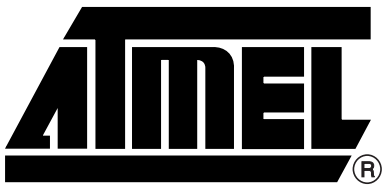
Atmel Toolbox 00.03.11.05

on the AT90SC Family of Devices

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 Toolbox 00.03.11.05 on the AT90SC Family Security Target Lite

1.1 Identification

1 Title: Atmel Toolbox 00.03.11.05 on the Atmel AT90SC Family Security Target Lite

2 Version: TPG0177A_(19 Dec 08)

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

1.2 Overview

Protection Profile Claims

4 This Security Target Lite (ST-Lite) is based on the Protection Profile BSI-PP-002-2001, with additions taken from the Smartcard Integrated Circuit Augmentations BSI-AUG-2002:

Document	Title	Date
BSI-PP-002-2001	Smartcard IC Platform Protection Profile V1.0	July 2001
BSI-AUG-2002	Smartcard Integrated Circuit Platform Augmentations	March 2002


Note

The complete Hardware and Software part that is the AT90SC product and the Atmel Cryptographic Toolbox is complaint to the BSI-PP-002-2001, this Security target details only the software part of the completed AT90SC part therefore this ST is based on the PP rather than fully compliant.

AT90SC Family Project Derivation

5 The AT90SC family of devices consists of a microcontroller (MCU) device with security features. The device is a member of a family of single chip MCU devices which are intended for use within Smartcard products. The family codename is AT90SC ASL4 and the ‘parent’ device of the family, the initial device in the family was the VEGA2 project, part number AT90SC19264RC, certified under the French CC scheme, Ref. 2002/04.

Cryptographic Toolbox

6 The IC dedicated Support Software defined in this Security Target, is a Cryptographic Toolbox that provides a set of cryptographic functions that can be used by the Smartcard embedded Software on the AT90SC hardware device. The AT90SC family provides a Cryptographic Accelerator and MCU to provide hardware support to the cryptographic toolbox functions. The crypto library is stored in the ROM* of the AT90SC family and is linked to the Smartcard Embedded Software.The initial standalone certified version of the Atmel cryptographic Toolbox is 00.03.01.07, this was certified under the French CC scheme, Ref 2008/03.


Note

* The AT90SC may also feature FLASH parts the crypto Toolbox and Smartcard Embedded Software would therefore be stored in FLASH, this Security Target will refer to ROM as the storage area for the Crpyto Toolbox, the Smartcard Embedded Software Developer should refer to the AT90SC device Security Target for details of the FLASH memory map.

Project Information:

TOE	Atmel Toolbox 00.03.11.05	Identifier
Toolbox Part Number	00.03.11.05	0x00031105*


Note

* The version number of the TOE is outputed by the TOE when the self test is ran [TBX].

Assurance Level

7 The TOE is being evaluated against the CC Smartcard IC Platform Protection Profile (BSI-PP-002-2001) to Evaluation Assurance Level 5 (EAL5) augmented with AVA_VLA.4, ALC_DVS.2 and AVA_MSU.3 under the Common Criteria scheme.

Sponsor

8 Atmel Smart Card ICs, a division of ATMEL Corporation, is the developer and the sponsor for the AT90SC ASL4 evaluations.

Atmel Corporation
3235 Orchard Parkway
San Jose
CA95131
USA

Evaluation Scheme

9 The TOE is evaluated under the French CC Scheme

Centre De Certification

Direction centrale de la securite des systemes d'information

51 bouleverard de la Tour-maubourg

75700 Paris

France

Evaluator

10 The TOE is independently verified by the following Test facility (ITSEF), registered with the French CC Scheme.

Thales

BPI 1414

18 avenue Edouard Belin

Toulouse

France

Brief TOE Description

11 The TOE is the Atmel Cryptograhic Toolbox 00.03.11.05, stored in ROM, on the AT90SC family of smartcards with cryptographic accelerator. The Atmel toolbox allows the smartcard embedded software the ability to perform the following cryptographic functions.

- SHA-1 algorithm
- RSA without CRT algorithm
- RSA with CRT algorithm
- Miller Rabin algorithm
- EC-DSA
- ECDH
- AIS31 Test Routines

1.3 Common Criteria Conformance Claim

12 This Security Target 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, the additional security functional requirement is defined in BSI-PP-002-2001 Protection Profile.
- Part 3 conformant: the security assurance requirements are in the form of an EAL (assurance package) that is based upon assurance components in part 3 of the Common Criteria (CC).The augmentations used are also taken from part 3 of the Common Criteria.

1.4 Document Objective

13 The purpose of this document is to satisfy the Common Criteria (CC) requirements for a Security Target; in particular, to specify the security requirements and functions, and the assurance requirements and measures, where applicable from the BSI-PP-002-2001, Smartcard IC Platform Protection Profile.

1.5 Document Structure

Section 1 introduces the Security Target, and includes sections on terminology, references and main actors.

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.

Section 3 describes the TOE security environment.

Section 4 describes the required security objectives.

Section 5 describes the TOE security functional requirements.

Section 6 describes the TOE security functions.

Section 7 describes the Protection Profile (PP) claims.

Appendix A provides a glossary of the terms and abbreviations

Appendix B gives the Toolbox Life Cycle Addresses

1.6 Scope and Terminology

14 Parts of this document are based on the Toolbox 3.x on AT90SCxxxxC Family with AdvX [TBX] application note.

15 The term *Target of Evaluation* (TOE) is standard CC terminology and refers to the software being evaluated, that is the Atmel Toolbox 00.03.11.05 on the AT90SC Family.The stated toolbox commands form the main part of the evaluation.

16 Security objectives are defined herein with labels in the form O.xx_xx. These labels are used elsewhere for reference. Similarly, modes, assets, subjects, threats, assumptions and organizational security policy are defined with labels of the form M.xx_xx, D.xx_xx, S.xx_xx, T.xx_xx, A.xx_xx, and P.xx_xx respectively.

17 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

18 The Toolbox 00.03.11.05 Deliverables List (EDL) identifies the latest revision of the following documents, the EDL list details all the deliverables sent as evidence, as part of the TOE evaluation.

- [ESOF] AT90SC Strength of Security Functions Analysis
- [TBX] Toolbox 00.03.11.xx For AT90SCxxxxC Family with AdvX (TPR0360)
- [APP_AdvX] AdvX for AT90SC Family (TPR0116)
- [APP_SCRY] Securing Cryptographic Operations on AT90SC Products with the Toolbox 3.x (TPR0375)

Within this security target the above are referred to with the use of [ ] brackets, for example [TBX] refers to the document Toolbox 00.03.11.xx For AT90SCxxxxC Family with AdvX, the ST-Lite user should refer to the this document for further information. Some documents listed above are only available to an ITSEF, the Composite product developer should refer to their ITSEF for guidance on what they require.

1.8 Revision History

Rev	Date	Description	Originator
A	19 Dec 08	Initial release	John Boggie

Target of Evaluation Description

19 This part of the Security Target (ST) describes the Target of Evaluation (TOE) as an aid to the understanding of its security requirements and address the product type, the intended usage and the general features of the TOE.

Note: The Smartcard Embedded Software Developer must take into consideration the AT90SC Security Target as well as this Security Target when using this document.

2.1 TOE Definition

20 The Target of Evaluation is the Cryptographic Software part of a AT90SC smartcard. The TOE can be as support software for cryptographic functions on an already certified Hardware Platform (AT90SC device).Figure 2-1 defines a complete Smart card device this includes both the Hardware and Software parts of the device.

