



PHILIPS

Business Line
Identification

Security Target
BSI-DSZ-CC-0153

Version 1.0

Page 1 of 30

Security Target BSI-DSZ-CC-0153

Version 1.0

September 20th, 1999

First Evaluation of Philips P8WE5032 Secure 8-bit Smart Card Controller


Developed and provided by

Philips Semiconductors

According to the
Common Criteria for Information Technology
Evaluation (CC) at Level EAL3

by

Philips Semiconductors Hamburg
Unternehmensbereich der Philips GmbH
Stresemannallee 101
22505 Hamburg

| | | |
|---|------------------------------------|---------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 2 of 30 |
|---|------------------------------------|---------------------------------|

1 Document Information

Document History

| Version | Date | Changes | Remarks |
|-------------|-------------------------------|---------|---------|
| Version 1.0 | Sept. 20 th , 1999 | | |

Latest version is: Version 1.0 (September 20th, 1999)

Document Invariants

| Name | Value (to be edited) | Test Output (to copy) |
|------------------------|---|---|
| file name and length | Automatically | st-phil5032-1-0.doc (161792 Byte) |
| latest version | Version 1.0 | Version 1.0 |
| date of this version | September 20 th , 1999 | September 20 th , 1999 |
| classification | Internal use | Internal use |
| product (short) | Philips 5032 smart card controller | Philips 5032 smart card controller |
| product (long) | Philips P8WE5032 Secure 8-bit Smart Card Controller | Philips P8WE5032 Secure 8-bit Smart Card Controller |
| developer (long) | Philips Semiconductors | Philips Semiconductors |
| developer (short) | Philips | Philips |
| registration number | BSI-DSZ-CC-0153 | BSI-DSZ-CC-0153 |
| list of authors | Hans-Gerd Albertsen, Dr. Jörg Pillath, Dr. Eberhard von Faber | Hans-Gerd Albertsen, Dr. Jörg Pillath, Dr. Eberhard von Faber |
| certific. body (short) | BSI | BSI |
| certific. body (long) | Bundesamt für Sicherheit in der Informationstechnik (BSI) | Bundesamt für Sicherheit in der Informationstechnik (BSI) |



| | | |
|---|--|--|
|  <p>PHILIPS</p> <p>Business Line Identification</p> | <p>Security Target BSI-DSZ-CC-0153</p> | <p>Version 1.0</p> <p>Page 3 of 30</p> |
|---|--|--|

Table of Contents

| | | |
|-------|--|----|
| 1 | Document Information | 2 |
| 2 | ST Introduction | 5 |
| 2.1 | ST Identification | 5 |
| 2.2 | ST Overview | 5 |
| 2.3 | CC Conformance | 5 |
| 3 | TOE Description | 6 |
| 4 | Security Environment | 7 |
| 4.1 | Assumptions | 7 |
| 4.2 | Threats | 8 |
| 4.3 | Organisational Security Policies | 9 |
| 5 | Security Objectives | 10 |
| 5.1 | TOE Security Objectives | 10 |
| 5.2 | Security Objectives for the Environment | 10 |
| 6 | IT Security Requirements | 11 |
| 6.1 | TOE Security Requirements | 11 |
| 6.1.1 | TOE Functional Requirements | 11 |
| 6.1.2 | TOE Security Assurance Requirements | 13 |
| 6.2 | Security Requirements for the Environment | 13 |
| 6.2.1 | Security Requirements for the IT-Environment | 13 |
| 6.2.2 | Security Requirements for the Non-IT Environment | 13 |
| 7 | TOE Summary Specification | 16 |
| 7.1 | TOE Security Functions | 16 |
| 7.2 | Assurance Measures | 18 |
| 8 | PP Claims | 19 |
| 9 | Rationale | 20 |
| 9.1 | Security Objectives Rationale | 20 |
| 9.2 | Security Requirements Rationale | 23 |

| | | |
|--|------------------------------------|---------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 4 of 30 |
|--|------------------------------------|---------------------------------|

| | | |
|-------|--|----|
| 9.2.1 | Security Functional Requirements | 23 |
| 9.2.2 | Assurance Requirements and Strength of Function Claim | 27 |
| 9.3 | TOE Summary Specification Rationale | 28 |
| 9.4 | PP Claims Rationale | 29 |
| 10 | Annex Definition of specific IT security functional requirements | 30 |

| | | |
|---|------------------------------------|---------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 5 of 30 |
|---|------------------------------------|---------------------------------|

2 ST Introduction

The chapter *ST Introduction* is divided into the following sections:

ST Identification

ST Overview

CC Conformance

2.1 ST Identification

This Security Target (st-phil5032-1-0km.doc, Version 1.0, September 20th, 1999) refers to the "Philips P8WE5032 Secure 8-bit Smart Card Controller", version P8WE5032V0B (TOE) for an Common Criteria evaluation.

2.2 ST Overview

The "Philips P8WE5032 Secure 8-bit Smart Card Controller" (TOE) mainly provides hardware platform for a smart card with

- functions to calculate the Data Encryption Algorithm (DEA) resistant to Differential Power Analysis (DPA) attacks and
- a random number generator.

2.3 CC Conformance

The Evaluation is based upon

- [1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; May 1999 and ISO 15408-1:1999
- [2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; May 1999 and ISO 15408-2:1999
- [3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; May 1999 and ISO 15408-3:1999

For the evaluation the following methodology will be used


- [4] Common Methodology for Information Technology Security Evaluation CEM-99/008 Part 2: Evaluation Methodology; Version 0.6; January 1999

The chosen level of assurance is

EAL3 (Evaluation Assurance Level 3)

This security Target claims the following conformances:

Part 2 extended, conformant Part 3, no PP conformance claim.


| | | |
|---|------------------------------------|---------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 6 of 30 |
|---|------------------------------------|---------------------------------|

3 TOE Description

The TOE is the chip Philips P8WE5032 Secure 8-bit Smart Card Controller, version P8WE5032V0B. The chip provides a hardware computing platform to run smart card applications executed by a smart card operating system. The smart card operating system and the application stored in the User-Mode ROM and in the EEPROM are not a part of the TOE. The code in the Test-Mode ROM of the TOE is used by the manufacturer of the smart card to check the chip function. This test code is disabled before the operational use of the smart card.

