BSI-DSZ-CC-0153-1999

for

Philips Smart Card Controller
P8WE5032V0B

from

Philips Semiconductors Hamburg
Unternehmensbereich der Philips GmbH
Business Line Identification

Certification Report

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0153-1999

Philips Smart Card Controller P8WE5032V0B

from

Philips Semiconductors Hamburg Unternehmensbereich der Philips GmbH Business Line Identification

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation (CEM) Version 0.6* and *CEM Part 2 Version 1.0 Annex B* for conformance to the *Common Criteria for IT Security Evaluation, Version 2.0 (CC)*.

Evaluation Results:

Functionality: **Cryptographic support**
Protection of the TOE Security Functions

Assurance Package: **EAL3**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the Bundesamt für Sicherheit in der Informationstechnik and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The remarks printed on the reverse side are part of this certificate.

Bonn, 15 November 1999

The President of the Bundesamt für
Sicherheit in der Informationstechnik

Dr. Henze L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 183 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 9582-111

In accordance with a decree issued by the Bundesministerium des Innern (German Ministry of the Interior), the Common Criteria and the application for this certificate, the strength of the cryptoalgorithms suitable for encryption and decryption was not evaluated.

This certificate is not an endorsement of the IT product by the Bundesamt für Sicherheit in der Informationstechnik or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by Bundesamt für Sicherheit in der Informationstechnik or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Bundesamt für Sicherheit in der Informationstechnik (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Bundesamt für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011
- BSI Certification – Description of the Procedure [BSI 7125]
- Common Criteria for Information Technology Security Evaluation [CC], Version 2.0[5]
- Common Methodology for IT Security Evaluation [CEM], Part 1 Version 0.6, Part 2 Version 0.6, Part 2 Version 1.0 Annex B

---

[2] Act setting up the Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Bundesamtes für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 29th 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministeriums des Innern of 16th February 1999 in the Gemeinsames Ministerialblatt p. 1945

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC - Certificates

An agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

2.2 CC - Certificates

An arrangement on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 became effective on 5 October 1998 between the national certification bodies of France, Germany, United Kingdom, Canada and the United States. The joint Certification Body of Australia and New Zealand became member of the Arrangement on 18 October 1999.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Philips Smart Card Controller P8WE5032V0B has undergone the certification procedure at BSI.

The evaluation of the product Philips Smart Card Controller P8WE5032V0B was conducted by debis Systemhaus Information Security Services GmbH and concluded on 3 November 1999. The debis Systemhaus Information Security Services GmbH is an evaluation facility recognised by BSI (ITSEF)[6].

The sponsor, vendor and distributor is Philips Semiconductors Hamburg, Unternehmensbereich der Philips GmbH, Business Line Identification.

The certification was concluded with

- the comparability check and
- the preparation of this Certification Report.

This work was completed by the BSI on 15 November 1999.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-12.

The product Philips Smart Card Controller P8WE5032V0B has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained via the BSI-Infoline 0228/9582-111.

Further copies of this Certification Report may be ordered from the vendor[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Philips Semiconductors Hamburg, Unternehmensbereich der Philips GmbH, Business Line Identification, P.O. Box 54 02 40, D-22502 Hamburg

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the corresponding evaluation results of the accredited and licensed evaluation facility,
- supplementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

The Target of Evaluation (TOE) is the *"Philips Smart Card Controller P8WE5032V0B"*. It provides a hardware platform for a smart card 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 part of the TOE. The TOE provides functionality to perform the Data Encryption Algorithm (DEA) resistant to Differential Power Analysis (DPA) attacks and to generate random numbers with a defined minimum quality.

The TOE was evaluated against the claims of the Security Target [ST] by debis Systemhaus Information Security Services GmbH. The evaluation was completed on 3 November 1999. The debis Systemhaus Information Security Services GmbH is an evaluation facility approved by BSI (ITSEF)[8].

The sponsor, vendor and distributor is Philips Semiconductors Hamburg, Unternehmensbereich der Philips GmbH, Business Line Identification.

