Public

Infineon Technologies AG

Security and Chipcard ICs

Evaluation Documentation

SLE66C82P/SLE66C42P / m1474/m1495

Security Target

Version 1.2
Date 23-10-2003
Author Georg Walter, Hans-Jürgen Novinsky

Print Date:	2/24/2004 2:05 PM
Filename:	SecurityTarget_12.doc

Revision History

Version	Page	Subject
1.0		22-10-2002: Initial version, based on SLE66CX322P with RSA2048
1.1		30-01-2002: Comments of certification body

TABLE OF CONTENTS

List of figures:

List of tables:

1 Introduction

1.1 Security Target Identification

The Security Target has the revision 1.2 and is dated 23-10-2003.

The Target of Evaluation (TOE) is a smart card IC (Security Controller). It can be configured to two versions which are named SLE66C82P or SLE66C42P. The TOE is internally registered under the development code m1474a15 (for SLE66C82P) and m1495a15 (for the SLE66C42P) and has the version number a15.

The Security Target is based on the Protection Profile Smartcard IC Platform Protection Profile.

The Protection Profile and the Security Target are built with Common Criteria V2.1.

Table 1: Identification

	Version number	Date	Registration
Security Target	1.2	23-10-2003	
Target of Evaluation	a15		m1474/m1495a15
Smartcard IC Platform Protection Profile	1.0	July 2001	BSI-PP-0002
Common Criteria	2.1		ISO15408

1.2 Security Target Overview

The Target of Evaluation (TOE), the SLE66C82P/SLE66C42P chip, is a smart card IC (Security Controller) meeting the highest requirements in terms of performance and security. It is manufactured by Infineon Technologies AG in a 0,22 µm CMOS technology. The IC is intended to be used in smart cards for particularly security-relevant applications.

In this security target the TOE (target of evaluation) is described and a summary specification is given. The security environment of the TOE during its different phases of the lifecycle is defined. The assets are identified which have to be protected through the security policy. The threats against these assets are described. The security objectives as the objectives of the security policy are defined as well as the security requirements. The requirements are built up of the security functional requirements as part of the security policy and the security assurance requirements as the steps during the evaluation and certification to show the TOE meets its requirements. The functionality of the TOE to meet the requirements is described.

The assets, threats, security objectives and the security functional requirements are defined in the Smartcard Integrated Circuit Platform Protection Profile Smartcard IC Platform Protection Profile and are referenced here. These requirements build up a minimal standard common for all Smartcards.

The security enforcing functions are defined here in the security target as property of this specific TOE, the SLE66C82P/SLE66C42P. Here it is shown how this specific TOE fulfils the requirements for the standard defined in the Protection Profile.

The TOE can be configured as two products with different EEPROM size. The size of the EEPROM can be blocked from 8kBytes to 4kBytes. In this case the name of the TOE is

SLE66C42P/m1495a15. The name of the non-blocked 8kBytes version is SLE66C82P/m1474a15. The blocking is done in the ROM mask not in the circuitry. The layout of the IC is identical for both ICs. The blocking mechanism resides in the EEPROM and is described in the Detailed Design. This blocking mechanism does not influence the security of the TOE as neither an asset nor a security enforcing function is affected. Therefore both products are evaluated together.

1.3 CC Conformance

This security target is conformant to Common Criteria V2.1 (ISO15408) part 2 extended, part 3 conformant and conformant to the Smartcard IC Platform Protection Profile. The assurance level is EAL5 augmented with components ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

1.4 Security functional requirements and Augmentations

The security requirements of the TOE according to the Smartcard IC Platform Protection Profile are listed in Table 7. The augmented security functional requirements (see Table 8) are listed and described in section 5.1.

2 Description of the Target of Evaluation (TOE)

The TOE description helps to understand the specific security environment and the security policy. In this context the assets, threats, security objectives and security functional requirements can be employed. The following is a more detailed description of the TOE than in the Smartcard IC Platform Protection Profile as it belongs to the specific TOE.

2.1 Product Type

The Target of Evaluation (TOE), the SLE66C82P/SLE66C42P chip, is a smart card IC (Security Controller) meeting the highest requirements in terms of performance and security. It is manufactured by Infineon Technologies AG in a 0,22 µm CMOS technology. The IC is intended to be used in smart cards for particularly security-relevant applications. That is based on its previous use as developing platform for smart card operating systems according to the lifecycle model (in Smartcard IC Platform Protection Profile).

The term user software is used in the following for all operating systems and applications stored and executed on the TOE. The TOE is the platform for the user software. The user software itself is not part of the TOE.

The SLE66C82P/SLE66C42P chip is a port of the SLE66CX320P architecture to a smaller production technology and is implemented in the 0,22 µm technology. As a side effect of this porting the most components are unchanged.

The IC, whose block diagram is shown in Figure 1, consists of a dedicated microprocessor (CPU) with a MMU (Memory Management Unit), several different memories, security logic, a timer and an interrupt-controlled I/O interface. A RNG (**R**andom **N**umber **G**enerator) and a checksum module (CRC module) are integrated on the chip.

The CPU is compatible with the SAB 8051 instruction set and is 6 times faster than the standard processor. It provides additional powerful instructions for smart card applications. The memory comprises 256 bytes of internal RAM (IRAM), 2 kBytes of extended RAM (XRAM), 64 kBytes of user ROM, 8 kByte of test ROM and 8 kBytes of EEPROM. It thus meets the requirements of the new generation of operating systems. The CPU accesses the memory via the integrated **M**emory **E**ncryption and **D**ecryption unit (MED). The access rights of the application to the memories can be controlled with the memory management unit (MMU). Security, sleep mode and interrupt logic as well as the RNG are specially designed for smart card applications. The sleep mode logic (clock stop mode per ISO/IEC 7816-3) is used to reduce the overall power consumption. The timer permits easy implementation of communication protocols such as T=1 and all other time-critical operations. The uart-controlled I/O interface allows the smart card and terminal to be operated in parallel. The PLL unit allows to operate the SLE66C82P/SLE66C42P with a multiplication factor over the external clock signal or free running with maximum frequency. The RNG does not supply a pseudorandom number sequence, but instead produces genuine random numbers under all conditions. The checksum module allows simple calculation of checksums per ISO 3309 (16 bit CRC).

One module for cryptographic operations is implemented on the TOE. The module is the DDC which provides the DES algorithm and support for elliptic curve (EC) cryptography. This module computes the complete DES algorithm within a few clock cycles. That module is especially designed to counter attacks like DPA or EMA.

The software (firmware) required for operating the chip consists of routines for programming the EEPROM from application programs and for online testing of the security enforcing functions. These are stored in a reserved user ROM area. In addition, the chip initialisation routine with security checks and identification mode as well as test routines for production testing are located in a separate test ROM.

The TOE offers a new, improved standard of integrated security features, thereby meeting the requirements of all smart card applications such as information integrity, access control, mobile telephone, as well as uses in electronic funds transfer and healthcare systems.

