment are evaluated based on the assurance measures that are part of the evaluation. For a list of material produced and processed by the TOE Manufacturer refer to paragraph 60. All listed items and the associated development and production environments are subject of the evaluation. Therefore, the organisational security policy P.Process-TOE is covered by this objective, as far as organisational measures are concerned.

96   The justification related to the assumption "Protection during Packaging, Finishing and Personalisation (A.Process-Sec-IC)" is as follows:

97   Since OE.Process-Sec-IC requires the Composite Product Manufacturer to implement those measures assumed in A.Process-Sec-IC, the assumption is covered by this objective.

98   The justification related to the threats "Inherent Information Leakage (T.Leak-Inherent)", "Physical Probing (T.Phys-Probing)", "Malfunction due to Environmental Stress (T.Malfunction)", "Physical Manipulation (T.Phys-Manipulation)", "Forced Information Leakage (T.Leak-Forced)", "Abuse of Functionality (T.Abuse-Func)" and "Deficiency of Random Numbers (T.RND)" is as follows:

99   For all threats the corresponding objectives (refer to Table 1) are stated in a way that directly corresponds to the description of the threat (refer to Section 3.2). It is clear from the description of each objective (refer to Section 4.1), that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds.

100   The justification related to the security objective "Additional Specific Security Functionality (O.Add-Functions)" is as follows:

101   Since O.Add-Functions requires the TOE to implement exactly the same specific security functionality as required by P.Add-Functions, the organizational security policy is covered by the objective.

102   Nevertheless the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality required by P.Add-Functions (Note that these objectives support that the specific security functionality is provided in a secure way as expected from P.Add-Functions). Especially O.Leak-Inherent and O.Leak-Forced refer to the protection of confidential data (User Data or TSF Data (section 7.1) in general. User Data are also processed by the specific security functionality required by P.Add-Functions.

103   The following text gives details of the clarification added to OE.Plat-Appl. If required
the Security IC Embedded Software shall use these cryptographic services of the
TOE and their interface as specified. In addition, the Security IC Embedded Software
must implement functions which perform operations on keys (if any) in such a manner
that they do not disclose information about confidential data. This addition ensures
that the assumption A.Plat-Appl is still covered by the objective OE-Plat-Appl
although additional functions are being supported according to O.Add-Functions.

104   The following text gives details of the clarification added to OE.Resp-Appl. By
definition cipher or plain text data and cryptographic keys, are defined as User Data.
So, the Security IC Embedded Software will protect such data if required and use
keys and functions appropriately in order to ensure the strength of cryptographic
operation. Strength and confidentiality must be maintained for keys that are imported
and/or derived from other keys. This implies that appropriate key management has to
be realised in the environment. These measures make sure that the assumption
A.Resp-Appl is still covered by the security objective OE.Resp-Appl although
additional functions are being supported according to P.Add-Functions.

105   The justification of the additional policy (P.Add-Functions) and assumption (A.Add-
Functions) do not contradict the rationale already given in the Protection Profile for
assumptions, policy and threats defined in the PP and within this Security Target.

5 Extended Components Definition

106   The extended components:

- FCS_RNG.1

- FMT_LIM.1

- FMT_LIM.2

- FAU_SAS.1

107   Are defined within the Protection Profile [PP] that this Security Target is strictly conformant to.

6 IT Security Requirements

108   The standard Security Requirements are shown in Figure 11. These security components are listed and explained below.
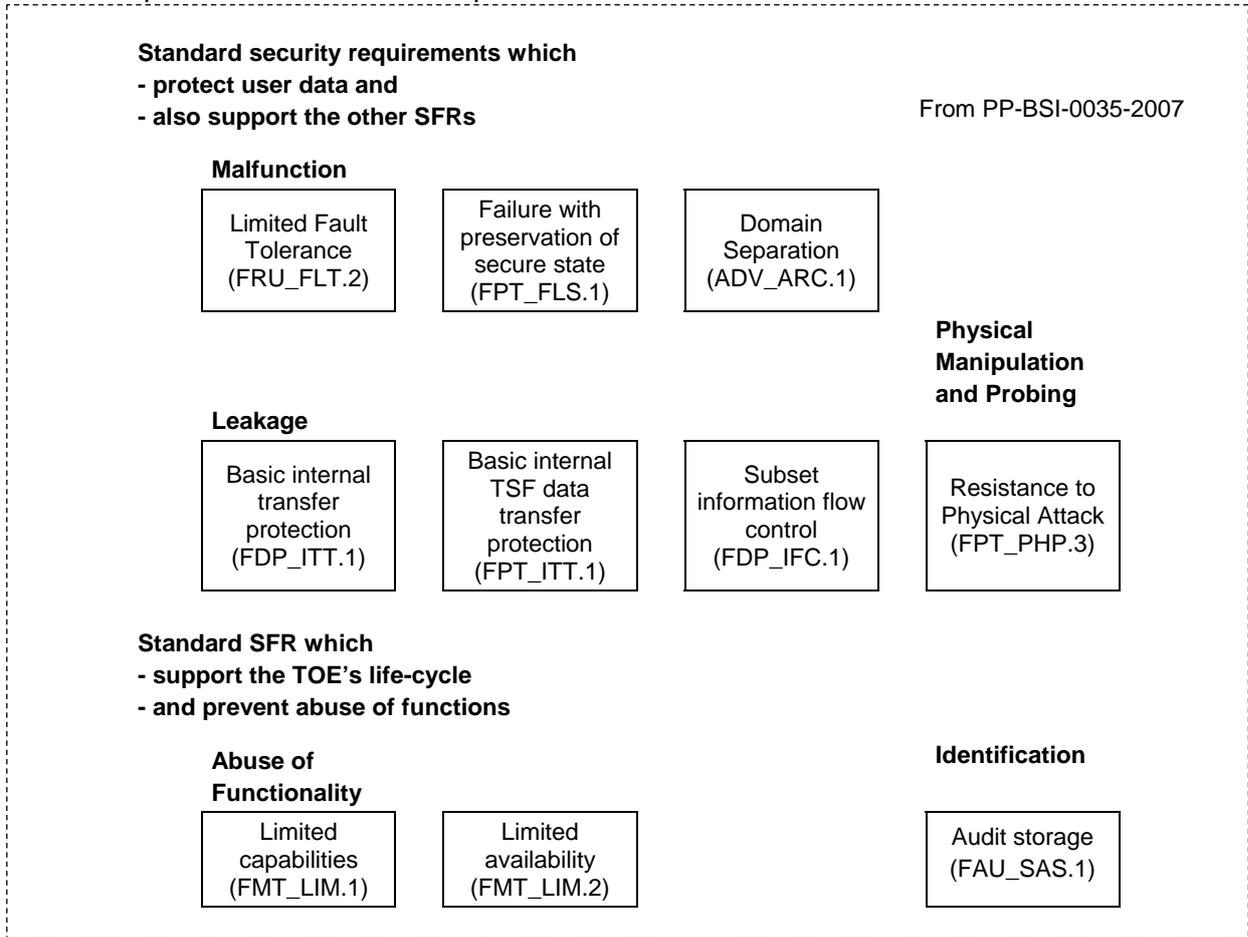
Standard security requirements which
- protect user data and
- also support the other SFRs

