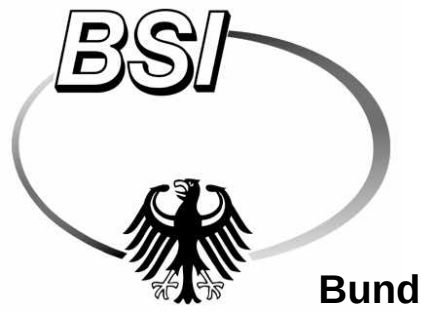

Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0166-2001

for

Philips Smart Card Controller P8WE6017 V1I

from

Philips Semiconductors Hamburg
Unternehmensbereich der Philips GmbH

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

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0166-2001

Philips Smart Card Controller P8WE6017 V1I

from

Philips Semiconductors Hamburg
Unternehmensbereich der Philips GmbH

IT Security Certified

SOGIS-MRA

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, Part 1 Version 0.6*, *Part 2 Version 1.0,* extended by advice of the Certification Body for components beyond EAL4 and Smartcard specific guidance, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria part 2 extended**
Assurance Package:	**EAL5 augmented by** **ADV_LLD.2 (Development - Semiformal low level design),** **ALC_DVS.2 (Life cycle support - Sufficiency of security measures),** **AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states)** **AVA_VLA.4 (Vulnerability assessment - Highly resistant)**

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 notes mentioned on the reverse side are part of this certificate.

Bonn, 12.07.2001

The President des Bundesamtes für
Sicherheit in der Informationstechnik

Dr. Henze L.S.

Common Criteria

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

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

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)
- The DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

---

[2] Act setting up the Bundesamt 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 22nd September 2000 in the Bundesanzeiger p. 19445

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/CC - Certificates

The SOGIS-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. The agreement on the mutual recognition of IT security certificates based on the CC was extended up to and including the evaluation level EAL7.

2.2 CC - Certificates

An arrangement (Common Criteria 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. As of November 2000, Israel joined the arrangement.

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 P8WE6017 V1I has undergone the certification procedure at BSI.

The evaluation of the product Philips Smart Card Controller P8WE6017 V1I was conducted by debis Systemhaus Information Security Services GmbH. The evaluation facility of 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.

The certification is concluded with

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

This work was completed by the BSI on 12.07.2001.

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-18.

The product Philips Smart Card Controller P8WE6017 V1I 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 from BSI-Infoline 0228/9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Philips Semiconductors Hamburg Unternehmensbereich der Philips GmbH, Business Unit 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 relevant evaluation results from the evaluation facility, and
- complementary 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 P8WE6017 V1I"*. It provides a hardware platform for a smart card to run smart card applications executed by a smart card operating system. The TOE is composed of a processing unit, security components, I/O ports, volatile or non-volatile memories (256 + 1024 Bytes RAM, 48 KBytes ROM, 16 KBytes EEPROM), a Triple-DES Co-processor and a Random number generator. The TOE also includes Philips proprietary IC Dedicated Software stored on the chip and used for testing purposes during production only. It does not provide additional services in the operational phase of the TOE. 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 is embedded in a micro-module or another sealed package. The micro-modules are embedded into a credit card sized plastic card. The EEPROM part of the TOE provides an ideal platform for applications requiring non-volatile data storage, including smart cards and portable data banks. Several security features independently implemented in hardware or controlled by software will be provided to ensure proper operations and integrity and confidentiality of stored data. This includes for example measures for memory protection and sensors to allow operations only under specified conditions.

The security target is written using the final draft version of the "Smartcard IC Platform Protection Profile" [9] which is under certification and registration. With reference to this draft Protection Profile, the smart card product life cycle is described in 7 phases and the development, production and operational user environment are described and referenced to these phases. The threats and objectives defined in this draft Protection Profile are used and augmented by an additional policy and security objective for cryptographic services.