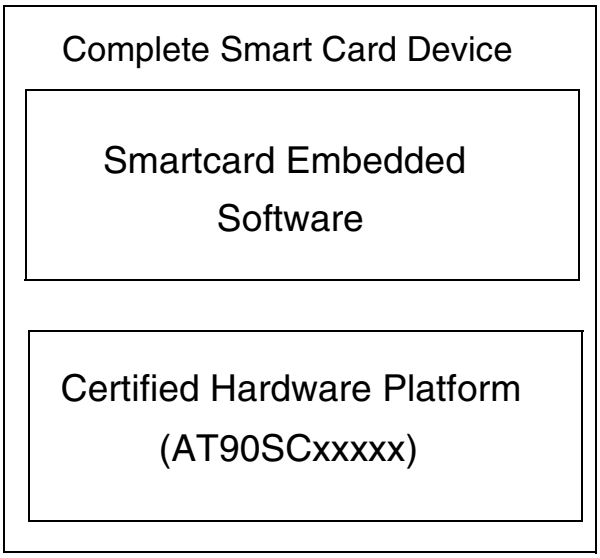


Figure 2-1 Complete Smartcard Device

Hardware Definition

21 The hardware part is the physical IC. This part of the Smartcard system is evaluated independently and may be used as the basis for many composite products (that is it may be used with various software applications).

Software Definition

22 The software is embedded in the hardware and is designed to operate the hardware. The software consists of a smartcard embedded software provided by a customer (Smartcard Embedded Software Developer), and a Cryptographic Toolbox (TBX) provided by Atmel, the TBX is merged with the Smartcard embedded software in Phase 2 of the life cycle. Figure 2-2 shows a further breakdown of the Smartcard Embedded Software.

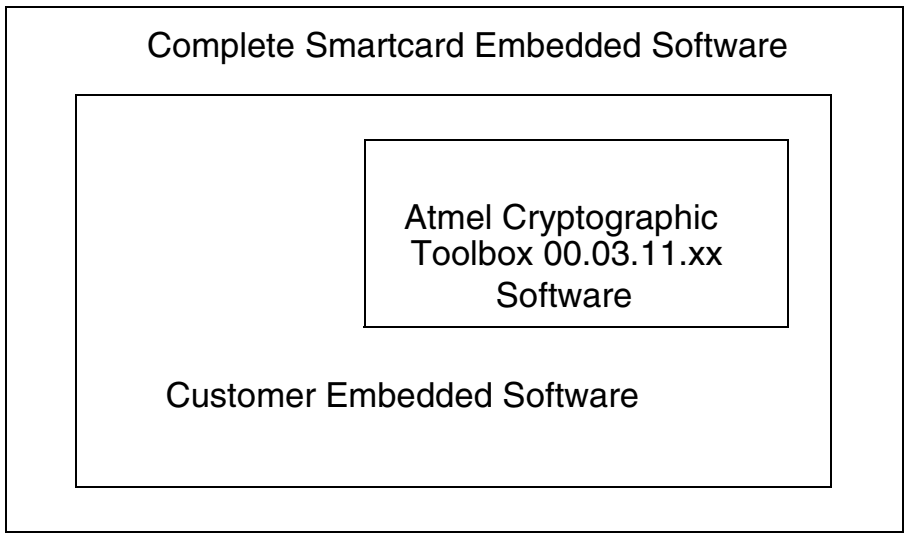


Figure 2-2 Smartcard Embedded Software

23 The TOE boundary is the Atmel Cryptographic Software as shown in Figure 2-2. As defined above this Crypto toolbox (TBX), forms part of a complete Smartcard application. The TOE can only be thought of as a part of the complete application. The TOE offers support to the Smartcard Embedded Software to allow cryptographic functions to be performed by the Hardware certified AT90SC device, at the request of the Smartcard Embedded Software.

00.03.11.xx Atmel Toolbox

24 The Atmel Toolbox [TBX], software library allows fast cryptographic algorithm implementations (RSA, SHA-1, Prime Generation,...) on the hardware AT90SC. The TOE shall also provide software cryptographic primitives to ease the customer proprietary software implementation of these algorithms (full multiply, square, partial multiply, division,...) as well as DSA and EC-DSA data signature. The primitives listed

as well as DSA and EC-DSA. The cryptographic library is stored in athe ROM of the AT90SC device.


Note

Please note that storage of the software Toolbox and the access rights applied are not discussed in this ST, the certified AT90SC Hardware ST gives full details of the Access Control and Firewall rules defined for the Hardware TOE.

25 The Smartcard Embedded Software when wishing to run a cryptographic function, calls a set command as listed in [TBX], this command will call a function to perform one of the following cryptograhic functions.

- SHA-1 algorithm
- RSA without CRT algorithm
- RSA with CRT algorithm
- Miller Rabin algorithm
- EC-DSA
- ECDH
- AIS31

TOE Interfaces

26 The TOE interfaces consist of:

- Interface between the Smartcard Embedded Software and the Atmel Toolbox
- The interface between the AT90SC CPU and the Atmel Toolbox
- The Interface between the AT90SC Crypto RAM and the Atmel Toolbox

TOE Development

27 As the TOE is developed to be part of the complete Smartcard device, the following documents are used by the TOE developer during the TOE development phase.

[AM_IS] AT90SC Address and Instruction Set

[TD_GEN] AT90SC Technical Data (TPR0160)

[APP_AdvX] AdvX for AT90SC Family (TPR0116)

[APP_CRYPT] Efficient use of AdvX for Implementing Cryptographic Operations (TPR0142)

Customer Software Guidance Documents

28 The guidance documents applicable for the development of the smartcard embedded software for this TOE are:

- [TBX] Toolbox 00.03.11.xx For AT90SCxxxxC Family with AdvX (TPR0360)
- [APP_AdvX] AdvX for AT90SC Family (TPR0116)
- [APP_SCRY] Securing Cryptographic Operations on AT90SC Products with the Toolbox 3.x (TPR0375)
- [APP_RNG] Generation of Random Numbers with a Controlled Entropy on AT90SC Family (TPR0166)

29 The software developer should refer to the Certification report issued by DCSSI for the correct revisions of the documents stated above.

2.1.1 Scope of Evaluation Summary

Part of the TOE

- Atmel Security User Guidance as detailed on page 18
- The TOE interfaces as detailed in Section 26
- Phases 2-3 of the Life Cycle
- The complete Atmel Toolbox 00.03.11.05 software
- Atmel Toolbox Cryptographic functions

Outwith the TOE

- Strength of Cryptographic Functions
- Phases 1 and 4-7 of the Life Cycle

2.2 TOE Life-cycle

30 To understand the Life Cycle of the TOE, it must be included in the overall Smartcard Life Cycle first.

2.2.1 Smartcard Life Cycle

31 The standard smartcard product life-cycle consisting of 7 phases where the following authorities are involved

.

Table 2-1 Smartcard Product Life-cycle

Phase 1	Smartcard software development	The smartcard software developer is in charge of the smartcard embedded software development and the specification of IC pre-personalization requirements,
Phase 2	IC Development	The IC designer designs the IC, develops IC dedicated software, provides information, software or tools to the smartcard software developer, and receives the software from the developer, through trusted delivery and verification procedures. From the IC design, IC dedicated software and smartcard embedded software, the IC designer constructs the smartcard IC database, necessary for the IC photomask fabrication.
Phase 3	IC manufacturing and testing	The IC manufacturer is responsible for producing the IC through three main steps: ■ IC manufacturing ■ IC testing ■ IC pre-personalization
Phase 4	IC packaging and testing	The IC packaging manufacturer is responsible for the IC packaging and testing.
Phase 5	Smartcard product finishing process	The smartcard product manufacturer is responsible for the smartcard product finishing process and testing.
Phase 6	Smartcard personalization	The personalizer is responsible for the smartcard personalization and final tests. Other application software may be loaded onto the chip at the personalization process.
Phase 7	Smartcard end-usage	The smartcard issuer is responsible for the smartcard product delivery to the smartcard end-user, and the end of life process.