To sum up, the TOE is a powerful smart card IC with a large amount of memory and special peripheral devices with both improved performance and optimised power consumption at minimal chip size. It therefore constitutes the basis for future smart card applications.

The size of the EEPROM can be blocked to 4 kB. In this case the name of the TOE is SLE66C42P/m1495a15. The name of the non-blocked 8 kB version is SLE66C82P/m1474a15. The blocking is done in the ROM mask. The layout of the IC is identical for both ICs. The blocking mechanism resides in the EEPROM and is described in the Detailed Design. This blocking mechanism does not affect the security of the TOE as neither an asset nor a security enforcing function is affected. Therefore both products are evaluated together.

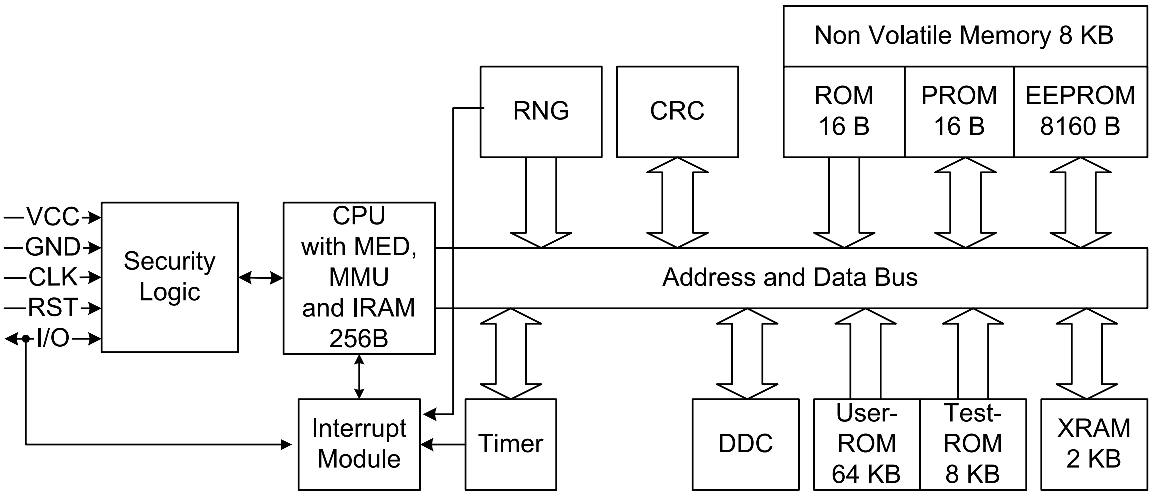


Figure 1: Block diagram of the SLE66C82P/SLE66C42P

2.2 Scope of the TOE

The TOE comprises the *hardware* of the smart card security controller, type SLE66C82P/SLE66C42P, manufactured by Infineon Technologies AG, and part of the associated *firmware* required for operation and provided in ROM. The documents described in section 2.2.3 and listed in Annex 9.1 are supplied as a manual. In the following description, the term “manufacturer” is short for Infineon Technologies AG, the manufacturer of the TOE. The user software is not part of the TOE.

2.2.1 Hardware of the TOE

The *hardware part* of the TOE (cf. Figure 1) as defined in Smartcard IC Platform Protection Profile is comprised of:

- Security logic (SEC)
- Microcontroller type ECO 2000 (CPU) with the subcomponents memory encryption and decryption unit (MED), memory management unit (MMU) and 256 bytes of internal RAM (IRAM)
- External memory comprising:
  - 2 kBytes extended RAM (XRAM)
  - 64 kBytes user ROM, including the routines for chip management (RMS)

- 8 KB test ROM containing the test routines (STS), and
- a total of 8 kBytes (SLE66C82P/m1474) EEPROM, which can be blocked to 4 kBytes (SLE66C42P/m1495) nonvolatile memory (EEPROM).

- True random number generator (RNG)
- Checksum module (CRC)
- Interrupt module (INT)
- Timer (TIM)
- Address and data bus (BUS)
- DES accelerator (DDC), used for fast calculations of the DES algorithm and provides EC2 support.

2.2.2 Firmware and software of the TOE

The entire firmware of the IC consists of two different parts. The one is the RMS routines for EEPROM programming and security function testing (**R**esource **M**anagement **S**ystem, IC Dedicated Support Software in Smartcard IC Platform Protection Profile). The RMS routines are stored from Infineon Technologies AG in a reserved area of the normal user ROM. The other is the STS which consists of test and initialization routines (**S**elf **T**est **S**oftware, IC Dedicated Test Software in Smartcard IC Platform Protection Profile).The STS routines are stored in the especially protected test ROM and are not accessible for the user software.

The above demarcations of the TOE result in the interfaces described below.

2.2.2.1 Interfaces of the TOE

- The physical interface of the TOE to the external environment is the entire surface of the IC.
- The electrical interface of the TOE to the external environment is constituted by the pads of the chip, particularly the contacted RES, I/O, CLK lines and supply lines VCC and GND.
- The data-oriented I/O interface to the TOE is formed by the I/O pad.
- The interface to the firmware is constituted by special registers used for hardware configuration and control (Special Function Registers, SFR).
- The interface of the TOE to the operating system is constituted on the one hand by the RMS routine calls and on the other by the instruction set of the TOE.
- The interface of the TOE to the test routines is formed by the STS test routine call, i.e. entry to test mode (STS-TM entry).

2.2.3 Guidance documentation

The guidance documentation consists of the [Databook] which contains the description of all interfaces of the software to the hardware relevant for programming the SLE66C82P/SLE66C42P.

In addition programming examples for more specific topics like secure use of cryptography are documented in form of application notes. The application notes are part of the development kit provided to the software developer. The monthly updated list of application notes is provided from Infineon Technologies AG [Status].

Finally the certification report will contain an overview of the recommendations to the software developer regarding the secure use of the platform SLE66C82P/SLE66C42P. These recommendations are also included in the ordinary documentation.

The list of guidance documentation is given in Annex 9.1.

2.2.4 Forms of delivery

The SLE66C82P/SLE66C42P can be delivered in form of complete modules or in form of plain wafers. The delivery can therefore be at the end of phase 3 or at the end of phase 4 according to Smartcard IC Platform Protection Profile. Nevertheless in both cases the TOE is finished and the extended test features are removed. In this document are always both cases mentioned to avoid incorrectness but from the security policy point of view the two cases are identical.

The delivery to the software developer (phase 2 -> phase 1) contains the development package and is delivered in form of documentation [Databook], data carriers containing the tools and emulators as development and debugging tool.

2.2.5 Production sites

The TOE may be produced in different production sites (listed in Table 2). The chip layout is not changed in this case and also the production testing does not differ. To distinguish the different production sites the chip identification number is coded as shown in Table 2. The exact coding of the chip identification data is described in [Databook] section 7.

The delivery measures are described in the ALC_DVS aspect.

Table 2: Production site in chip identification

Production Site	Chip Identification (first nibble, hex format)
Dresden	2
UMC	4

3 TOE Security Environment

For this chapter the Smartcard IC Platform Protection Profile can be applied completely. A summary is given in the following.