From PP-BSI-0035-2007

Malfunction

Limited Fault Tolerance (FRU_FLT.2)	Failure with preservation of secure state (FPT_FLS.1)	Domain Separation (ADV_ARC.1)

Physical Manipulation and Probing

Leakage

Basic internal transfer protection (FDP_ITT.1)	Basic internal TSF data transfer protection (FPT_ITT.1)	Subset information flow control (FDP_IFC.1)	Resistance to Physical Attack (FPT_PHP.3)

Standard SFR which
- support the TOE's life-cycle
- and prevent abuse of functions

Abuse of Functionality

Identification

Limited capabilities (FMT_LIM.1)	Limited availability (FMT_LIM.2)	Audit storage (FAU_SAS.1)

Figure 11: Standard Security Requirements

109   The Security Functional Requirements related to Specific Functionality are shown in Figure 12. These security functional components are listed and explained below.

Standard SFR related to Specific Functionality

Random Numbers   From PP-BSI-0035-2007   From [AUG]   **Cryptography**

Random Number Generation (FCS_RNG.1)	Cryptographic Operation (FCS_COP.1)
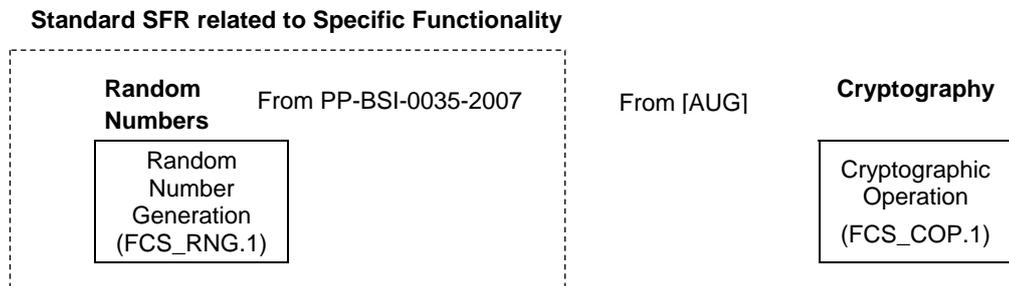
Figure 12: Security Functional Requirements related to Specific Functionality

6.1 Security Functional Requirements for the TOE

110 In order to define the Security Functional Requirements Part 2 of the Common Criteria was used. However, some Security Functional Requirements have been refined (please refer to the Protection Profile [PP]).

Malfunctions

111 The TOE shall meet the requirement "Limited fault tolerance (FRU_FLT.2)" as specified below.

FRU_FLT.2	Limited fault tolerance
Hierarchical to:	FRU_FLT.1 Degraded fault tolerance
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)*** [c]**.**
Dependencies:	FPT_FLS.1 Failure with preservation of secure state.

112 The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below.

FPT_FLS.1	Failure with preservation of secure state
Hierarchical to:	No other components.
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*** [d]**.**
Dependencies:	No dependencies.
Refinement:	**The term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.**

---

[c]   The TOE operates in a stable way within this operating window, this is verified during the development and manufacturing phase of the life cycle. This is verified by the ITSEF during the ATE Assurance Class analysis.

[d]   TSF_AUDIT_ACTION details the operating conditions that are not tolerated by the TOE. The TOE takes action through TSF_AUDIT_ACTION to ensure the TOE fails in a secure state.

Abuse of Functionality

113   The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.1	Limited capabilities
Hierarchical to:	No other components.
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[e].***
Dependencies:	FMT_LIM.2 Limited availability.

114   The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.2	Limited availability
Hierarchical to:	No other components.
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[f].***
Dependencies:	FMT_LIM.1 Limited capabilities.

115   The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria Part 2 extended).

FAU_SAS.1	Audit storage
Hierarchical to:	No other components.
Dependencies:	No dependencies.

---

[e]   TSF_TEST details the Limited capability and availability policy.

[f]   TSF_TEST details the Limited capability and availability policy.

FAU_SAS.1.1 The TSF shall provide **the test process before TOE Delivery**[g] with the capability to store **the Initialisation Data and/or Pre-personalisation Data and/or supplements of the Security IC Embedded Software**[h] in the **Non-Volatile Memory**.

Physical Manipulation and Probing

116 The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below.

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** [i] to the **TSF**[j] 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.**

---

[g] The code entry process allows the Security IC Embedded Software developer to deliver pre-personalisation data, details are given in the smartACT manual [ACT]. Some configuration of the TOE is allowed using the [COF].

[h] The Security IC Embedded Software Developer may deliver data during the code entry process [ACT].

[i] Direct Probing, manipulation by operating the TOE, out with the specified operating conditions [TD].

[j] The TSF are detailed in TOE Summary Specification Section.

TPG0214B_VIC_18Jul11

Leakage

117   The TOE shall meet the requirement "Basic internal transfer protection (FDP_ITT.1)" as specified below.

      FDP_ITT.1   Basic internal transfer protection

      Hierarchical to: No other components.

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

      Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

      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.**

118   The TOE shall meet the requirement "Basic internal TSF data transfer protection (FPT_ITT.1)" as specified below.

      FPT_ITT.1   Basic internal TSF data transfer protection

      Hierarchical to: No other components.

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

      Dependencies: No dependencies.

      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.**

This requirement is equivalent to FDP_ITT.1 above but refers to TSF data instead of User Data. Therefore, it should be understood as to refer to the same **Data Processing Policy** defined under FDP_IFC.1 below.

119   The TOE shall meet the requirement " Subset information flow control (FDP_IFC.1)" as specified below:

      FDP_IFC.1   Subset information flow control

      Hierarchical to: No other components.

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

---

[a]   The user of this document should refer to TSF_LEAK_PROTECT for the SFP: Data Processing Policy

Dependencies: FDP_IFF.1 Simple security attributes

120 The following Security Function Policy (SFP) **Data Processing Policy** is defined for the requirement " Subset information flow control (FDP_IFC.1)":

User Data and TSF data shall not be accessible from the TOE except when the Security IC Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security IC Embedded Software.