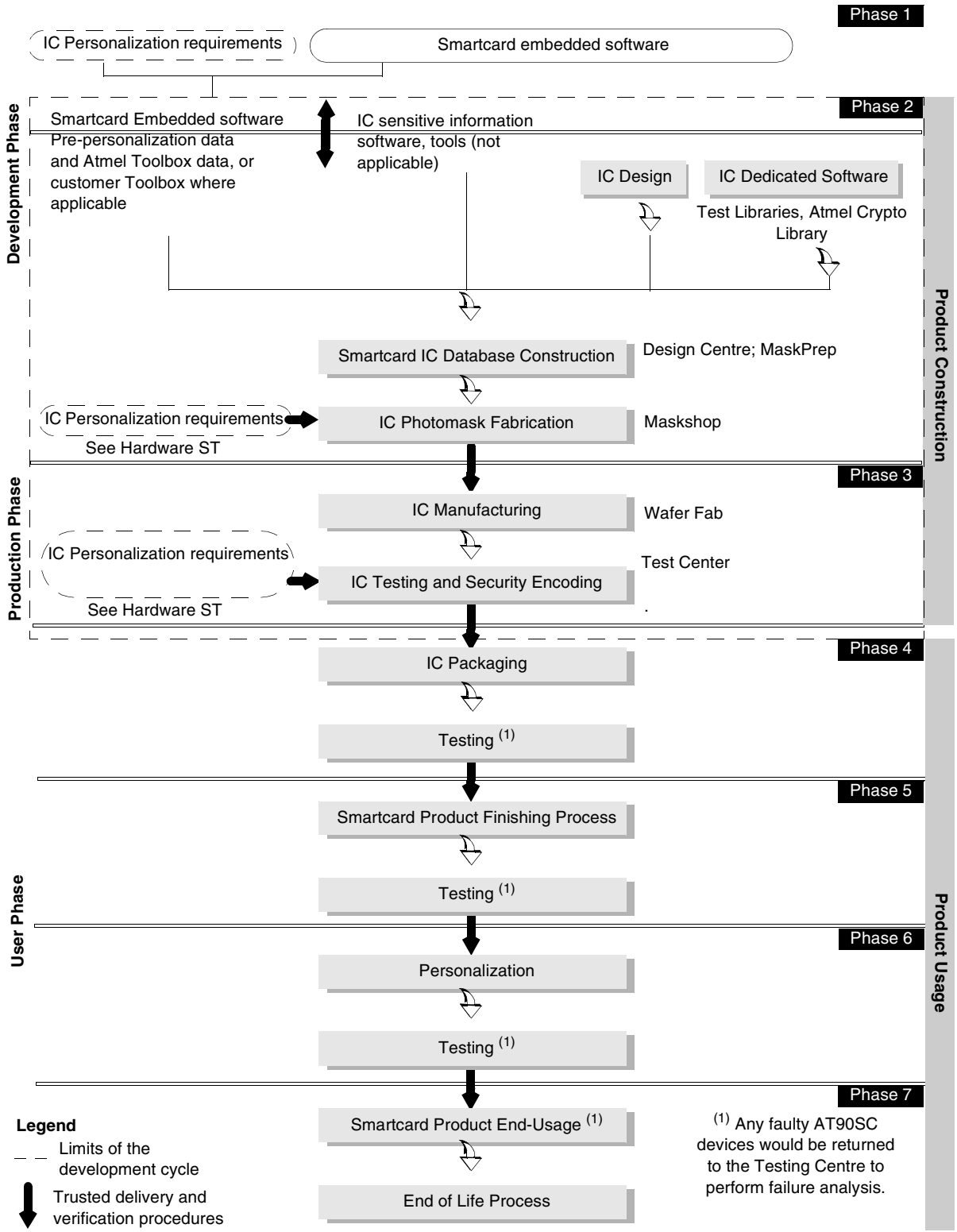


Figure 2-3 Smartcard Product Life Cycle

2.2.2 Atmel Toolbox Life Cycle

32 The Atmel Toolbox integrates into the smartcard life cycle in phase 2 development phase, before this in phase 1 and after this in phases 4-7 the toolbox must be considered as part of the smartcard is protected by the smartcard delivery procedures.

33 The applicable phase to the toolbox is phase 2 of the smartcard, to show the life of the TOE this phase requires to be refined, as detailed in Table 2-2.

Table 2-2 Toolbox Product Life-cycle

Phase 2 TOE Development	(a) Specification
	(b) Conception
	(c) Coding
	(d) Validation
	(e) Code Entry
	(f) ROMGEN

2.3 TOE Environment

34 Considering the TOE, two types of environments are defined:

- Software development environment corresponding to Phase 2 (a,b,c)
- Code Entry environment corresponding to Phase 2 (e,f)

2.3.1 Software Development Environment

35 The Software Development Environment pertains to:

- Specification (a)
- Conception (b)
- Coding (c)
- Validation (d)

36 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 sign a log book and record 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.

37 Specification and Conception of the TOE is performed by the Software Developer. Specification and conception documentation is stored using a file management system. The file management system, and stored files are located on the Atmel Development centre Server. The software development engineer uses appropriate software tools running on a secure network with the necessary password controls to make his code, test scripts, and generation of the TOE data secure and only available to authenticated engineers. Sensitive documents, databases on tapes, diskettes are stored in appropriate locked cupboards and safes. Disposal of unwanted confidential data is carried out by shredding (paper documents) or complete electronic erasures (electronic documents, databases, etc.).

2.3.2 TOE Code Entry Environment

38 The Code Entry Environment pertains to:

- Code Entry
- ROMGEN

39 As with the Software development environment, to assure security, the environment in which the Code Entry takes place is made secure with controllable accesses having traceability. Access to the development building is strictly monitored by a security person. Visitors must sign a log book and record 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.

40 The Software Developer releases the final Toolbox code to the Code Entry team. The Toolbox code is transferred to Code Entry by means of an encrypted link to a secure dropbox, this dropbox is only accessible by the Code Entry team. The processing of the Toolbox data by the Code Entry and ROMGEN teams is performed on a secure network accessible to authenticated engineers with password controls to ensure that the data is protected at all times. As with the Development environment sensitive documents, databases on tapes, diskettes are stored in appropriate locked cupboards and safes. Disposal of unwanted confidential data is carried out by shredding (paper documents) or complete electronic erasures (electronic documents, databases, etc.).

2.3.3 TOE User Environment

41 From after ROMGEN the TOE must be considered as part of the AT90SC hardware TOE, the user of the TOE must refer to the AT90SC Security Target for information on, the secure handling and delivery processes, from this stage onwards.

2.4 TOE Intended Usage

42 The TOE can be incorporated in several applications such as:

- Banking and finance market for credit/debit cards, electronic purse (stored value cards) and electronic commerce.

- Network based transaction processing such as mobile phones (GSM SIM cards), pay-TV (subscriber and pay-per-view cards), communication highways (Internet access and transaction processing).
- Transport and ticketing market (access control cards).
- Governmental cards (ID-cards, healthcards, driver license etc).
- Multimedia commerce and Intellectual Property Rights protection.