3.1 Definition of Assets

The primary assets concern the User Data which includes the data as well as program code (Smartcard Embedded Software). This asset has to be protected while being executed and on the other hand when the TOE is not in operation. This leads to the three primary assets

- User Data
- Smartcard Embedded Software
- TOE's correct operation

The specific functions of the TOE introduce additional assets.

- the random numbers generated by the TOE

The class of secondary assets consists of the following.

- logical design data,
- physical design data,
- IC Dedicated Software, Initialisation Data and Pre-personalisation Data, TSF data
- specific development aids,
- test and characterisation related data,
- material for software development support, and
- photomasks and products in any form

For details see Smartcard IC Platform Protection Profile section 3.1.

3.2 Assumptions

The assumptions defined in the Smartcard IC Platform Protection Profile concern the phases where the TOE has left the chip manufacturer.

A.Process-Card	Protection during Packaging, Finishing and Personalisation
A.Plat-Appl	Usage of Hardware Platform
A.Resp-Appl	Treatment of User Data

The support of cipher schemas needs to make a additional assumption.

The developer of the Smartcard Embedded Software must ensure the appropriate “Usage of Key-dependent Functions (A.Key-Function)” while developing this software in Phase 1 as specified below.

A.Key-Function Usage of Key-dependent Functions

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

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

For details see Smartcard IC Platform Protection Profile section 3.2.

3.3 Threats

The threats are directed against the assets. The threat is a general description of “What one wants to do” and might contain several specific attacks (“How one wants to do it”). The more detailed description of specific attacks is given later on in the process of evaluation and certification. An overview on attacks is given in Smartcard IC Platform Protection Profile.

Table 3: Threats to Smartcards according to the Protection Profile

T.Phys-Manipulation	Physical Manipulation
T.Phys-Probing	Physical Probing
T.Malfunction	Malfunction due to Environmental Stress
T.Leak-Inherent	Inherent Information Leakage
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

For details see Smartcard IC Platform Protection Profile section 3.2.

3.4 Organisational Security Policies

The SLE66C82P/SLE66C42P has to be protected during the first phases of his lifecycle (phases 2-TOE delivery)[1]. Later on the TOE has to protect itself. The organisational security policy covers this aspect.

[1] The TOE can be delivered either after phase 3 or after phase 4.

P.Process-TOE Protection during TOE Development and Production

See Smartcard IC Platform Protection Profile for a detailed description.

Due to the augmentations of the Smartcard IC Platform Protection Profile an additional policy is introduced.

3.4.1 Augmented organisational security policy

The TOE provides specific security functionality which can be used by the Smartcard Embedded Software. In the following specific security functionality is listed which is not derived from threats identified for the TOE's environment because it can only be decided in the context of the smartcard application, against which threats the Smartcard Embedded Software will use the specific security functionality.

The IC Developer / Manufacturer must apply the policy "Additional Specific Security Functionality (P.Add-Functions)" as specified below.

P.Add-Functions Additional Specific Security Functionality

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

- *Area based Memory Access Control*
- *Data Encryption Standard (DES),*
- *Triple Data Encryption Standard (3DES),*

4 Security objectives

For this chapter the Smartcard IC Platform Protection Profile can be applied completely. Only a short overview is given in the following.

4.1 Security objectives for the TOE

See Smartcard IC Platform Protection Profile.

Table 4: Objectives for Smartcards according to the Protection Profile

O.Phys-Manipulation	Protection against Physical Manipulation
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunction due to Environmental Stress
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality
O.Identification	TOE Identification
O.RND	Random Numbers

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 Smartcard Embedded Software:

- *Area based Memory Access Control*
- *Data Encryption Standard (DES),*
- *Triple Data Encryption Standard (3DES),*

Table 5: Additional objectives due to TOE specific functions and augmentations

O.Add-Functions	Additional specific security functionality

4.2 Security objectives for the environment

The detailed description of the environmental security objectives is given in the Smartcard IC Platform Protection Profile. The list of objectives is in Table 6.

Table 6: Security objectives for the environment

Phase 1		
	OE.Plat-Appl	Usage of Hardware Platform
	OE.Resp-Appl	Treatment of User Data
Phase 2 up to TOE delivery		
	OE.Process-TOE	Protection during TOE Development and Production
TOE delivery up to end of phase 6		
	OE.Process-Card	Protection during Packaging, Finishing and Personalisation

4.2.1 Clarification of “Usage of Hardware Platform (OE.Plat-Appl)”

Regarding the cryptographic services this objective of the environment has to be clarified. The TOE supports cipher schemes as additional specific security functionality. If required the Smartcard Embedded Software shall use these cryptographic services of the TOE and their interface as specified. When key-dependent functions implemented in the Smartcard Embedded Software are just being executed, the Smartcard Embedded Software must provide protection against disclosure of confidential data (User Data) stored and/or processed in the TOE by using the methods described under “Inherent Information Leakage (T.Leak-Inherent)” and “Forced Information Leakage (T.Leak-Forced)“.

Regarding the area based access control this objective of the environment has to be clarified. For the separation of different applications the Smartcard Embedded Software (Operating System) may implement a memory management scheme based upon security mechanisms of the TOE.

4.2.2 Clarification of “Treatment of User Data (OE.Resp-Appl)”

Regarding the cryptographic services this objective of the environment has to be clarified. By definition cipher or plain text data and cryptographic keys are User Data. The Smartcard Embedded Software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the TOE and use keys and functions appropriately in order to ensure the strength of cryptographic operation.

This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. For example, it must be ensured that it is beyond practicality to derive the private key from a public key if asymmetric algorithms are used. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realised in the environment.

Regarding the area based access control this objective of the environment has to be clarified. The treatment of User Data is also required when a multi-application operating system is implemented as part of the Smartcard Embedded Software on the TOE. In this case the multi-application operating system should not disclose security relevant user data of one application to another application when it is processed or stored on the TOE.

5 IT security requirements

For this chapter the Smartcard IC Platform Protection Profile can be applied completely.

5.1 TOE security requirements

See Smartcard IC Platform Protection Profile.

5.1.1 TOE security functional requirements

The detailed description of the security functional requirements is given in the Smartcard IC Platform Protection Profile. These security functional requirements are listed in Table 7. The additional security functional requirements are listed in Table 8. The necessary assignments are done in section 7.2. The description of the additional security functional requirements is given in the following.

5.1.1.1 Subset TOE security testing (FPT_TST.2)

The security is strongly dependent on the correct operation of the security functions. Therefore, the TOE shall support that particular security functions or mechanisms are tested in the operational phase (Phase 7). The tests can be initiated by the Smartcard Embedded Software and/or by the TOE.

Part 2 of the Common Criteria provides the security functional component “TSF testing (FPT_TST.1)”. The component FPT_TST.1 provides the ability to test the TSF’s correct operation.

For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT_TST.1 requires to verify the integrity of TSF data and stored TSF executable code which might violate the security policy. Therefore, the security functional component **Subset TOE security testing (FPT_TST.2)** has been newly created. This component allows that particular parts of the security mechanisms and functions provided by the TOE are tested.