Random Numbers (Applicable to the Secure Core True RNG)

121 The TOE shall meet the requirement "Quality metric for random numbers (FCS_RNG.1)" as specified below (Common Criteria Part 2 extended).

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, and online test capability* .
FCS_RNG.1.2	The TSF shall provide random numbers that meet *AIS31 Class P2 quality metric.*
Dependencies:	No dependencies.

Random Numbers (Applicable to the Master Core Deterministic RNG)

122 The TOE shall meet the requirement "Quality metric for random numbers (FCS_RNG.1)" as specified below (Common Criteria Part 2 extended).

FCS_RNG.1	Random number generation
Hierarchical to:	No other components.
FCS_RNG.1.1	The TSF shall provide a *deterministic* random number generator that implements *hardware post processing, and total failure test of the random source.*
FCS_RNG.1.2	The TSF shall provide random numbers that meet *AIS20 Class K4 High quality metric.*

---

[a] The user of this document should refer to TSF_LEAK_PROTECT for the SFP: Data Processing Policy

[b] The sensitive information that must be protected includes information when transferred from one memory location to another by the user or Security IC Embedded Software or being operated on by the hardware processors. This information must be protected as it would allow an attacker to gain knowledge of the functions of the TOE TSF, or gain access to cryptographic key information.

TPG0214B_VIC_18Jul11

Dependencies: No dependencies.
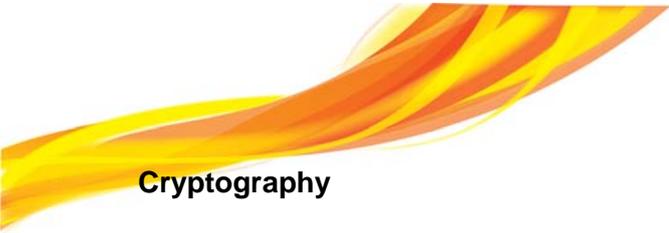
Cryptography

123   The TOE shall meet the requirement "Cryptographic Operation (FCS_COP.1)" as specified below.

FCS_COP.1	Cryptographic operation
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform **hardware TDES encryption and decryption** in accordance with a specified cryptographic algorithm: **triple Data Encryption Standard (TDES)** and cryptographic key sizes: **112-bit cryptographic key sizes** that meet the following: **E-D-E two-key triple-encryption implementation of the Data Encryption Standard, FIPS PUB 46-3, 25th October 1999[a].**
Dependencies:	(FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction

FCS_COP.1	Cryptographic operation
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform **hardware AES encryption and decryption** in accordance with a specified cryptographic algorithm: **Advanced Encryption Standard (AES)** and cryptographic key sizes: **128-bit, 192-bit and 256-bit cryptographic key sizes** that meet the following: **FIPS 197 November 26, 2001.**
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

---

[a]   E-D-E =The simplest variant of TDES operates as follows: DES(k3;DES(k2;DES(k1;M))), where M is the message block to be encrypted and k1, k2, and k3 are DES keys. This variant is commonly known as EEE because all three DES operations are encryptions. In order to simplify interoperability between DES and TDES the middle step is usually replaced with decryption (EDE mode): DES(k3;DES - 1(k2;DES(k1;M))) and so a single DES encryption with key k can be represented as TDES-EDE with k1 = k2 = k3 = k. The choice of decryption for the middle step does not affect the security of the algorithm.

TPG0214B_VIC_18Jul11

FCS_COP.1   Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1   The TSF shall perform *data signing* in accordance with a specified cryptographic algorithm: *SHA-1* and cryptographic key sizes: *no cryptographic key size* that meet the following: *Secure Hash Standard, FIPS 180-2, 2002 August 1.*

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

FCS_COP.1   Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1   The TSF shall perform *data signing* in accordance with a specified cryptographic algorithm: *SHA-224* and cryptographic key sizes: *no cryptographic key size* that meet the following: *Secure Hash Standard, FIPS 180-2, 2002 August 1.*

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

FCS_COP.1   Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1   The TSF shall perform *data signing* in accordance with a specified cryptographic algorithm: *SHA-256* and cryptographic key sizes: *no cryptographic key size* that meet the following: *Secure Hash Standard, FIPS 180-2, 2002 August 1.*

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

FCS_COP.1   Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1   The TSF shall perform *data encryption and decryption* in accordance with a specified cryptographic algorithm: *RSA without CRT* and cryptographic key sizes: *between 96 bits and 2624 bits* that meet the following: *PKCS#1 V2.0, 1st October, 1998.*

Dependencies: (FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or

TPG0214B_VIC_18Jul11

FCS_CKM.1 Cryptographic key generation)
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1   Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1   The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm: **RSA with CRT data** and cryptographic key sizes: **between 192 bits and 3520 bits** that meet the following: **PKCS#1 V2.0, 1st October, 1998.**

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

FCS_COP.1   Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1   The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm: **EC-DSA** and cryptographic key sizes: **between 192 bits and 521 bits** that meet the following: **FIPS 186-2, 27th January, 2007 for Digital signatures.**

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

FCS_COP.1   Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1   The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm: **ECDH** and cryptographic key sizes: **between 192 bits and 521 bits** that meet the following: **ISO 15946-3:2002 for ECDH standard.**

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

6.2 Security Assurance Requirements for the TOE

124   This Security Target is evaluated according to

125   Security Target evaluation (Class ASE)

126   The "Security Assurance Requirements for the TOE", for the evaluation of the Algol
        TOE are those taken from the

        Evaluation Assurance Level 5 (EAL5)

and augmented by taking the following components:

        ALC_DVS.2, and AVA_VAN.5.

127   The assurance requirements are (augmentation from EAL5+ highlighted)

Class ADV: Development
Architectural design	(ADV_ARC.1)
Functional specification	(ADV_FSP.5)
Implementation representation	(ADV_IMP.1)
Well-structured internals	(ADV_INT.2)
TOE design	(ADV_TDS.4)

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.5)
Delivery	(ALC_DEL.1)
Development security	(ALC_DVS.2)
Life-cycle definition	(ALC_LCD.1)
Tools and techniques	(ALC_TAT.2)

Class ASE: Security Target evaluation
Conformance claims	(ASE_CCL.1)
Extended components definition	(ASE_ECD.1)
ST introduction	(ASE_INT.1)
Security objectives	(ASE_OBJ.2)
Derived security requirements	(ASE_REQ.2)
Security problem definition	(ASE_SPD.1)
TOE summary specification	(ASE_TSS.1)

Class ATE: Tests
Coverage	(ATE_COV.2)
Depth	(ATE_DPT.3)
Functional tests	(ATE_FUN.1)

Independent testing   (ATE_IND.2)
Class AVA: Vulnerability assessment
Vulnerability analysis   (AVA_VAN.5)

6.2.1 Refinements of the TOE Assurance Requirements

128   The Protection Profile BSI-PP-0035 defines refinements to the Security Assurance requirements defined in CC V3.1 Part 3. The TOE is assessed to EAL5 Level with additional augmentations which are taken into account in this analysis.

