

General Business Use

**AT91SO100/101**  
**Security Target Lite**



## Important notice to readers...

Atmel makes no warranty for the use of its products, other than those expressly contained in the Company's standard warranty which is detailed in Atmel's Terms and Conditions located on the Company's web site. The Company assumes no responsibility for any errors which may appear in this document, reserves the right to change devices or specifications detailed herein at any time without notice, and does not make any commitment to update the information contained herein. No licenses to patents or other intellectual property of Atmel are granted by the Company in connection with the sale of Atmel products, expressly or by implication. Atmel's products are not authorized for use as critical components in life support devices or systems.

The security of any system in which the product is used will depend on the system's security as a whole. Where security or cryptography features are mentioned in this document this refers to features which are intended to increase the security of the product under normal use and in normal circumstances.

All products are sold subject to Atmel's Terms & Conditions of Supply and the provisions of any agreements made between Atmel and the Customer. In ordering a product covered by this document the Customer agrees to be bound by those Terms & Conditions and agreements and nothing contained in this document constitutes or forms part of a contract (with the exception of the contents of this Notice). A copy of Atmel's Terms & Conditions of Supply is available on request.

© Atmel Corporation 2008

---

<b>Section 1</b>	AT90SO100/101 Security Target Lite.....	9
	1.1 Identification.....	9
	1.2 Overview.....	9
	1.3 Common Criteria Conformance Claim.....	10
	1.4 Document Objective.....	10
	1.5 Document Structure.....	11
	1.6 Scope and Terminology.....	11
	1.7 References.....	12
	1.8 Revision History.....	13
<hr/>		
<b>Section 2</b>	Target of Evaluation Description.....	15
	2.1 AT90SO100/101 Hardware.....	15
	2.2 Product Type.....	16
	2.3 Product Life-cycle.....	21
	2.4 TOE Environment.....	24
	2.5 TOE Logical Phases.....	25
	2.6 TOE Intended Usage.....	25
	2.7 Scope of Evaluation Summary.....	28
<hr/>		
<b>Section 3</b>	TOE Security Environment.....	29
	3.1 Assets.....	29
	3.2 Assumptions.....	31
	3.3 Threats.....	33
	3.4 Organizational Security Policies.....	39
<hr/>		
<b>Section 4</b>	Security Objectives.....	41
	4.1 Introduction.....	41



	4.2 Security Objectives for the TOE.....	41
	4.3 Security Objectives for the Environment.....	47
<hr/>		
<b>Section 5</b>	IT Security Requirements .....	51
	5.1 TOE Functional Requirements.....	51
	5.2 TOE Security Assurance Requirements .....	67
	5.3 Definition of Extended Security Functional Requirements.....	68
<hr/>		
<b>Section 6</b>	TOE Summary Specification.....	73
	6.1 TOE Security Functions .....	73
	6.2 TOE Assurance Measures.....	79
<hr/>		
<b>Section 7</b>	PP conformance claim.....	83
<hr/>		
<b>Appendix A</b>	Glossary.....	84



Figure 2-1 AT91SO100 and AT91SO101 part numbers ..... 15

Figure 2-2 AT91SO101 package and the multishark in more detail..... 16

Figure 2-3 AT90SO100/101 Product Life Cycle ..... 23

Figure 3-1 Standard Threats ..... 33

Figure 3-2 Attack Model for the TOE ..... 34

Figure 3-3 Organizational Security Policies..... 39

Figure 4-1 Standard Security Objectives ..... 42

Figure 4-2 Security Objectives related to Specific Functionality..... 42





Table 2-1	Product Life-cycle.....	21
Table 2-2	Phases 4 to 7 Product Users .....	27
Table 5-1	Overview of the ST Functional Requirements.....	51
Table 6-1	Relationship Between Assurance Requirements and Measures .....	79







---

## AT90SO100/101 Security Target Lite

---

### 1.1 Identification

1 Title: AT90SO100/101 Security Target Lite.

2 This Security Target Lite has been constructed with Common Criteria (CC) Version 2.3.

---

### 1.2 Overview

The framework for this Security Target Lite (ST\_Lite) is based on the existing Smartcard IC Platform Protection Profile [BSI\_PP] and on the Smartcard Integrated Circuit Augmentations [BSI\_AUG], adapted to a different type of product.



Please note that elements of the Life Cycle were taken from the [PP9806] smartcard protection profile. This is clearly stated where relevant.

Note

3 The TOE is the AT90SO100/101 chip and is sold to customers in two packages as the AT91SO100 Package and the AT91SO101 Package

4 AT90SO100/101 is being evaluated to Evaluation Assurance Level 4 (EAL4) augmented with AVA\_VLA.4, ADV\_IMP.2, ALC\_DVS.2 and AVA\_MSU.3 under the Common Criteria scheme. Part 2 is extended, the extended SFRs are defined in chapter Section 5.3. Atmel Smart Card ICs, a division of Atmel Corporation, is the developer and the sponsor.

5 AT90SO100/101 chip is a low-power, high-performance, SC100 32-bit microcontroller based on the ARM<sup>®</sup> enhanced RISC architecture.

6 The TOE can be sold in 2 package part numbers:

7 The AT91SO100 part is the AT90SO100/101 packaged in an industry standard BGA 256 pin package (Ball Grid Array) [TD].

8 Customers are also offered an alternative package part number AT91SO101 this is the same as the AT58815 device in a BGA 256 pin package but with an added interface chip, section 2.1 of this document describes the scope of the evaluation and defines the AT91SO100 and AT91SO101 package part numbers in more detail.



---

### 1.3 Common Criteria Conformance Claim

9 This Security Target Lite is conformant to parts 2 and 3 of the Common Criteria, V2.3, as follows:

- Part 2 extended: the security functional requirements are based on those identified in Part 2 of the Common Criteria and additional security requirements introduced in Section 5.3.
- Part 3 conformant: the security assurance requirements are in the form of an EAL4 (assurance package) based upon assurance components in Part 3 of the Common Criteria.

---

### 1.4 Document Objective

10 The purpose of this document is to satisfy the Common Criteria (CC) requirements for a Security Target Lite; in particular, to specify the security requirements and functions, and the assurance requirements and measures.



---

## 1.5 Document Structure

- 11 Section 1 introduces the Security Target Lite, and includes sections on terminology and references.
- 12 Section 2 contains the product description and describes the TOE as an aid to the understanding of its security requirements and addresses the product type, the intended usage and the general features of the TOE.
- 13 Section 3 describes the TOE security environment.
- 14 Section 4 describes the required security objectives.
- 15 Section 5 describes the TOE security functional requirements and the security assurance requirements.
- 16 Section 6 describes the TOE security functions.
- 17 Section 7 describes the PP Claims
- 18 Appendix A provides a glossary of the terms and abbreviations.

---

## 1.6 Scope and Terminology

- 19 This document is based on the AT90SO100/101 Technical Data Sheet [TD].
- 20 The term *Target of Evaluation* (TOE) is standard CC terminology and refers to the product being evaluated, the AT90SO100/101 project in this case (section 2 defines the scope of the evaluation). The stated toolbox commands are also part of the evaluation. Downloaded test software will be used for evaluation purposes but is outside the scope of the TOE. Description of how to use the security features can be found in [TD].
- 21 Security objectives are defined herein with labels in the form O.xx. These labels are used elsewhere for reference. Similarly, threats, assumptions and organizational security policy are defined with labels of the form T.xx, A.xx, and P.xx respectively.
- 22 Hexadecimal numbers are prefixed by \$, e.g. \$FF is 255 decimal. Binary numbers are prefixed by%, e.g.%0001 1011 is decimal 27. An integer value may be expressed as a hexadecimal, binary or decimal number, whichever form is the most convenient.















---

## 1.7 References

23

The following identifies the latest revision of the documents.

-  [TD] AT91SO100/101 Technical Datasheet (TPR0101)
-  [APP\_TBX] Toolbox 3.x on AT91SO100 with AdvX (TPR0203)
-  [APP\_AdvX] AdvX for AT91SO100 Family (TPR0204)
-  [APP\_CRYPT] Efficient use of AdvX for Implementing Cryptographic Operations (TPR0142)
-  [TBX\_SDD] Toolbox 3.x AdvX Software Development (TPR0152)
-  [BSI\_AUG] Smartcard Integrated Circuit Platform Augmentations Version 1.0, March 2002
-  [BSI\_PP] Smartcard IC Platform Protection Profile (BSI-PP-0002). Version 1.0, July 2001
-  [PP9806] Smartcard Integrated Circuit Protection Profile. Version 2.0, September 1998
-  [EMV] Integrated Circuit Card Specifications for Payment Systems. Version 4.1, May 2004.
-  [PCI-PED] PCI POS PIN Entry Device Security Requirements Manual. Version 1.3, February 2005.
-  [FINREAD] Financial Transactional IC Card Reader (FINREAD) CWA Nr 14 174. October 2003.
-  [NIST\_RNG] NIST Digital Signature Standard FIPS Pub 186-2 Jan 27 2000



---

**1.8 Revision History**

<b>Rev</b>	<b>Date</b>	<b>Description</b>	<b>Originator</b>
A	28 Jul 08	Initial Release	Gordon Caffrey
B	09 Sep 08	Changed part number to AT91SO100/101	John Boggie





## Target of Evaluation Description

- 24 This part of the Security Target Lite (ST\_Lite) describes the Target of Evaluation (TOE) as an aid to the understanding of its security requirements and addresses the product type, the intended usage and the general features of the TOE.

### 2.1 AT90SO100/101 Hardware

#### 2.1.1 AT91SO100 and AT91SO101 package definition

- 25 The AT90SO100/101 project can be ordered by a customer in two package part numbers Figure 2-1 shows the definition of the 2 part numbers.

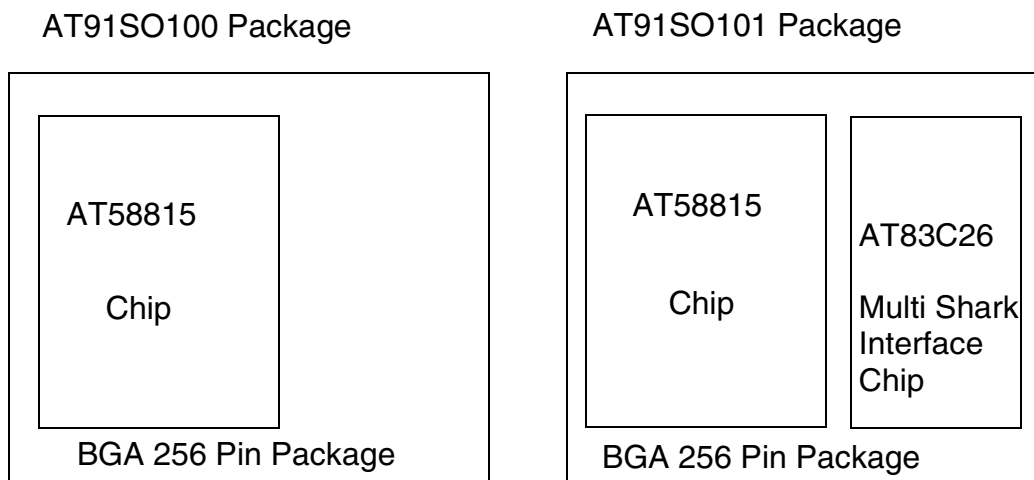


Figure 2-1 AT91SO100 and AT91SO101 part numbers

- 26 The AT91SO101 package contains the same AT58815 chip as the AT91SO100 package but it also has an additional Multi-shark interface chip packaged beside it, the multi shark is bonded to the pin outs of the BGA package only, that is there is no connection directly to the AT58815 chip also packaged in the AT91SO101 package. To connect the Multi-shark interface chip to the AT58815 chip within the AT91SO101



package the customer must externally connect the pin out for the Multi -shark device to the AT58815 chip pin outs as detailed in [TD]. Figure 2-2 shows the AT91SO101 package in further detail.