FPT_TST.2

The security functional component Subset TOE security testing (FPT_TST.2) has been newly created (Common Criteria Part 2 extended). This component allows that particular parts of the security mechanisms and functions provided by the TOE can be tested after TOE Delivery. This security functional component is used instead of the functional component FPT_TST.1 from Common Criteria Part 2. For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT_TST.1 requires to verify the integrity of TSF data and stored TSF executable code which might violate the security policy.

The TOE shall meet the requirement “Subset TOE testing (FPT_TST.2)” as specified below (Common Criteria Part 2 extended).

FPT_TST.2 Subset TOE testing

Hierarchical to: No other components.

FPT_TST.2.1 The TSF shall run a suite of self tests *at the request of the authorised user*[2] to demonstrate the correct operation of the *environmental sensor mechanisms M1.1, M1.2, M1.5 and M1.6*[3]*, of the RNG with help of the live test and of the active shield.*

Dependencies: FPT_AMT.1 Abstract machine testing

5.1.1.2 Memory access control

Usage of multiple applications in one Smartcard often requires to separate code and data in order to prevent that one application can access code and/or data of another application. To support this the TOE provides Area based Memory Access Control. The underlying memory management unit (MMU) is documented in section 5 of the [DataBook].

The security service being provided is described in the Security Function Policy (SFP) **Memory Access Control Policy**. The security functional requirement **"Subset access control (FDP_ACC.1)"** requires that this policy is in place and defines the scope were it applies. The security functional requirement **"Security attribute based access control (FDP_ACF.1)"** defines addresses security attribute usage and characteristics of policies. It describes the rules for the function that implements the Security Function Policy (SFP) as identified in FDP_ACC.1. The decision whether an access is permitted or not is taken based upon attributes allocated to the software. The user software defines the attributes and memory areas. The corresponding permission control information is evaluated "on-the-fly" by the hardware so that access is granted/effective or denied/inoperable.

The security functional requirement **"Static attribute initialisation (FMT_MSA.3)"** ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. Alternative values can be specified by any subject provided that the **Memory Access Control Policy** allows that. This is described by the security functional requirement **"Management of security attributes (FMT_MSA.1)"**. The attributes are determined during TOE manufacturing (FMT_MSA.3) or set at run-time (FMT_MSA.1).

From TOE´s point of view the different roles in the user software can be distinguished according to the memory based access control. However the definition of the roles belongs to the user software.

The following Security Function Policy (SFP) **Memory Access Control Policy** is defined for the requirement "Security attribute based access control (FDP_ACF.1)":

Memory Access Control Policy

The TOE shall control *read, write, delete, execute accesses* of *software running at two different modes (system mode active during interrupt execution or application mode active during other executing)* on *data and code stored in memory areas*.

The TOE shall restrict the ability to define, to change or at least to finally accept the applied rules (as mentioned in FDP_ACF.1) to *software running at interrupt level (in the system mode)*.

[2] The term "authorised user" refers to the user software running on the TOE

[3] The definition of the self test function (SleSlcTest) can be found in [Databook] chapter 6

The TOE shall meet the requirement “Subset access control (FDP_ACC.1)” as specified below.

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the *Memory Access Control Policy* on *all subjects (software running at system mode active during interrupt execution or application mode active during other executing), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy*.

Dependencies: FDP_ACF.1 Security attribute based access control

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 *Memory Access Control Policy* to objects based on *the execution level where the software is executed (interrupt / non-interrupt) and/or the memory area where the access is performed to and/or the operation to be performed*.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *evaluate the corresponding permission control information before the access so that accesses to be denied can not be utilised by the subject attempting to perform the operation*.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the *following additional rules: none*.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

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 *Memory Access Control Policy* to provide *well defined*[4] 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 Memory Access Control Policy is enforced and the necessary access is therefore*

[4] The static definition of the access rules is documented in [DataBook] section 5

allowed) [5] 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

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 *Memory Access Control Policy* to restrict the ability to *change_default, modify or delete* the security attributes *permission control information* to *software running at interrupt level (system mode)*.

Dependencies: [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

The TOE shall meet the requirement “ Specification of management functions (FMT_SMF.1)” as specified below:

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions*: access the configuration registers of the MMU*.

Dependencies: No dependencies

[5] The user software is intended to set the memory access control policy

5.1.1.3 Support of cipher schemas

FCS_COP.1 Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard. The dependencies will be discussed in Section 8.2.

The following additional specific security functionality is implemented in the TOE:

- *Data Encryption Standard (DES),*
- *Triple Data Encryption Standard (3DES),*

DES Operation

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

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform *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

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

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Triple Data Encryption Standard (3DES)* and cryptographic key sizes *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, keying option 2

Dependencies: [FDP_ITC.1 Import of user data without security attributes

or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

5.1.1.4 Overview

Table 7: Security functional requirements defined in Smartcard IC Platform Protection Profile

Security Functional Requirement	
FRU_FLT.2	“Limited fault tolerance“
FPT_FLS.1	“Failure with preservation of secure state”
FPT_SEP.1	“TSF domain separation”
FMT_LIM.1	“Limited capabilities”
FMT_LIM.2	“Limited availability”
FAU_SAS.1	“Audit storage”
FPT_PHP.3	“Resistance to physical attack”
FDP_ITT.1	“Basic internal transfer protection”
FDP_IFC.1	“Subset information flow control”
FPT_ITT.1	“Basic internal TSF data transfer protection”
FCS_RND.1	“Quality metric for random numbers”

Table 8: Augmented security functional requirements

Security Functional Requirement
FPT_TST.2 “Subset TOE security testing“
FDP_ACC.1 “Subset access control”
FDP_ACF.1 “Security attribute based access control”
FMT_MSA.3 “Static attribute initialisation”
FMT_MSA.1 “Management of security attributes”
FMT_SMF.1 “Specification of Management functions”
FCS_COP.1 “Cryptographic support”

5.1.2 TOE security assurance requirements

The evaluation assurance level is EAL 5 augmented. In Table 9 the security assurance requirements are given. The increase of the assurance components compared to the Smartcard IC Platform Protection Profileis expressed with bold letters. The augmentation of the assurance components to level EAL5 is given in italic letters.