43 During the phase 2 of the AT90SC life cycle the TOE is being developed and produced. The administrators are the following:

- The smartcard embedded software developer
- The Atmel Code Entry Team
- The Atmel ROMGEN Team

44 This Security Target is based on the BSI-PP-002-2001 protection profile.

45 This section describes the security aspects of the environment in which the certified AT90SC device is intended to be used, and addresses the description of the assets to be protected, the assumptions, the threats, and the organizational security policies.

46 Section 3 and 4 are taken directly from the BSI-PP-002-2001 Protection Profile to fully comply with the Protection Profile the complete system AT90SC Certified Hardware platform and the TOE must be taken into account, section 3 and 4 deal only with the parts of the PP that deal specifically with the Software Toolbox.


Note

The Smartcard Embedded Software developer should refer to this document and also the specific AT90SC family member Security Target. Section 3 onwards can be though of as a building block that fits directly into the appropriate AT90SC Security Target.

3.1 Assets

3.1.1 Assets regarding the Threats

47 Assets are security relevant elements of the TOE that include the Primary and Secondary assets.

Primary Assets

- User application data (D.xxx_DATA) of the TOE comprising the IC pre-personalization requirements, located in:
  - Crypto ROM (D.CRYPTO_ROM_DATA)

The User data can be subject to manipulation and disclosure while being stored or processed by the TOE.

- Smartcard embedded software (D.xxx_SOFT) located in:
  - Crypto ROM (D.CRYPTO_ROM_SOFT)

Smartcard Embedded software needs to be protected to prevent manipulation and disclosure.

- IC dedicated software (D.xxx_DSOFT) located in:

- Crypto ROM (D.CRYPTO_ROM_DSOFT))

48 Therefore, the complete TOE itself is an asset.

Secondary Assets

49 There are many ways to manipulate or disclose the User Data:

1. An attacker may manipulate the smartcard Embedded Software or the TOE (Primary assets)

Such attacks usually require design information of the TOE to be obtained. Therefore, the design information is a secondary asset.

- IC specification (D.IC_SPEC)
- Design (D.DESIGN)
- Development tools (D.DEV_TOOLS)
- Technology (D.TECHNO)
- Photomasks (D.MASK)

50 The above secondary assets disclose the following information to an attacker and therefore need to be protected.

1. The IC dedicated Software with the parts IC Dedicated Test software, and IC dedicated support software
2. The TSF data

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

Grouping of Assets / Object Definition

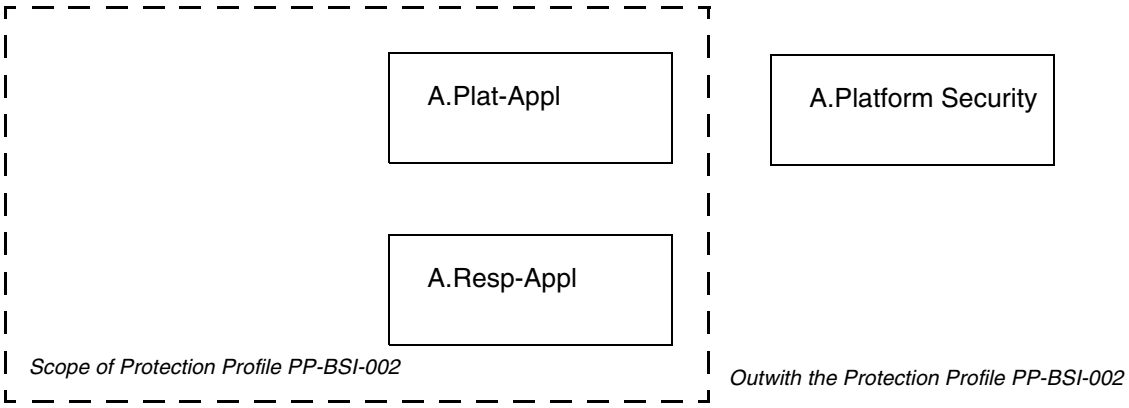
52 These assets can be grouped to define objects that must be protected, which is useful for the following sections of this document.

- O3: Crypto ROM: covering D.CRYPTO_ROM_DATA, D.CRYPTO_ROM_SOFT, D.CRYPTO_ROM_DSOFT

3.2 Assumptions

53 This Security Target is based on the BSI-PP-002-2001 “Smartcard IC Platform Protection Profile”, the assumptions defined in section 3.2 of the PP (where applicable) are valid for this security target and are listed below.

Figure 3-1 Assumptions



A.Plaform Security	**Hardware Platform Security** The security of the Hardware Platform on which the TOE is loaded, shall have sufficient security to fully protect the TOE and its assets. The random numbers generated by the Platform shall not be predictable and have sufficient entropy. The platform will ensure that no information about produced random numbers is available to an attacker, as this information may be used to generate cryptographic keys.
A.Plat-Appl	**Usage of Platform** The Smartcard Embedded Software shall be designed according to the latest TOE user guidance as stated in Section 28. The Smartcard Embedded Software designer should also take into account the findings of the TOE evaluation report. **Applies to Phase 1**
A.Resp-Appl	**Treatment of User Data** User data is owned by the Smartcard Embedded Software. Therefore, is assumed that security relevant User Data for example Cryptographic keys, are treated by the Smartcard Embedded Software according to the requirements of the specific end application. **Applies to Phase 1**

3.3 Threats

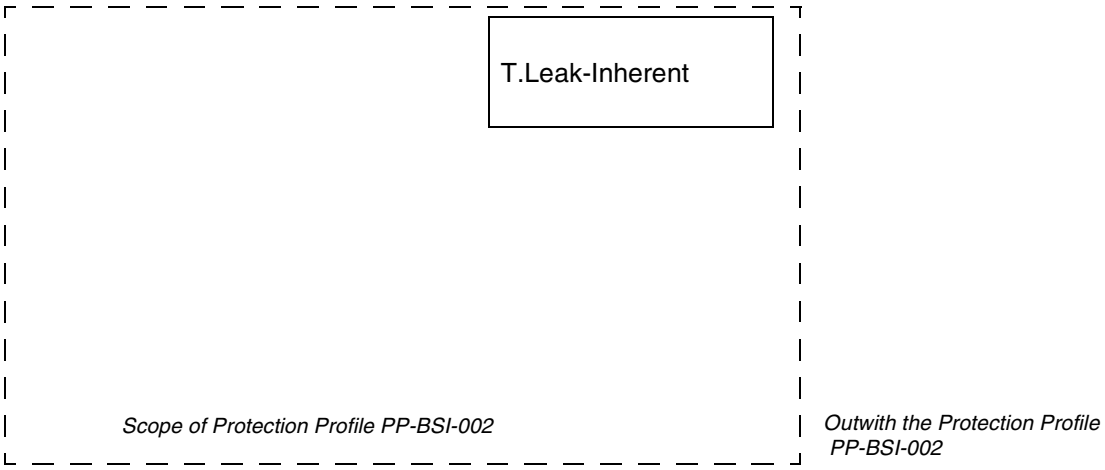
54 This Security Target is based on the BSI-PP-002-2001 “Smartcard IC Platform Protection Profile”, the threats defined in section 3.3 of the PP (where applicable) are valid for this security target and are listed below

According to BSI-PP-002-2001, there are the following standard high-level security concerns

SC1	Manipulation of User Data and of the Smartcard Embedded Software (while being executed/processed and while being stored in the TOE’s memories)
SC2	Disclosure of User Data and of the Smartcard Embedded Software (while being processed and while being stored in the TOE’s memories)