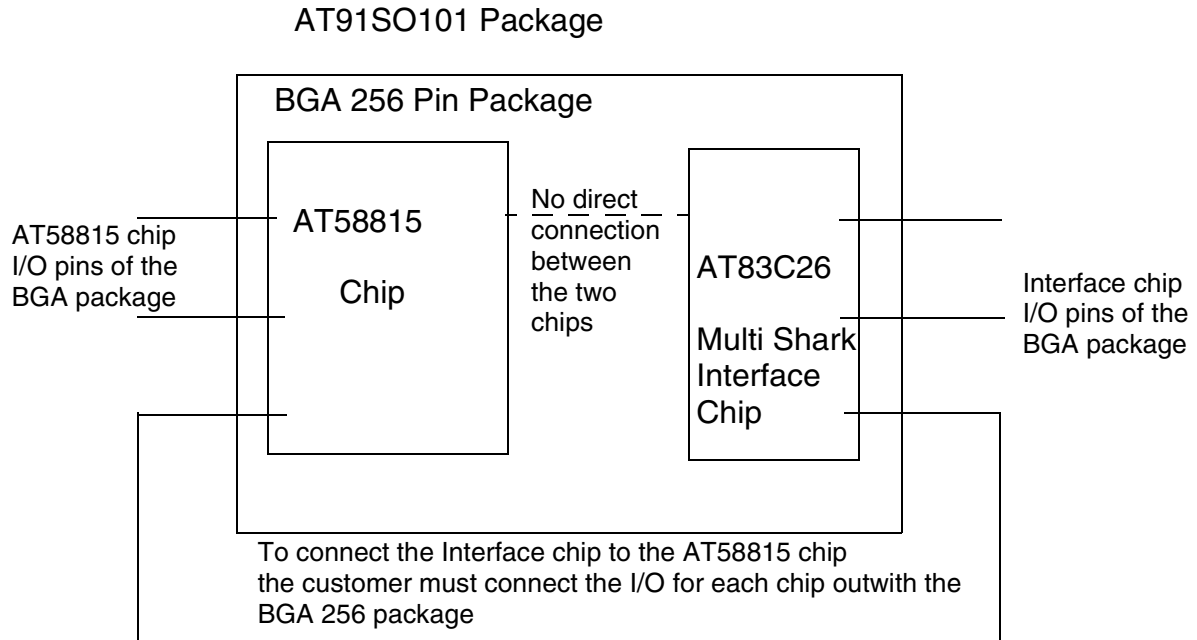


Figure 2-2 AT91SO101 package and the multishark in more detail

**Scope of the Evaluation - definition of Hardware part**

- 27 The scope of the evaluation can be considered as the AT58815 chip bonded out in a 256 BGA package whether that is the AT91SO100 package or the AT91SO101 package, in operation both packages are identical as the AT83CT6 Interface device is not connected to the AT58815 chip.
- 28 For the purpose of this evaluation both package parts will now be identified within this Security Target Lite as the AT91SO101 TOE.

**2.2 Product Type**

- 29 AT90SO100/101 is a low-power, high-performance, SC100 32-bit microcontroller based on the ARM® enhanced RISC architecture. This new SC100 core allows the linear addressing of up to 1M bytes of code and data as well as a number of new functional and security features. A 3-level instruction pipeline allows the performance of one instruction in a single clock cycle; the AT91SO100 achieves throughputs close to 1 MIPS per MHz. The SC100 processor employs a unique architectural strategy known as Thumb®: a super reduced instruction set that is ideally suited for high volume applications with memory restrictions and applications where code density is an important factor.





- 30 AT90SO100/101 has an internal EEPROM that can be used as program or data memory. It also includes a ROM (for the boot and some native functions) and a large SRAM. AT90SO100/101 can also address, via pages, up to 16Mbytes of external memory.
- 31 AT90SO100/101 also comprises of strong security mechanisms and has an impressive set of cryptography features, hardware DES/TDES, hardware AES, hardware SHA-1 and SHA-256, hardware cryptography accelerator for asymmetric algorithms (RSA, Prime generation) and a true random number generator.
- 32 The AT58815 die includes a lot of interfaces dedicated to peripherals such as smartcard and magnetic stripe card interface, as well as USB, SPI, UARTs and I/O ports.
- 33 The AT90SO100/101 product can be thought of as a device that is used in banking systems such as EFT-POS payment terminals or PINPED Pin entry devices. However, it should be kept in mind that the AT90SO100/101 product could also be used for other applications as secure tokens or hardware security modules.

---

#### In Summary

- AT90SO100/101 is a secure microcontroller to embed in an EFT POS, PINPED devices with:
  - Powerful secure cryptography HW/SW services
  - Embedded program/data memories
  - Different communication channels
  - Security mechanisms
- AT90SO100/101 is intended to group the security of payment systems into a single device by:
  - Securely store banking keys in a battery backed up area
  - Securely manipulate sensitive information as PIN code, card user proprietary information (card number, bank count number, transaction information,...) in order to match the security requirements of the banking community
- ARM SC100 core contains the:
  - ARM MPU
  - ARM bridge
  - Atmel Firewall

---

#### AT90SO100/101 Device Testing

- 34 The TOE requires embedded software to test the device and demonstrate certain security characteristics during the development phase. In the end-usage phase there will be no embedded test software in the TOE. Test software will be downloaded into the device EEPROM and be fully erased before devices leave the test environment. This test software is only used in the testing phase of the TOE life cycle and is fully erased before disabling Test Mode and entering User Mode, therefore this software is outwith the scope of the evaluation. Test Mode disable is achieved by sawing the wafer.



35 Any faulty devices returned by a customer can be put into Package Mode. This allows the test engineer to access the EEPROM to analyse the failure. On entering Package Mode the EEPROM is erased clearing any customer data, Package Mode only allows a limited set of operations and inputs.

---

### **AT90SO100/101 Configuration and personalisation**

36 Some configuration options can be chosen by the customer at product order.

37 The TOE is manufactured in a low voltage (2.5V +/- 10%) CMOS process. The device will operate at a supply voltage of 3.3V +/- 10% with the internal supply regulated to the required operating voltage.

38 Once manufactured, the product operates by executing the Product Embedded Software, which is stored in CPU ROM. The contents of the CPU ROM cannot be modified, whereas the contents of the EEPROM can, in general, be written to or erased, under the control of the Product Embedded Software.

39 The EEPROM includes OTP bytes, which can be used to store security-related information such as cryptographic keys. The OTP bytes cannot be erased in User Mode.

40 The FireWall (Memory Protection Unit) allows the Product Embedded Software to prevent read/write/execute access to (parts of) ROM, EEPROM, RAM, and peripherals from EEPROM.

## **2.2.1 Features of the AT90SO100/101 TOE**

---

### **General**

- High-performance, Low-power 32-bit ARM®-SC100 Enhanced RISC Architecture
- Von Neumann Load / Store Architecture
- Single 32-bit Data Bus for Instructions and Data
- Memory Protection Unit (MPU)
- Internal Oscillator (VFO) (up to 50 MHz)
- ESD Protection to ± 2000V (± 6000V on the ISO interfaces)
- Operating Ranges: 3.3V (+/- 10%)

---

### **Memory**

- 256 bits of Key Storage (battery backup)
- 32K Bytes of internal ROM Memory (BOOT, library)
- 256K Bytes of Internal EEPROM, Including 128 OTP Bytes and 384-byte Bit-addressable Bytes
  - 1 to 128-byte Program/Erase
  - 2 ms Program, 2 ms Erase



- Endurance: 300,000 Write/Erase Cycles at temperature of 25 degrees C
  - 10 Years Data Retention
- 100K Bytes of Internal RAM (4KB Crypto RAM)
- Up to 16M Bytes of External Memory (accessed by page)

#### **Peripherals**

- Page Unit to access External Memory Page
- Static Memory Controller
- Two ISO 7816 controllers with DC/DC (one of them can be multiplexed to address 4 SAM)
- USB 2.0 Full Speed (8 endpoints)
- SPI Controller (up to 12 Mbps)
- 2 Universal Synchronous/Asynchronous Receiver Transmitters (USART)
- Triple Track Magstripe Logical Interface
- 5 8-bit I/O Port Interface (LEDs, Keyboard, LCD, spare...)
- 2 product ISO7816 controllers = 1 electrical multiplexer 1 to 4
- Real Time Clock (RTC) with Alarm interrupt
- System Timer including a 16-bit Counter, Watchdog and Second Counter
- Six-channel 16-bit Timer/counter
- 2-level, 12-interrupt Controller
- Hardware DES and Triple DES
- Hardware AES Engine
- Atmel Crypto Toolbox:
  - DES/TDES
  - AES
  - SHA
  - RSA Key generation (Prime generation)
- Atmel Secure Bootstrap and FSL Library (IC dedicated support software)
  - EEPROM download capabilities for production use
- Hardware Random Number Generator (RNG)
- Two CRC 16 Engines and one CRC 32 Engine (Compliant with ISO/IEC 3309)
- AdvX™ - Advanced crypto multiplier for cryptography and authentication (including RSA, Key Generation in)

#### **Security**

- Dedicated Hardware for Protection Against SPA/DPA Attacks
- Advanced Protection Against Physical Attack, Including Active Shield
- Internal Control for External Intrusion sensors
  - Intrusion Switch Sensors



- Intrusion Mesh Sensors
- Environmental Protection Systems (Voltage, Frequency, UV and Temperature)
- Secure Memory Management/Access Protection (MPU)
- Real time clock and battery back up
- Compliant with EMV standard, PCI-PED and FINREAD

---

**Cryptographic Toolbox**

41 The TOE also includes a cryptographic accelerator (AdvX) that allows fast cryptographic algorithm implementations on the ARM SC100 (such as multiplications).

---

**Scope of Evaluation Software Part**

42 Atmel provides a proprietary cryptographic library with cryptographic primitives. This crypto ROM library is considered as IC dedicated software and is part of the TOE.

43 The AT90SO100/101 device also features a Secure Bootstrap and FSL IC dedicated support software library.



## 2.3 Product Life-cycle

44 The product life-cycle consists of 7 phases where the following authorities are involved.

Table 2-1 Product Life-cycle

<b>Phase 1</b>	Development of the embedded software (the OS and the applications)	The software developer is in charge of the embedded software development and the specification of IC pre-personalization requirements,
<b>Phase 2</b>	Development of the IC, of the IC dedicated test software and of the IC dedicated support software	The IC designer designs the IC, develops IC dedicated software, provides information, software or tools to the product software developer, and receives the software from the developer, through trusted delivery and verification procedures. From the IC design, IC dedicated software and product embedded software, the IC designer constructs the product IC database, necessary for the IC photomask fabrication.
<b>Phase 3</b>	Manufacturing and test of the IC	The IC manufacturer is responsible for producing the IC through three main steps: <ul style="list-style-type: none"> <li>■ IC manufacturing</li> <li>■ IC testing</li> <li>■ IC pre-personalization (optional)</li> </ul>
<b>Phase 4</b>	Packaging and test of the IC	The IC packaging manufacturer is responsible for the IC wafer sawing, packaging and testing.
<b>Phase 5</b>	Manufacturing and test of the system (EFT POS)	The product manufacturer is responsible for the system manufacturing and testing.
<b>Phase 6</b>	Personalisation of the system (EFT POS) by loading of the OS, application, keys	The personalizer is responsible for the product personalization and final tests. Other application software may be loaded onto the chip at the personalization process.
<b>Phase 7</b>	End usage (in the field)	The product issuer is responsible for the product delivery to the product end-user, and the end of life process.

45 The phases of the [PP9806] and [BSI\_PP] protection profiles are taken as a reference and adapted to this kind of system.