The applications need the security functions of the operating system based on the security features of the TOE. With respect to security the composition of this TOE, the operating system, and the smart card application is important. Within this composition the security functionality is only partly provided by the TOE and causes dependencies between the TOE security functions and the functions provided by the operating system or the smart card application on top. Nevertheless the TOE provides to a great extent independent of the operating system a symmetric block cipher algorithm and a random number generator to perform cryptographic operations in a secure way. The block cipher algorithm may be used as a cryptographic primitive for encryption of user data and for authentication of user data and entities. The random number generator may be used by the software of the TOE environment for the generation of cryptographic parameters on the smart card and especially of keys. These strong keys should be used when the cryptographic primitives of the TOE are invoked by the software of the environment.

The chip contains a FameX co-processor which accelerates modulo calculation for public key cryptosystems. This co-processor needs appropriate control by the operating system and cannot provide a security function on its own. The FameX co-processor is out of the scope of this evaluation.

| | | |
|---|--|--|
|  <p>PHILIPS</p> <p>Business Line Identification</p> | <p>Security Target BSI-DSZ-CC-0153</p> | <p>Version 1.0</p> <p>Page 7 of 30</p> |
|---|--|--|

4 Security Environment

The chapter Security Environment is divided into the following sections:

Assumptions

Threats

Organisational Security Policies

Definition of Subjects


- S.OFF-CARD Off Card Attacker: A human or a process acting on behalf of him being located outside the smart card.
- S.ON-CARD Any application software process or parts of the smart card operating system which reside on the card but is not a part of the TOE.

Data Objects

- D.PLAIN-TEXT User data used as input parameter for encryption or as output of decryption stored in an input register of the block cipher algorithm of the TOE.
- D.CIPHER-TEXT User data as output of encryption and as input of decryption by the block cipher algorithm of the TOE.
- D.KEY Cryptographic Keys used as input parameter for encryption or decryption stored in a register of the block cipher algorithm of the TOE.
- D.RANDOM Random numbers generated as an output value of the random number generator of the TOE.

4.1 Assumptions

- A.RESP-APPL All cryptographic keys (D.KEY) are owned by S.ON-CARD. Therefore, it must be assumed that security relevant User Data (especially data which will be used as D.KEY or D.PLAIN-TEXT) are treated by the S.ON-CARD as defined within its Security Policy. It is assumed that this Security Policy does not contradict the Security Objectives of the TOE.
- A.STRONG-KEY S.ON-CARD uses only appropriate secret keys (chosen from a large key space) as input for the cryptographic function of the TOE to ensure the strength of cryptographic operation. These keys may be generated or loaded by S.ON-CARD.
- A.TAMPER The environment in which the smart card (plastic card with the embedded chip) is used guarantees the physical integrity of the TOE embedded in the smart card and the usage of the TOE under the defined working conditions (which are described in the user documentation). By doing so the environment ensures that security relevant user data and cryptographic keys will not be disclosed and that the random number generator can not be manipulated by tamper attacks.


| | | |
|---|------------------------------------|---------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 8 of 30 |
|---|------------------------------------|---------------------------------|

Note that the preceding assumptions A.RESP-APPL and A.STRONG-KEY refer to S.ON-CARD as the user of the TOE. The assumptions can also be seen as personal assumptions about the developers of the Application Software or Operating System since they have to ensure that the software fulfils the assumptions. In particular the assumptions imply that developers are trusted to develop software that fulfils the assumptions.

4.2 Threats

Threats which should be averted by the TOE

| | |
|-------|--|
| T.ENC | An Off Card Attacker (S.OFF-CARD) may compromise user data (D.PLAIN-TEXT) being encrypted by the TOE or he may compromise the key needed to calculate D.PLAIN-TEXT from D.CIPHER-TEXT. To perform this attack S.OFF-CARD only gets knowledge of D.CIPHER-TEXT and is neither able to use the decryption function of the TOE nor to observe the behaviour of the TOE during the cryptographic operation. The attacker needs specialised expertise, methods and resources for this attack. Note that it is assumed here that the attacker does not possess the key. For direct attacks on the key refer to T.DPA and T.RND. This threat does not include the possibility of active physical attacks to the card, since that has to be averted by the environment (see A.TAMPER and OE.TAMPER). |
| T.DPA | An Off Card Attacker (S.OFF-CARD) may compromise cryptographic keys (D.KEY) by analysing the power consumption of the smart card chip during the cryptographic operation (Differential Power Analysis, DPA). The attacker needs specialised expertise, methods and resources for this attack without specific knowledge about the TOE itself. On the other hand the opportunities for realising it may even include the possibility to do it unnoticed, because only the possibility of passive monitoring of the power supply is needed. This threat does not include the possibility of active physical attacks to the card, since that has to be averted by the environment (see A.TAMPER and OE.TAMPER). |
| T.RND | An Off Card Attacker (S.OFF-CARD) may compromise cryptographic keys (D.KEY) generated by S.ON-CARD using the random number generator of the TOE. To perform this attack the attacker tries to guess the random number which had been used to generate the cryptographic key. Here the attacker is expected to take advantage of statistical properties of the random numbers generated by the TOE without specific knowledge about the TOE's generator. The attacker needs to have mathematical knowledge especially about statistics. This threat does not include the possibility of active physical attacks to the card, since that has to be averted by the environment (see A.TAMPER and OE.TAMPER). |

| | | |
|---|------------------------------------|---------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 9 of 30 |
|---|------------------------------------|---------------------------------|

Threats which should be averted by the environment


T.KEY-OPERATION Key-dependent functions may be implemented in S.ON-CARD. If such routines are executed an Off Card Attacker (S.OFF-CARD) may compromise cryptographic keys (D.KEY) using the Differential Power Analysis (DPA).

The attacker needs specialised expertise, methods and resources for this attack without specific knowledge about the smart card itself. On the other hand the opportunities for realising it may even include the possibility to do it unnoticed, because only the possibility of passive monitoring of the power supply is needed. This threat does not include the possibility of active physical attacks to the card, since that has to be averted by the environment (see A.TAMPER and OE.TAMPER).

Note that here the routines which may compromise keys when being executed are part of the S.ON-CARD. In contrast to this the threat T.DPA addresses the cryptographic routines being a part of the TOE.

4.3 Organisational Security Policies

Since the security objectives are derived solely from the threats, the description of organisational security policies is omitted here.

| | | |
|---|------------------------------------|----------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 10 of 30 |
|---|------------------------------------|----------------------------------|

5 Security Objectives

The chapter *Security Objectives* is divided into the following sections:

TOE Security Objectives


Security Objectives for the Environment

5.1 TOE Security Objectives

- O.BLOCK-CIPHER The TOE will implement a cryptographic strong symmetric block cipher algorithm to ensure the confidentiality of D.PLAIN-TEXT by encryption and to support secure authentication protocols.
- O.DPA The TOE will ensure the confidentiality of D.KEY during cryptographic function performed by the TOE.
- O.RND The TOE will ensure the cryptographic quality of random number generation.