55 The security concerns 1 and 2 give rise to the following threats:

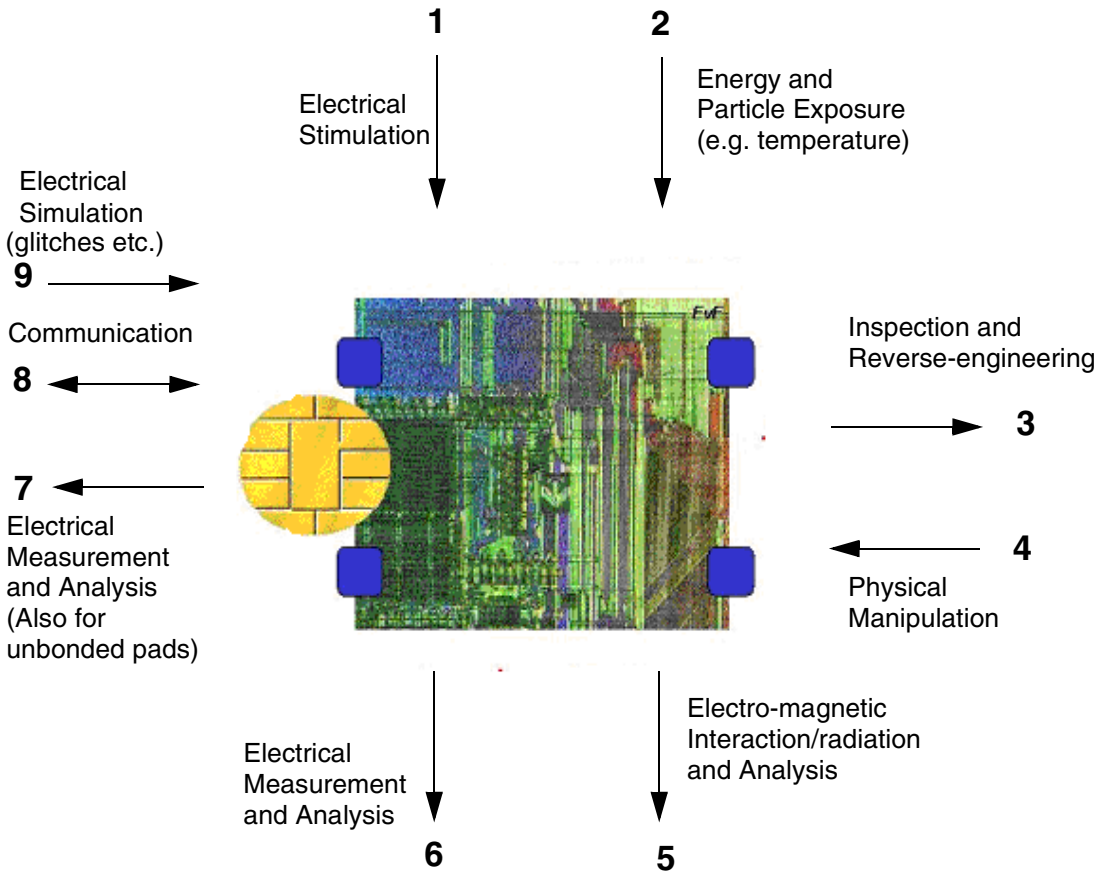
Figure 3-2 Standard Threats



56 The complete AT90SC device is exposed to different types of influences or interactions with it’s outside world. Some of them may result from just using the TOE, others may

also indicate an attack. The different types of influences or interactions are shown in Figure 3-3.

Figure 3-3 Attack Model for the TOE



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

58 The Smartcard Embedded Software must contribute to averting the threats: At least it must not undermine the security provided by the TOE. For details refer to the assumptions regarding the Smartcard Embedded Software, specified in Section 3.2.

Standard Threats (referring to SC1 and SC2).

59 From the threats stated in Figure 3-3, the TOE shall avert the applicable threats listed below:

T.Leak-Inherent	**Inherent Information Leakage** An attacker may exploit information which is leaked from the TOE during usage of the complete smartcard system in order to disclose confidential data (User Data or TSF data). No direct contact with the smartcard internal 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 Figure 3-3) or measurement of emanations (number 5) and can be related to the specific operation being performed.

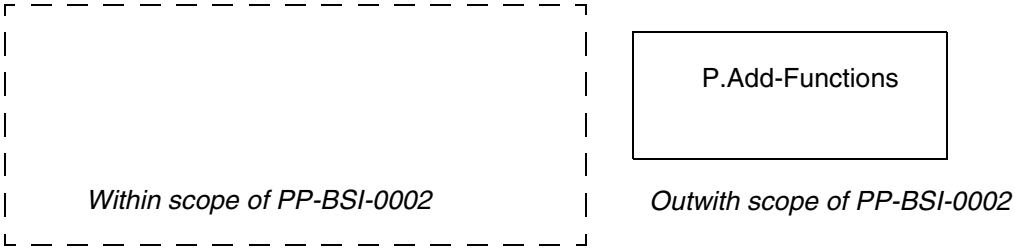
3.4 Organizational Security Policies

60 This Security Target is based on the BSI-PP-002-2001 “Smartcard IC Platform Protection Profile”, the Security Policy defined in section 3.4 of the PP (where applicable) are valid for this security target and are listed below.

61 The TOE may provide specific security functionality which can be used by the Smartcard Embedded Software. Particular specific security functionality may not necessarily be derived from threats identified for the TOE's environment because it can only be decided in the context of the smartcard application, against which threats the Smartcard Embedded Software will use the specific security functionality. Therefore,

the necessity of some specific functionality may not derived from a threat. The Security organizational policies are shown in Figure 3-4.

Figure 3-4 Organizational Security Policies



62 The IC developer 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 Smartcard Embedded Software, according to accepted international standard:

- Secure Hash Algorithm (SHA)**)**
- Rivest-Shamir-Adleman (RSA) With CRT
- Rivest-Shamir-Adleman (RSA) Without CRT
- Elliptical Curve Computation (ECC)
- RSA Key Generation
- Test routines for RNG data

The TOE must provide means to identify the correct revision of the TOE on request by the TOE user.

Security Objectives

63 This Security Target is based on the BSI-PP-002-2001 protection profile.

64 The security objectives of the TOE contains the following sections:

- Security Objectives for the TOE
- Security Objectives for the Environment

4.1 Security Objectives for the TOE

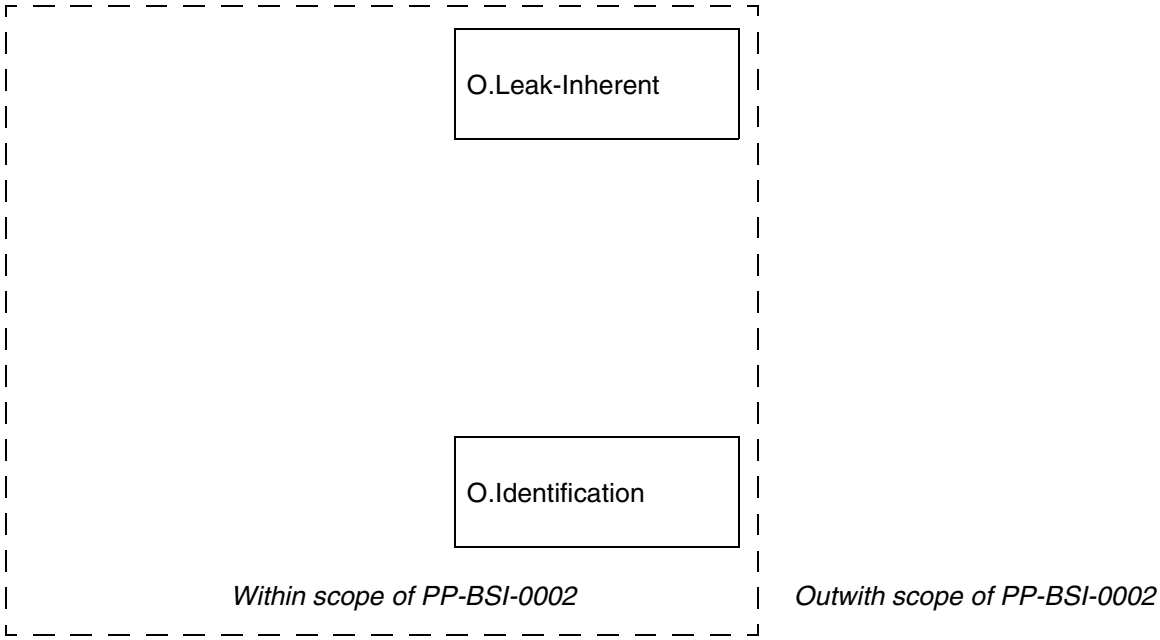
According to this Security Target, there are the following standard high level security goals:

SG1	Maintain the integrity of User Data and of the Smartcard Embedded Software (when executing TOE functions).
SG2	maintain the confidentiality of User Data and of the Smartcard Embedded Software (when executing TOE functions).