Table 9: Assurance components

Aspect	Acronym	Description	Refinement
Configuration management	ACM_AUT.1	Partial CM automation	
	ACM_CAP.4	Generation support and acceptance procedures	in PP
	ACM_SCP.3	**Development tools CM coverage**	**in ST**
Delivery and operation	ADO_DEL.2	Detection of modification	in PP
	ADO_IGS.1	Installation, generation, and start-up procedures	in PP
Development	**ADV_FSP.3**	**Semiformal functional specification**	**in ST**
	ADV_HLD.3	**Semiformal high-level design**	
	ADV_IMP.2	Implementation of the TSF	
	ADV_INT.1	**Modularity**	
	ADV_LLD.1	Descriptive low-level design	
	ADV_RCR.2	**Semiformal correspondence demonstration**	
	ADV_SPM.3	**Formal TOE security policy model**	
Guidance documents	AGD_ADM.1	Administrator guidance	in PP
	AGD_USR.1	User guidance	in PP
Life cycle support	*ALC_DVS.2*	*Sufficiency of security measures*	*in PP*
	ALC_LCD.2	**Standardised life-cycle model**	
	ALC_TAT.2	**Compliance with implementation standards**	
Tests	ATE_COV.2	Analysis of coverage	in PP
	ATE_DPT.2	**Testing: low-level design**	
	ATE_FUN.1	Functional testing	
	ATE_IND.2	Independent testing – sample	
Vulnerability assessment	**AVA_CCA.1**	**Covert channel analysis**	
	AVA_MSU.3	*Validation of analysis*	
	AVA_SOF.1	Strength of TOE security function evaluation	
	AVA_VLA.4	*Highly resistant*	

5.1.3 Refinements

Some refinements are taken unchanged from the Smartcard IC Platform Protection Profile. In some cases a clarification is necessary. In Table 9 a overview is given where the refinement is done. Two refinements from the Smartcard IC Platform Protection Profile have to be discussed here in the Security Target, as the assurance level is increased.

Configuration Management Scope (ACM_SCP)

The refinement from the Smartcard IC Platform Protection Profile can be applied even at the chosen assurance level EAL 5 augmented with ACM_SCP.3. The assurance package ACM_SCP.2 is extended to ACM_SCP.3 with aspects regarding the development tools. The refinement is not touched.

Refinement for CM scope (ACM_SCP)

The "TOE implementation representation" within the scope of the CM shall include at

least:

- logical design data,
- physical design data,
- IC Dedicated Software,
- Smartcard Embedded Software,
- final physical design data necessary to produce the photomasks, and
- photomasks.

Functional Specification (ADV_FSP)

The refinement from the Smartcard IC Platform Protection Profile can be applied even at the chosen assurance level EAL 5 augmented with ADV_FSP.3. The assurance package ADV_FSP.2 is extended to ADV_FSP.3 with aspects regarding the descriptive level. The level is increased from informal to semi formal with informal description The refinement is not touched from this measure.

For details of the refinement see Smartcard IC Platform Protection Profile.

5.2 Security requirements for the Environment

5.2.1 Security requirements for the IT Environment

See Smartcard IC Platform Protection Profile.

5.2.2 Security Requirements for the Non-IT-Environment

In the following security requirements for the Non-IT-Environment are defined. For the development of the Smartcard Embedded Software (in Phase 1) the requirement 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 way that it meets the requirements from the following documents: (i) hardware data sheet for the TOE, (ii) TOE application notes, and (iii) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.

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.

The responsible parties for the Phases 4-6 are required to support the security of the TOE by appropriate measures:

RE.Process-Card Protection during Packaging, Finishing and Personalisation

The Card Manufacturer (after TOE Delivery up to the end of Phase 6) shall use adequate security measures 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).

The Smartcard Embedded Software shall meet the requirements “Cipher Schemas (RE.Cipher)” as specified below.

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. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that an appropriate key management has to be realised in the environment.

6 TOE summary specification

The product overview is given in section 2.1. In the following the security functionality is described and the relation to the security functional requirements is shown.

The TOE is equipped with 9 security enforcing functions to meet the security functional requirements. The functions are:

SEF1: Operating state checking

SEF2: Phase management with test mode lock-out

SEF3: Protection against snooping

SEF4: Data encryption and data disguising

SEF5: Random number generation

SEF6: TSF self test

SEF7: Notification of physical attack

SEF8: Memory Management Unit (MMU)

SEF9: Cryptographic support

The following description of the security enforcing functions is a complete representation of the TSF.

6.1 SEF1: Operating state checking

Correct function of the SLE66C82P/SLE66C42P is only given in the specified range of the environmental operating parameters. To prevent an attack exploiting that circumstances it is necessary to detect if the specified range is left.

All operating signals are filtered to prevent malfunction. The FRU_FLT.2 “Limited fault tolerance” requirement is satisfied.

In addition the operating state is monitored with sensors for the operating voltage, clock signal frequency, temperature and electro magnetic radiation. The TOE falls into the defined secure state in case of a specified range violation[6]. The defined secure state causes the chip internal reset process. The FPT_FLS.1 “Failure with preservation of secure state“ requirement is satisfied.

The covered security functional requirements are FRU_FLT.2 and FPT_FLS.1. The SEF1 does not use probabilistic or permutational effects.

6.2 SEF2: Phase management with test mode lock-out

The life cycle of the TOE is split-up in several phases. Chip development and production (phase 2, 3, 4) and final use (phase 4-7) is a rough split-up from TOE point of view. These phases are implemented in the SLE66C82P/SLE66C42P as test mode (phase 2, 3, 4) and user mode (phase 1, 4-7). In addition a chip identification mode exists which is active in all phases.

During start-up of the SLE66C82P/SLE66C42P the decision for the user mode or the test mode is taken dependent on several phase identifiers (phase management). If test mode is the active phase the SLE66C82P/SLE66C42P requests authentication before any action (test mode lock-out). FMT_LIM.1 and FMT_LIM.2 are satisfied.

[6] The operating state checking SEF1 can only work when the TOE is running and can not prevent reverse engineering.

If the chip identification mode is requested the chip identification data (O.Identification) stored in a non modifiable EEPROM area is reported. FAU_SAS.1 “Audit storage” is satisfied.

The phase management is used to provide the separation between the security enforcing functions and the user software. FPT_SEP.1 “TSF domain separation“ is satisfied.

The covered security functional requirements are FMT_LIM.1, FMT_LIM.2, FPT_SEP.1 and FAU_SAS.1. The test mode lock-out uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF *high*.

6.3 SEF3: Protection against snooping

Several mechanisms protect the SLE66C82P/SLE66C42P against snooping the design or the user data during operation and even if it is out of operation (power down).

There are topological design measures for disguise, such as the use of the top metal layer with active signals for protecting critical data. The entire design is kept in a non standard way to prevent attacks using standard analysis methods. A Smartcard dedicated CPU with a non public bus protocol is used which makes analysis complicated.

The covered security functional requirement is FPT_PHP.3 “Resistance to physical attack“ as these measures make it difficult to do the physical analysis necessary before manipulation. The protection against snooping uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF high.

6.4 SEF4: Data encryption and data disguising

The readout of data can be controlled with the use of encryption An attacker can not use the data he has espionaged, because he must break the encryption.

The memory contents of the SLE66C82P/SLE66C42P are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. To prevent interpretation of leaked processed or transferred information randomness is inserted in the information. In addition important parts of the CPU and the complete DES component are especially designed to counter leakage attacks like DPA or EMA. The current consumption is independent of the processed data.

The information leakage is kept low with special design measures. An interpretation of leaked data is not possible as all the data is encrypted. The covered security functional requirements are FDP_ITT.1 “Basic internal transfer protection“ and FPT_ITT.1 “Basic internal TSF data transfer protection“. The encryption covers the data processing policy and FDP_IFC.1 “Subset information flow control“. The SEF4 uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF high.