46 Connection between Phase 1 and Phase 2 is optional since all the embedded software can be loaded in Phase 5.

47 The limits of the evaluation correspond to phases 2-3-4.



48            These different phases may be performed at different sites; procedures on the delivery process of the TOE shall exist and be applied for every delivery within a phase or between phases. This includes any kind of delivery performed from phase 1 to phase 7, including:

- Intermediate delivery of the TOE or the TOE under construction within a phase
- Delivery of the TOE or the TOE under construction from one phase to the next

49            These procedures shall be compliant with the assumptions developed in Section 3.3.4.

50            Figure 2-3 shows the AT90SO100/101 life cycle flow.



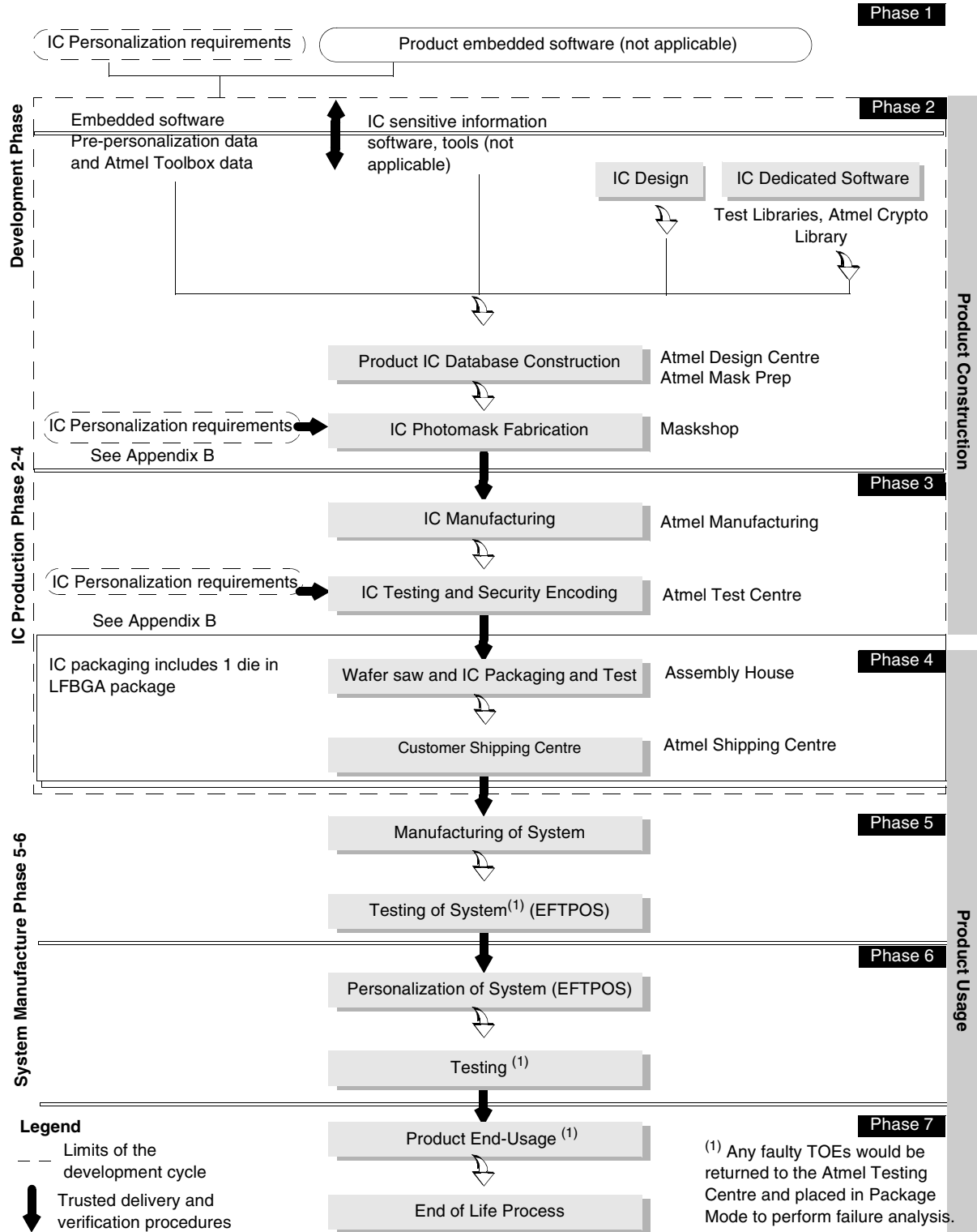


Figure 2-3 AT90SO100/101 Product Life Cycle



---

## 2.4 TOE Environment

51 Considering the TOE, three types of environments are defined:

- Development environment corresponding to phase 2
- Production environment corresponding to phases 3 and 4
- User environment, from phase 5 to phase 7

### 2.4.1 TOE Development Environment

52 To assure security, the environment in which the development takes place is made secure with controllable accesses having traceability. Access to the development building is strictly monitored by a Security person. Visitors must be registered in a log book that records the time of arrival and time of departure to the building. All visitors are escorted by authorized personnel at all times. All authorized personnel involved fully understand the importance and the rigid implementation of the defined security procedures.

53 The development begins with the TOE's specification. All parties in contact with sensitive information are required to abide by Non-Disclosure Agreements.

54 The Interface die life cycle is outwith the scope of the TOE development environment.

55 Reticles and photomasks are generated from the verified IC database. These are manufactured by a Maskshop, for wafer fab processing undertaken in Atmel Manufacturing Facility. The reticles and photomasks are then transferred to the wafer fab processing facilities using a secure shipment procedure.

### 2.4.2 TOE Production Environment

56 Production starts within the ATMEL Manufacturing Facility; here the silicon wafers undergo diffusion processing. Computer tracking at wafer level throughout the process is achieved by the batch tracking system.

57 The batch tracking system is an on-line manufacturing tracking system which monitors the progress of the wafers through the fabrication cycle. After fabrication the wafers are sent to Atmel Test Centre where they are thinned to a pre-specified thickness and tested. Atmel EKB test the TOE to assure conformance with the device specification. During the IC testing, security encoding is performed where the security configuration of the device is frozen, some of the EEPROM bytes are programmed with the unique traceability information, and the customer software is loaded in the EEPROM.

58 The wafers are inked to separate the functional ICs from the non-functional ICs.





### 2.4.3 Packaging and testing of IC

- 59 At the end of phase 3 the device is sent to an assembly house for wafer sawing and packaging.
- 60 BGA package assembly and test takes place within the assembly house. Test operations consist of basic open/short test and “CPU ready” test to ensure that the packaging operation has not damaged the device.
- 61 TOE returned by secure carrier to Atmel Shipping Centre, for secure shipping to customers.

### 2.4.4 TOE User Environment

- 62 The TOE user environment is the environment of phases 4 to 7.
- 63 At phases 4, 5, and 6, the TOE user environment is a controlled environment.
- 64 Following the sawing step, the wafers are split into individual dies. The good ICs are assembled into modules in a module assembly plant.
- 65 Atmel Shipping Centre, ensures the shipment of the modules to the product manufacturer (embedder) by means of a secure carrier.
- 66 Additional testing occurs followed by personalization, then delivery to the device issuer.

---

#### End-user environment (Phase 7)

- 67 The TOE is used in a range of applications to assure authorized conditional access. Examples of such as, Banking, card reader.
- 68 Therefore, the user environment covers a wide spectrum of very different functions, thus making it difficult to avoid or monitor any abuse of the TOE.

---

## 2.5 TOE Logical Phases

- 69 During its construction usage, the TOE may be under several life logical phases. These phases are sorted under a logical controlled sequence. The change from one phase to the next shall be under the TOE control.

---

## 2.6 TOE Intended Usage

- 70 During the phases 1, 2, 3, the product is being developed and produced. The administrators are the following:
- The product embedded software developer



## Security Target Lite


- The product IC designer  
The Atmel toolbox is developed during Phase 2 of the product life cycle.
- The IC manufacturer



71

Table 2-2 lists the users of the product during phases 4 to 7.

Table 2-2 Phases 4 to 7 Product Users

<b>Phase 4</b>	<ul style="list-style-type: none"> <li>■ Packaging manufacturer (administrator)</li> <li>■ Product embedded software developer</li> <li>■ System integrator, such as the terminal software developer</li> </ul>
<b>Phase 5</b>	<ul style="list-style-type: none"> <li>■ Product manufacturer (administrator)</li> <li>■ Product embedded software developer</li> <li>■ System integrator, such as the terminal software developer</li> </ul>
<b>Phase 6</b>	<ul style="list-style-type: none"> <li>■ Personalizer (administrator)</li> <li>■ Customers who, before manufacture, determine the product's mask options and the initial memory contents (i.e. the application program), and who, after manufacture, incorporate the product into devices. Customers are trusted and privileged users.</li> <li>■ Product issuer (administrator).</li> <li>■ Product embedded software developer.</li> <li>■ System integrator, such as the terminal software developer.</li> </ul>
<b>Phase 7</b>	<ul style="list-style-type: none"> <li>■ Product issuer (administrator)</li> <li>■ Product end-user, who use devices incorporating the product. End-users are not trusted and may attempt to attack the product.</li> <li>■ Product software developer.</li> <li>■ System integrator, such as the terminal software developer.</li> </ul>
	<p> <b>Note</b> The IC manufacturer and the product manufacturer may also receive ICs for analysis, should problems occur during the product usage.</p>

72

The product may be used in the following modes:

- a) Test Mode, in which the product runs under the control of dedicated test software. This mode is intended to be used solely by authorized development staff. This mode is reserved for Phases 2 and 3, and disabled in Phase 4. During the initial part of the manufacturing process the product is set to Test Mode. Authorized development staff then test the product. After testing, Test Mode is permanently disabled, and the product is set to User Mode.



- b) Package Mode is a mode similar to Test Mode for testing returns from Phases 4-7. Package Mode runs a limited subset of test commands. This mode is intended to be used solely by authorized staff.
- c) User Mode, in which the product runs under control of the Product Embedded Software. It is intended that customers and end-users will always use the product in User Mode. This mode is reserved for Phases 4 to 7. If a faulty TOE is returned from the field then analysis can be done either in User Mode, or Package Mode by an authorized test engineer.

73

The only modes of operation are those stated in paragraph 72 a), b) and c).

---

## 2.7 Scope of Evaluation Summary

---

### Within the Scope of the Evaluation

- AT58815 Hardware Die
  - AT91SO100 BGA package
  - AT91SO101 BGA package
- Package Mode
- Atmel security User Guidance
- External Intrusion Sensors (Mesh and Switches)
- TOE interfaces
- Embedded Software
  - Atmel Cryptographic Toolbox (ROM)
  - Secure Bootstrap and FSL IC dedicated support software library
- RNG compliant with PCI-PED and FINREAD
- Phases 2-4 of the Life Cycle

---

### Outwith the Scope of the Evaluation

- The AT83C26 Interface Chip
- Strength of Cryptographic Functions
- Test software loaded in Phase 2-3 of the Life Cycle, used to test the TOE
- Phases 1 and 5-7 of the Life Cycle
- The life cycle of the AT83C26 Interface chip
- Embedded Software
  - Atmel Cryptographic Toolbox (E2PROM)



---

## TOE Security Environment

74 This section describes the security aspects of the environment in which the TOE is intended to be used, and addresses the description of the assets to be protected, the assumptions, the threats, and the organizational security policies.

75 All these environment elements are derived from [BSI\_PP] and [BSI\_AUG], and adapted to the AT90SO100/101 system to cover all the phases of its life cycle and the delivery from one phase to another.

---

### 3.1 Assets

76 Assets are security relevant elements of the TOE that include the primary and secondary assets.

#### 3.1.1 Primary Assets

- IC embedded software (program and data), such as:
  - PIN code of users
  - Cryptographic keys
  - Transaction related sensitive data
  - OS program and data stored in the TOE
  - Application program and data stored in the TOE
  - Random numbers generated by the TOE
- IC dedicated support software:
  - Toolbox library program and data
  - Secure program and data
- Sensitive communication information with external components of the system
  - Keyboard
  - Product
  - Display



### 3.1.2 Secondary Assets

- IC specification, design, tools and technology
- IC dedicated test software

77 Therefore, the TOE itself is an asset.

78 Assets must be protected in terms of confidentiality and integrity.



---

## 3.2 Assumptions

79

This section concerns the following items:

- Any assumption on the Product Embedded Software,
- Any assumption on the System,
- Any assumption on the TOE delivery process.