The TOE security assurance requirements are based entirely on the assurance components and classes defined in Part 3 of the Common Criteria (see Annex C or [CC] Part 3 for details). The TOE meets the assurance requirements of assurance level EAL 3 (Evaluation Assurance Level 3).

The TOE provides functions (F.DEA) according to the Data Encryption Algorithm (DEA) of the Data Encryption Standard (DES). F.DEA is a modular basic cryptographic function which provides the DEA algorithm as defined by FIPS PUB 46 [FIPS46] by means of a hardware co-processor and supports the 2-key Triple DES algorithm according to ISO 8732 (1988), Chapter 12.1.3 [ISO8732]. The 56 bit key for (single) DEA and the two 56 bit keys (112 bit) for the 2-key Triple DES algorithm are to be provided by the environment of the TOE.

The TOE implements functions (F.DPA) which avert that the 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).

Additionally, the TOE implements a physical hardware random number generator (F.RND). This generator continuously produces random numbers with a length of one byte. Each byte will at least contain a 6 bit entropy. The random numbers could be used by the smart card operating system or by smart card applications if necessary.

The threats which were assumed for the evaluation and averted by the TOE are specified in the Security Target [ST] and can be summarized as follows. It is assumed that the attacker is a human or a process acting on behalf of him being located outside the smart card. The attacker may compromise user data being encrypted by the TOE or he may compromise the key needed to calculate the plain text from cipher text. It is assumed that the attacker has knowledge of the cipher text only and is not able to use the decryption function of the TOE nor

[8] Information Technology Security Evaluation Facility

being able to observe the behaviour of the TOE during the cryptographic operation. Furthermore, an attacker may compromise cryptographic keys by analysing the power consumption of the smart card chip during the cryptographic operation of the TOE (Differential Power Analysis, DPA) or the attacker may compromise cryptographic keys generated by using the random number generator of the TOE.

In addition, a threat is assumed that can affect the security of the TOE and must be averted by the TOE security environment. This threat covers key-dependent functions which may be implemented in the smart card operating system or applications executed on the smart card chip but not in the TOE itself. An attacker may compromise cryptographic keys during these key-dependent functions using the Differential Power Analysis (DPA).

Since the security objectives are derived solely from the threats, no organisational security policy is described.

The TOE has two different operating modes, *user mode* and *test mode*. The application software being executed on the TOE shall not use the *test mode*. The TOE is delivered as a hardware unit at the end of the chip manufacturing process. At this point in time the operating system software is already stored in the non-volatile memories of the chip and the *test mode* is disabled. Thus, there are no special procedures for generation or installation that are important for a secure use of the TOE. The further production and delivery processes, like the integration into a smart card, personalization and the delivery of the smart card to an end user, have to be organized in a way that excludes all possibilities of physical manipulation of the TOE. There are no special security measures for the startup of the TOE besides the requirement that the controller has to be used under the well-defined operating conditions as described in the user documentation.

The smart card operating system and the smart card application software have to use security relevant user data of the TOE (especially keys and plain text data) in a secure way. It is assumed that the Security Policy of the environment does not contradict the Security Objectives of the TOE. Only appropriate secret keys as input for the cryptographic function of the TOE have to be used to ensure the strength of cryptographic operation.

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 operating conditions (which are described in the user documentation).

The developers of the application software or the operating system have to ensure that the software fulfils the assumptions for a secure use of the TOE. In particular the assumptions imply that developers are trusted to develop software that fulfils the assumptions.

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Bundesamt für Sicherheit in der Informationstechnik (BSI) or any other

organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification

The following TOE deliverables are provided for a customer who purchases the TOE:

No	Type	Identifier	Form of Delivery
1	HW	The 8-bit smart card controller Philips P8WE5032V0B	Hardware Chip
2	DOC	The Data Sheet [DS]	Hardcopy
3	DOC	The Guidance, Delivery and Operation Manual [GDO]	Hardcopy

Deliverables of the TOE

The TOE is identified by P8WE5032V0B. A so called on-chip code is printed onto the chip during production and can be checked by the customer, too. Additionally, a FabKey according to the defined FabKey-procedures supports the secure delivery and the identification of the TOE.