5.2 Security Objectives for the Environment

- OE.TAMPER The environment will not expose the TOE to attacks which directly affect or manipulate the smart card. Thus the environment will ensure that security relevant user data and cryptographic keys will not be disclosed and that the random number generator will not be manipulated.
- OE.RESP-APPL S.ON-CARD will not disclose security relevant user data (especially data which will be used as D.KEY or D.PLAIN-TEXT) to unauthorised users or processes when communicating with a terminal.
- OE.KEY-OPERATION When the S.ON-CARD is just being executed no information about cryptographic keys can be gathered by analysing the power consumption of the smart card (DPA).
- OE.STRONG-KEY S.ON-CARD will only use appropriate secret cryptographic keys (chosen from a sufficient key space and with sufficient entropy) as an input for the TOE's cryptographic function.

| | | |
|---|------------------------------------|----------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 11 of 30 |
|---|------------------------------------|----------------------------------|

6 IT Security Requirements

The chapter *IT Security Requirements* is divided into the following sections and subsections:

- TOE Security Requirements*
- TOE Functional Requirements*
- TOE Security Assurance Requirements*
- Security Requirements for the Environment*

6.1 TOE Security Requirements

6.1.1 TOE Functional Requirements

To achieve the security objectives for the TOE defined in chapter 5 and to avert the assumed threats defined for the TOE in chapter 4.2 the TOE's security functions have to fulfil the following functional requirements.

The following TOE functional requirements are derived from the functional classes, families and components defined in the CC part 2, [2] as indicated. To highlight the parts of the requirements which have been assigned or selected these parts are printed in an italic face.

The TOE security functional requirements for the random number generator (FCS_RND.1) are not taken from the CC, part 2 but are defined specifically for the TOE.

6.1.1.1 Encryption Function

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform *encryption and decryption*¹ in accordance with a specified cryptographic algorithm *Data Encryption Algorithm (DEA)*² and cryptographic key sizes of *56 bit and 112 bit (Triple-DES)*³ that meet the following *list of standards*:⁴

- *U.S. Department of Commerce / National Bureau of Standards Data Encryption Standard, FIPS PUB 46, 1977 January 15*
- *International Organization for Standardization: Banking - Key Management, International Standard ISO 8732 (1988), Chapter 12.1.3*


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

¹ [assignment: list of crypto-graphic operations]

² [assignment: cryptographic algorithm]

³ [assignment: cryptographic key sizes]

⁴ [assignment: list of standards]

| | | |
|---|------------------------------------|----------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 12 of 30 |
|---|------------------------------------|----------------------------------|

6.1.1.2 DPA Resistant Data Encryption Algorithm Implementation

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist *the physical tempering scenario: Differential Power Analysis during DEA-operation (refer to FCS_COP.1)*⁵ to the externally accessible interfaces of the smart-card⁶ by responding automatically such that the TSP is not violated.

Dependencies: No dependencies.

Note: The hardware part of the TOE will implement appropriate measures to counter continuously the Differential Power Analysis during a DEA-operation of the chip. Due to the nature of that attack (observing power consumption), the TOE can by no means detect the attack. Therefore, permanent protection against the Differential Power Analysis is required ensuring that the TSP could not be violated at any time. Hence, automatic response here means (i) assuming that there might be an attack at any time and (ii) therefore providing countermeasures at any time.

6.1.1.3 Random Number Generation

FCS_RND.1 Quality metric for random numbers

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that have an *entropy of at least 6 bit in each byte*⁷.

Dependencies: No dependencies.

Note: The entropy of the random number is measured by the Shannon-Entropy as follows:

$$E = - \sum_{i=0}^{255} p_i \cdot \log_2 p_i$$

where p_i is the probability that the byte (b_7, b_6, \dots, b_0) is equal to i as binary number. Here term "bit" means measure of the Shannon-Entropy.


6.1.1.4 Minimum Strength of Function Level

The TOE claims to have a minimum strength of function level of SOF-basic.

⁵ [assignment: physical tampering scenarios]

⁶ [assignment: list of TSF devices/elements]

⁷ [assignment: a defined quality metric]

| | | |
|---|--|---|
|  <p>PHILIPS</p> <p>Business Line Identification</p> | <p>Security Target BSI-DSZ-CC-0153</p> | <p>Version 1.0</p> <p>Page 13 of 30</p> |
|---|--|---|

6.1.2 TOE Security Assurance Requirements

The *TOE security assurance requirements* equals to the Evaluation Assurance Level EAL3. In detail the following Security Assurance Requirements are chosen for the TOE:

| | |
|--|---------------------|
| Components for Configuration management (Class ACM) | corresponds to EAL3 |
| CM Capabilities (Component ACM_CAP.3) | |
| CM Scope (Component ACM_SCP.1) | |
| Components for Delivery and operation (Class ADO) | correspond to EAL3 |
| Delivery (Component ADO_DEL.1) | |
| Installation, generation, and start-up (Component ADO_IGS.1) | |
| Components for Development (Class ADV) | correspond to EAL3 |
| Functional Specification (Component ADV_FSP.1) | |
| High-Level Design (Component ADV_HLD.2) | |
| Representation Correspondence (Component ADV_RCR.1) | |
| Components for Guidance documents (Class AGD) | correspond to EAL3 |
| Administrator Guidance (Component AGD_ADM.1) | |
| User guidance (Component AGD_USR.1) | |
| Components for Life cycle support (Class ALC) | corresponds to EAL3 |
| Development Security (Component ALC_DVS.1) | |
| Components for Tests (Class ATE) | corresponds to EAL3 |
| Coverage (Component ATE_COV.2) | |
| Depth (Component ATE_DPT.1) | |
| Functional Tests (Component ATE_FUN.1) | |
| Independent Testing (Component ATE_IND.2) | |
| Components for Vulnerability assessment (Class AVA) | correspond to EAL3 |
| Misuse (Component AVA_MSU.1) | |
| Strength of TOE Security Functions (Component AVA_SOF.1) | |
| Vulnerability Analysis (Component AVA_VLA.1) | |


6.2 Security Requirements for the Environment

6.2.1 Security Requirements for the IT-Environment

The security objectives for the environment will be ensured by Non-IT security requirements only (see the next subsection and the rationale, section 9.2.1).