65 Though the Smartcard Embedded Software stored in the AT90SC ROM, will in many cases not contain secret data or algorithms, it must be protected from being disclosed, since for instance knowledge of specific implementation details may assist an attacker.

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

Figure 4-1 Standard Security Objectives

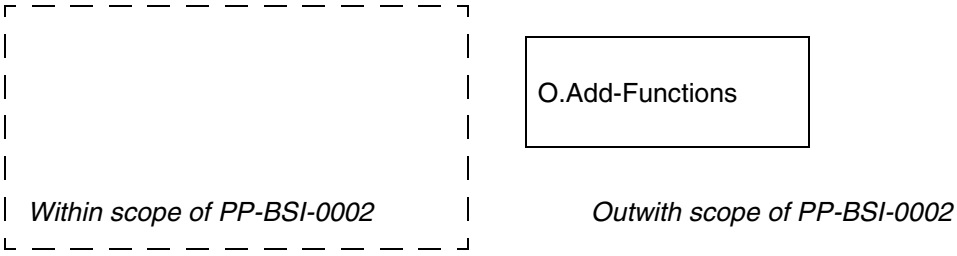


67 According to this security target there are the following high level security goals related to specific functionality:

SG4 Provide additional security functionality.

68 The additional high level security considerations are refined below by defining security objectives as required by the Common Criteria.

Figure 4-2 Security Objectives Related to Specific Functionality



Standard Security Objectives (referring to SG1 and SG2)

69 The TOE shall provide protection on each of the Standard Security Objectives as listed 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 smartcard 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. Details correspond to an analysis of attack scenarios which is not given here.

O.Identification **TOE Identification**

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

Security Objectives Relating to Specific Functionality (referring to SG3 and SG4)

70 The TOE shall provide protection on each of the Specific Functionality Security Objectives as listed below:

O.Add-Function **Additional Specific Security Functionality**

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

- Secure Hash Algorithm (SHA)
- Rivest-Shamir-Adleman (RSA) With CRT
- Rivest-Shamir-Adleman (RSA) Without CRT
- Elliptical Curve Computation (ECC)
- RSA Key Generation
- Test routines for RNG

4.2 Security Objectives for the Environment

Phase 1

71 The Smartcard Embedded Software shall provide for each of the Security Objectives for the Environment as stated below.

OE.Plat-Appl **Usage of TOE Platform**

To ensure that the TOE is used in a secure manner the Smartcard Embedded Software shall be designed so that the requirements from the following documents are met:

- TOE application notes
- Findings of the TOE evaluation reports relevant for the Smartcard Embedded Software

OE.Resp-Appl **Treatment of User Data**

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

For example the Smartcard Embedded Software will not disclose security relevant user data to unauthorised users or processes when communicating with a terminal.

Phase 2

72 The hardware Platform shall provide for the Security Objective for the environment as stated below.

OE.Platform security **Hardware Platform Security**

The security of the Hardware Platform on which the TOE is loaded, must be of a sufficient quality to fully protect the TOE and its assets.

The security of the hardware platform is especially relevant when taking into account the RNG used in conjuction with the TOE to produce cryptographic keys. The hardware platform RNG must be tested against a recognised quality metric.

TOE Security Functional Requirements

73 This security target is based on the BSI-PP-002-2001 protection profile.

74 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 functional requirements defined in BSI-PP-002-2001.

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


Note

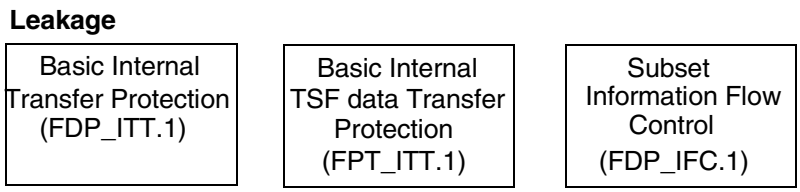
The Smartcard Embedded Software Developer must consider the whole product, to comply with the BSI-PP-002-2001 Protection Profile, the full AT90SC system SFRs must be considered, the developer should refer to both security targets.

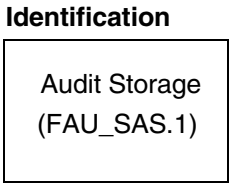
5.1 The TOE Functional Requirements

Standard Security Functional Requirements

76 The Standard TOE Security Functional Requirements (where applicable to the TOE) as listed within the BSI-PP-002-2001 are shown in Figure 5-1

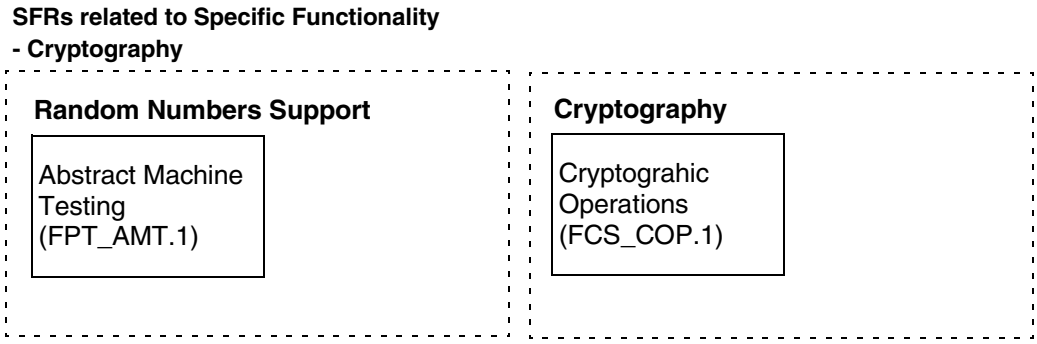
Figure 5-1 Standard Security Functional Requirements





77 The Security Functional Requirements related to specific Functionality are shown in Figure 5-2.

Figure 5-2 Security Functional Requirements related to Specific Functionality



5.1.1 Functional Requirements Relating to Leakage

Basic Internal Transfer Protection (FDP_ITT.1)

78 The TOE **shall** meet the requirement “Basic internal transfer protection” 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 Smartcard device (e.g. a cryptographic co-processor) are seen as physically-separated parts of the Smartcard device.

Basic Internal TSF data transfer protection (FPT_ITT.1)

79 The TOE **shall** meet the requirement “Basic internal TSF data transfer protection” 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 smartcard device (e.g. a cryptographic co-processor) are seen as separated parts of the Smartcard device. This requirement is equivalent to FDP_ITT.1 above but refers to TSF data instead of User Data. Therefore, it should be understood as to refer to the same Data Processing Policy defined under FDP_IFC.1.