129   The [PP] allows the TOE to be evaluated above the EAL4+ requirements given in the [PP], therefore the fact that this Security Target is assessed to EAL5 level, it still maintains the conformance claim to [PP]. The refinements stated in [PP] remain consistent with the EAL5 package claims of this Security Target.

6.3 Security Requirements Rationale

6.3.1 Rationale for the security functional requirements

130   Table 2 below gives an overview of how the security functional requirements are combined to meet the security objectives. The detailed justification follows after the table.

Objective	TOE Security Functional and Assurance Requirements
O.Leak-Inherent	- FDP_ITT.1 "Basic internal transfer protection" - FPT_ITT.1 "Basic internal TSF data transfer protection" - FDP_IFC.1 "Subset information flow control"
O.Phys-Probing	- FPT_PHP.3 "Resistance to physical attack"
O.Malfunction	- FRU_FLT.2 "Limited fault tolerance - FPT_FLS.1 "Failure with preservation of secure state"
O.Phys-Manipulation	- FPT_PHP.3 "Resistance to physical attack"
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

Objective	TOE Security Functional and Assurance Requirements
O.Abuse-Func	- FMT_LIM.1 "Limited capabilities" - FMT_LIM.2 "Limited availability" 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 "Audit storage"
O.RND	- FCS_RNG.1 "Quality metric for random numbers" 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.Add-Functions	- FCS_COP.1 "Cryptographic Operation"
OE.Plat-Appl	not applicable
OE.Resp-Appl	not applicable
OE.Process-Sec-IC	not applicable

Table 2: Security Requirements versus Security Objectives

131   It should be noted by the user of this Security Target Lite that the justification related to the security objective "Random Numbers (O.RND)" contains the following note:

132   Depending on the functionality of the TOE the Security IC Embedded Software will have to support the objective by providing runtime-tests of the random number generator (for instance by implementing FPT_AMT.1). Together, these requirements allow the TOE to provide cryptographically good random numbers and to ensure that no information about the produced random numbers is available to an attacker.

133   It should be noted by the user of this Security Target Lite that the justification related to the security objective "Additional Specific Security Functionality" (O.Add-Functions)" contains the following note:

134   Depending on the functionality of the end composite device the Security IC Embedded Software will have to support the objective by using the additional functions as specified by the [CC]. The user data processed by the functions relating to FCS_COP.1 is protected as defined for the end application. The Embedded Software will have to support the objective O.Add-Functions by implementing the security functional requirements below:

- [FDP_ITC.1 Import of User data without security attributes or FDP_ITC.2 import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]

- FCS_CKM.4 Cryptographic key destruction

6.3.2 Dependencies of security functional requirements

135   Table 3 below lists the security functional requirements defined in this Security Target, their dependencies and whether they are satisfied by other security requirements defined in this Security Target. The text following the table discusses the remaining cases.

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this PP
FRU_FLT.2	FPT_FLS.1	Yes
FPT_FLS.1	None	No dependency
FMT_LIM.1	FMT_LIM.2	Yes
FMT_LIM.2	FMT_LIM.1	Yes
FAU_SAS.1	None	No dependency
FPT_PHP.3	None	No dependency
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes
FDP_IFC.1	FDP_IFF.1	See discussion below
FPT_ITT.1	None	No dependency
FCS_RNG.1	None	No dependency
FCS_COP.1	FDP_ITC.1 or FCS_ITC.2 or FCS_CKM.1 FCS_CKM.4	See discussion below

Table 3: Dependencies of the Security Functional Requirements

TPG0214B_VIC_18Jul11

7 TOE Summary Specification

136   This section demonstrates how the TOE matches the Security Functional requirements as detailed in section 6.1 (Security functional Requirements).

137   It gives a description of the TSF elements of the TOE to allow an understanding of how the security of the TOE matches the SFR of section 6.1, and also how they TOE protects itself against tampering, interfering and bypass of the TSF Features of the TOE.

7.1   Description of TSF Features of the TOE

7.1.1 TSF_TEST Test Interface

- Test Mode (TME)

- Serial Number Registers Write

- Test Mode Disable (User Mode)

- Package Mode (PME)

138   The TOE has two engineering test modes Test Mode (TME) and Package Mode (PME).

139   **Test Mode Entry:** TME is protected by a Test mode entry condition and is only accessible to authenticated test engineers.

140   **Serial Number Register Write:** In test mode it is possible to store pre-personalisation data etc, also the serial number information is written at this time.

141   **Test Mode Disable:** TME is permanently disabled by wafer saw.

142   **Package Mode Entry:** The TOE also offers another test mode called Package Mode (PME), this is considered as a subset of TME, it does not offer the full access to the various memories, as is allowed in TME. On entry into Package mode a full NVM erase is performed, to further protect any sensitive data stored in the TOE. PME is protected by entry conditions.

SFP: Limited capability and availability Policy	The TOE Test features are only available to authenticated Inside Secure engineers with the knowledge of the Test Mode Entry and Package Mode Entry sequence. Once the wafer is sawn Test Mode is not available. A subset of the Test Mode features is available after TEST Mode Disable, but only to authenticated users with the knowledge of the Package Mode Entry Sequence.