6.2.2 Security Requirements for the Non-IT Environment

The TOE provides a hardware computing platform to run smart card applications executed by a smart card operating system. The applications need the security functions of the operating system based on the security features of the TOE. The security objectives for the environment shall be achieved in accordance with these security needs by the design and the development of S.ON-


| | | |
|---|------------------------------------|----------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 14 of 30 |
|---|------------------------------------|----------------------------------|

CARD. To achieve the security objectives for the environment the following as Non-IT security requirements for the environment of the TOE are given (see the rationale, section 9.2.1).

| | |
|--------------------|---|
| RE.TAMPER-RESIST | <p>The environment of the TOE (and of the plastic card the TOE will be a part of) shall take appropriate measures to guarantee the physical integrity of the TOE embedded in the smart card and the TOE usage under the defined working conditions.</p> <p>This must be ensured by (i) the smart card holder protecting his smart card against manipulations and recognising obvious violations of the integrity of his smart card and (ii) the construction of the interface device (terminal) in which the TOE is going to be used and an attentive user who does not use the TOE with obscure terminals.</p> <p>This requirement is important since no assumptions and claims are made concerning the resistance of the TOE itself against active physical attacks.</p> |
| RE.RESP-APPL | <p>The developers shall implement S.ON-CARD in a way that it will not disclose security relevant user data (especially data which will be used as D.KEY or D.PLAIN-TEXT) to unauthorised users or processes.</p> <p>This shall be ensured by the design of S.ON-CARD which realises the I/O operations. It shall only implement appropriate operations.</p> |
| RE.KEY-CALCULATION | <p>The developers of S.ON-CARD shall not implement repeatedly performed operations $y = F(x, k)$ with different values x and a fixed key k if F does not use k exclusively as argument of the symmetric block cipher algorithm provided by the TOE.</p> <p>Implementing and repeatedly performing such kind of functions by the TOE environment could allow an attacker to misuse these functions to gather information about the key which is used in the computation of the function. The TOE shall counter the Differential Power Analysis (DPA) when offering its cryptographic functions to S.ON-CARD. But if S.ON-CARD performs its own operations using a cryptographic key without using the cryptographic functions of the TOE the confidentiality of the keys must be ensured by itself.</p> |
| RE.STRONG-KEY | <p>The developers shall implement S.ON-CARD in way that it will use only appropriate cryptographic keys as input of the TOE's cryptographic function as required in FCS_COP.1.</p> <p>This may be ensured by generating cryptographic keys with the support of the required random number generation for the TOE (see FCS_RND.1). However there are other possibilities to work with strong keys, i. e. securely loading them from outside of the smart card, by derivation from Masterkeys or by other key exchange protocols.</p> |

| | | |
|--|------------------------------------|------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 15 of 30 |
|--|------------------------------------|------------------------------|

In addition this requirement implies that an appropriate key management has to be realised in the environment.

| | | |
|---|------------------------------------|----------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 16 of 30 |
|---|------------------------------------|----------------------------------|

7 TOE Summary Specification

The chapter TOE Summary Specification is divided into the following sections:

- TOE Security Functions
- Assurance Measures

7.1 TOE Security Functions

The IT security functions directly correspond to the TOE security functional requirements defined in chapter 6.1.1. So, the definitions of the IT security functions refer to the corresponding security functional requirements.

F.DEA

The TOE provide functions according to the Data Encryption Algorithm (DEA) of the Data Encryption Standard (DES). This functionality is required by the security functional component FCS_COP.1 taken from the Common Criteria Part 2.


F.DEA is a modular basic cryptographic function which provides the DEA algorithm as defined by FIPS PUB 46 by means of an hardware co-processor and supports the 2-key Triple DES algorithm according to ISO 8732 (1988), Chapter 12.1.3. The 56 bit key for (single) DEA and the two 56 bit keys (112 bit) for the 2-key Triple DES algorithm (D.KEY) shall be given by S.ON-CARD. For encryption S.ON-CARD provides 8 byte of D.PLAIN-TEXT and F.DEA calculates 8 byte D.CIPHER-TEXT. The output of calculation is read by S.ON-CARD. For decryption S.ON-CARD also provides 8 byte of D.CIPHER-TEXT and F.DEA calculates 8 byte D.PLAIN-TEXT. The output of calculation is read by S.ON-CARD.

F.DPA

The TOE implements functions which avert that the key (D.KEY) used for encryption and decryption during the calculation of F.DEA could be disclosed by externally measuring the power consumption of the smart card chip (Differential Power Attack, DPA). The TOE uses probabilistic and other methods to masquerade the usage of D.KEY during the F.DEA calculation. This functionality is required by the security functional component FPT_PHP.3 taken from the Common Criteria Part 2.

F.RND

The TOE implements a physical hardware random number generator. This generator continuously produces random numbers with a length of one byte. Each byte will at least contain a 6 bit entropy. S.ON-CARD could read out such numbers if necessary. This functionality is required by the security functional component FCS_RND.1 specially defined for this purpose here (for further details see chapter 10).


| | | |
|---|------------------------------------|----------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 17 of 30 |
|---|------------------------------------|----------------------------------|

Strength of security function claim

The following table states the claimed strength for the security functions:

| Security Function | type of mechanism | claimed strength |
|-------------------|-------------------|------------------|
| F.DEA | (not applicable) | (not applicable) |
| F.DPA | probabilistic | SOF-basic |
| F.RND | probabilistic | SOF-basic |

Note: Due to CEM [4], paragraph 382, the strength of cryptographic algorithms is outside the scope of the CC. Strength of function only applies to non-cryptographic, probabilistic or permutational mechanisms.

| | | |
|---|------------------------------------|----------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 18 of 30 |
|---|------------------------------------|----------------------------------|

7.2 Assurance Measures


Appropriate assurance measures will be employed to satisfy the security assurance requirements listed in chapter 6.1.2. The developer will provide documents containing the measures and further information needed to check conformance of the measures to the assurance requirements. The following table gives a mapping between the assurance requirements and the documents containing the information needed for the respective requirement either directly or referring to further documents containing this information.