### 3.2.1 Assumptions on the Product Embedded Software

A.Plat-Appl	<p>Usage of Hardware Platform</p> <p>The Product Embedded Software shall be designed according to: the TOE user guidances, such as the hardware data sheet, and the TOE evaluation reports relevant for the Product Embedded Software Developer.</p> <p>Applies to Phase 1</p>
A.Resp-Appl	<p>Treatment of User Data</p> <p>The Product Embedded Software shall manage and protect the User Data, specially security related data such as cryptographic keys or User PINs, according to the requirements of the applicative context.</p> <p>Applies to Phase 1</p>
A.Key-Function	<p>Implementation of key-dependent functions</p> <p>Key dependant functions (if any) shall be implemented in the Product Embedded Software not to be susceptible to leakage attacks.</p> <p>Applies to Phase 1</p>
A.Dev-Org	<p>Protection of Product Embedded Software</p> <p>Procedures dealing with physical, personnel, organizational, technical measures for the confidentiality and integrity of the Product Embedded Software (e.g. source code and any associated documents) and IC designer proprietary information (tools, software, documentation) shall exist and be applied in software development environment during the whole life of the TOE.</p> <p>Applies to Phases 1 to 7</p>



### 3.2.2 Assumptions on the System

- |                  |  |
|------------------|--|
| A.Design-System  | Usage and connection of TOE<br><br>System (EFT POS/PINPED) shall be designed making appropriate use of the internal control for external security mechanisms of the TOE (intrusion switches, intrusion mesh inside the PCB,...) so that access to the physical interface of the TOE is made difficult for an attacker.<br><br>Moreover, the TOE is fixed on a PCB, permanently backed up by an external battery and connected to an external 32kHz XTAL.<br><br>Applies to Phase 5 to 7  |
| A.Process-System | Protection during Packaging, Finishing and Personalization<br><br>Security procedures shall be in place during all System manufacturing and test operations (after delivery of the TOE by the TOE Manufacturer up to the delivery to the End-User) to maintain confidentiality and integrity of the TOE and of related data. These procedures shall prevent any possible copy, modification, retention, theft or unauthorized use of the TOE or the system.<br><br>In the case where unsawn wafers are delivered, appropriate guidance on sawing will be known and used by the customer.<br><br>Applies to Phases 4 to 6 |

### 3.2.3 Assumptions on the TOE Delivery Process (Phases 4 to 7)

- |            |   |
|------------|---|
| A.Delivery | Delivery Procedures<br><br>Procedures shall ensure protection of TOE material and information under delivery and storage. A procedure shall ensure protection of the TOE for unsawn wafer delivery.<br><br>Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.<br><br>Procedures shall ensure that people dealing with the procedure for delivery have got the required skill. |
|------------|---|





### 3.3 Threats

80 The definition of the threats for the TOE are based on threats defined in [BSI\_PP] and [BSI\_AUG] which are relevant to the TOE.

81 The security concerns are derived from considering the end-usage phase (Phase 7) since:

- Phase 1 and Phases from TOE Delivery up to the end of Phase 6 are covered by assumptions and
- The development and production environment starting with Phase 2 up to TOE Delivery are covered by organisational security policies.

82 According to [BSI\_PP], there are the following standard high-level security concerns:

- |     |  |
|-----|--|
| SC1 | Manipulation of User Data and of the Product Embedded Software (while being executed/processed and while being stored in the TOE's memories) and |
| SC2 | Disclosure of User Data and of the Product Embedded Software (while being processed and while being stored in the TOE's memories).               |

83 These security concerns give rise to a number of threats, shown in Figure 3-1.

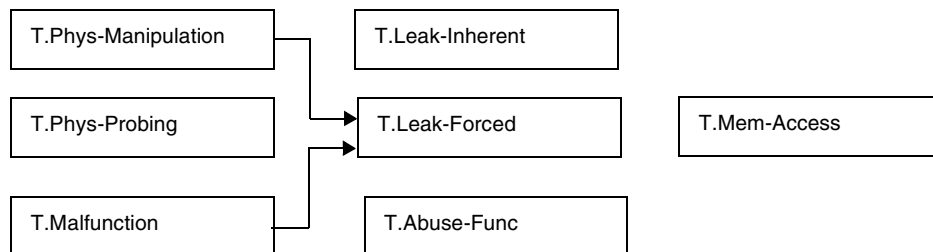
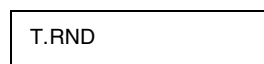


Figure 3-1 Standard Threats

84 According to this Security Target Lite there are the following high-level security concerns related to specific functionality:

- |     |                              |
|-----|------------------------------|
| SC3 | Deficiency of random numbers |
|-----|------------------------------|

85 This security concern gives rise to a specific threat:



86 The TOE is exposed to different types of influences or interactions with its outer world. Some of them may result from using the TOE only but others may also indicate an attack. The different types of influences or interactions are visualized in Figure 3-2.

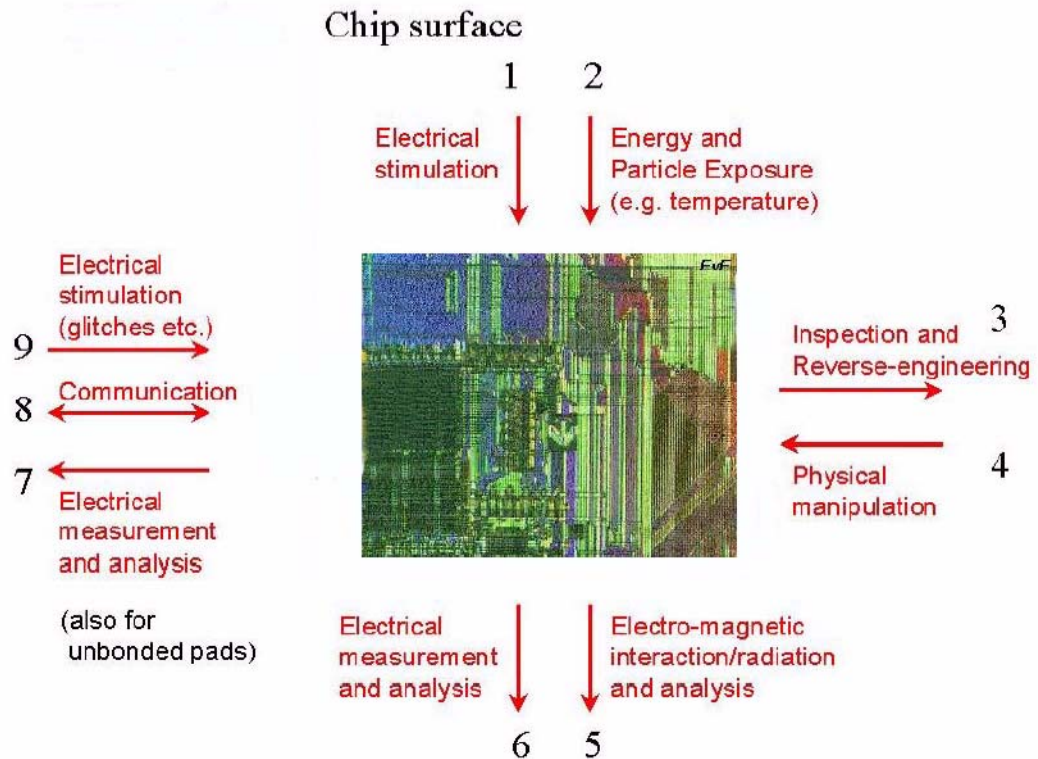


Figure 3-2 Attack Model for the TOE

87 An interaction with the TOE can be done through the ISO interfaces (Number 7 – 9 in Figure 3-2) which are realized using contacts and/or a contactless interface. Influences or interactions with the TOE also occurs through the chip surface (Number 1 – 6 in Figure 3-2). In Number 1 and 6 galvanic contacts are used. In Number 2 and 5 the influence (arrow directed to the chip) or the measurement (arrow starts from the chip) does not require a contact. Number 3 and 4 refer to specific situations where the TOE and its functional behaviour is not only influenced but definite changes are made by applying mechanical, chemical and other methods (such as 1, 2). Many attacks require a prior inspection and some reverse-engineering (Number 3).

88 The TOE’s countermeasures are designed to avert the threats described below. Nevertheless, they may be effective in earlier phases (Phases 4 to 6).

89 The Product Embedded Software and the System (e.g. EFT-POS) must contribute to averting the threats: At least they must not undermine the security provided by the TOE. For detail refer to the assumptions regarding the Product Embedded Software and the System specified in Section 3.2.



---

**Standard Threats (referring to SC1 and SC2)**

90

The TOE shall avert the threat “Inherent Information Leakage (T.Leak-Inherent)” as specified below.

T.Leak-Inherent

Inherent Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Product in order to disclose confidential data (User Data or TSF data).

No direct contact with the Product internals is required here. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. One example is the Differential Power Analysis (DPA). This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from direct (contact) measurements (Numbers 6 and 7 in Figure 3-2) or measurement of emanations (Number 5 in Figure 3-2) and can then be related to the specific operation being performed.



91 The TOE shall avert the threat “Physical Probing (T.Phys-Probing)” as specified below.

T.Phys-Probing

Physical Probing

An attacker may perform physical probing of the TOE in order to:

- Disclose User Data
- Disclose/reconstruct the Product Embedded Software or
- Or to disclose other critical operational information especially TSF data.

Physical probing requires direct interaction with the Product Integrated Circuit internals (Numbers 5 and 6 in Figure 3-2). Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used.

Before that hardware security mechanisms and layout characteristics need to be identified (Number 3 in Figure 3-2). Determination of software design including treatment of User Data may also be a pre-requisite

This pertains to “measurements” using galvanic contacts or any type of charge interaction whereas manipulations are considered under the threat “Physical Manipulation (T.Phys-Manipulation)”. The threats “Inherent Information Leakage (T.Leak-Inherent)” and “Forced Information Leakage (T.Leak-Forced)” may use physical probing but require complex signal processing in addition.

92 The TOE shall avert the threat “Malfunction due to Environmental Stress (T.Malfunction)” as specified below.

T.Malfunction

Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of the Product Embedded Software by applying environmental stress in order to:

- Deactivate or modify security features or functions of the TOE
- Or to deactivate or modify security functions of the Product Embedded Software. This may be achieved by operating the Product outside the normal operating conditions (Numbers 1, 2 and 9 in Figure 3-2).

To exploit this an attacker needs information about the functional operation.



93 The TOE shall avert the threat “Physical Manipulation (T.Phys-Manipulation)” as specified below.

T.Phys-Manipulation Physical Manipulation

An attacker may physically modify the Product in order to:

- Modify security features or functions of the TOE
- Modify security functions of the Product Embedded Software
- Or to modify User Data

The modification may be achieved through techniques commonly employed in IC failure analysis (Numbers 1, 2 and 4 in Figure 3-2) and IC reverse engineering efforts (Number 3 in Figure 3-2). The modification may result in the deactivation of a security function. Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data may also be a pre-requisite. Changes of circuitry or data can be permanent or temporary.

In contrast to malfunctions (refer to T.Malfunction) the attacker requires to gather significant knowledge about the TOE’s internal construction here (Number 3 in Figure 3-2).

94 The TOE shall avert the threat “Forced Information Leakage (T.Leak-Forced)” as specified below:

T.Leak-Forced Forced Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Product in order to disclose confidential data (User Data or TSF data) even if the information leakage is not inherent but caused by the attacker.

This threat pertains to attacks where methods described in “Malfunction due to Environmental Stress” (refer to T.Malfunction) and/or “Physical Manipulation” (refer to T.Phys-Manipulation) are used to cause leakage from signals (Numbers 5, 6, 7 and 8 in Figure 3-2) which normally do not contain significant information about secrets.



95 The TOE shall avert the threat “Abuse of Functionality (T.Abuse-Func)” as specified below.

T.Abuse-Func	Abuse of Functionality  An attacker may use functions of the TOE which may not be used after TOE Delivery in order to: <ul style="list-style-type: none"><li>■ Disclose or manipulate User Data</li><li>■ Manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or of the Product Embedded Software</li><li>■ Or to enable an attack.</li></ul>
--------------	--

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

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

---

**Threats related to Specific Functionality (referring to SC3)**

97 The TOE shall avert the threat “Deficiency of Random Numbers (T.RND)” as specified below.

T.RND	Deficiency of Random Numbers  An attacker may predict or obtain information about random numbers generated by the TOE for instance because of a lack of entropy of the random numbers provided  An attacker may gather information about the produced random numbers which might be a problem because they may be used for instance to generate cryptographic keys.  Here the attacker is expected to take advantage of statistical properties of the random numbers generated by the TOE without specific knowledge about the TOE’s generator. Malfunctions or premature ageing are also considered which may assist in getting information about random numbers.
-------	--



---

### 3.4 Organizational Security Policies

98 The following Figure 3-3 shows the policies applied to the TOE during Phases 2 to 4 of  
its life cycle (that is, in the Development and Production Environment).

99



Figure 3-3 Organizational Security Policies

100 The TOE Developer/Manufacturer must apply the policy “Protection during TOE  
Development and Production (P.Process-TOE)” as specified below.