Subset Information Flow Control (FDP_IFC.1)

80 The TOE **shall** meet the requirement “Subset information flow control” 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 Smartcard Embedded Software**.
Dependencies	FDP_IFF.1 Simple security attributes

81 The following Security Functional Policy (SFP) Data Processing Policy is defined for the requirement “Subset information flow control”:

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

5.1.2 Functional Requirements Relating to Identification

Audit Storage (FAU_SAS.1)

82 The TOE **shall** meet the requirement “Audit storage” as specified below:

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 Smartcard Embedded Software** in the audit records.
Dependencies	No dependencies

5.1.3 Functional Requirements Relating to Cryptography

Abstract machine testing (FPT_AMT.1)

83 The TOE **shall** meet the requirement “Abstract machine testing” as specified below:

FPT_AMT.1	Abstract machine testing
Hierarchical to	No other components
FPT_AMT.1.1	The TSF shall run a suite of tests **at the request of an authorised user** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.
Dependencies	No dependencies

Cryptographic operation (FCS_COP.1)

84 The TOE **shall** meet the requirement “Cryptographic operation” on cryptographic operations as specified below:

FCS_COP.1	Cryptographic operation
Hierarchical to	No other components
FCS_COP.1.1	The TSF shall perform software: ▪ **data signing** in accordance with a specified cryptographic algorithm: **SHA-1,** and cryptographic key size:**with no cryptographic key size** that meet the following **Secure Hash Standard, Federal Information Processing Standards Publication 180-2, 2002 August 1** ▪ **data signing** in accordance with a specified cryptographic algorithm: **SHA-224,** and cryptographic key size:**with no cryptographic key size** that meet the following **Secure Hash Standard, Federal Information Processing Standards Publication 180-2, 2002 August 1** ▪ **data signing** in accordance with a specified cryptographic algorithm: **SHA-256,** and cryptographic key size:**with no cryptographic key size** that meet the following **Secure Hash Standard, Federal Information Processing Standards Publication 180-2, 2002 August 1** ▪ **data encryption and decryption** in accordance with a specified cryptographic algorithm: **RSA without CRT data,** and cryptographic key size:**between 96 bits and 2624 bits** that meet the following**, PKCS#1 V2.0, 1st October, 1998.**

	■ **data encryption and decryption** in accordance with a specified cryptographic algorithm: **RSA with CRT data,** and cryptographic key size:**between 192 bits and 3520 bits** that meet the following **PKCS#1 V2.0, 1st October, 1998.**
	■ **data encryption and decryption** in accordance with a specified cryptographic algorithm: **EC-DSA,** and cryptographic key size:**between 192 and 521 bits** that meet the following**, FIPS 186-2, 27th January, 2007 for Digital Signatures.**
	■ **data encryption and decryption** in accordance with a specified cryptographic algorithm: **ECDH,** and cryptographic key size:**between 192 and 521 bits key size** that meet the following **ISO 15946-3:2002 for ECDH standard.**
Dependencies	(FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation) FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

5.2 Security Requirements for the Environment

5.2.1 Security Requirements for the IT-Environment

85 The environment shall meet the requirement “Quality metric for random numbers” as detailed below:

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

5.2.2 Security Requirements for the NON-IT-Environment

86 In the following, security requirements for the Non-IT-Environment are defined.

87 For the Hardware Platform the requirement " Hardware Platform Security (RE.Hardware Platform)" is valid.

RE.Platform Security	Hardware Platform Security
	The TOE user must ensure that the security of the Hardware Platform on which the TOE is loaded, must be of a sufficiently quality to fully protect the TOE and its assets. The security of the hardware platform is especially relevant when taking into account the RNG used in conjuction with the TOE to produce cryptographic keys. The hardware platform RNG must be tested against a recognised quality metric.

88 For the development of the Smartcard Embedded Software (in Phase 1) the requirement "Design and implementation of the Smartcard Embedded Software (RE.Phase-1)" is valid.

RE.Phase-1	Design and Implementation of the Smartcard Embedded Software
	The developers shall design and implement the Smartcard Embedded Software in such a way that it meets the requirements from the following documents (i) data sheet for the TOE, (ii) TOE application notes, and (iii) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software. (See section 2.1 Customer Software Guidance) The developers shall implement the Smartcard Embedded Software in a way that it protects security relevant User Data (especially cryptographic keys) as required by the security needs of the specific application context.

89 The Smartcard Embedded Software shall meet the requirements RE.Cipher.

RE.Cipher	Cipher Schemas
	The developers of Smartcard Embedded Software must not implement routines in a way which may compromise keys when the routines are executed as part of the Smartcard Embedded Software. Performing functions which access cryptographic keys could allow an attacker to misuse these functions to gather information about the key which is used in the computation of the function. Keys must be kept confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. For example, it must be ensured that it is not possible to derive the private key from a public key if asymmetric algorithms are used. This implies that an appropriate key management has to be realized in the environment.

5.3 TOE Security Assurance Requirements

90 The assurance requirement is EAL5 augmented of additional assurance components listed in Table 5-1.

91 Some of the augmentation components are hierarchical ones to the components specified in EAL5.

92 All the components are drawn from Common Criteria Part 3.

Table 5-1 EAL5 Package and Augmentation

Assurance Class	EAL5 Package	TBX_00.03.11.05 EAL5+ Package	Augmented From EAL5
ACM_AUT	1	1	No
ACM_CAP	4	4	No
ACM_SCP	3	3	No
ADO_DEL	2	2	No
ADO_IGS	1	1	No
ADV_FSP	3	3	No
ADV_HLD	3	3	No
ADV_IMP	2	2	No
ADV_INT	1	1	No
ADV_LLD	1	1	No
ADV_RCR	2	2	No
ADV_SPM	3	3	No
AGD_ADM	1	1	No
AGD_USR	1	1	No
ALC_DVS	1	2	Yes
ALC_FLR	N/A	N/A	No
ALC_LCD	2	2	No
ALC_TAT	2	2	No
ATE_COV	2	2	No
ATE_DPT	2	2	No
ATE_FUN	1	1	No
ATE_IND	2	2	No
AVA_CCA	1	1	No
AVA_MSU	2	3	Yes
AVA_SOF	1	1	No
AVA_VLA	3	4	Yes

93 The refinements to the assurance requirements as stated within the Protection Profile BSI-PP002-2001 have been taken into account.

94 This section defines the TOE security functions that implement the security functional requirements defined in Section 5.1, and the TOE assurance measures that implement the security assurance requirements defined in Section 5.3.

The TSF and Security Mechanism (Mx.x) are numbered in a way to allow the Smartcard Embedded Software Developer to see how the TSF detailed fits into the equivalent TSFs for the certified AT90SC ST.

6.1 TOE Security Functions

6.1.1 RNG (SF4)

95 The TSF shall provide the ability to perform testing of an AIS31 compliant RNG. To allow the testing the TOE provides a routine and subservices.

96 The TOE offers the end user a TOT-test subservice. The TOE offers the end user an Online-test. Full details of how to use the subservices to provide AIS31 complaint random data is given in guidance document [APP_RNG_ENT].

97 The Strength of Function claimed for the RNG security function is high.

6.1.2 Cryptography (SF10)

98 The TSF shall provide a cryptographic algorithm to be able to transmit and receive objects in a manner protected from data retrieval or modification.