| Document containing or referring to the relevant information / file name of this document | Input evidence contained or referred to in the document according to the names used in CEM [4] | required for assurance component(s) |
|---|--|--|
| [5] Informal Functional Specification, debis, Philips | functional specification | ADV_FSP.1, ADV_HLD.2, ADV_RCR.1, AGD_ADM.1, AGD_USR.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2, AVA_MSU.1, AVA_SOF.1, AVA_VLA.1 |
| | correspondence analysis between the TOE summary specification and the functional specification | ADV_RCR.1 |
| [6] High Level design, debis, Philips | high-level design | ADV_RCR.1, ADV_HLD.2, AGD_ADM.1, AGD_USR.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, AVA_MSU.1, AVA_SOF.1, AVA_VLA.1 |
| | correspondence analysis between functional specification and high-level design | ADV_RCR.1 |
| [7] Configuration Management and Life Cycle documentation, debis, Philips | configuration management documentation | ACM_CAP.3, ACM_SCP.1 |
| | development security documentation | ALC_DVS.1 |
| | delivery documentation | ADO_DEL.1 |
| [8] Guidance, Delivery and Operation, debis, Philips | administrator guidance | ADO_IGS.1, AGD_ADM.1, AGD_USR.1, ADV_FSP.1, ATE_IND.2, AVA_MSU.1, AVA_VLA.1 |
| | secure installation, generation, and start-up procedures | ADO_IGS.1, AGD_ADM.1, AGD_USR.1, ATE_IND.2, AVA_MSU.1, AVA_VLA.1 |
| | user guidance | AGD_ADM.1, AGD_USR.1, ADV_FSP.1, ATE_IND.2, AVA_MSU.1, AVA_VLA.1 |
| [9] Vulnerability Assessment, debis, Philips | vulnerability analysis | AGD_ADM.1, AGD_USR.1, AVA_VLA.1 |
| | strength of function claims analysis | AVA_SOF.1 |
| [10] Test Documentation, debis, Philips | test documentation | ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2 |
| | test coverage analysis | ATE_COV.2, ATE_IND.2 |
| | depth of testing analysis | ATE_DPT.1, ATE_IND.2 |

| | | |
|---|------------------------------------|----------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 19 of 30 |
|---|------------------------------------|----------------------------------|

8 PP Claims

This Security Target TOE does not claim conformance to any Protection Profile.

| | | |
|---|------------------------------------|----------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 20 of 30 |
|---|------------------------------------|----------------------------------|

9 Rationale

The chapter *Rationale* is divided into the following sections:

- Security Objectives Rationale*
- Security Requirements Rationale*
- TOE Summary Specification Rationale*
- PP Claims Rationale*

9.1 Security Objectives Rationale


The Rationale of the Security Objectives shall demonstrate that the identified Security Objectives are suitable and cover all aspects defined in the Security Environment of the TOE (see chapter 4). The following table cross-references the threats and assumptions of the Security Environment against the Security Objectives which are intended to address them. Note that because the Security Environment does not state any Organisational Security Policy there is no need to address this aspect in the Security Objectives Rationale too.

| | Assumption/Threat | is addressed by |
|----|-------------------|--|
| #1 | A.RESP-APPL | OE.RESP-APPL, OE.TAMPER |
| #2 | A.STRONG-KEY | OE.STRONG-KEY, OE.TAMPER |
| #3 | A.TAMPER | OE.TAMPER |
| #4 | T.ENC | O.BLOCK-CIPHER, OE.STRONG-KEY, OE.RESP-APPL, OE.TAMPER |
| #5 | T.DPA | O.DPA, OE.KEY-OPERATION, OE.RESP-APPL, OE.TAMPER |
| #6 | T.RND | O.RND, OE.TAMPER |
| #7 | T.KEY-OPERATION | OE.KEY-OPERATION, OE.TAMPER |

The cross-reference table given above shows that each security objective covers at least one threat or assumption specified for the Security Environment of the TOE. This demonstrates that each Security Objective is necessary and none of the Objectives could be omitted.

The table does also show that each threat or assumption is covered by at least one Security Objective.

Remark: The objective OE.TAMPER is listed for all assumptions and threats for the following reason. An attacker who would be able to manipulate the smart card hardware might be able not only to manipulate the cryptographic operation and the random number generator but also memory areas containing the application software (S.ON-CARD). So all other security objectives require support from OE.TAMPER.


| | | |
|---|--|---|
|  <p>PHILIPS</p> <p>Business Line Identification</p> | <p>Security Target BSI-DSZ-CC-0153</p> | <p>Version 1.0</p> <p>Page 21 of 30</p> |
|---|--|---|

The following informal descriptions will demonstrate for each threat that the Security Objectives which are intended to address this threat are sufficient to cover the threat. Moreover it can be seen from the descriptions that the security objectives are mutually supportive where necessary.

- #1 The assumption A.RESP-APPL addresses that security relevant user data (especially cryptographic keys D.KEY and D.PLAIN-TEXT) do belong to S.ON-CARD. According to the assumption S.ON-CARD is responsible on its own to treat these data correctly. At least it must be ensured that S.ON-CARD does not disclose any cryptographic keys or security relevant user data. To reach this the security objective OE.RESP-APPL requires the developer of S.ON-CARD to develop it in order to treat cryptographic keys and security relevant user data in a confidential way.
Hence if the Security Objective OE.RESP-APPL (and as remarked above OE.TAMPER) is met it will be assured that the assumption A.RESP-APPL is satisfied.
- #2 The assumption A.STRONG-KEY deals with the situation where S.ON-CARD uses cryptographic secret keys as input of the cryptographic function of the TOE. To ensure the strength of the cryptographic function of the TOE it is assumed that S.ON-CARD has to provide only strong cryptographic keys as input to the TOE. This assumption will be met if the security objective OE.STRONG-KEY (and as remarked above OE.TAMPER) is fulfilled.
- #3 The assumption A.TAMPER addresses the physical integrity of the TOE embedded in the smart card and the usage under the defined working conditions. An Off Card Attacker (S.OFF-CARD) may try directly to manipulate the smart card. It is imaginable that an attacker may try to remove the TOE from the plastic card and micro-module or to manipulate it. By doing so an attacker may get unauthorised knowledge of user data and cryptographic keys. A violation of the working conditions (as supply voltage range, temperature) of the TOE may take affect on the random number generator and impair the quality of the random numbers.
The assumption A.TAMPER will be sufficiently ensured if the security objective OE.TAMPER is met. Reaching the objective the environment will guarantee the physical integrity of the TOE and the defined working conditions. The TOE will not be exposed to tamper attacks.
- #4 The threat T.ENC addresses that an attacker tries to compromise user data D.PLAIN-TEXT encrypted as D.CIPHER-TEXT by the TOE with a secret key D.KEY. Or the attacker tries to determine the D.KEY needed to calculate the plain-text from the cipher-text. To perform the attack the attacker only gets knowledge of D.CIPHER-TEXT. This threat will be averted if (i) the block cipher algorithm implemented by the TOE and used for encryption is cryptographic secure (O.BLOCK-CIPHER) and (ii) the used key is appropriate and kept secret (OE.STRONG-KEY). If OE.RESP-APPL is met S.ON-CARD will not disclose D.PLAIN-TEXT or D.KEY to unauthorised users or processes when communicating with a terminal will ensure. As remarked above, OE.TAMPER has to be fulfilled in order to guarantee the correct operation of the block cipher.