P.Process-TOE	<p>Protection during TOE Development and Production</p> <p>The TOE Manufacturer must ensure that the development and production of the IC (Phase 2 up to TOE Delivery) is secure so that no information is unintentionally made available for the operational phase of the TOE. For example, the confidentiality and integrity of design information and test data shall be guaranteed; access to samples, development tools and other material shall be restricted to authorised persons only; scrap will be destroyed etc. This not only pertains to the TOE but also to all information and material exchanged with the developer of the Product Embedded Software and the manufacturer of the final System. This includes the delivery (exchange) procedures as far as they can be controlled by the TOE Manufacturer.</p> <p>An accurate unique identification must be established for each instance of the TOE.</p>
---------------	---

101 The TOE provides specific security functionality which can be used by the Product  
Embedded Software to counter threats that are not necessarily identified for the TOE  
but arise in the context of the applications. This functionality is provided according to a  
security policy (refer to Smartcard Integrated Circuit Platform Augmentations  
[BSI\_AUG]).



102 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 must provide the following specific security functionality to the Product Embedded Software, according to accepted international standards:

- Data Encryption Standard (DES)
- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)
- Rivest-Shamir-Adleman (RSA)
- Secure Hash Algorithm (SHA)
- Prime Generation (RSA Key generation)





---

## Security Objectives

---

### 4.1 Introduction

103 This section is based on the [BSI\_PP] and [BSI\_AUG].

104 The security objectives for the TOE and its Environment cover principally the following aspects:

- Integrity and confidentiality of assets
- Protection of the TOE and associated documentation during development and production phases

---

### 4.2 Security Objectives for the TOE

105 According to this Security Target Lite, there are the following standard high-level security goals:

SG1 Maintain the integrity of User Data and of the Product Embedded Software (when being executed/processed and when being stored in the TOE's memories).

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

106 Though the Product Embedded Software 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. In many cases critical User Data will be stored in the EEPROM.

107 These standard high-level security goals are refined below by defining security objectives as required by the Common Criteria (see Figure 4-1). Note that the integrity of the TOE is a means to reach these objectives.



108

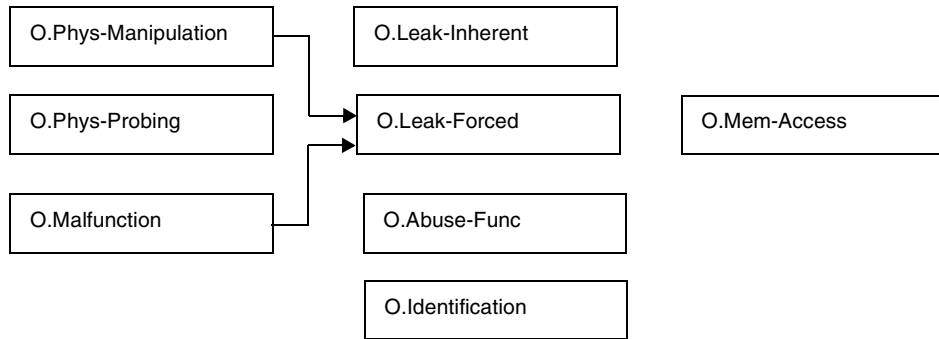


Figure 4-1 Standard Security Objectives

109

According to this Security Target Lite there are the following high-level security goals related to specific functionality:

- SG3 Provide random numbers
- SG4 Provide additional security functionality

110

The additional high-level security considerations are refined below by defining security objectives as required by the Common Criteria (see Figure 4-2).

111



Figure 4-2 Security Objectives related to Specific Functionality.



**Standard Security Objectives (referring to SG1 and SG2)**

112 The TOE shall provide “Protection against Inherent Information Leakage (O.Leak-Inherent)” as specified below.

O.Leak-Inherent      Protection against Inherent Information Leakage

The TOE must provide protection against disclosure of confidential data (User Data or TSF data) stored and/or processed in the Product IC:

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

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

113 The TOE shall provide “Protection against Physical Probing (O.Phys-Probing)” as specified below.

O.Phys-Probing      Protection against Physical Probing

The TOE must provide protection against disclosure of User Data, against the disclosure/reconstruction of the Product Embedded Software or against the disclosure of other critical operational information. This includes protection against:

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

with a prior

- Reverse-engineering to understand the design and its properties and functions.



114 The TOE shall provide “Protection against Malfunctions (O.Malfunction)” as specified below.

O.Malfunction

Protection against Malfunction

The TOE must ensure its correct operation.

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

Remark: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective O.Phys-Manipulation) provided that detailed knowledge about the TOE’s internal construction is required and the attack is performed in a controlled manner.

115 The TOE shall provide “Protection against Physical Manipulation (O.Phys-Manipulation)” as specified below.

O.Phys-Manipulation

Protection against Physical Manipulation

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

- Reverse-engineering (understanding the design and its properties and functions),
- Manipulation of the hardware and any data, as well as
- Controlled manipulation of memory contents (User Data)
- The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.



- 116 The TOE shall provide “Protection against Forced Information Leakage (O.Leak-Forced)” as specified below:
- O.Leak-Forced                      Protection against Forced Information Leakage
- The Product must be protected against disclosure of confidential data (User Data or TSF data) processed in the Card (using methods as described under O.Leak-Inherent) even if the information leakage is not inherent but caused by the attacker
- By forcing a malfunction (refer to “Protection against Malfunction due to Environmental Stress (O.Malfunction)” and/or
  - By a physical manipulation (refer to “Protection against Physical Manipulation (O.Phys-Manipulation)”
- If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.
- 117 The TOE shall provide “Protection against Abuse of Functionality (O.Abuse-Func)” as specified below.
- O.Abuse-Func                      Protection against Abuse of Functionality
- The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to:
- Disclose critical User Data
  - Manipulate critical User Data of the Product Embedded Software
  - Manipulate Soft-coded Product Embedded Software
  - Bypass, deactivate, change or explore security features or functions of the TOE.
  - Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.
- 118 The TOE shall provide “TOE Identification (O.Identification)” as specified below.
- O.Identification                      TOE Identification
- The TOE must provide means to store Initialisation Data and Pre-personalisation Data in its non-volatile memory. The Initialisation Data (or parts of them) are used for TOE identification.



119 The TOE shall provide “Area based Memory Access Control (O.Mem-Access)” as specified below.

O.Mem-Access

Area based Memory Access Control

The TOE must provide the Product Embedded Software with the capability to define restricted access memory areas. The TOE must then enforce the partitioning of such memory areas so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

---

**Security Objectives related to Specific Functionality (referring to SG3 and SG4)**

120 The TOE shall provide “Random Numbers (O.RND)” as specified below.

O.RND

Random Numbers

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

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

121 The TOE shall provide “Additional Specific Security Functionality (O.Add-Functions) as specified below.

O.Add-Functions

Additional Specific Security Functionality

The TOE must provide the following specific security functionality to the Product Embedded Software:

- Data Encryption Standard (DES)
- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)
- Rivest-Shamir-Adleman (RSA)
- Secure Hash Algorithm (SHA)
- Prime Generation (RSA key generation)



---

### 4.3 Security Objectives for the Environment

122 This section concerns the following items:

- Any objective for the Product Embedded Software environment
- Any objective for the TOE development and production environment
- Any objective for the delivery process
- Any objective for the System manufacturing environment

---

#### Objectives for the Product Embedded Software Environment

123 The Product Embedded Software shall provide “Usage of Hardware Platform (OE.Plat-Appl)” as specified below.

OE.Plat-Appl	<p>Usage of Hardware Platform and Key-functions implementation</p> <p>To ensure that the TOE is used in a secure manner the Product Embedded Software shall be designed so that the requirements from the following documents are met:</p> <ul style="list-style-type: none"> <li>■ Hardware data sheet for the TOE</li> <li>■ TOE application notes, and</li> <li>■ Findings of the TOE evaluation reports relevant for the Product Embedded Software.</li> </ul> <p>The product embedded software shall be designed in a secure manner, by using exclusively software development tools (compilers, assemblers, linkers, simulators etc.) and software-hardware integration testing tools (emulators) that will grant the integrity of program and data.</p>
--------------	--

124 The Product Embedded Software shall provide “Treatment of User Data (OE.Resp-Appl)” as specified below.

OE.Resp-Appl	<p>Treatment of User Data</p> <p>Security relevant User Data (especially cryptographic keys) are treated by the Product Embedded Software as required by the security needs of the specific application context.</p> <p>For example the Product Embedded Software will not disclose security relevant User Data to unauthorised users or processes when communicating with a terminal.</p>
--------------	--



125 The Product Embedded Software shall provide “Implementation of key-dependant functions (OE.Key-Function)” as specified below.

OE.Key-Function Implementation of key-dependant functions  
The Product Embedded Software implements key dependant functions (if any) so as to counter leakage attacks that could disclose sensitive data (cryptographic keys, PINs, etc).

126 The Product Embedded Software shall provide “Protection of Product Embedded Software (OE.Dev-Org)” as specified below.

OE.Dev-Org Protection of Product Embedded Software  
The Product Embedded Software Developer shall ensure that procedures for the confidentiality and integrity of the Product Embedded Software and IC designer proprietary information exist and are applied in software development environment during the whole life of the TOE.

---

**Objectives for the TOE Development and Production Environment**

127 The TOE Manufacturer shall ensure the “Protection during TOE Development and Production (OE.Process-TOE)” as specified below.

OE.Process-TOE Protection during TOE Development and Production  
The TOE Manufacturer must ensure that the development and production of the TOE (Phases 2 and 3 up to TOE Delivery, is secure so that no information is unintentionally made available for the operational phase of the TOE. For example, the confidentiality and integrity of design information and test data must be guaranteed, access to samples, development tools and other material must be restricted to authorised persons only, scrap must be destroyed. This not only pertains to the TOE but also to all information and material exchanged with the developer of the Product Embedded Software and therefore especially to the Product Embedded Software itself.  
The TOE designer must have procedures to control the sales, distribution, storage and usage of the software and hardware development tools and classified documents, suitable to maintain the integrity and the confidentiality of the assets of the TOE.





---

**Objectives for the Delivery Process**

128 The Embedded Software Developer / TOE Manufacturer / System Manufacturer shall ensure the “Delivery Procedures (OE.Process-TOE)” as specified below.

OE.Delivery

Delivery Procedures

Procedures shall protect the TOE material and information under delivery and storage. A procedure shall ensure protection of the TOE for unsawn wafer delivery.

Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.

Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

It must be ensured that:

- IC Tools are only delivered to the parties authorized personnel.
- Confidential information such as data sheets and general information on defined assets are only delivered to the parties authorized personnel on the basis of need-to-know.

The Product Embedded Software must be delivered from the product embedded software developer (Phase 1) to the IC designer through a trusted delivery and verification procedure that shall be able to maintain the integrity of the software and its confidentiality, if applicable.

---

**Objectives for the System Manufacturing Environment**

129 The System Manufacturer shall ensure the “Protection during system manufacturing (OE.Process-System)” as specified below.

OE.Process-System

Protection during System manufacturing.

Security procedures shall be used after TOE Delivery up to delivery to the end-user 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 must be protected appropriately.



130 The System Manufacturer shall ensure the “Usage and connection of the TOE (OE.Design-System)” as specified below.

OE.Design-System

Usage and connection of the TOE

System (EFT POS/PINPED) shall be designed making appropriate use of the internal control for external security mechanisms of the TOE (intrusion switches, intrusion mesh inside the PCB, ...) so that access to the physical interface of the TOE is made difficult for an attacker.

Moreover, the TOE shall be fixed on a PCB, permanently backed up by an external battery and connected to an external 32kHz XTAL.



## IT Security Requirements

131 The TOE security functional requirements define the functional requirements for the TOE using functional requirements components drawn from the Common Criteria Part 2 and extended requirements defined in Section 5.3.

132 The minimum strength of function level for the TOE security requirements is SOF-high.

133 There is no specific strength of function claim for the individual SFRs.

### 5.1 TOE Functional Requirements

Table 5-1 Overview of the ST Functional Requirements

Category	Functional Requirement	Detail
Physical probing and manipulation	FPT_PHP.3	Resistance to physical attacks
Malfunction	FRU_FLT.2	Limited fault tolerance
	FPT_FLS.1	Failure with preservation of secure state
	FPT_SEP.1	Domain separation
Leakage	FDP_ITT.1	Basic internal transfer protection
	FPT_ITT.1	Basic internal TSF data transfer protection
	FDP_IFC.1	Subset information flow control
Abuse of test functionalities	FMT_LIM.1	Limited capabilities
	FMT_LIM.2	Limited availability
Identification	FAU_SAS.1	Audit storage
Random numbers	FCS_RND.1	Quality metric for random numbers
Cryptography	FCS_COP.1	Cryptographic operation
	FCS_CKM.1	Cryptographic key generation
Test of security functions	FPT_TST.2	TOE security functions testing, selftest done by the IC dedicated support software
	FDP_SDI.1	Stored data integrity



Table 5-1 (Continued) Overview of the ST Functional Requirements

Configuration of security system	FMT_MOF.1	Management of security function behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
SW memory access	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control

134

Table 5-1 presents the security functional requirements used in this Security Target Lite, adapted from [BSI\_PP] and [BSI\_AUG]. The only additions are FDP\_SDI.1 and FMT\_MOF.1. taken directly from the Common Criteria part 2.