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	Identifier
FCS	**Cryptographic support**
FCS_COP.1	Cryptographic operation
FDP	**User data protection**
FDP_IFC.1	Subset information overflow control
FDP_ITT.1	Basic internal transfer protection
FPT	**Protection of the TOE Security Functions**

Security Functional Requirement	Identifier
FPT_FLS.1	Failure with preservation of secure state
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_PHP.3	Resistance to physical attack
FPT_SEP.1	TSF domain separation
FRU	**Resource utilisation**
FRU_FLT.2	Limited fault tolerance

SFRs taken from CC part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Identifier
FAU	**Security Audit**
FAU_SAS.1	Audit storage
FCS	**Cryptographic support**
FCS_RND.1	Quality metric for random numbers
FMT	**Security management**
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability

SFRs CC part 2 extended

The security functions (SF) of the TOE are applicable to the phases 4 to 7. Some of the security functions are configured at the end of phase 3 and all security functions are already active during the delivery from phase 3 to phase 4.:

F.RNG: Random Number Generator

The random number generator continuously produces random numbers with a length of one byte. Each byte will at least contain a 7 bit entropy. The TOE implements the F.RNG by means of a physical hardware random number generator working stable within the limits guaranteed by F.OPC (operational conditions).

F.DEA: Triple-DES Coprocessor

The TOE provides the Triple Data Encryption Algorithm (TDEA) of the Data Encryption Standard (DES) [12]. F.DEA is a modular basic cryptographic function which provides the TDEA algorithm as defined by FIPS PUB 46 by means of a hardware co-processor and supports the 2-key Triple DEA algorithm according to keying option 2 in FIPS PUB 46-3

[13]. The TOE implements functions ensuring that attackers are unable to observe the keys and plain text by measuring the external behaviour during the Triple-DES-operation. This includes: Differential Power Attack (DPA), Timing Attacks, Differential Fault Analysis and Simple Power Analysis.

F.OPC: Control of Operation Conditions

F.OPC filters the power supply and the frequency of the clock. It also monitors the power supply, the frequency of the clock, the temperature of the chip and the high voltage for the write process to the EEPROM by means of sensors and controls the program execution. Before delivery the mode-switch is set to user mode. In user mode the TOE enables the sensors automatically when operated. The TOE prevents that the application program disables the sensors.

F.PHY Protection against Physical Manipulation

F.PHY protects against manipulation of (i) the hardware, (ii) the test software in the ROM, (iii) the application software in the ROM and the EEPROM, (iv) the application data in the EEPROM and RAM, (v) the configuration data in the security row of the EEPROM and (vi) the mode-switch. It also protects secret user data against the disclosure when stored in EEPROM and RAM or while being processed by the TOE. The protection comprises different features of the construction of the TOE.

F.COMP Protection of Mode and Configuration

F.COMP provides access control by means of TOE modes of operation selected by a mode-switch: (i) test mode and (ii) user mode. In the test mode the TOE (i) allows to execute the test software and (ii) prevents to execute the application software. In the user mode the TOE (i) allows to execute the application software and (ii) prevents to execute the test software. The initial TOE mode is the test mode. The TOE allows to change the mode-switch from the test mode into the user mode. The TOE prevents to change the mode-switch from the user mode into the test mode. In test mode F.COMP also provides the capability to store identification and/or pre-personalisation data and/or supplements of the Smartcard Embedded Software into the EEPROM. Before delivery the TOE is switched to user-mode.

The TOE was evaluated against the claims of the Security Target [6] by debis Systemhaus Information Security Services GmbH and completed on 11.07.2001. The evaluation facility of debis Systemhaus Information Security Services GmbH is an evaluation facility recognised by BSI (ITSEF)[8].