| | | |
|---|--|---|
|  <p>PHILIPS</p> <p>Business Line Identification</p> | <p>Security Target BSI-DSZ-CC-0153</p> | <p>Version 1.0</p> <p>Page 22 of 30</p> |
|---|--|---|

- #5 The threat T.DPA addresses the attack that S.OFF-CARD tries to compromise cryptographic keys (D.KEY) by performing a Differential Power Analysis (DPA). For a successful Differential Power Analysis the attacker must measure the power consumption repeatedly during the block cipher computation of the TOE and this power consumption must contain sufficient information about the used key. If the Security Objective O.DPA is met it is prevented in particular that the power consumption will contain sufficient information about the cryptographic key used during the block cipher computation of the TOE.
- The threat T.DPA must also be addressed by some security objective for the environment. Otherwise it may happen that the TOE provides security but its environment rebuilds exactly the same functionality not providing the protection offered by the TOE. So, the security objective OE.KEY-OPERATION and OE.RESP-APPL have been added. If OE.KEY-OPERATION is fulfilled the cryptographic keys will not be disclosed by DPA during the computation of S.ON-CARD and if OE.RESP-APPL is fulfilled S.ON-CARD will not disclose cryptographic keys by an output operation. As remarked above, OE.TAMPER supports the other objectives by preventing physical manipulations.
- #6 The threat T.RND addresses the situation where an attacker tries to compromise a cryptographic key by guessing the random number which was used during the generation of the key. The random number which was used by S.ON-CARD for key generation was formerly produced by the random number generator of the TOE. The attacker expects to take advantage of statistical properties of the TOE's random number generator.
- The threat T.RND will be averted if the security objectives O.RND and OE.TAMPER are fulfilled. If O.RND is met S.ON-CARD will get random numbers with a high cryptographic quality produced by the TOE. As remarked above, OE.TAMPER supports the other objectives by preventing physical manipulations.
- #7 T.KEY-OPERATION describes the threat for the environment which could arise if the S.ON-CARD does implement functions which do use a cryptographic key during calculation. Then an Off Card Attacker (S.OFF-CARD) may be able to disclose the cryptographic keys used during computation by performing a DPA attack. This threat must be understood in addition to the threat T.DPA for the TOE.
- To avert the threat T.KEY-OPERATION it is sufficient to reach the security objective OE.KEY-OPERATION. If OE.KEY-OPERATION is met an external attacker isn't able to successfully perform any DPA attacks against the Application Software. As remarked above, OE.TAMPER supports the other objectives by preventing physical manipulations (e. g. of the application software).

| | | |
|--|------------------------------------|----------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 23 of 30 |
|--|------------------------------------|----------------------------------|

9.2 Security Requirements Rationale

9.2.1 Security Functional Requirements

The purpose of the Security Requirements Rationale is to demonstrate that the security requirements (see chapter 6.1) are suitable to meet the Security Objectives identified in chapter 5. Taking the section 9.1 into consideration it is thereby shown that the Security Requirements are also suitable to cover the security needs specified in chapter 5.


The following table shows by which security functional requirements each security objective is addressed. Additionally the supporting Security Objectives for the environment and corresponding Requirements are shown. Some of them appear multiple times since they support multiple Security Objectives of the TOE.

| Security Objectives | | is addressed by | | |
|---------------------|----------------|---|-----------|--|
| | TOE | TOE Environment Support | TOE SFR | Supporting Requirement for Environment |
| #8 | O.BLOCK-CIPHER | OE.STRONG-KEY OE.RESP-APPL OE.TAMPER | FCS_COP.1 | RE.STRONG-KEY RE.RESP-APPL RE.TAMPER-RESIST |
| #9 | O.DPA | OE.KEY-OPERATION OE.RESP-APPL OE.TAMPER | FPT_PHP.3 | RE.KEY-CALCULATION RE.RESP-APPL RE.TAMPER-RESIST |
| #10 | O.RND | OE.TAMPER | FCS_RND.1 | RE.TAMPER-RESIST |


The cross-reference table given above shows that each functional requirement addresses at least one security objective of the TOE. This demonstrates that each functional requirement is necessary and none of the functional requirements could be omitted.

The table does also show that each security objective for the TOE is covered by at least one functional requirement.

The following informal description will demonstrate for each Security Objective that the TOE security functional requirements which are intended to address the objective are sufficient to cover it. In addition, it is shown how the TOE security requirements are supported by and coordinated with those for the IT environment.

| | | |
|---|--|---|
|  <p>PHILIPS</p> <p>Business Line Identification</p> | <p>Security Target BSI-DSZ-CC-0153</p> | <p>Version 1.0</p> <p>Page 24 of 30</p> |
|---|--|---|