To ensure that the customer receives this evaluated version, the delivery procedures described in [GDO] have to be followed.

3 Security Policy

The security policy of the TOE is to provide basic security functions to be used by the smart card operating system and the smart card application thus providing an overall smart card system security. Therefore the TOE will implement a cryptographic symmetric block cipher algorithm to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols. Additionally, the TOE will ensure the confidentiality of cryptographic keys during cryptographic functions performed by the TOE and it will provide a random number generation of appropriate quality.

4 Assumptions and Clarification of Scope

The smart card operating system and the application stored in the User-Mode ROM and in the EEPROM are not 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 smart card applications need the security functions of the smart card 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. These dependencies are expressed by environmental and secure usage assumptions as outlined in the user documentation.

The chip contains a FameX co-processor which accelerates modulo calculation for public key cryptosystems. The FameX co-processor is out of the scope of this evaluation.

The threats assumed do not include active physical attacks to the smart card chip. These have to be averted by the environmental assumption (see [ST] chapter 4). The security functionality of the TOE presupposes that the integrity of the Philips 5032 smart card controller is not being violated in any form.

If the smart card operating system developer and application software programmer are not the same, it is important that the operating system developer has to document all information regarding security relevant restrictions to the application software programmer, especially for all those restrictions which have to be fulfilled by the application software.

5 Architectural Information

The Philips 5032 smart card controller is an integrated circuit (IC) providing a hardware platform to a smart card operating system and smart card application software. For the implementation of the TOE Security Functions the components 8-bit 80C51 CPU, Special Function Registers (SFR), Triple-DES Co-Processor and a Random Number Generator (RNG) are used. The complete hardware description of the Philips 5032 smart card controller is to be found in the Data Sheet [DS]. The complete instruction set of the Philips 5032 smart card controller is also described in the Data Sheet.

During evaluation the TOE was divided into major subsystems to describe the TOE Security Functions. Correspondingly, the security enforcing subsystems IC.DEA, IC.RNG and IC.POW mainly implement the three security functions of the TOE as described within the Security Target [ST].

The security function F.DEA is the encryption and decryption of 8 byte text blocks with 56 bit keys, conformant to the Digital Encryption Standard DES. Furthermore, F.DEA supports the 2-key triple-DES encryption/decryption, which makes it possible to encrypt 8 byte text blocks with 112 bit long keys (two 56 bit keys). It is implemented mainly by the subsystem IC.DEA.

The security function F.DPA is the property of the TOE to resist Differential Power Analysis attacks during the execution of F.DEA. The subsystem IC.DEA will take countermeasures to avert, that the power consumption of the TOE contains sufficient information about the key, which is used by IC.DEA for its calculation. The subsystem IC.POW realises the power supply of the smart card.

The security function F.RND is the continuous production of random numbers with the length of one byte. These numbers will have a Shannon entropy of at least 6 bit per byte randomly produced. This is implemented by a physical hardware random number generator in the subsystem IC.RNG.

Certain Special Function Registers (SFR) are part of the subsystems IC.DEA and IC.RND mentioned above and provide the interface to the software using the security functions of the TOE.

6 Documentation

The following documentation is provided with the product by the developer to the consumer:

- The Data Sheet [DS] and
- The Guidance, Delivery and Operation Manual [GDO].

Note that the customer who buys the TOE is normally the developer of the operating system and/or application software which will use the TOE as hardware computing platform. The documents [GDO] and [DS] will be used by the customer to implement the software (operating system / application software) which will use the TOE.

7 IT Product Testing

The developer provided extensive testing of the TOE Security Functions.

The tests performed by the developer can be divided into three categories. First, there are tests which are performed in a simulation environment. The developer provided evidence that the probabilistic countermeasures against DPA are functional by testing the internal operation of the subsystem which implements these countermeasures. The second category uses a user program which resides in the User-EEPROM of the TOE. These programs are used to stimulate the TSF in order to obtain test results. The last category uses the Test-ROM of the chip in the same way.