143

TPG0214B_VIC_18Jul11

7.1.1.1 SFR to TSF Test Interface

```
┌──────────────────┐      ┌────────────────────────┐
│ Abuse of         │─────▶│ FMT_LIM.1 Limited      │────┐
│ Function         │      │ Capabilities           │    │
│                  │      └────────────────────────┘    │   ╭──────────────────────╮
│                  │─────▶┌────────────────────────┐    ├──▶│ TSF_TEST             │
└──────────────────┘      │ FMT_LIM.2 Limited      │────┘   │                      │
                          │ Availability           │        │ Test Interface       │
                          └────────────────────────┘        │                      │
┌──────────────────┐      ┌────────────────────────┐        ╰──────────────────────╯
│ Identification   │─────▶│ FAU_SAS.1 Audit        │
│                  │      │ Storage                │
└──────────────────┘      └────────────────────────┘
```
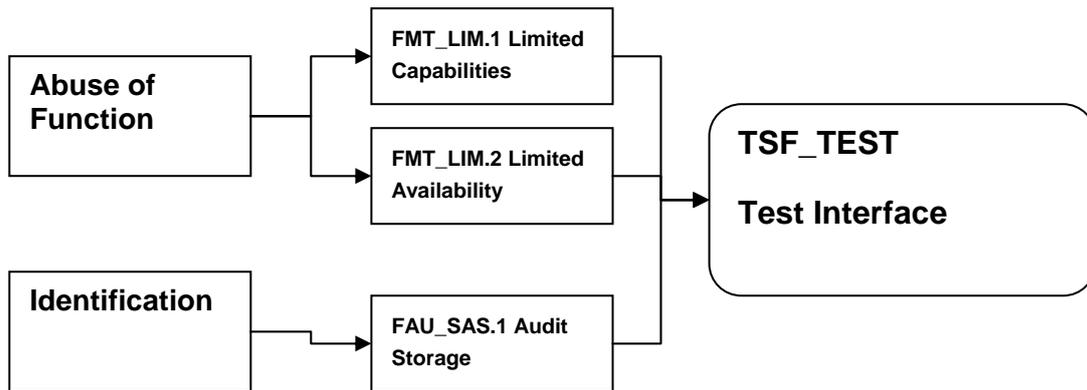
7.1.2 TSF_ENV_PROTECT Environmental Protection

- Hardware Protection (Active Shield)

- Voltage Monitor

- Frequency Monitor

- Temperature Monitor

- Light Scan Detector

- Memory Encryption (Scramblers)

- Bus Encryption [a]

- Structure and Layout[b]

144   **Hardware Protection:** The TOE has an active shield that covers the top of the chip, this provides tamper evidence protection, if violated a flag is raised.

145   **Voltage Monitor:** The power supply lines to the TOE are monitored to protect the TOE from the supply going out of bounds.

146   **Frequency Monitor:** The external clock is monitored to protect the TOE from the frequency going out of bounds.

147   **Temperature Monitor:** The operating temperature of the TOE is monitored to prevent the TOE from being operated out-with the correct operating conditions.

148   **Light Scan Detector:** The TOE provides a Light scan Detector (LSD) to protect against laser (or focused light) scanning of the TOE.

---

[a]   The security mechanism **Bus Encryption** utilises the layout process of the design. This mechanism has no TSFI.

[b]   The security mechanism **Structure and Layout** utilises the TOE design technology, and the layout process of the design. This mechanism has no TSFI.

149 **Memory encryption:** The memories are encrypted also the secure Twincore register file is encrypted.

150 **Bus Encryption:** Layout structures are implemented to make internal bus probing difficult. The TOE contains no visible bus structures.

151 **Structure and Layout:.** This provides complexity to any attack that involves identifying specific areas of the TOE.

7.1.2.1 SFR to TSF_ENV_PROTECT

```
┌───────────────┐      ┌───────────────┐
│   Physical    │      │   FPT_PHP.3   │
│ Manipulation  │─────▶│  Resistance to│              ┌────────────────────┐
│  and Probing  │      │Physical Attacks│             │  TSF_ENV_PROTECT   │
└───────────────┘      └───────────────┘              │                    │
                                                      │    Environmental   │
┌───────────────┐      ┌───────────────┐              │     Protection     │
│  Malfunction  │─────▶│ FRU_FLT.2 Limited│           └────────────────────┘
│               │      │  Fault Tolerance │
└───────────────┘      └───────────────┘
```
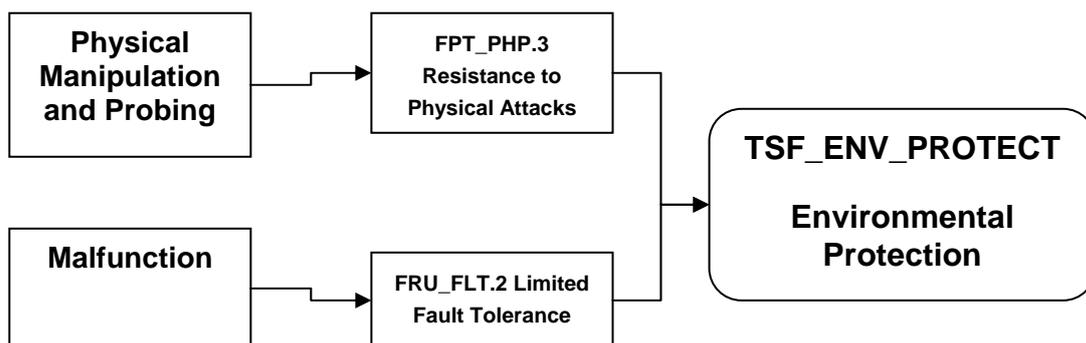
7.1.3 TSF_LEAK_PROTECT Leakage Protection

- Internal Clock (VFO)

- VFO Jitter

- Dummy Interrupt

- Dummy Instruction Generator

- Frequency Divider

- Power Scrambling

152 **Internal Clock:** The TOE provides an internal Variable Frequency Oscillator (VFO).

153 **VFO Jitter:** The VFO frequency offers variances of the frequency through time (Jitter), to help against side channel leakage analysis.

154 **Dummy Interrupt:** The TOE can trigger Dummy Interrupts.

155 **Dummy Instruction Generator:** The TOE can trigger Dummy instructions.

156 **Frequency Divider:** The VFO clock can be varied.

157 **Power Scrambling:** Power scrambling introduces a random component into the power signature of the chip.

SFP: Data Processing Policy	When processing or moving information within the TOE, the TOE should not leak any specific information that would allow an attacker to gain sufficient knowledge to gain access to secret information stored within the TOE memories.