- #8 O.BLOCK-CIPHER: The aim of the security objective O.BLOCK-CIPHER is to provide a cryptographic strong symmetric block cipher algorithm. This algorithm shall ensure the confidentiality of D.PLAIN-TEXT by encryption and support secure authentication protocols.
- To reach this objective the TOE has to realise the functional requirement FCS_COP.1 (Cryptographic support – Cryptographic Operation) which covers the requirement that the TOE has to implement the cryptographic algorithm Data Encryption Algorithm (DEA) with a cryptographic key sizes of 56 Bit and the 2-key Triple-DES with a cryptographic key sizes of 112 Bit. If this algorithm is correctly implemented and used by the environment (S.ON-CARD, see paragraphs below) it provides a sufficient protection of the confidentiality of D.PLAIN-TEXT, a sufficient support of authentication protocols and the functional requirement FCS_COP.1 is met.
- The TOE can ensure the cryptographic strengths of encryption and cryptographic authentication protocols only if the cryptographic keys are appropriately chosen and kept confidential. The security objective for the environment OE.STRONG-KEY is needed to ensure that the environment (S.ON-CARD) uses the cryptographic function of the TOE only with appropriate secret cryptographic keys. This goal will be achieved if the developers implement S.ON-CARD in way that it will use only appropriate cryptographic keys as input of the TOE's cryptographic function as required by RE.STRONG-KEYS.
- The security objective O.BLOCK-CIPHER addresses the protection of user data (D.PLAIN-TEXT). So, the security objective OE.RESP-APPL for the environment has to be taken into account: S.ON-CARD using I/O operations to communicate with an IFD (terminal) outside the smart card shall not disclose security relevant user data to unauthorised users or processes. If the requirement RE.RESP-APPL is met then the developers shall implement S.ON-CARD in a way that it will not disclose security relevant user data (especially data which will be used as D.KEY or D.PLAIN-TEXT) to unauthorised users or processes.
- The security objective OE.TAMPER takes aim at and the corresponding requirement RE.TAMPER-RESIST shall ensure that the TOE is not exposed to attacks which directly affect or manipulate the smart card (and especially the random number generator). The smart card holder shall protect his smart card against manipulations and recognise obvious violations of the integrity of his smart card. An attentive user shall prevent usage of obscure terminals. The interface device (IFD, terminal) in which the TOE is going to be used must take appropriate measures to guarantee the physical integrity of the TOE embedded in the smart card and the TOE usage under the defined working conditions by the construction.
- The requirements RE.STRONG-KEY, RE.RESP-APPL and RE.TAMPER-RESIST for the environment together with the TOE's functional requirements ensure the confidentiality of security relevant user data (D.PLAIN-TEXT).
- #9 O.DPA: The aim of Security Objective O.DPA is to avert that the power consumption which can be externally measured during a calculation of the block cipher algorithm of the TOE contains sufficient information to retrieve the key value by performing a Differential Power Analysis.

| | | |
|---|--|---|
|  <p>PHILIPS</p> <p>Business Line Identification</p> | <p>Security Target BSI-DSZ-CC-0153</p> | <p>Version 1.0</p> <p>Page 25 of 30</p> |
|---|--|---|

To reach this objective the TOE has to fulfil the functional requirement FPT_PHP.3. After having required that the TOE has to implement a block cipher algorithm the functional requirement FPT_PHP.3 (Protection of TSF - TSF physical protection) demands the protection of this DEA function against the Differential Power Attack. Hence, if the TOE does implement the functional requirement FPT_PHP.3 the Security Objective O.DPA is met by the TOE.

The security objective for the environment OE.KEY-OPERATION is needed to avoid that the environment undergoes the security provided by the TOE (refer to chapter 9.1). The environment (here S.ON-CARD) shall not implement any functionality which possibly discloses the cryptographic key because it may not provide the DPA protection as offered by the TOE. This is addressed by the requirement RE.KEY-CALCULATION requiring the developers of S.ON-CARD not to dodge the DPA protection by implementation of repeatedly performed operations $y = F(x, k)$ with different values x and a fixed key k (if F does not use k exclusively as argument of the symmetric block cipher algorithm provided by the TOE and therefore protected against DPA).

The security objective O.DPA addresses the protection of keys. This is additionally supported by the security objective OE.RESP-APPL for the environment. The I/O protocols used to communicate with an IFD (terminal) outside the smart card shall not disclose cryptographic keys to unauthorised users or processes. This will be ensured if the requirement RE.RESP-APPL is met.


The security objective OE.TAMPER takes aim at and the corresponding requirement RE.TAMPER-RESIST shall ensure that the TOE is not exposed to attacks which directly affect or manipulate the smart card (and especially the random number generator). The smart card holder shall protect his smart card against manipulations and recognise obvious violations of the integrity of his smart card. An attentive user shall prevent usage of obscure terminals. The interface device (IFD, terminal) in which the TOE is going to be used must take appropriate measures to guarantee the physical integrity of the TOE embedded in the smart card and the TOE usage under the defined working conditions by the construction.

The requirements RE.KEY-CALCULATION, RE.RESP-APPL and RE.TAMPER-RESIST for the environment together with the TOE's functional requirements to avert the DPA guarantee that cryptographic keys are not disclosed.

#10

O.RND: The aim of Security Objective O.RND is to ensure the cryptographic quality of random number generation. This random numbers have to achieve a certain level of entropy (6 bit per byte). To reach this objective the TOE has to realise the functional requirement FCS_RND.1. This requirement was not taken from CC, part 2 since no requirements on the quality of random numbers exist in the CC, part 2 at present.

The security objective OE.TAMPER takes aim at and the corresponding requirement RE.TAMPER-RESIST shall ensure that the TOE is not exposed to attacks which directly affect or manipulate the smart card (and especially the random number generator). The smart card holder shall protect his smart card against manipulations and recognise obvious violations of the integrity of his smart card. An

| | | |
|---|--|---|
|  <p>PHILIPS</p> <p>Business Line Identification</p> | <p>Security Target BSI-DSZ-CC-0153</p> | <p>Version 1.0</p> <p>Page 26 of 30</p> |
|---|--|---|

attentive user shall prevent usage of obscure terminals. The interface device (IFD, terminal) in which the TOE is going to be used must take appropriate measures to guarantee the physical integrity of the TOE embedded in the smart card and the TOE usage under the defined working conditions by the construction. The requirement RE.TAMPER-RESIST for the environment together with the TOE's functional requirements (FCS_RND.1) ensures the generation of random numbers with a high cryptographic quality by the TOE.

The operations applied on the functional requirements are indicated in chapter 6.1.1.

The security functional requirements for the environment have been formulated as Non-IT security requirements for the following reasons:

RE.TAMPER-RESIST will probably not be fulfilled by the IT environment alone. It includes requirements for the card holder.

RE.KEY-CALCULATION, RE.RESP-APPL and RE.STRONG-KEY are requirements which may be fulfilled by the IT environment (e. g. the smart card software S.ON-CARD) but even this is not decided definitely by this ST. For example one could think of an environment where parts of the key management functionality required to guarantee that the keys are protected and of sufficient cryptographic quality (which is required by RE.RESP-APPL together with RE.STRONG-key) is realised by organisational measures outside of the smart card. But even for the case where the requirements will eventually be fulfilled by the smart card software it would restrict the developers freedom to decide how to fulfil the requirements if they were formulated on the level of IT security functional requirements.

Dependencies of security functional requirements


The following discussion demonstrates how the dependencies defined by the CC, part 2 (see [2]) for the requirement FCS_COP.1 are satisfied (there are no dependencies for FPT_PHP.3 and so the dependencies of FCS_COP.1 are the only ones from CC, part 2).

The dependencies defined in [2] are

- [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.

The dependency requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function. All requirements concerning key management shall be fulfilled by the environment according to the requirements RE.RESP-APPL and RE.STRONG-KEY (see clause 6.2).