6.5 SEF5: Random number generation

Random data is essential for cryptography as well as for physical security mechanisms. The SLE66C82P/SLE66C42P is equipped with a true random generator based on physical probabilistic controlled effects. The random data can be used from the user software as well as from the security enforcing functions.

The generated numbers are true random due to the construction principle. The covered security functional requirement is FCS_RND.1.

6.6 SEF6: TSF self test

The TSF of the SLE66C82P/SLE66C42P has either a hardware controlled self test which can be started from the user software by a RMS function call or can be tested directly from the user software for the active shield. The tested security enforcing functions are SEF1, SEF5 and SEF7.

As any attempt to modify the sensor devices will be detected from the test, the covered security functional requirement is FPT_TST.2. The TSF self test does not use probabilistic or permutational effects.

6.7 SEF7: Notification of physical attack

The entire surface of the SLE66C82P/SLE66C42P is protected with the active shield. Attacks over the surface are detected when the shield lines are cut or get contact.

The attempt to use an opened device will be detected. The covered security functional requirement is FPT_PHP.3. Especially manipulation and the usage of galvanic contacts to gain information on the chip or the data is covered of this security enforcing function. The SEF7 “Notification of physical attack” does not use probabilistic or permutational effects.

6.8 SEF8: Memory Management Unit (MMU)

The MMU in the SLE66C82P/SLE66C42P gives the user software the possibility to define different access rights for memory areas and components. In case of a access violation the MMU will generate a non maskable interrupt (NMI). Then a interrupt service routine (ISR) can react on the access violation.

The MMU is used to map the logical address range of 64 kByte in the 8051 architecture to the physical memory range of 1 MByte and to control access to the component’s special function registers. The MMU provides the privileged system mode (at interrupt level) and the regular application mode. Both modes own two descriptors for data access and two descriptors for code access. The descriptor table defines the physical base address and the length of the memory range in 256 byte granularity which will be used for the logical to physical address translation. Two additional registers contain the access information of the component’s SFR. Access violation is caused if the physical address is not in the range defined from the descriptor or the access to the SFR is not granted. The reaction on access violation is a non maskable interrupt (NMI).

Only system mode has access to the descriptor table. The MMU has to be enabled as the default mode after reset is a compatibility mode without access permission (transparent mode).

As the TOE provides support for separation of memory areas the covered security functional requirements are FDP_ACC.1 as access control is provided, FDP_ACF.1 as a privileged and a regular mode exists, FMT_MSA.3 is covered from the initial (transparent) mode, FMT_MSA.1 is covered from the possibility to enable the MMU and FMT_SMF.1 is covered from the access to the special function register. The SEF8 “Memory Management Unit” does not use probabilistic or permutational effects.

6.9 SEF9: Cryptographic Support

The TOE is equipped with several hardware accelerators to support the standard cryptographic operations. This security enforcing function is introduced to include the cryptographic operation in the scope of the evaluation as the cryptographic function itself is not used from the TOE security policy. On the other hand these functions are of special interest for the use of the hardware as platform for the software. The component is a hardware DES encryption unit. The key for the cryptographic operations are provided from the user software (environment).

As defined cryptographic operations are provided by the TOE, the covered security functional requirement is FCS_COP.1. The SEF9 does use probabilistic or permutational effects, but cryptographic algorithms are excluded from the SOF assessment.

6.10 Mapping of Security Functional Requirements

The justification of the mapping between Security Functional Requirements and the Security Enforcing Functions is given in sections 6.1-6.9. The results are shown in Table 10. The security functional requirements are addressed by one relating security enforcing function except the security functional requirement FPT_PHP.3. The security functional requirement FPT_PHP.3 is covered from the SEF3 for the aspect of making the reverse engineering harder even if the TOE is out of operation and from SEF7 for the aspect of detecting the attempt to modify the TOE when the chip is running. The SEF3 and the SEF7 are mutually supportive to cover FPT_PHP.3.

Table 10: Mapping of SFR and SEF

	SEF 1	SEF 2	SEF 3	SEF 4	SEF 5	SEF 6	SEF 7	SEF 8	SEF 9
FAU_SAS.1		X							
FCS_RND.1					X				
FDP_IFC.1				X					
FDP_ITT.1				X					
FMT_LIM.1		X							
FMT_LIM.2		X							
FPT_FLS.1	X								
FPT_ITT.1				X					
FPT_PHP.3			X				X		
FPT_SEP.1		X							
FRU_FLT.2	X								
FPT_TST.2						X			
FDP_ACC.1								X	
FDP_ACF.1								X	
FMT_SMF.1								X	
FMT_MSA.3								X	
FMT_MSA.1								X	
FCS_COP.1									X

6.11 Assurance Measures

In Table 11 the TOE specific assurance measures are listed. These measures fulfil the requirements from Table 9.

This Security Target is the first document in the course of an evaluation. The exact references (version numbers and date) of the documents are not final during the evaluation of the security target. To avoid an update of the security target at the end of the evaluation the exact references are listed in the configuration list (ACM_SCP.3) of the evaluation.

Table 11: Assurance measures

Assurance measure	Acronym	Document
Security Target	ASE	Security Target
Configuration management	ACM_AUT.1	Configuration management (ACM)
	ACM_CAP.4	
	ACM_SCP.3	Configuration management scope (ACM_SCP)
Delivery and operation	ADO_DEL.2	Delivery (ADO)
	ADO_IGS.1	
Development	ADV_FSP.3	Functional Specification (ADV_FSP.3)
	ADV_HLD.3	High Level Design (ADV_HLD.3)
	ADV_IMP.2	Implementation (ADV_IMP.2)
	ADV_INT.1	High Level Design (ADV_HLD.3)
	ADV_LLD.1	
		Low Level Design K1 SEC (ADV_LLD.1)
		Low Level Design K2 CPU (ADV_LLD.1)
		Low Level Design K3 RNG (ADV_LLD.1)
		Low Level Design K5 EEPROM (ADV_LLD.1)
		Low Level Design K7 BUS (ADV_LLD.1)
		Low Level Design K10 XRAM (ADV_LLD.1)
		Low Level Design K11 ROM (ADV_LLD.1)
		Low Level Design K12 STS (ADV_LLD.1)
		Low Level Design K13 DDC (ADV_LLD.1)
		Low Level Design K4, K8, K9, K14, K15
	ADV_RCR.2	Representation Correspondance (ADV_RCR.2)
	ADV_SPM.3	LKW model
Guidance documents	AGD_ADM.1	Documentation (AGD)
	AGD_USR.1	
Life cycle support	ALC_DVS.2	Life Cycle Support (ALC)
	ALC_LCD.2	
	ALC_TAT.2	
Tests	ATE_COV.2	Test Documentation (ATE)
	ATE_DPT.2	
	ATE_FUN.1	
	ATE_IND.2	
Vulnerability assessment	AVA_CCA.1	Vulnerability Assessment (AVA)
	AVA_MSU.3	
	AVA_SOF.1	
	AVA_VLA.4	

7 PP claims

7.1 PP reference

This security target is conformant to the Smartcard IC Platform Protection Profile.