For F.DEA it was shown that the subsystem implementing F.DEA is conformant to the NIST specification [FIPS46]. The implementation of the TOE was checked using the methodology and the reference data from the NIST publication [500-61]. Additionally, the results were compared to results from an independent implementation of the DES algorithm. Furthermore, encryption of random data with both implementations was also performed and compared. After having performed these tests the independent DEA implementation was also used to get evidence of the correct triple-DES implementation according to [ISO8732]. Both DEA implementations were used to encrypt/decrypt reference data and the results have been compared.

To test F.DPA a simulator test was done first to get evidence that the DPA countermeasures have been correctly implemented in the respective subsystem of the TOE. Then a real DPA attack on the chip assuming an outside attacker knowledge was performed. This test was performed in a lab specialized for these kind of attacks.

To test F.RND the developer performed a set of statistical tests, FIPS 140 tests [FIPS140] (monobit-test, poker-test, runs-test and longruns-test) and the calculation of the Shannon entropy. Almost every element of this set of statistical analyses have been performed by the developer under various conditions. All tests provide evidence that F.RND was well realised and all chips tested produced random numbers with an empirical Shannon entropy of at least 7.9 bits per bytes.

The evaluators performed independent tests to supplement, augment and to verify the tests performed by the developer. The test strategy applied by the evaluators was, to test each TSF of the TOE with at least one test. Besides repeating exactly the developers tests, test parameters were varied and additional analysis was done.

The test results confirm the correct implementation of the TOE Security Functions.

For penetration testing the evaluators took all security functions into consideration. Because it was assumed within the Security Target not to consider the physical tampering of the TOE, penetration tests using such effects were not appropriate. For the security function F.DPA the evaluators performed penetration attacks by varying certain operational parameters of the TOE. The penetration tests did not detect any insecure state.

8 Evaluated Configuration

The TOE is identified by P8WE5032V0B. There is only one configuration of the TOE (all TSF are active and usable). All information of how to use the TOE and its security functions by the software is provided within the user documentation.

The TOE has two different operating modes, *user mode* and *test mode*. The application software being executed on the TOE shall not use the *test mode*. Thus, the evaluation was mainly performed in the *user mode*. For all evaluation activities performed in *test mode,* there was a rationale why the results were valid for the *user mode*, too.

9 Results of the Evaluation

The Evaluation Technical Report [ETR] was provided by the ITSEF according to the requirements of the Scheme, the Common Criteria [CC] and Methodology [CEM].

The verdicts for the CC, part 3 assurance classes and components (according to EAL3 and the class ASE for the Security Target Evaluation) are summarised in the following table.

EAL3 assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	n.a.
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration Management	CC Class ACM	PASS
Authorisation controls	ACM_CAP.3	PASS
TOE CM coverage	ACM_SCP.1	PASS

EAL3 assurance classes and components		Verdict
Delivery and operation	CC Class ADO	PASS
Delivery procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Examination of guidance	AVA_MSU.1	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

Verdicts for the assurance components (n.a.= not applicable)

All assurance components were assessed with the verdict PASS. This includes that all evaluator action elements being part of the assurance components are also assessed with PASS. Therefore, the TOE as defined in the Security Target [ST] is considered to be Part 3 conformant.

The Security Target [ST], chapter 6.1 claims, that the TOE will fulfil the following TOE security functional requirements:

a) Requirements taken from Part 2 of the [CC] (CC Part 2 conformant) are

- FCS_COP.1 Cryptographic operation
- FPT_PHP.3 Resistance to physical attack

b) Requirements that are explicitly stated without reference to the [CC] and defined within the Security Target [ST], chapter 10 Annex (CC Part 2 extended):

- FCS_RND.1 Generation of random numbers

The evaluation performed in accordance to EAL3 has shown that the TOE security functional requirements are correctly realised by the TOE security functions. Thus, in realising these functional requirements, it is assured that the TOE will meet the security objectives claimed in the Security Target [ST].

The evaluation has shown that the TOE will fulfil the claimed strength of function SOF-basic for the probabilistic implemented TOE Security Functions (i) Random Number Generation and (ii) resistance of the Triple-DES co-processor against Differential Power Analysis (DPA). For the TOE Security Function (iii) DES encryption and decryption by the Triple-DES co-processor no strength of function claim has been applied.