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

[8] Information Technology Security Evaluation Facility

1.1 Assurance package

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 [1], Part 3 for details). The TOE meets the assurance requirements of assurance level EAL5+ (Evaluation Assurance Level 5 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL5	TOE evaluation: Semiformally designed and tested
+: ADV_LLD.2	Development - Semiformal low level design
+: ALC_DVS.2	Life cycle support - Sufficiency of security measures
+: AVA_MSU.3	Vulnerability assessment - Analysis and testing of insecure states
+: AVA_VLA.4	Vulnerability assessment - Highly resistant

Assurance components and EAL-augmentation

The level of assurance is chosen in order to allow the confirmation that the TOE is suitable for use within devices compliant with the German Digital Signature Law [14] and is therefore higher than required by the above mentioned final draft version of the "Smartcard IC Platform Protection Profile" [9].

1.2 Strength of Function

The TOE‘ s strength of functions is rated ‘high’ (SOF-high). The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

1.3 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The threats which were assumed for the evaluation and averted by the TOE and the organisational security policies defined for the TOE are specified in the Security Target [7] and can be summarized as follows.

It is assumed that the attacker is a human being or a process acting on behalf of him being located outside the smart card.

First, the Security Target [7] defines so called standard high-level security concerns derived from considering the end-usage phase (Phase 7 of the life cycle as described in the Security Target) as follows:

- manipulation of User Data and of the Smartcard Embedded Software (while being executed/processed and while being stored in the TOE’s memories),
- disclosure of User Data and of the Smartcard Embedded Software (while being processed and while being stored in the TOE’s memories) and

- deficiency of random numbers.

These high-level security concerns are refined by defining threats on a more technical level for

- Inherent Information Leakage
- Physical Probing
- Malfunction due to Environmental Stress
- Physical Manipulation
- Forced Information Leakage
- Abuse of Functionality and
- Deficiency of Random Numbers.

Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by assumptions (see below).

The development and production environment starting with Phase 2 up to TOE Delivery are covered by an organisational security policy outlining that the IC Developer / Manufacturer must apply the policy “Protection during TOE Development and Production (P.Process-TOE)” so that no information is unintentionally made available for the operational phase of the TOE. The Policy ensures confidentiality and integrity of the TOE and its related design information and data. Access to samples, tools and material must be restricted.

A specific additional security functionality for Triple DES encryption and decryption must be provided by the TOE according to an additional security policy defined in the Security Target.

1.4 Special configuration requirements

The TOE has two different operating modes, *user mode* and *test mode*. The application software being executed on the TOE can 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 requirements on the software to be applied as described in the user documentation.

1.5 Assumptions about the operating environment

With respect to the life cycle defined in the Security Target, Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by assumptions.

The developer of the Smartcard Embedded Software (Phase 1) must ensure:

- the appropriate “Usage of Hardware Platform (A.Plat-Appl)” while developing this software in Phase 1. Therefore, it has to be ensured, 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 appropriate “Treatment of User Data (A.Resp-Appl)” while developing this software in Phase 1. 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.

Security procedures during Packaging, Finishing and Personalisation (A.Process-Card) are assumed after TOE Delivery up to the end of Phase 6, as well as during the delivery to Phase 7.

1.6 Disclaimers

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 of the TOE

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

No	Type	Identifier	Release	Date	Form of Delivery
1	HW	Philips P8WE6017 V1I Secure 8-bit Smart Card Controller	V1I	13.07.2000	hardware chip
2	SW	Test ROM Software *(the IC dedicated software)*	xk033a	19.07.2000	test-ROM on the chip

No	Type	Identifier	Release	Date	Form of Delivery
3	DOC	Guidance, Delivery and Operation Manual [10]	1.1	10.07.2001	printed document
4	DOC	Data Sheet [11]	3.1	26.01.2001	printed document

Deliverables of the TOE

The TOE is identified by P8WE6017 V1I. A so called on-chip code is printed onto the chip during production and can be checked by the customer, too. This code is different for the two production sites as outlined in the guidance documentation [10]. 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 [10] 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 symmetric cryptographic block cipher algorithm to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a random number generation of appropriate quality.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against abuse of functionality.