7.2 PP tailoring

The assignments and selections foreseen in the Smartcard IC Platform Protection Profile are done here.

7.2.1 FCS_RND

The random numbers are generated from SEF5. The quality level of the random numbers is defined with the tests T0-T8 of the [AIS31].

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet *the test criteria specified in tests T0-T8 of [AIS31].*

7.3 PP additions

Additional objectives and security functional requirements are explicitly mentioned in this security target.

8 Rational

The rational from the Smartcard IC Platform Protection Profile is used here and it is not changed. The augmentations are designed to be conform to the rational of the Smartcard IC Platform Protection Profile. The necessary extensions to the Smartcard IC Platform Protection Profile rational are given in the following.

8.1 Security Objectives Rationale

Assumption, Threat or Organisational Security Policy	Security Objective	Note
P.Add-Functions	O.Add-Functions	
A.Key-Function	OE.Plat-Appl OE.Resp-Appl	

The justification related to the security objective "Additional Specific Security Functionality (O.Add-Functions)" is as follows: Since O.Add-Functions requires the TOE to implement exactly the same specific security functionality as required by P.Add-Functions, the organisational security policy is covered by the objective.

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

Compared to Smartcard IC Platform Protection Profilea clarification has been made for the security objective "Usage of Hardware Platform (OE.Plat-Appl)": If required the Smartcard Embedded Software shall use these cryptographic services of the TOE and their interface as specified. In addition, the Smartcard Embedded Software must implement functions which perform operations on keys (if any) in such a manner that they do not disclose information about confidential data. The non disclosure due to leakage A.Key-Function attacks is included in this objective OE.Plat-Appl. This addition ensures that the assumption A.Plat-Appl is still covered by the objective OE.Plat-Appl although additional functions are being supported according to O.Add-Functions.

Compared to Smartcard IC Platform Protection Profilea clarification has been made for the security objective "Treatment of User Data (OE.Resp-Appl)": By definition cipher or plain text data and cryptographic keys are User Data. So, the Smartcard Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realised in the environment. That is expressed by the assumption A.Key—Function which is covered from OE.Resp–Appl. These measures make sure that the assumption A.Resp-Appl is still covered by the security objective OE.Resp-Appl although additional functions are being supported according to P.Add-Functions.

The justification of the additional policy and the additional assumption show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there.

8.2 Security Requirements Rationale

8.2.1 Rationale for the security functional requirements

Cryptographic operation (FCS_COP.1)

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.Add-Functions	- FCS_COP.1 „Cryptographic operation“	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” with RE.Cipher
OE.Plat-Appl OE.Resp-Appl		RE.Cipher

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

The security functional requirement(s) “Cryptographic operation (FCS_COP.1)” exactly require those functions to be implemented which are demanded by O.Add-Functions. Therefore, FCS_COP.1 is suitable to meet the security objective.

Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context. These issues are addressed by the requirement RE.Phase-1 and more specific by the security functional requirements

- [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.

to be met by the environment.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality. However, key-dependent functions could be implemented in the Smartcard Embedded Software. In this case RE.Cipher requires that these functions ensure that confidential data (User Data) can not be disclosed while they are just being processed by the Smartcard Embedded Software. Therefore, with respect to the Smartcard Embedded Software the issues addressed by the objectives just mentioned are addressed by the requirement RE.Cipher.

The usage of cryptographic algorithms requires to use appropriate keys. Otherwise they do not provide security. The requirement RE.Cipher addresses these specific issues since cryptographic keys and other data are provided by the Smartcard Embedded Software. RE.Cipher requires that keys must be kept confidential. They must be unique with a very high probability, cryptographically strong etc. If keys are imported into the TOE (usually after TOE Delivery), it must be ensured that quality and confidentiality is maintained. Therefore, with respect to the environment the issues addressed (i) by the objectives just mentioned and (ii) implicitly by O.Add-Functions are addressed by the requirement RE.Cipher.

In this ST the objectives for the environment OE.Plat-Appl and OE.Resp-Appl have been clarified. The requirement for the environment Re.Cipher has been introduced to cover the objectives

OE.Plat-Appl and OE.Resp-Appl (in addition to O.Add-Functions). The Smartcard Embedded Software defines the use of the cryptographic functions FCS_COP.1 provided by the TOE.

The justification of the security objective and the additional requirements (both for the TOE and its environment) show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there.

Subset TOE security testing (FPT_TST.2)

The security functional component Subset TOE security testing (FPT_TST.2) has been newly created (Common Criteria Part 2 extended). This component allows that particular parts of the security mechanisms and functions provided by the TOE can be tested after TOE Delivery. This security functional component is used instead of the functional component FPT_TST.1 from Common Criteria Part 2. For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT_TST.1 requires to verify the integrity of TSF data and stored TSF executable code which might violate the security policy.

The tested security enforcing function is SEF1, SEF5 and SEF7.

The security functional requirement FPT_TST.2 will detect attempts to conduce a physical manipulation on the monitoring functions of the TOE. The objective of FPT_TST.2 is O.Phys-Manipulation. The physical manipulation will be tried to overcome security enforcing functions.

Memory Access Control Policy

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.Add-Functions	- FDP_ACC.1 “Subset access control” - FDP_ACF.1 “Security attribute based access control” - FMT_MSA.3 “Static attribute initialisation” - FMT_MSA.1 “Management of security attributes” - FMT_SMF.1 “Specification of Management Functions”	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software”

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

The security functional requirement “Subset access control (FDP_ACC.1)” with the related Security Function Policy (SFP) “Memory Access Control Policy” exactly require to implement an area based memory access control as demanded by O.Add-Functions. Therefore, FDP_ACC.1 with its SFP is suitable to meet the security objective.

Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context. These issues are addressed by the requirement RE.Phase-1. The TOE only provides the tool to implement the policy defined in the context of the application.

8.2.2 Dependencies of security functional requirements

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_COP.1	FCS_CKM.1	Yes (by the environment)
	FDP_ITC.1 (if not FCS_CKM.1) FCS_CKM.4 FMT_MSA.2	Yes (by the environment)

The dependencies FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2 must be covered from the environment (the smartcard embedded software) and are addressed by the requirement RE.Cipher.

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FPT_TST.2	FPT_AMT.1	See discussion below

The following discussion demonstrates how the dependencies defined by Part 2 of the Common Criteria for the requirement FPT_TST.2 are satisfied. The dependency defined in the Common Criteria is Abstract machine testing (FPT_AMT.1).

Part 2 of the Common Criteria explains that „the term ‚underlying abstract machine‘ typically refers to the hardware components upon which the TSF has been implemented. However, the phrase can also be used to refer to an underlying, previously evaluated hardware and software combination behaving as a virtual machine upon which the TSF relies.“

The TOE is already a platform representing the lowest level in a Smartcard. There is no lower or “underlying abstract machine” used by the TOE which can be tested. There is no need to perform testing according to FPT_AMT.1 and the dependency in the requirement FPT_TST.2 is therefore considered to be satisfied.