7.1.3.1 SFR to TSF_LEAK_PROTECT
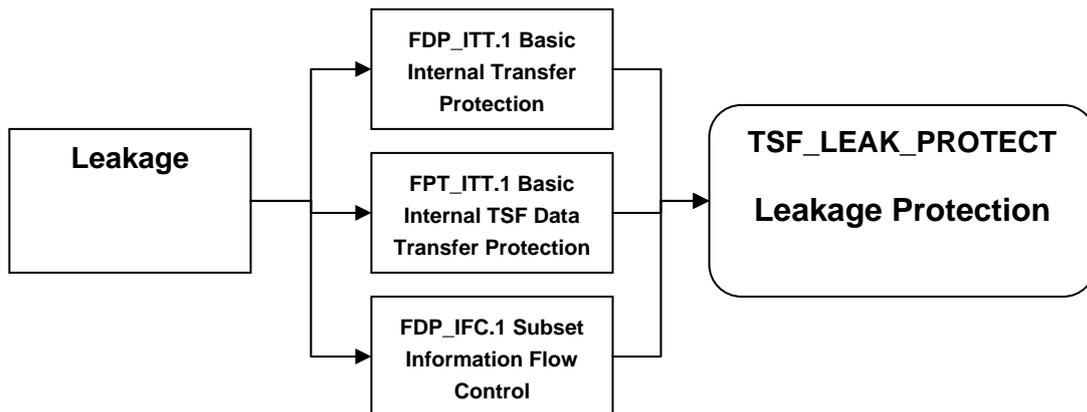
7.1.4 TSF_DATA_PROTECT Data Protection

- Secure Memory Management

- CRC / Checksum

- Code Signature Module

- Parity Checker ROM/RAM/Registers

- Register Mirroring

- Enhanced Protection Object (EPO) NVM

- CStack Checker

- SecureLink

- Glitch Detectors

158   **Secure Memory Management:** The TOE features a memory access protection mechanism.

159   **CRC / Checksum:** The TOE provides a Cyclic Redundancy Check (CRC32 or CRC16) and a Checksum Accelerator.

160   **Code Signature Module:** The TOE provides a Code Signature Module.

161   **Parity Checker ROM/RAM/Registers:** The TOE features parity checking on the ROM, RAM, and Twincore Registers.

162   **Register Mirroring:** Some of the internal security registers have been duplicated/mirrored.

163   **Enhanced Protection Object:** The NVM read is protected against attempted perturbations.

164   **CStack Checker:** The TOE provides a CStack Checker

165   **SecureLink:** The SecureLink interface between the Master Core (Black Domain) and Secure Core (Red Domain) only allows verified data to transfer.

166   **Glitch Detectors:** The Glitch Detectors can detect a glitch on the Vcc signal. This protects against attempted perturbations.

7.1.4.1 SFR to TSF_DATA_PROTECT
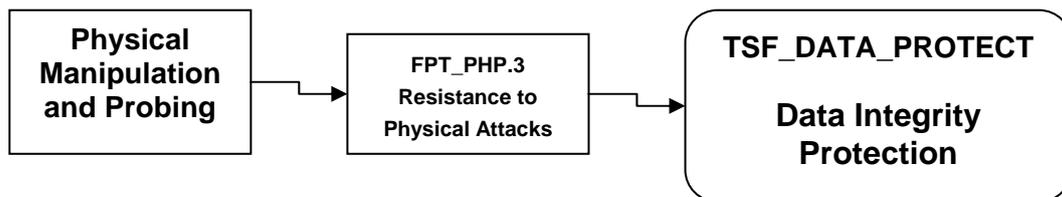
7.1.5 TSF_AUDIT_ACTION Event Audit and Action

- Reset System

- Security Registers

167   **Reset System:** The TOE allows the security IC Embedded Software to select the response the TOE makes to a security violation. The TOE has several modes when reacting to a security issue to ensure that the device fails in a safe mode.

168   **Security registers:** The TOE includes several registers to report failures (violations) detected by the security mechanisms of the TOE.

TPG0214B_VIC_18Jul11

7.1.5.1 SFR to TSF_AUDIT_ACTION
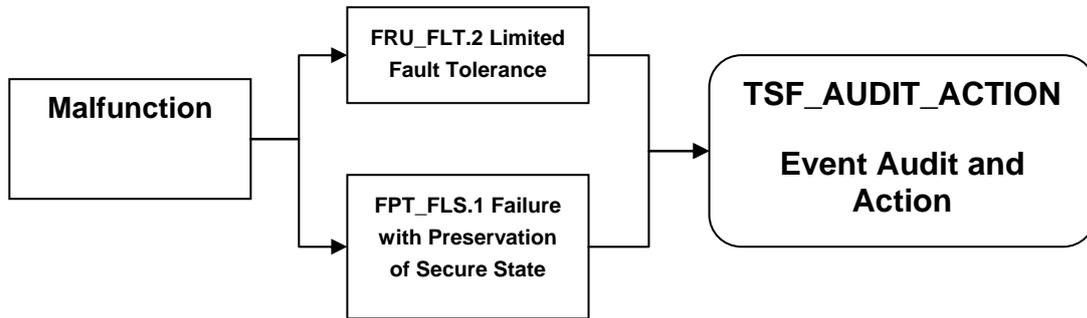
7.1.6 TSF_RNG Random Number Generator

- True RNG (only applicable to the Secure Core)

- Deterministic Number Generator (only Applicable to the Master Core)

- Random Number Total Failure Bit

- RNGDAS (only applicable to the Secure Core)

- RDWDR (applicable to both cores)

169   **True RNG:** The Secure Core has an analogue noise source that can be used to provide random numbers when required by the Security IC Embedded Software.

170   **Deterministic RNG:** The Master Core has a deterministic RNG that has hardware post processing.

171   **Random Number Total Failure Bit:** The TOE sets a flag if the analogue noise source fails.

172   **RNGDAS:** The Analogue Noise Source is sampled to create a digitized analogue source that is observable to the Security IC Embedded Software through the RNGDAS register.