4 Assumptions and Clarification of Scope

The smart card operating system and the application software 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 (IC dedicated software) is used by the manufacturer of the smart card to check the chip function.

The TOE is delivered as a hardware unit at the end of the chip manufacturing process (phase 3 of the life cycle defined). 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.

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.

5 Architectural Information

The Philips P8WE6017 V1I smart card controller is an integrated circuit (IC) providing a hardware platform to a smart card operating system and smart card application software. A top level block diagramm and a list of subsystems can be found within the TOE description of the Security Target [7]. The complete hardware description and the complete instruction set of the Philips P8WE6017 V1I smart card controller is to be found in the Data Sheet [11].

For the implementation of the TOE Security Functions basically the components 8-bit 80C51 CPU, Special Function Registers, Triple-DES Co-Processor, a Random Number Generator (RNG), Security Sensors and Security Logic and a Clock Filter are used. Security measures for Physical Protection are realized within the layout of the whole circuitry.

The Special Function Registers 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 Guidance, Delivery and Operation Manual [10] and
- The Data Sheet [11].

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 [10] and [11] will be used by the customer to implement the software (operating system / application software) which will use the TOE.

7 IT Product Testing

The tests performed by the developer were divided into four categories: (i) tests which are performed in a simulation environment, (ii) production tests, which are done as a last step of the production process for every chip to check its correct functionality, (iii) characterization tests, which were used to determine the behaviour of the chip with respect to different operating conditions and (iv) special verification tests for security functions which were done with samples of the TOE.

The developer tests cover all security functions and all security mechanisms as identified in the functional specification, the high level design and the low level design. Chips from both production sites were used for tests.

The evaluators could repeat all tests of the developer either using the library of programs and tools delivered to the evaluator or at the developers site. They performed independent tests to supplement, augment and to verify the tests performed by the developer by sampling. Besides repeating exactly the developers tests, test parameters were varied and additional analysis was done. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections.

The evaluators gave evidence that the actual version of the TOE (V1I) provides the security functions as specified. The test results confirm the correct implementation of the TOE security functions.

For penetration testing the evaluators took all security functions into consideration. Intensive penetration testing was performed to consider the physical tampering of the TOE using highly sophisticated equipment and expertised know how.

8 Evaluated Configuration

The TOE is identified by P8WE6017 V1I. 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 can 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) [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all relevant interpretations and guidelines of the Scheme (AIS) as relevant for the TOE.

For the evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in coordination with the Certification Body. For Smartcard IC specific methodology the guidance documents (i) *Joint Interpratation Library - The application of CC to Integrated Circuits* and (ii) *Joint Interpratation Library - Integrated Circuit Hardware Evaluation Methodology* (see [4]: AIS 25, ASI 26) were used. The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

The verdicts for the CC, part 3 assurance classes and components (according to EAL5 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

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
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Development tools CM coverage	ACM_SCP.3	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Semiformal functional specification	ADV_FSP.3	PASS
Semiformal high-level design	ADV_HLD.3	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Modularity	ADV_INT.1	PASS
Semiformal low-level design	ADV_LLD.2	PASS
Semiformal correspondence demonstration	ADV_RCR.2	PASS
Formal TOE security policy model	ADV_SPM.3	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
Sufficiency of security measures	ALC_DVS.2	PASS
Standardised life-cycle model	ALC_LCD.2	PASS
Compliance with implementation standards	ALC_TAT.2	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-low design	ATE_DPT.2	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Covert chanel analysis	AVA_CCA.1	PASS
Analysis and testing for insecure states	AVA_MSU.3	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

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

The evaluation has shown that the TOE will fulfil the claimed strength of function for the (i) Random Number Generation and (ii) resistance of the Triple-DES co-processor against Differential Power Analysis (DPA).

For the security enforcing function F.DEA, which is Triple-DES encryption and decryption by the hardware co-processor, the strength was not evaluated as it is

a cryptoalgorithm suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

The evaluation of the development and production environment was focused on the development site (a), the production sites (b) and (c) and the test centre (d).