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes See discussion below
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes See discussion below Yes

The dependency FMT_SMR.1 introduced by the two components FMT_MSA.1 and FMT_MSA.3 is considered to be satisfied because the access control specified for the intended TOE is not rolebased but enforced for each subject. Therefore, there is no need to identify roles in form of an security functional requirement FMT_SMR.1.

8.2.3 Rationale for the Assurance Requirements and the Strength of Function Level

The chosen assurance level EAL 5 augmented determines the assurance requirements. In Table 9 the different assurance levels are shown as well as the augmentations. The augmentations are not changed compared to the Protection Profile

The assurance level EAL5 and the augmentation with the requirements ALC_DVS.2, AVA_MSU.3, and AVA_VLA.4 were chosen in order to meet assurance expectations. An assurance level of EAL5 is required for this type of TOE since it is intended to defend against highly sophisticated attacks without a protected environment. This evaluation assurance level was selected since it provides even a formal evidence on the conducted vulnerability assessment. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defense against such attacks, the evaluators have access to all information regarding the TOE including the low level design and source code.

The rational for the strength of function level from the Smartcard IC Platform Protection Profile is used as the level is not changed.

8.3 Security Requirements are Mutually Supportive and Internally Consistent

In addition to the discussion in section 7.3 of the Smartcard IC Platform Protection Profile the security functional requirement FCS_COP.1 is introduced. The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms implemented according to the security functional requirement FCS_COP.1. Therefore, these security functional requirements support the secure implementation and operation of FCS_COP.1.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the self-test functions implemented according to the security functional requirement FPT_TST.2. Therefore, these security functional requirements support the secure implementation and operation of FPT_TST.2.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the area based memory access control function implemented according to the security functional requirement described in the security functional requirement FDP_ACC.1 with reference to the Memory Access Control Policy and details given in FDP_ACF.1. Therefore, those security functional requirements support the secure implementation and operation of FDP_ACF.1 with its dependent security functional requirements.

9 References

9.1 Documents and User Guidance

Table 12: User guidance

[Status]	Status report, List of all available user guidance including application notes	01.03
[DataBook]	Data Book, SLE66CxxxP	09.02

9.2 Literature

Table 13: Table of Criteria

[ProtectionProfile]	Smartcard IC Platform Protection Profile	BSI-PP-0002; Version 1.0, July 2001
[AIS31]	Functionality classes and evaluation methodology for physical random number generators	AIS31, Version1, 25.9.2001
[CC]	Common Criteria for Information Technology Security Evaluation	Version 2.1, August 1999

9.3 List of abbreviations

CC	Common Criteria
CI	Chip Identification mode (STS-CI)
CIM	Chip Identification Mode (STS-CI), same as CI
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DPA	Differential Power Analysis
DFA	Differential Failure Analysis
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMA	Electro magnetic analysis
HW	Hardware
IC	Integrated Circuit
ID	Identification
I/O	Input/Output
IRAM	Internal Random Access Memory
ITSEC	Information Technology Security Evaluation Criteria
M	Mechanism
MED	Memory Encryption and Decryption
MMU	Memory Management Unit
MOVC	MOVe Code

O	Object
OS	Operating system
PLL	Phase Locked Loop
PROM	Programmable Read Only Memory
RAM	Random Access Memory
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read Only Memory
S	Subject
SF	Security function
SFR	Special Function Register, as well as Security Functional Requirement The specific meaning is given in the context
SPA	Simple power analysis
STS	Self Test Software
SW	Software
SO	Security objective
T	Threat
TM	Test Mode (STS)
TOE	Target of Evaluation
UM	User Mode (STS)
UMC	Production site in Taiwan
XRAM	eXtended Random Access Memory

9.4 Glossary

Application Program/Data

Software which implements the actual TOE functionality provided for the user or the data required for that purpose

Threat

Action or event that might prejudice security

Operating System

Software which implements the basic TOE actions necessary for operation

Central Processing Unit

Logic circuitry for digital information processing

Chip → Integrated Circuit

Chip Identification Data

Data stored in the EEPROM containing the chip type, lot number (including the production site), die position on wafer and production week and data stored in the ROM containing the STS version number

Chip Identification Mode

Operational status phase of the TOE, in which actions for identifying the individual chip by transmitting the Chip Identification Data take place

Smart Card

Plastic card in credit card format with built-in chip

Controller

IC with integrated memory, CPU and peripheral devices

Cyclic Redundancy Check

Process for calculating checksums for error detection

Electrically Erasable and Programmable Read Only Memory (EEPROM)

Nonvolatile memory permitting electrical read and write operations

End User

Person in contact with a TOE who makes use of its operational capability

Firmware

Part of the software implemented as hardware

Hardware

Physically present part of a functional system (item)

Integrated Circuit

Component comprising several electronic circuits implemented in a highly miniaturized device using semiconductor technology

Internal Random Access Memory

RAM integrated in the CPU

Mechanism

Logic or algorithm which implements a specific security function in hardware or software

Memory Encryption and Decryption

Method of encoding/decoding data transfer between CPU and memory

Microcontroller → Controller

Microprocessor → CPU

Move Code

Instruction in the CPU's instruction set for transferring program memory contents to an internal register

Object

Physical or non-physical part of a system which contains information and is acted upon by subjects

Programmable Read Only Memory

Nonvolatile memory which can be written once and then only permits read operations

Random Access Memory

Volatile memory which permits write and read operations

Random Number Generator

Hardware part for generating random numbers

Read Only Memory

Nonvolatile memory which permits read operations only

Resource Management System

Part of the firmware containing EEPROM programming routines

Self Test Software

Part of the firmware with routines for controlling the operating state and testing the TOE hardware

Security Function

Part(s) of the TOE used to implement part(s) of the security objectives

Security Target

Description of the intended state for countering threats

Software

Information (non-physical part of the system) which is required to implement functionality in conjunction with the hardware (program)

Memory

Hardware part containing digital information (binary data)

Subject

Entity, generally in the form of a person, who performs actions

Target of Evaluation

Product or system which is being subjected to an evaluation

Test Mode

Operational status phase of the TOE in which actions to test the TOE hardware take place

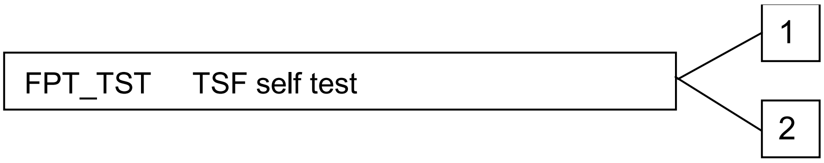
User Mode

Operational status phase of the TOE in which actions intended for the user take place

10 Definition of the Security Functional Component FPT_TST.2

The following additions are made to „TSF self test (FPT_TST)“ in Common Criteria:

Component levelling



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.

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.

The security functional component family “Subset TOE testing (FPT_TST.2)” is specified as follows.

FPT_TST.2 Subset TOE testing

Hierarchical to: No other components.

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].

Dependencies: FPT_AMT.1 Abstract machine testing