7.1.6.1 SFR to TSF_RNG
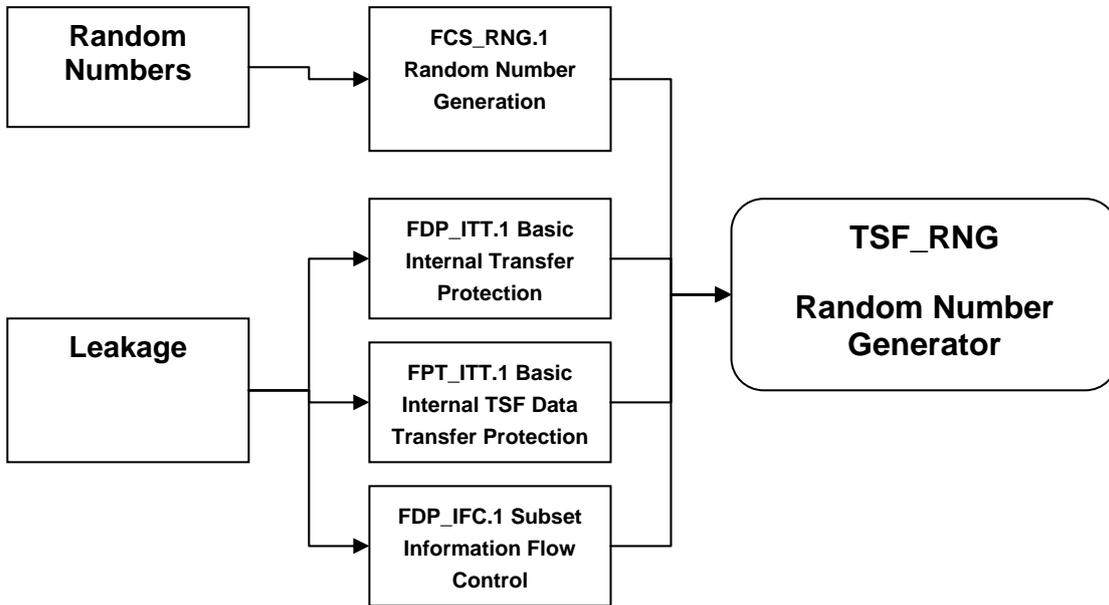
7.1.7 TSF_CRYPTO_HW Hardware Cryptography

- Hardware Triple DES

- Hardware AES

173 **Hardware Triple DES:** The TOE provides a hardware DES / TDES engine which enables fast cryptographic computations.

174 **Hardware AES:** The TOE provides a hardware AES encryption engine which enables fast cryptographic computations.

7.1.7.1 SFR to TSF_CRYPTO_HW

TPG0214B_VIC_18Jul11
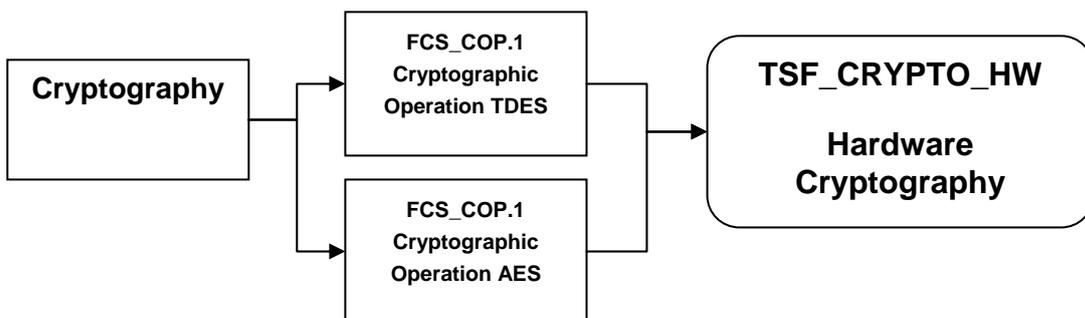
7.1.8 TSF_CRYPTO_SW Toolbox Cryptography

- AIS31 Online Test

- SHA

- RSA

- RSA with CRT

- PrimeGen (Miller Rabin)

- ECDSA

- EC-DH

- Self-Test

175 **AIS31 Online Test:** The TOE provides the ability to run online tests of the random numbers provided to the RNGDAS register.

176 **SHA:** The TOE provides Secure Hash data signing capability

177 **RSA:** The TOE provides RSA without CRT (Modular Exponentiation) data encryption decryption functions.

178 **RSA with CRT:** The TOE provides RSA with CRT data encryption decryption functions.

179 **PrimeGen:** The TOE provides RSA cryptographic key generation capability using Miller Rabin algorithm with confidence criteria (t parameter) between 0 and 255.

180 **EC-DSA:** The TOE provides EC-DSA Cryptographic capability

181 **ECDH:** The TOE provides ECDH Cryptographic capability

182 **Self-Test:** The TOE can perform a test of the crypto toolbox at the request of the Security IC Embedded Software

7.1.8.1 SFR to TSF_CRYPTO_SW

| Cryptography | → | FCS_COP.1 Cryptographic Operation | → | |
| Random Numbers | → | FCS_RNG.1 Random Number Generation | → | TSF_CRYPTO_SW Software Cryptography |
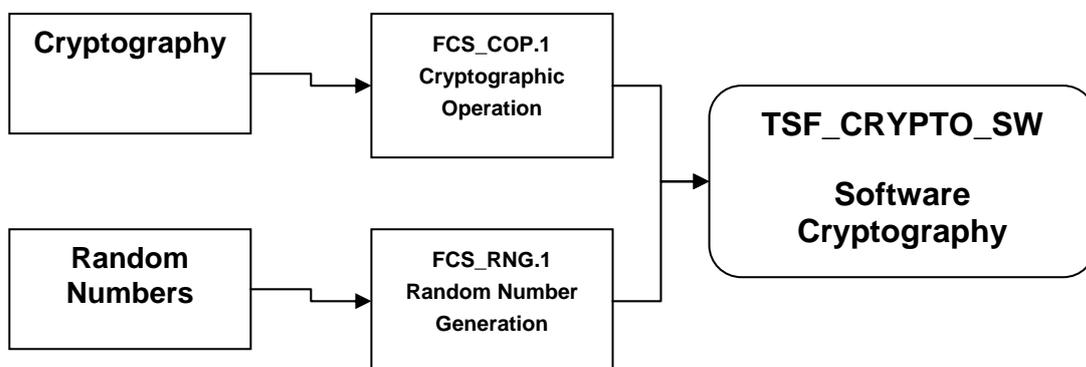
7.2 Rationale for TSF

183 This section demonstrates how the TSF contribute and work together to fulfil the SFR defined in section 6.

7.2.1 Summary of TSF to SFR

184 Table 4 gives an overview of the TSF that contribute to the SFRs.

		Security Functional Requirements										
		Malfunctions		**Leakage**			**Physical Manipulation and Probing**	**Abuse of Functionality**		**Identification**	**Random Number Generation**	**Cryptography**
		FRU_FLT.2	FPT_FLS.1	FDP_ITT.1	FPT_ITT.1	FDP_IFC.1	FPT_PHP.3	FMT_LIM.1	FMT_LIM.2	FAU_SAS.1	FCS_RNG.1	FCS_COP.1
TSF Features	TSF_TEST							X	X	X		
	TSF_ENV_PROTECT	X					X					
	TSF_LEAK_PROTECT			X	X	X						
	TSF_DATA_PROTECT						X					
	TSF_AUDIT_ACTION	X	X									
	TSF_RNG			X	X	X					X	
	TSF_CRYPTO_HW											X
	TSF_CRYPTO_SW										X	X