(a) Philips Semiconductors Hamburg
Unternehmensbereich der Philips GmbH
Georg-Heyken-Straße 1
21147 Hamburg – Germany

(b) MOS4YOU
Gerstweg 2
6534 AE Nijmegen
The Netherlands

(c) Philips Semiconductors Fishkill (PSF)
Hudson Valley Research Park
1580 Route 52, P.O. Box 1279
Hopewell Junction, New York 12533

(d) Philips Semiconductors Hamburg
Unternehmensbereich der Philips GmbH
Stresemannallee 101
22529 Hamburg – Germany

Additionally, security procedures for mask production and deliveries were analysed. The evaluators verified, that the organisational security policy and the security objective for the TOEs life cycle phases 2 up to delivery as stated in the Security Target are fulfilled by the regulations and practices of the Philips sites.

The evaluation performed has shown that the TOE security functions will meet the security objectives claimed in the Security Target.

The results of the evaluation are only applicable to Philips Smart Card Controller P8WE6017 V1I. 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 of the modified product does not reveal any security deficiencies.

10 Evaluator Comments/Recommendations

1. The operational documentation [10] and [11] contains necessary information about the usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [7] has to be taken into account.
2. For evaluations of products or systems including the TOE as a part or using the TOE as a platform (for example smart card operating systems or complete smart cards), specific information resulting from this

evaluation is of importance and shall be given to the succeeding evaluation.

11 Annexes

none

12 Security Target

For the purpose of publishing, the security target [7] of the target of evaluation (TOE) is provided within a separate document. It is a sanitized version from the complete security target [6] used for the evaluation performed.

13 Definitions

13.1 Acronyms

CC	Common Criteria for IT Security Evaluation (see [1])
DES	Data Encryption Standard; symmetric block cipher algorithm
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
OTP	One Time Programmable (a certain part of the EEPROM)
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
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

13.2 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 Part2 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.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

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

[4] Applicaton Notes and Interpretations of the Scheme (AIS) as relevant for the TOE, e.g.
AIS 25, Version 1, 29.02.2000 for *Joint Interpretation Library – The application of CC to Integrated Circuits, Version 1.0, January 2000*
AIS 26, Version 1, 26.06.2000 for: *Joint Interpratation Library - Integrated Circuit Hardware Evaluation Methodology, Version 1.3, April 2000*

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-CC-0166, Version 1.1, June 11th 2001, Evaluation of Philips P8WE6017 V1I Secure 8-bit Smart Card Controller, Philips Semiconductors (confidential document)

[7] Security Target BSI-DSZ-CC-0166, Version 1.2, July 10th 2001, Evaluation of Philips P8WE6017 V1I Secure 8-bit Smart Card Controller, Philips Semiconductors (sanitized public document)

[8] Evaluation Technical Report, Philips P8WE6017 V1I Secure 8 bit Smart Card Controller, Version 1.0, 11.07.2001 (confidential document)

[9] Smartcard IC Platform Protection Profile (under certification and registration at BSI, ID: BSI-PP-0002), final draft version 0.99, June 5, 2001

[10] Guidance, Delivery and Operation Manual of Philips P8WE6017 V1I Secure 8-bit Smart Card Controller, Version 1.1, 10 July 2001 (confidential document)

[11] Data Sheet, P8WE6017 Secure 8-bit Smart Card Controller, Product Specification, Philips Semiconductors, Revision 3.1, January 26th 2001 (confidential document)

[12] Data Encryption Standard (DES), FIPS PUB 46, US NBS, 1977, Washington

[13] FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION DATA ENCRYPTION STANDARD (DES) Reaffirmed 1999 October 25

[14] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001, BGBl. I, S. 876); veröffentlicht am 21. Mai 2001

This page is intentionally left blank.

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 Part 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 in as much 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.