No Protection Profile (PP) conformance claims were made in the Security Target [ST]. Thus, the evaluation results do not confirm any PP conformance.

The results of the evaluation are only applicable to *Philips Smart Card Controller P8WE5032V0B*. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

10 Evaluator Comments/Recommendations

The operational documentation [GDO] and [DS] contains all necessary information about the usage of the TOE. Besides this information, which the user has to follow, the evaluators have no further recommendations to the user of the TOE.

11 Security Target

The Security Target [ST] of the TOE is provided within a separate document.

12 Definitions

12.1 Acronyms

CC	Common Criteria for IT Security Evaluation
DES	Data Encryption Standard; symmetric block cipher algorithm
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
Triple-DES	Symmetric block cipher algorithm based on the DES
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from Part3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[CC] Common Criteria for IT Security Evaluation, Version 2.0

[CEM] Common Methodology for IT Security Evaluation (CEM), Part 1 Version 0.6, Part 2 Version 0.6, Part 2 Version 1.0 Annex B

[BSI 7125] BSI certification: Procedural Description (BSI 7125, Version 5.1, January 1998)

[ST] Security Target of the First Evaluation of Philips P8WE5032 Smart Card Controller, Version 1.0, September 20th 1999

[GDO] Guidance, Delivery and Operation Manual of the First Evaluation of Philips P8WE5032 Smart Card Controller, Version 1.0, October 5th 1999

[DS] Data Sheet – Philips P8WE5032 Secure 8-bit Smart Card Controller, Preliminary Specification, Revision 2.1, June 1999

[ETR] Evaluation Technical Report of the Philips P8WE5032V0B Smart Card Controller, Version 1.0, November 2nd 1999 (non-public Document)

[FIPS46] U.S. Department of Commerce / National Bureau of Standards Data Encryption Standard, FIPS PUB 46, 1977 January 15

[ISO8732] International Organization for Standardization: Banking – Key Management, International Standard ISO 8732 (1988), Chapter 12.1.3

[FIPS140] U.S. Department of Commerce / National Bureau of Standards Processing Standards Publication 140-1 1994 - SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, 1994 January 11

[500-61] U.S. Department of Commerce / National Bureau of Standards; NBS Special Publication 500-61, Maintenance Testing for the Data Encryption Standard, August 1980

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (Kapitel 5.4)

„The pass result of evaluation shall be a statement that describes the extent to which the PP or TOE can be trusted to conform to the requirements. The results shall be caveated with respect to Part 2 (functional requirements), Part 3 (assurance requirements) or directly to a PP, as listed below.

a) **Part 2 conformant** - A PP or TOE is Part 2 conformant if the functional requirements are only based upon functional components in Part 2.

b) **Part 2 extended** - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2.

c) **Part 3 conformant** - A PP or TOE is Part 3 conformant if the assurance requirements are in the form of an **EAL** or **assurance package** that is based only upon assurance components in Part 3.

d) **Part 3 augmented** - A PP or TOE is Part 3 augmented if the assurance requirements are in the form of an **EAL** or **assurance package**, plus other assurance components in Part 3.

e) **Part 3 extended** - A PP or TOE is Part 3 extended if the assurance requirements are in the form of an **EAL** associated with additional assurance requirements not in Part 3 or an **assurance package** that includes (or is entirely made up from) assurance requirements not in Part 3.

f) **Conformant to PP** - A TOE is conformant to a PP only if it is compliant with all parts of the PP.“

CC Teil 3:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

Evaluation assurance level (EAL) overview (chapter 6.1)

„Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation“ allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component“ is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	**EAL2**	**EAL3**	**EAL4**	**EAL5**	**EAL6**	**EAL7**
Configuration management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	3
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life cycle support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Table 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

„Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.“

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 6.2.3)

„Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.“

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 6.2.4)

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the

highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.“

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

„Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.“

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

„Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.“

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 6.2.7)

„Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

„Objectives
Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.“

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

„Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.“

„Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.“

„Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“