135

The justification for the choice of SFRs is listed below against the Security Goals defined in section 4.2.

**SG1** Integrity of User Data and Product Embedded Software

and

**SG2** Maintain confidentiality of User Data and Product Embedded Software

FDP\_ITT.1 Basic Internal Transfer Protection - *Protection of Data when transferred between areas of the TOE*

FPT\_ITT.1 Basic Internal TSF data transfer protection - *The SFR is as above but refers to TSF data instead of User Data*

FDP\_IFC.1 Subset information flow control - *Protection of confidential data when processed or transferred by the TOE or by the Product Embedded Software*

FMT\_MOF.1 Management of Security Functions Behaviour - *Manage the modification of TSF to privileged authorised users*

FPT\_PHP.3 Resistance to Physical Attack - *Protection of assets from physical manipulation*

FPDP\_SDI.1 Stored Data Integrity Monitoring - *This SFR ensures that the stored data can be checked to identify if a physical attack has taken place*

FRU\_FLT.2 Limited Fault Tolerance - *This defines the operating conditions that the TOE will operate normally.*

PPT\_FLS.1 Failure with Preservation of Secure State - *If the conditions defined by FRU\_FLT.2 are violated then this SFR ensures that no assets are leaked.*

FPT\_SEP.1 TSF Domain Separation - *Maintains safe areas for the assets to be stored within the TOE, and defines the domain boundaries*

FPT\_TST.2 Subset TOE testing - *The TOE requires to be tested to ensure the correct operation of the TSF*

FMT\_LIM.1 Limited capabilities - *This SFR prevents the Test Mode capability being misused by an attacker*

FMT\_LIM.2 Limited availability - *As above this prevents the misuse of Test Mode*

FAU\_SAS.1 Audit Storage - *this SFR ensures that the TM administrator stores records within the TOE, that allows the developer to trace the individual TOE through it's life cycle.*



<b>SG1</b> and <b>SG2</b> cont.	<p>FDP_ACC.1 Complete Access Control - <i>This SFR defines the firewall/MPU subjects and objects</i></p> <p>FDP_ACF.1 Security Attribute Based Access Control- <i>This SFR allows the definition which subject is allowed to access what object and what restrictions are placed on the subject</i></p> <p>FMT_MSA.3 Static Attribute Initialisation - <i>This SFR provides a statement on what subjects are allowed to modify the Firewall/MPU rules</i></p> <p>FMT_MSA.1 Management of Security Functions - <i>As above this defines which authenticated subjects are allowed to modify the access control policy</i></p>
<b>SG3</b> Provide Random Numbers	FCS_RND.1 Quality Metric for Random Numbers - <i>This SFR is included to define the standard that the hardware RNG requires to meet</i>
<b>SG4</b> Provide Additional security functionality	FCS-COP.1 Cryptographic Operation - <i>This defines the cryptographic functions the TOE requires to meet</i>

136

The SFRs defined above can be grouped into specific objectives to show how they combine to achieve the security objectives defined in section 4.2.

- Leak of Information
  - FDP\_ITT.1
  - FPT\_ITT.1
  - FDP\_IFC.1
  - FMT\_MOF.1
- Physical Probing and Manipulation
  - FPT\_PHP.3
  - FDP\_SDI.1
- Malfunction of TOE
  - FRU\_FLT.2
  - FPT\_FLS.1
  - FPT\_SEP.1
  - FMT\_MOF.1
  - FPT\_TST.2
- Abuse of functionality
  - FMT\_LIM.1
  - FMT\_LIM.2
- Identification of TOE
  - FAU\_SAS.1
- Protection of Memory Access
  - FDP\_ACC.2
  - FDP\_ACF.1



- FMT\_MSA.3
- FMT\_MSA.1
- FMT\_MOF.1
- Random Number Generation
  - FCS\_RND.1
- Cryptography
  - FCS\_COP.1
  - FCS\_CKM.1

137 The ST does not define any SFRs required for the IT Environment.

### 5.1.1 Functional Requirements related to Physical Probing and Manipulation

138 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
FPT_PHP.3.1	The TSF shall resist physical manipulation and physical probing to the TSF by responding automatically such that the TSP is not violated.
Refinement:	The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, “automatic response” means here: <ul style="list-style-type: none"> <li>■ Assuming that there might be an attack at any time</li> <li>■ and countermeasures are provided at any time.</li> </ul>
Dependencies:	No dependencies.



### 5.1.2 Functional Requirements Related to Physical Malfunction

139 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
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) .
Dependencies	FPT_FLS.1 Failure with preservation of secure state
Refinement:	The term “failure” above means “circumstances”. The TOE prevents failures for the “circumstances” defined above.

140 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 .
Dependencies	ADV_SPM.1 Informal TOE security policy model
Refinement	The term “failure” above also covers “circumstances”. The TOE prevents failures for the “circumstances” defined above





141 The TOE shall meet the requirement “TSF domain separation (FPT\_SEP.1)” as specified below.

<b>FPT_SEP.1</b>	TSF domain separation
Hierarchical to	No other components
FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC
Dependencies	No dependencies
Refinement:	Those parts of the TOE which support the security functional requirements “Limited fault tolerance (FRU_FLT.2)” and “Failure with preservation of secure state (FPT_FLS.1)” shall be protected from interference of the Product Embedded Software.

### 5.1.3 Functional Requirements Related to Leakage

142 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 to prevent the disclosure 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.



143 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 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 <i>Data Processing Policy</i> defined under FDP_IFC.1 below.

144 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 on all confidential data when they are processed or transferred by the TOE or by the Product Embedded Software
Dependencies	FDP_IFF.1 Simple security attributes



#### 5.1.4 Functional Requirements Related to Abuse of Test Functions

145 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 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.
Dependencies	FMT_LIM.2 Limited availability

146 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 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
Dependencies	FMT_LIM.1 Limited capabilities



**5.1.5 Functional Requirements Related to Identification**

147 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
FAU_SAS.1.1	The TSF shall provide test personnel before TOE Delivery with the capability to store the Initialisation Data and/or Pre-personalisation Data and/or supplements of the Product Embedded Software in the audit records.
Dependencies	No dependencies

**5.1.6 Functional Requirements Related to Random Numbers**

148 The TOE shall meet the requirement “Quality metric for random numbers (FCS\_RND.1)” as specified below (Common Criteria Part 2 extended).

FCS_RND.1	Quality metric for random numbers
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet PCI POS PED document Appendix C [PCI-PED] quality metric.
Dependencies	No dependencies

**5.1.7 Functional Requirements Related to Cryptography**

**DES Operation**

149 The TOE shall meet the requirement “Cryptographic operation (FCS\_COP.1)” on DES operations as specified below.

FCS_COP.1	Cryptographic operation
-----------	-------------------------



Hierarchical to:	No other components
FCS_COP.1.1	The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Data Encryption Standard (DES) and cryptographic key sizes of 56 bit that meet the following standards:  U.S. Department of Commerce / National Bureau of Standards, Data Encryption Standard (DES), FIPS PUB 46-3, 1999 October 25.
Dependencies:	(FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation)  FCS_CKM.4 Cryptographic key destruction  FMT_MSA.2 Secure security attributes

#### Triple DES Operation

150 The TOE shall meet the requirement “Cryptographic operation (FCS\_COP.1)” on Triple DES operations as specified below.

FCS_COP.1	Cryptographic operation
Hierarchical to:	No other components
FCS_COP.1.1	The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Triple Data Encryption Standard (T-DES) and cryptographic key size of 112 bit that meet the following standards:  U.S. Department of Commerce / National Bureau of Standards Data Encryption Standard (DES), FIPS PUB 46-3, 1999 October 25.
Dependencies:	(FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation)  FCS_CKM.4 Cryptographic key destruction  FMT_MSA.2 Secure security attributes



---

**Advanced Encryption Standard (AES)**

151 The TOE shall meet the requirement “Cryptographic operation (FCS\_COP.1)” on AES operations as specified below.

FCS\_COP.1 Cryptographic operation

Hierarchical to: No other components

FCS\_COP.1.1 The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Advanced Encryption Standard (AES) and cryptographic key sizes of 128, 192, and 256 bits that meet the following standards:

Federal Information Processing Standards (FIPS)  
Publication draft available at the AES home page:  
<http://www.nist.gov/aes/>.

J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES  
Algorithm Submission, September 3, 1999.

Dependencies: (FDP\_ITC.1 Import of user data without security attributes  
or FCS\_CKM.1 Cryptographic key generation])

FCS\_CKM.4 Cryptographic key destruction

FMT\_MSA.2 Secure security attributes



**Rivest-Shamir-Adleman (RSA)**

152 The TOE shall meet the requirement “Cryptographic operation (FCS\_COP.1)” on modular arithmetic operation as specified below.

FCS_COP.1	Cryptographic operation
Hierarchical to:	No other components
FCS_COP.1.1	The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Rivest-Shamir-Adleman (RSA), with and without CRT and cryptographic key sizes 1024 bits to 4096 bits that meet the following standards:  ISO/IEC 9796-1, Annex A, sections A.4 and A.5, and Annex C.
Dependencies:	(FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation)  FCS_CKM.4 Cryptographic key destruction  FMT_MSA.2 Secure security attributes

**Secure Hash Algorithm (SHA)**

153 The TOE shall meet the requirement “Cryptographic operation (FCS\_COP.1)” on SHA operations as specified below.

FCS_COP.1	Cryptographic operation
Hierarchical to	No other components
FCS_COP.1.1	The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm Secure Hash Algorithm SHA-1, SHA-256, SHA-384, SHA-512 that meet the following standards:  FIPS 180-2 Secure Hash Standard, August 2002
Dependencies:	(FDP_ITC.1 Import of user data without security attributes or FCS_CKM.1 Cryptographic key generation)  FCS_CKM.4 Cryptographic key destruction  FMT_MSA.2 Secure security attributes
Note:	An example for the [assignment: cryptographic key sizes] is “of 160 bits and modulus size N bits, where N is a multiple of 64 such that $512 \leq N \leq 1024$ bit.”



**Prime Generation (RSA key generation)**

154 The TOE shall meet the requirement “Cryptographic Key Generation (FCS\_CKM.1)” as specified below.

FCS_CKM.1	Cryptographic Key Generation
Hierarchical to	No other components
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with cryptographic key generation Miller Rabin algorithm with confidence criteria (t) between 0 and 255 and specified cryptographic key sizes between 192-bits and 4096-bits (respectively 2 primes of size between 96 bits and 2048 bits) specified by the NIST special publication 800-2, April 1991.
Dependencies:	(FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation) FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

**5.1.8 Functional Requirements Related to Test of Security Functions**

155 The TOE shall meet the requirement “Subset TOE testing (FPT\_TST.2)” as specified below.

FPT_TST.2	Subset TOE testing
Hierarchical to:	No other components
FPT_TST.2	The TSF shall run a suite of self tests at the request of the environmental mechanisms
Dependencies:	FPT_AMT.1 (Abstract Machine Testing)

156 The TOE shall meet the requirement “Stored data integrity monitoring (FDP\_SDI.1)” as specified below.

FDP_SDI.1	Stored data integrity monitoring
Hierarchical to	No other components
FDP_SDI.1.1	The TSF shall monitor User Data stored within the TSC for integrity errors on all objects, based on the following attributes: <b>Not Disclosed in ST-Lite</b>
Dependencies	No dependencies





### 5.1.9 Functional Requirements Related to the Configuration of Security System

157 The TOE shall meet the requirement “Management of security functions behavior (FMT\_MOF.1)” as specified below

FMT_MOF.1	Management of security functions behaviour
Hierarchical to:	No other components.
FMT_MOF.1.1	The TSF shall restrict the ability to modify the behaviour of the functions: <b>Not Disclosed in ST-Lite</b> provided the ACSF access control policy is enforced.
Dependencies:	FMT_SMF.1 FMT_SMR.1
<i>Application note:</i>	<i>This statement only concerns modifications of the security functions behavior that impacts the security. <b>Not Disclosed in ST-Lite.</b></i>