Table 4 Dependencies of the TOE Security Features

185 Table 5 Gives further details of how the SFR FCS_COP.1 relates to TSF_CRYPTO_HW and TSF_CRYPTO_SW.
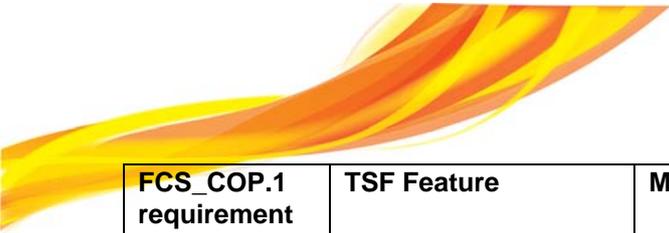
FCS_COP.1 requirement	TSF Feature	Mechanism	Note
TDES	TSF_CRYPTO_HW	Triple DES	The TOE has a TDES hardware engine and therefore is present independent of Toolbox
AES	TSF_CRYPTO_HW	AES	The TOE has an AES hardware engine and therefore is present independent of Toolbox
SHA-1	TSF_CRYPTO_SW	Secure Hash	
SHA-224	TSF_CRYPTO_SW	Secure Hash	
SHA-256	TSF_CRYPTO_SW	Secure Hash	
RSA without CRT	TSF_CRYPTO_SW	RSA Without CRT	
RSA with CRT	TSF_CRYPTO_SW	RSA with CRT	
EC-DSA	TSF_CRYPTO_SW	EC-DSA	
ECDH	TSF_CRYPTO_SW	ECDH	
N/A	TSF_CRYPTO_SW	Self test	This performs an integrity check on the Toolbox
N/A	TSF_CRYPTO_SW	AIS31 Online test	This online test for RNG data is provided to support the FCS_RNG.1 requirements

Table 5 Cryptographic Functions Overview

7.2.2 Note on ADV_ARC.1

186 The Assurance component ADV_ARC.1 states that the TOE should be self protected against any tampering or bypassing of the TSF of the TOE.

187 The TSF Features TSF_ENV_PROTECT , TSF_AUDIT_ACTION and TSF_DATA_PROTECT contain mechanisms that that fully protected the TOE against any external tamper or bypass.

188 The Security Mechanisms applicable to this protection are:

TSF_ENV_PROTECT

- Hardware Protection (Active Shield)

- Voltage Monitor

- Temperature Monitor

- Frequency Monitor

- Memory Encryption

- Laser Scan Detectors

TSF_AUDIT_ACTION

- Reset System

TSF_DATA_PROTECT

- Glitch Detectors

TPG0214B_VIC_18Jul11

8 Annex

8.1 Glossary of Vocabulary

Application Data	All data managed by the Security IC Embedded Software in the application context. Application data comprise all data in the final Security IC.
Composite Product Integrator	Role installing or finalising the IC Embedded Software and the applications on platform transforming the TOE into the un-personalised Composite Product after TOE delivery.
	The TOE Manufacturer may implement IC Embedded Software delivered by the Security IC Embedded Software Developer before TOE delivery (e.g. if the IC Embedded Software is implemented in ROM or is stored in the non-volatile memory as service provided by the IC Manufacturer or IC Packaging Manufacturer).
Composite Product Manufacturer	The Composite Product Manufacturer has the following roles (i) the Security IC Embedded Software Developer (Phase 1), (ii) the Composite Product Integrator (Phase 5) and (iii) the Personaliser (Phase 6). If the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice) he has the role of the IC Packaging Manufacturer (Phase 4) in addition.
	The customer of the TOE Manufacturer who receives the TOE during TOE Delivery. The Composite Product Manufacturer includes the Security IC Embedded Software developer and all roles after TOE Delivery up to Phase 6.
End-consumer	User of the Composite Product in Phase 7.
IC Dedicated Software	IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.
IC Dedicated Support Software	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

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).
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
Pre-personalisation Data	Any data supplied by the Card Manufacturer that is programmed into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). This data is for example used for traceability and/or to secure shipment between phases.
Security IC	(as used in this Protection Profile) Composition of the TOE, the Security IC Embedded Software, User Data and the package (the Security IC carrier).
Security IC Embedded Software	Software embedded in a Security IC and normally not being developed by the IC Designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3 or in later phases of the Security IC product life-cycle. Some part of that software may actually implement a Security IC application others may provide standard services. Nevertheless, this distinction doesn't matter here so that the Security IC Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.
Security IC Product	Composite product which includes the Security Integrated Circuit (i.e. the TOE) and the Embedded Software and is evaluated as composite target of evaluation in the sense of the Supporting Document
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 either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.
TOE Manufacturer	The TOE Manufacturer must ensure that all requirements for the TOE and its development and production environment are fulfilled.

The TOE Manufacturer has the following roles: (i) IC Developer (Phase 2) and (ii) IC Manufacturer (Phase 3). If the TOE is delivered after Phase 4 in form of packaged products, he has the role of the (iii) IC Packaging Manufacturer (Phase 4) in addition.

TSF data

Data 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 E^2PROM) 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.

8.2 Literature

[CC_PART1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3, July 2009

[CC_PART2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 3, July 2009

[CC_PART3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 3, July 2009

[CEM] Common Methodology for Information Technology Security Evaluation (CEM), Part 2: Evaluation Methodology; Version 3.1, Revision 3, July 2009

[JHAS] Supporting Document, Mandatory Technical Document: Application of Attack Potential to Smartcards, April 2006, Version 2.1, Revision 1, CCDB-2006-04-002

[AIS34] Supporting Document, Mandatory Technical Document: The Application of CC to Integrated Circuits, April 2006, Version 2.1, Revision 1, CCDB-2006-04-003

[COMP] Supporting Document: Composite product evaluation for Smart Cards and similar devices, CCDB-2007-09-001, Sept. 2007

[PP] Security IC Platform Protection Profile, BSI-CC-PP-0035-2007, V1.0

[AIS31] AIS31: Functionality classes and evaluation methodology for true (physical) random number generators, Version 3.1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

[AIS20] AIS20: Functionality classes and evaluation methodology for deterministic random number generators. Version 1 (02.12.1999), Bundesamt für Sicherheit in der Informationstechnik

[AUG] Smartcard Integrated Circuit Augmentations Version 1.0, March 2202, registered under the German Certification Scheme BSI-AUG-2202

TPG0214B_VIC_18Jul11

8.3 List of Abbreviations

CC	Common Criteria.
EAL	Evaluation Assurance Level.
IC	Integrated circuit.
IT	Information Technology.
PP	Protection Profile.
ST	Security Target.
TOE	Target of Evaluation.
TSC	TSF Scope of Control.
TSF	TOE Security Functionality.

TPG0214B_VIC_18Jul11