99 The TSF shall provide **software** cryptographic functionality as detailed below:

100 M10.2 the TSF shall provide secure Hash, SHA-1, 224, 256, data signing capability

101 M10.3 the TSF shall provide RSA without CRT (i.e. modular exponentation) data encryption decryption function.

- Secure encryption

- Fast encryption: function **(see note*)**

102 M10.4 the TSF shall provide RSA with CRTdata encryption decryption function.

- Secure encryption
- Fast encryption **(see note*)**

103 M10.5 the TSF shall provide RSA cryptographic key generation capability using Miller Rabin algorithm with confidence criteria (t parameter) between 0 and 255

- Secure generation
- Fast generation **(see note*)**

104 M10.6 the TSF shall provide digital signature confirming to EC-DSA standard.

- Secure digital signature generate
- Secure digital signature verify
- Fast digital signature generate **(see note*)**
- Fast digital signature verify **(see note*)**

105 M10.7 the TSF shall provide point multiplication on an elliptical curve, conforming to EC-DSA standard

- Secure multiply
- Secure multiply **(see note*)**

106 M10.8 the TSF shall provide point addition on an elliptical curve, conforming to EC-DSA standard

- Secure addition
- Secure multiply **(see note*)**

107 M10.9 the TSF shall provide point doubling on an elliptical curve, conforming to EC-DSA standard

- Secure multiply
- Secure multiply **(see note*)**

108 M10.10 the TSF shall provide ECDH cryptographic capability using Elliptic Curve point operations (point addition, point doubling and point multiply).

109 M10.12 the TSF shall provide a function that performs a selftest operation of the TOE, at the end of the selftest function the TOE will output a Version number.

110 M10.13 the TSF shall provide Coordinates Conversion on an elliptical curve, conforming to EC-DSA standard. Projective to Affine Coordinates Conversion. .


Note

***** The **Fast** functions of M10.3, M10.4, M10.5, M10.7, M10.8, M10.9, do not offer any DPA/SPA protection and **must** not be used for secure data.

111 The Strength of Function claimed for the cryptography security function is high.

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

- RSA without CRT algorithm
- RSA with CRT algorithm
- EC-DSA
- ECDH

113 The following functions use probabilistic or permutational effects and have a strength of function claim of high.

- SHA algorithm
- Miller Rabin algorithm

114 The Strength of Function claimed for the cryptography security function is high.

6.1.3 Security Functions Based on Permutations/combinations

115 Parts of SF10 use probabilistic or permutational effects.

6.2 TOE Assurance Measures

116 Table 6-1 specifies how they satisfy the TOE security assurance requirements.

Table 6-1 Relationship Between Assurance Requirements and Measures

		Security Target	Configuration Management	Delivery and Operation	Development Activity	Guidance	Life Cycle Support	Test Activity	Vulnerability assessment	Smartcard Devices	Development Site	Test Site	Manufacturing Site	Sub-contractor Site
Assurance Requirement		**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.3			x								x	x	x	x
ADO_DEL.2				x							x	x	x	x
ADO_IGS.1				x							x	x	x	x
ADV_FSP.3					x									
ADV_HLD.3					x									
ADV_IMP.2					x									
ADV_LLD.1					x									
ADV_RCR.2					x									
ADV_SPM.3					x									
AGD_ADM.1						x								
AGD_USR.1						x								
ALC_DVS.2							x				x	x	x	x
ALC_LCD.2							x				x	x	x	x
ALC_TAT.2							x				x	x	x	x
ATE_COV.2								x		x		x		
ATE_DPT.2								x		x		x		
ATE_FUN.1								x		x		x		
ATE_IND.2								x		x		x		
AVA_CCA.1									x	x				
AVA_MSU.3									x	x				
AVA_SOF.1									x	x				
AVA_VLA.4									x	x				

Security Target (SA1)

117 SA1 shall provide the “TOE Security Target” document plus its references.

Configuration Management (SA2)

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

Delivery and Operation (SA3)

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

Development Activity (SA4)

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

Guidance (SA5)

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

Life Cycle Support (SA6)

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

Test Activity (SA7)

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

Vulnerability Assessment (SA8)

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

Smart Card Devices (SA9)

125 SA9 shall provide functional AT90SC smart card devices with TBX 3.x loaded and an engineering ROM to allow TOE testing.

Development Site (SA10)

126 SA10 shall provide access to the development site.

Test Site (SA11)

127 SA11 shall provide access to the test site.

Manufacturing Site (SA12)

128 SA12 shall provide access to the manufacturing site.

Sub-contractor Sites (SA13)

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

7.1 PP Reference

130 This Security Target is based on the Protection Profile “Smartcard IC Platform Protection Profile” V1.0 July 2001,and has been registered under the German Certification Scheme (BSI) under the reference BSI-PP-002-2001.

7.2 PP Refinements

131 For clarification of this Security Target, modes, assets, subjects, threats, assumptions and organizational security policy are defined with labels of the form M.xx_xx, D.xx_xx, S.xx_xx, T.xx_xx, A.xx_xx, and P.xx_xx respectively.

7.3 PP Additions

132 The PP additions fall into the following categories, the additions:

- taken directly from Common Criteria V2.3
- assumption and security objective for environment, defined in Section 3.2 of this Security Target

7.3.1 Additions from BSI-AUG-2002

133 Additions include Assumptions, Threats, Organisational security Policies, Security Objectives and Security Functional Requirements.

7.3.1.1 Assumptions

134 This security target specifies the additional Assumption, A.Platform Security. This assumption relates to the Hardware Platform security.

7.3.1.2 Organizational Security Policies

135 This security target specifies the additional organizational security policies, P.Add-Functions this policy relates to the cryptographic functions provided by the TOE.

7.3.1.3 Security Objectives

136 This security target specifies the additional security objective, O.Add-Functions this objective relates to the cryptographic functions provided by the TOE.

7.3.1.4 Security Functional Requirements

137 This security target specifies the additional security functional requirements:

- FCS_COP.1 relating to the cryptographic functions provided by the TOE
- FPT_AMT.1 relating to support for random numbers provided by the TOE

7.3.1.5 Security Functional Requirements for the NON-IT-Environment

138 This security target specifies the additional security functional requirement for the NON-IT-Environment:

- RE.Cipher relating to the Smartcard Embedded Software development

7.3.2 Additions Defined in this Security Target

7.3.2.1 Security Functional Requirements for the NON-IT-Environment

139 This security target defines the additional security functional requirement for the NON-IT-Environment:

- RE.Platform Security relating to the Security of the Hardware Platform the TOE is loaded onto.

Glossary

A.1 Terms

HASH	Transformation of a string of characters into a usually shorter fixed length value or key that represents the original string.
IC Dedicated Software	IC Proprietary software which is required for testing purposes and to implement special functions. For Roper this includes the embedded test software and additional test programmes which are run from outside of the IC. The Crypto libraries also form part of the IC dedicated software.
IC Designer	Institution (or its agent) responsible for the IC Development. Atmel is the institution in respect of the TOE.
IC Manufacturer	Institution (or its agent) responsible for the IC manufacturing, testing and pre-personalization. Atmel is the institution in respect of the TOE.
IC Packaging Manufacturer	Institution (or its agent) responsible for the IC packaging and testing.
IC Pre-personalization Data	Required information to enable the smartcard IC to be configured by means of ROM options and to enable programming of the EEPROM with customer specified data.
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
Personalizer	Institution (or its agent) responsible for the smartcard personalization and final testing.
Smartcard	A credit sized plastic card which has a non volatile memory and a processing unit embedded within it.

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

Appendix B

Toolbox Life Cycle Addresses

140 The table below details the relevant addresses for the Toolbox 00.03.11.05 Project

Centre	Address
Development	Atmel Rousset Zone Industrielle 13106 Rousset Cedex France
Code Entry and ROMGEN	Atmel Secure Products Division Scottish Technology Park East Kilbride Scotland United Kingdom G75 0QR

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 Arsenaux 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

TPG0177A–SMS–19Dec08