### 5.1.10 Functional Requirements Related to SW Memory Access

158 The TOE shall meet the requirement “Complete access control (FDP\_ACC.2)” as specified below.

FDP_ACC.2	Complete access control
Hierarchical to	FDP_ACC.1 Subset access control
FDP_ACC.2.1	The TSF shall enforce the ACSF access control SFP on: <b>Not Disclosed in ST-Lite</b> and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2	The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP
Dependencies:	FDP_ACF.1 Security attribute based access control

159 The TOE shall meet the requirement “Security attribute based access control (FDP\_ACF.1)” as specified below.

FDP_ACF.1	Security attribute based access control
Hierarchical to:	No other components
FDP_ACF.1.1	The TSF shall enforce the ACSF access control SFP to objects based on the following: <b>Not Disclosed in ST-Lite</b>



	FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <b>Not Disclosed in ST-Lite</b>
	FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: <b>Not Disclosed in ST-Lite</b>
	FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: <b>Not Disclosed in ST-Lite</b>
	Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
160	The TOE shall meet the requirement “Static attribute initialisation (FMT_MSA.3)” as specified below.	
	FMT_MSA.3	Static attribute initialisation
	Hierarchical to:	No other components
	FMT_MSA.3.1	The TSF shall enforce the ACSF access control SFP to provide restrictive default values for security attributes that are used to enforce the SFP.
	FMT_MSA.3.2	The TSF shall allow any subject (provided that the ACSF access control policy is enforced and the necessary access is therefore allowed) to specify alternative initial values to override the default values when an object or information is created.
	Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
	<i>Application Note:</i>	<b>Not Disclosed in ST-Lite</b>
161	The TOE shall meet the requirement “Management of security attributes (FMT_MSA.1)” as specified below.	
	FMT_MSA.1	Management of security attributes
	Hierarchical to	No other components
	FMT_MSA.1.1	The TSF shall enforce the ACSF access control SFP to restrict the ability to modify <b>Not Disclosed in ST-Lite</b> .
	Dependencies:	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control) FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions



---

## 5.2 TOE Security Assurance Requirements

162 The assurance requirement are those EAL4 augmented with ALC\_DVS.2, ADV\_IMP.2, AVA\_MSU.3 and AVA\_VLA.4.

163 All the components are drawn from Common Criteria Part 3, V2.3.

164 High strength of function is claimed.

---

### TOE Security Assurance Requirements

- Development activities (ADV class)
  - ADV\_FSP.2
  - ADV\_SPM.1
  - ADV\_HLD.2
  - ADV\_LLD.1
  - ADV\_IMP.2
  - ADV\_RCR.1
- Test activities (ATE class)
  - ATE\_COV.2
  - ATE\_DPT.1
  - ATE\_FUN.1
  - ATE\_IND.2
- Deliveries and operation activities (ADO class)
  - ADO\_DEL.2
  - ADO\_IGS.1
- Guidance documents activities (AGD class)
  - AGD\_ADM.1
  - AGD\_USR.1
- Configuration management activities (ACM class)
  - ACM\_AUT.1
  - ACM\_CAP.4
  - ACM\_SCP.2



- Life cycle support activities (ALC class)
  - ALC\_DVS.2
  - ALC\_LCD.1
  - ALC\_TAT.1
- Vulnerability assessment activities (AVA class)
  - AVA\_MSU.3
  - AVA\_SOF.1
  - AVA\_VLA.4

---

### 5.3 Definition of Extended Security Functional Requirements

165 The extended security functional requirements used in this Security Target Lite have been defined in [BSI\_PP].

#### 5.3.1 Definition of the family FCS\_RND

166 To define the IT security functional requirements of the TOE an additional family (FCS\_RND) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

#### 167 **FCS\_RND Generation of random numbers**

Family behaviour

This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

Component levelling:

FCS\_RND Generation of random numbers 1

FCS\_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS\_RND.1

There are no management activities foreseen.

Audit: FCS\_RND.1

There are no actions defined to be auditable.

FCS\_RND.1 Quality metric for random numbers

Hierarchical to: No other components.



FCS\_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].

Dependencies: No dependencies.

### 5.3.2 Definition of the family FMT\_LIM

168 To define the IT security functional requirements of the TOE an additional family (FMT\_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE (refer to Section 5.1.1) show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

169 The family “Limited capabilities and availability (FMT\_LIM)” is specified as follows.

#### 170 **FMT\_LIM Limited capabilities and availability**

171 Family behaviour

172 This family defines requirements that limits the capabilities and availability of functions in a combined manner. Note that FDP\_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

173 Component levelling:

174 FMT\_LIM Limited capabilities and availability: 1 - 2

175 FMT\_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

176 FMT\_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT\_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s life-cycle.

177 Management: FMT\_LIM.1, FMT\_LIM.2

178 There are no management activities foreseen.

179 Audit: FMT\_LIM.1, FMT\_LIM.2

180 There are no actions defined to be auditable.

181 The TOE Functional Requirement “Limited capabilities (FMT\_LIM.1)” is specified as follows.



182           **FMT\_LIM.1** Limited capabilities

183           Hierarchical to: No other components.

184           FMT\_LIM.1.1 The TSF shall be designed in a manner that limits their capabilities so that in conjunction with “Limited availability (FMT\_LIM.2)” the following policy is enforced [assignment: Limited capability and availability policy].

185           Dependencies: FMT\_LIM.2 Limited availability.

186           The TOE Functional Requirement “Limited availability (FMT\_LIM.2)” is specified as follows.

187           **FMT\_LIM.2** Limited availability

188           Hierarchical to: No other components.

189           FMT\_Lim.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with “Limited capabilities (FMT\_LIM.1)” the following policy is enforced [assignment: Limited capability and availability policy].

190           Dependencies: FMT\_LIM.1 Limited capabilities.

191           Application note: The functional requirements FMT\_LIM.1 and FMT\_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

192           the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced or conversely

193           the TSF is designed with high functionality but is removed or disabled in the product in its user environment.

194           The combination of both requirements shall enforce the policy.

### **5.3.3 Definition of family FAU\_SAS**

195           To define the security functional requirements of the TOE an additional family (FAU\_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirement for the storage of audit data. It has a more general approach than FAU\_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

196           The family “Audit data storage (FAU\_SAS)” is specified as follows.

197           **FAU\_SAS** Audit data storage



198 Family behaviour

199 This family defines functional requirements for the storage of audit data.

200 Component levelling

201 FAU\_SAS Audit data storage: 1

202 FAU\_SAS.1 Requires the TOE to provide the possibility to store audit data.

203 Management: FAU\_SAS.1

204 There are no management activities foreseen.

205 Audit: FAU\_SAS.1

206 There are no actions defined to be auditable.

207 **FAU\_SAS.1** Audit storage

208 Hierarchical to: No other components.

209 FAU\_SAS.1.1 The TSF shall provide [assignment: authorised users] with the capability to store [assignment: list of audit information] in the audit records.

210 Dependencies: No dependencies.

#### **5.3.4 Definition of the security functional component FPT\_TST.2**

211 The following addition is made to “TSF self test (FPT\_TST)” in Common Criteria for Information Technology Security Evaluation, Part 2.

212 Component levelling

213 FPT\_TST TSF self test: 1 - 2

214 FPT\_TST.1 TSF testing, provides the ability to test the TSF’s correct operation. These tests may be performed at start-up, periodically, at the request of the authorised user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and executable code.

215 FPT\_TST.2 Subset TOE security testing, provides the ability to test the correct operation of particular security functions or mechanisms. These tests may be performed at start-up, periodically, at the request of the authorised user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and executable code.

216 The security functional component family “Subset TOE testing (FPT\_TST.2)” is specified as follows.



## Security Target Lite

- 217            **FPT\_TST.2** Subset TOE testing
- 218            Hierarchical to: No other components.
- 219            FPT\_TST.2.1 The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, and/or at the conditions [assignment: conditions under which self test should occur] to demonstrate the correct operation of [assignment: functions and/or mechanisms].
- 220            Dependencies: FPT\_AMT.1 Abstract machine testing





---

## TOE Summary Specification

221 This section presents the TOE security functions that implement the security functional requirements defined in 5.1 and the TOE assurance measures that implement the security assurance requirements defined in 5.2.

---

### 6.1 TOE Security Functions

#### 6.1.1 SF1 (F.CORR\_OPERATION)

222 SF1: hardware protection against out-of-range environmental conditions

223 The TOE provides the following mechanisms for detecting out-of-range environmental conditions and responding automatically so that a secure state is preserved

- Voltage monitors for power supply pins. These monitors cannot be disabled.
- Frequency monitors for different clock signals. These monitors cannot be disabled by software.
- Temperature monitor. This monitor cannot be disabled by software.
- Watchdog timer for preventing system lock-up if software becomes trapped in a deadlock.

224 Depending on the kind of violation, SF1 responds automatically either immediately, or after one or two occurrences, as defined in [TD].

225 Whenever possible, the TOE logs the causes of the violation in specific registers, accessible to privileged users only [TD].

226 SF1 also provides the exception handling management of reset, abort and interruptions.



**6.1.2 SF2 (F.LOGICAL\_PROTECTION)**

227 SF2: logical protection against leakage

228 The TOE provides mechanisms that protects the TOE's assets against leakage.

229 Mechanisms against power (SPA, DPA), timing and differential fault analysis



**6.1.3 SF3 (F.PHYSICAL\_PROTECTION)**

230 SF3: Physical protection against physical probing and manipulation

231 The TOE provides mechanisms and security-aware design features against physical probing and manipulation.

232 The physical monitors cannot be deactivated by software.

**6.1.4 SF4 (F.PREV\_ABUSE)**

233 SF4: Test functionality and prevention of abuse after delivery

234 The TOE provides limited availability of the test functionality after delivery, through a restricted Package mode entry, and limited capabilities of the test functionalities in this mode. SF4 is involved in two phases:

- Before delivery:
  - Test Mode entry
- After delivery:
  - Package Mode entry

**6.1.5 SF5 (F.IDENTIFICATION)**

235 SF5: TOE unique identification

236 The TOE provides means to store Initialization/Pre-personalization TOE and Embedded Software Data, in particular the unique chip serial number that allows to identify the TOE all along its life cycle.

**6.1.6 SF6 (F.RNG)**

237 SF6: Random Number Generator

238 The TOE includes a hardware random number generator

239 The Random Number Generator has been tested according to the document PCI POS PED:

- PCI POS PIN Entry Device Derived Tests Requirements Version 1.3 February 2005, Appendix C "Configuration and Use of the sts Tool" describes the Random Number Generator Test
- The random generation is made by using The Hardware Number Generator and a post processing function.

240 The post processing function is a Deterministic Random Number Generator (DRNG) defined by:



- The DRNG is described in the document NIST Digital Signature Standard (DSS) FIPS Pub 186-2 January 27, 2000 Appendix 3.1
- The FIPS 186-2 Change Notice 1 dated 2001 October 5 paragraph "Revised Algorithm for computing m values of x (Appendix 3.1 of FIPS 186-2)" that modifies this algorithm.

241 The DRNG used is the one described in the change notice. The FIPS PUB 140-2 "Security Requirements for Cryptographic Modules" in its Annex C "Approved Random Number Generators" lists the DRNG:

- NIST DSS FIPS 186-2 January 27 2000 Appendix 3.1.
- The Change Notice 1 dated 2001 October 5 is also applicable according to Elaine Barker [elaine.barker@nist.gov] (National Institute of Standards and Technology 100 Bureau Drive, Stop 8930 Gaithersburg, MD 20899-8930)

242 The Strength of Function claimed for SF6 is high.

### 6.1.7 SF 7 (F. Crypto)

243 SF7: Cryptographic support

244 The TOE provides hardware cryptographic engines and software cryptographic libraries to support Product Embedded Software data encryption, decryption, signature generation and verification, and integrity protection.