It was decided not to include the functional requirements [FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4 and FMT_MSA.2 *explicitly* as security functional requirements for the environment because this would mean a restriction for the realisation of the smart card software (S.ON-CARD) that is not justifiable. The possibility was seen that special smart card

| | | |
|---|--|---|
|  <p>PHILIPS</p> <p>Business Line Identification</p> | <p>Security Target BSI-DSZ-CC-0153</p> | <p>Version 1.0</p> <p>Page 27 of 30</p> |
|---|--|---|

applications may be designed that are able to resolve the dependencies without use of all the explicit functional requirements (for example by moving some of the functional responsibilities to organisational measures outside of the smart card). So the more abstract requirements RE.RESP-APPL and RE.STRONG-KEY were chosen to give the developers of the smart card software the freedom to choose how to fulfil them.

The same argument holds for further indirect dependencies of FCS_COP.1.1 according to [2] (FDP_ACC.1, FDP_IFC.1, FDP_ACF.1, FDP_IFF.1, FMT_MSA.3, FCS_CKM.2, FMT_MSA.1, FMT_SMR.1, FIA_UID.1 and ADV_SPM.1).

Dependencies between the functional security requirements for the environment exist if they are fulfilled (in part) by the smart card hardware or software which is very likely. In this case they all depend on RE.TAMPER-RESIST because in a scenario where an attacker is able to manipulate the smart card hardware (and consequently also the software) it is not possible to fulfil any requirement.

The requirement RE.STRONG-KEY can be supported by the TOE requirement FCS_RND.1 especially if FCS_CKM.1 Cryptographic key generation (see above) is realised in the smart card software. But since other application dependent ways to produce the necessary strong cryptographic keys are feasible (e. g. derivation from other keys) this at most results in an optional dependency.

There are no potential conflicts between the SFRs of the TOE or the environment. Together with the dependency analysis above and earlier demonstration of mutual support this shows that the SFRs are as a whole mutually supportive and internally consistent.

9.2.2 Assurance Requirements and Strength of Function Claim


The *TOE security assurance requirements* are equal to the Evaluation Assurance Level EAL3. The justification that this level is sufficient with respect to the threats is as follows.

The threats T.ENC, T.DPA and T.RND require specialised knowledge of attack methods but no special knowledge of the TOE. The development documentation provided for EAL3 is sufficient to assess the attack potential needed for these attacks.

The assurance in the correct implementation of F.DEA, F.DPA and F.RND can be provided sufficiently on level EAL3, because the assumptions on the environment imply, that an attacker can try to exploit the external interfaces of the smart card but has no possibility to physically tamper with it.

The TOE considered here is the hardware platform only for the software (S.ON-CARD) which resides on the smart card. The evaluation of the TOE is a first step giving software developers confidence in the assurance of the TOE's functionality (the next step is to get assurance in the concrete application context which is not included into this ST). For this reason too a rather low assurance level is considered to be appropriate.

EAL3 has been chosen since it provides a moderate level of independently assured security and a thorough investigation of the TOE and its development without substantial re-engineering.

| | | |
|---|------------------------------------|----------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 28 of 30 |
|---|------------------------------------|----------------------------------|

Since F.RND is a cryptographic primitive provided by the hardware to the smart card software in a very similar way to F.DEA, it is feasible that the assurance requirements from EAL3 are applicable and appropriate for the evaluation of this function although it implements a requirement (FCS_RND.1) which is not taken from the CC, part 2.

This argument is the last one needed to demonstrate that the security requirements as a whole mutually support each other and are internally consistent. (For the SFRs alone this has been stated at the end of section 9.2.1, for the SARs alone it is known because they are taken from EAL3 and for the combination of SFRs and SARs it is again known for SFRs taken from CC, part 2 together with an EAL, provided that all dependencies are satisfied. So the combination of Non-Part 2 SFRs and SARs was the only open issue here.)

The SOF level basic was chosen for the same reasons given for the selection of level EAL3. The most important one is that an attacker can try to exploit the external interfaces of the smart card but has no possibility to physically tamper with it.


9.3 TOE Summary Specification Rationale

The purpose of the TOE Summary Specification Rationale is to demonstrate that the TOE security functions (see chapter 7.1) work together so as to meet the security requirements (see chapter 6). The following table cross-references the security requirements against the TOE security functions which are intended to address them.

| Functional Requirement | Security Function | |
|---|-------------------|--|
| FCS_COP.1 Cryptographic operation | F.DEA | TSF F.DEA is a modular basic cryptographic function which implements 2-key Triple DES algorithm as an hardware co-processor. |
| FPT_PHP.3 Resistance to physical attack | F.DPA | TSF F.DPA averts Differential Power Attack against the key used for encryption/decryption by F.DEA. |
| FCS_RND.1 Quality metric for random numbers | F.RND | TSF F.RND generates random bytes by means of a physical hardware random number generator. |

The cross-reference table given above shows that each functional requirement is addressed by at least one security function of the TOE.

For a demonstration that the TSFs are suitable to meet the SFRs refer to clause 7.1, where the security functions are explained using the SFRs.


| | | |
|--|------------------------------------|------------------------------|
|  PHILIPS Business Line Identification | Security Target BSI-DSZ-CC-0153 | Version 1.0 Page 29 of 30 |
|--|------------------------------------|------------------------------|

The TSFs F.DEA and F.DPA on the one hand and TSF F.RND on the other hand are independent of each other. The TSF F.DPA ensures the confidentiality of the key used by the TSF F.DEA during its execution. The F.RND can be used by S.ON-CARD to generate appropriate keys for the TSF F.DEA. Together with the preceding clauses this implies that the TSFs work together, are complete, and consistent.

The TOE shall be evaluated according to the Evaluation Assurance Level EAL3. The assurance components are exclusively taken from part 3 of the Common Criteria. Therefore, there is no need to define explicit assurance measures to be taken and to demonstrate that these assurance measures meet the TOE security assurance requirements. The developer assures that appropriate measures will be taken to satisfy the assurance requirements of EAL3.

9.4 PP Claims Rationale

This Security Target TOE does not claim conformance to any Protection Profile.

| | | |
|---|--|---|
|  <p>PHILIPS</p> <p>Business Line Identification</p> | <p>Security Target BSI-DSZ-CC-0153</p> | <p>Version 1.0</p> <p>Page 30 of 30</p> |
|---|--|---|

10 Annex Definition of specific IT security functional requirements

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

FCS_RND Generation of random numbers

Family behaviour

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

Component levelling



FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that have an [assignment: a defined quality metric].

Dependencies: No dependencies.