---

#### **F.Crypto.DES: DES/TDES encrypt/decrypt (CBC, ECB and MAC modes)**

- HW DES engine
- SW DES in crypto library

245 SF7 provides DES and Triple DES encryption and decryption in CBC, ECB and MAC modes.

---

#### **F.Crypto.AES: AES encrypt/decrypt (CBC, ECB, and MAC modes)**

- HW AES engine
- SW AES in crypto library

246 SF7 provides AES 128-Bit, AES 192-Bit and AES 256-Bit encryption and decryption in CBC, ECB and MAC modes.

247 The hardware AES engine is compliant with FIPS PUBS 197 Specifications.



---

**F.Crypto.RSA: RSA encrypt/decrypt (with/without CRT)**

- HW AdvX arithmetic coprocessor
- SW RSA in crypto library

248 SF7 provides RSA with and without CRT and cryptographic key sizes 1024 bits to 4096 bits.

249 The AdvX is a free running cryptographic accelerator, providing mathematical primitives.

---

**F.Crypto.PRIME: Prime generation**

- HW AdvX arithmetic coprocessor.
- SW in crypto library.

250 SF7 provides software prime generation (RSA cryptographic key generation) capability using Miller Rabin algorithm with confidence criteria (t parameter) between 0 and 255.

---

**F.Crypto.SHA: Secure Hash Algorithm**

- SHA-1, SHA-256 (HW AdvX arithmetic coprocessor + SHA engine + SW Library)
- SHA-384 and SHA-512 (SW Library only)

251 SF7 provides the above mentioned Secure Hash Algorithms, combining AdvX and the SW library.

252 An assessment of the strength of the following algorithms does not form part of the evaluation:

- DES algorithm
- TDES algorithm
- SHA algorithms
- RSA without CRT algorithm
- RSA with CRT algorithm
- Miller Rabin algorithm



#### 6.1.8 SF8 (F.MEMORY\_ACCESS)

253 SF8: Area based memory access control

254 The TOE provides mechanisms to restrict and control access (read, write, execute) to memories (RAM, ROM, EEPROM, etc).

#### 6.1.9 SF9 (F.INTEGRITY)

255 SF9: Integrity support

256 The TOE provides a Cyclic Redundancy Check (CRC) accelerator to support integrity checks that accepts either two CRC16 or one CRC32 polynomes.

257 The TOE also provides a HW User key integrity engine.

#### 6.1.10 SF10 (F.SECURE\_BOOTSTRAP)

258 SF10: Secure Bootstrap

259 The TOE provides a secure bootstrap routine in ROM. **Not Disclosed in ST-Lite**

#### 6.1.11 Security Functions Based on Permutations/combinations

260 The Security function SF4 is based on mechanisms using permutation and/or combination properties.

261 SF2 and SF8 include some memory hardware encryption mechanisms, and can be considered as using permutation and/or combination properties.

262 SF3 includes active shield mechanisms, and can be considered as using permutation and/or combination properties.

SF7 deals with cryptographic operations, and can be considered as using permutation and/or combination properties. It is however reminded that an assessment of the strength of the algorithms of SF7 does not form part of the evaluation.

263 Therefore, the resistance of SF2, SF4, SF3, SF7 and SF8 should be evaluated against attacks using brute force techniques.



6.2 TOE Assurance Measures

Table 6-1 lists the TOE specific assurance measures.

Table 6-1 Relationship Between Assurance Requirements and Measures

Assurance Requirement	Security Target Lite	Configuration Management	Delivery and Operation	Development Activity	Guidance	Life Cycle Support	Test Activity	Vulnerability assessment	Product Devices	Development Site	Test Site	Manufacturing Site	Sub-contractor Site
	SA1	SA2	SA3	SA4	SA5	SA6	SA7	SA8	SA9	SA10	SA11	SA12	SA13
ASE_xxx	x												
ACM_AUT.1		x								x	x	x	x
ACM_CAP.4		x								x	x	x	x
ACM_SCP.2		x								x	x	x	x
ADO_DEL.2			x							x	x	x	x
ADO_IGS.1			x							x	x	x	x
ADV_FSP.2				x									
ADV_HLD.2				x									
ADV_IMP.2				x									
ADV_LLD.1				x									
ADV_RCR.1				x									
ADV_SPM.1				x									
AGD_ADM.1					x								
AGD_USR.1					x								
ALC_DVS.2						x				x	x	x	x
ALC_LCD.1						x				x	x	x	x
ALC_TAT.1						x				x	x	x	x
ATE_COV.2							x		x		x		
ATE_DPT.1							x		x		x		
ATE_FUN.1							x		x		x		
ATE_IND.2							x		x		x		
AVA_MSU.3								x	x				
AVA_SOF.1								x	x				
AVA_VLA.4								x	x				



**6.2.1 Security Target Lite (SA1)**

264 SA1 shall provide the “Security Target Lite” document plus its references.

**6.2.2 Configuration Management (SA2)**

265 SA2 shall provide the “CC Configuration Management (ACM)” interface document plus its references.

**6.2.3 Delivery and Operation (SA3)**

266 SA3 shall provide the “CC Delivery and Operation (ADO)” interface document plus its references.

**6.2.4 Development Activity (SA4)**

267 SA4 shall provide the “CC Development Activity (ADV)” interface document plus its references.

**6.2.5 Guidance (SA5)**

268 SA5 shall provide the “CC Guidance (AGD)” interface document plus its references.

**6.2.6 Life Cycle Support (SA6)**

269 SA6 shall provide the “CC Life Cycle Support (ALC)” interface document plus its references.

**6.2.7 Test Activity (SA7)**

270 SA7 shall provide the “CC Test Activity (ATE)” interface document plus its references, and undertaking of testing described therein.

**6.2.8 Vulnerability Assessment (SA8)**

271 SA8 shall provide the “CC Vulnerability Assessment (AVA)” interface document plus its references, and undertaking of vulnerability assessment described therein.

**6.2.9 Product Devices (SA9)**

272 SA9 shall provide functional AT90SO100/101 product devices.





**6.2.10 Development Site (SA10)**

273 SA10 shall provide access to the development site.

**6.2.11 Test Site (SA11)**

274 SA11 shall provide access to the test site.

**6.2.12 Manufacturing Site (SA12)**

275 SA12 shall provide access to the manufacturing site.

**6.2.13 Sub-contractor Sites (SA13)**

276 SA13 shall provide access to the sub-contractor sites.





PP conformance claim

277      Nothing to report.



---

## A.1 Terms

<b>Control Bytes</b>	Reserved bytes of EEPROM which can be programmed with traceability information.
<b>CRC-32</b>	Algorithm used to compute powerful checksum on memory blocks
<b>HASH</b>	Transformation of a string of characters into a usually shorter fixed length value or key that represents the original string.
<b>IC Dedicated Software</b>	<p>IC Proprietary software which is required for testing purposes and to implement special functions. For AT90SO100/101 this includes the embedded test software and additional test programmes which are run from outside of the IC.</p> <p>The Crypto libraries also form part of the IC dedicated software.</p>
<b>IC Designer</b>	Institution (or its agent) responsible for the IC Development. Atmel is the institution in respect of the TOE.
<b>IC Manufacturer</b>	Institution (or its agent) responsible for the IC manufacturing, testing and pre-personalization. Atmel is the institution in respect of the TOE.
<b>IC Packaging Manufacturer</b>	Institution (or its agent) responsible for the IC packaging and testing.
<b>IC Pre-personalization Data</b>	Required information to enable the product IC to be configured by means of ROM options and to enable programming of the EEPROM with customer specified data.
<b>Integrated Circuit (IC)</b>	Electronic component(s) designed to perform processing and/or memory functions.



<b>Personalizer</b>	Institution (or its agent) responsible for the product personalization and final testing.
<b>Product Embedded Software</b>	Software embedded in the product application (product application software). This software is provided by product embedded software developer (customer). Embedded software may be in any part of User ROM or EEPROM.
<b>Product Embedded Software Developer</b>	Institution (or its agent) responsible for the Product embedded software development and the specification of pre-personalization requirements.
<b>Product Issuer</b>	Institution (or its agent) responsible for the product delivery to the end-user.
<b>Product Manufacturer</b>	Institution (or its agent) responsible for the product finishing process and testing.



---

## A.2 Abbreviations

<b>AdvX</b>	32-bit Crypto Accelerator developed and produced by ATMEL
<b>CC</b>	Common Criteria
<b>CPU</b>	Central Processing Unit
<b>CRC</b>	Cyclic Redundancy Check
<b>CSO</b>	Colarado Springs Operation
<b>DES</b>	Data Encryption Standard
<b>DPA</b>	Differential Power Analysis
<b>EEPROM</b>	Electrically Erasable Programmable ROM
<b>FIB</b>	Focussed Ion Beam
<b>HCMOS</b>	High Speed Complementary Metal Oxide Semiconductor
<b>I/O</b>	Input/Output
<b>IC</b>	Integrated Circuit
<b>ISO</b>	International Standards Organization
<b>LFSR</b>	Linear Feedback Shift Register
<b>MAC</b>	Master Authentication Key
<b>NVM</b>	Non Volatile Memory
<b>OTP</b>	One Time Programmable
<b>PME</b>	Package Mode Entry
<b>PMT</b>	Package Mode Test
<b>PP</b>	Protection Profile
<b>RAM</b>	Random-Access Memory
<b>RFO</b>	Rousset France Operations
<b>RISC</b>	Reduced Instruction Set Core
<b>RNG</b>	Random Number Generator
<b>ROM</b>	Read-Only Memory
<b>SPA</b>	Simple Power Analysis
<b>TD</b>	Technical Data
<b>TME</b>	Test Mode Entry
<b>TOE</b>	Target of Evaluation
<b>VFO</b>	Variable Frequency Oscillator





## Atmel Corporation

2325 Orchard Parkway  
San Jose, CA 95131, USA  
Tel: 1(408) 441-0311  
Fax: 1(408) 487-2600

## Regional Headquarters

### Europe

Atmel Sarl  
Route des Arsenalux 41  
Case Postale 80  
CH-1705 Fribourg  
Switzerland  
Tel: (41) 26-426-5555  
Fax: (41) 26-426-5500

### Asia

Room 1219  
Chinachem Golden Plaza  
77 Mody Road Tsimshatsui  
East Kowloon  
Hong Kong  
Tel: (852) 2721-9778  
Fax: (852) 2722-1369

### Japan

9F, Tonetsu Shinkawa Bldg.  
1-24-8 Shinkawa  
Chuo-ku, Tokyo 104-0033  
Japan  
Tel: (81) 3-3523-3551  
Fax: (81) 3-3523-7581

## Atmel Operations

### Memory

2325 Orchard Parkway  
San Jose, CA 95131, USA  
Tel: 1(408) 441-0311  
Fax: 1(408) 436-4314

### Microcontrollers

2325 Orchard Parkway  
San Jose, CA 95131, USA  
Tel: 1(408) 441-0311  
Fax: 1(408) 436-4314

La Chantrerie  
BP 70602  
44306 Nantes Cedex 3, France  
Tel: (33) 2-40-18-18-18  
Fax: (33) 2-40-18-19-60

### ASIC/ASSP/Smart Cards

Zone Industrielle  
13106 Rousset Cedex, France  
Tel: (33) 4-42-53-60-00  
Fax: (33) 4-42-53-60-01

1150 East Cheyenne Mtn. Blvd.  
Colorado Springs, CO 80906, USA  
Tel: 1(719) 576-3300  
Fax: 1(719) 540-1759

Scottish Enterprise Technology Park  
Maxwell Building  
East Kilbride G75 0QR, Scotland  
Tel: (44) 1355-803-000  
Fax: (44) 1355-242-743

### RF/Automotive

Theresienstrasse 2  
Postfach 3535  
74025 Heilbronn, Germany  
Tel: (49) 71-31-67-0  
Fax: (49) 71-31-67-2340

1150 East Cheyenne Mtn. Blvd.  
Colorado Springs, CO 80906, USA  
Tel: 1(719) 576-3300  
Fax: 1(719) 540-1759

### Biometrics/Imaging/Hi-Rel MPU/ High Speed Converters/RF Datacom

Avenue de Rochepleine  
BP 123  
38521 Saint-Egreve Cedex, France  
Tel: (33) 4-76-58-30-00  
Fax: (33) 4-76-58-34-80

---

## Literature Requests

[www.atmel.com/literature](http://www.atmel.com/literature)

**Disclaimer:** The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. **EXCEPT AS SET FORTH IN ATMEL'S TERMS AND CONDITIONS OF SALE LOCATED ON ATMEL'S WEB SITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.** Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel's products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

© Atmel Corporation 2008. All rights reserved. Atmel®, logo and combinations thereof, Everywhere You Are® and others, are registered trademarks or trademarks of Atmel Corporation or its subsidiaries. Other terms and product names may be trademarks of others.



Printed on recycled paper.