Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0203-2003

for

Philips Smart Card Controller P16WX064V0C

from

Philips Semiconductors GmbH
Business Line Identification

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-0203-2003

Philips Smart Card Controller P16WX064V0C

from

Philips Semiconductors GmbH Business Line Identification

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 smart card specific guidance, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC15408: 1999).*

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0002-2001**
Functionality:	**BSI-PP-0002-2001 conformant plus product specific extensions Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant EAL5 augmented by** 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, 18 June 2003

The Vice President of the Bundesamt für Sicherheit in der Informationstechnik

Common Criteria

Hange L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - 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)
- 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)
- Advice from the Certification Body on methodology for assurance components above EAL4

---

[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 Bundesamt 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 October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium 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. This agreement on the mutual recognition of IT security certificates based on the CC was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

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 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002 and Austria in November 2002.

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 P16WX064V0C has undergone the certification procedure at the BSI.

The evaluation of the product Philips Smart Card Controller P16WX064V0C was conducted by T-Systems GEI GmbH, Business Unit ITC Security. The evaluation facility of T-Systems GEI GmbH is an evaluation facility recognised by the BSI (ITSEF)[6].

The sponsor, vendor and distributor is Philips Semiconductors GmbH, Business Line Identification, Stresemannallee 101, P.O. Box 54 02 40, D-22502 Hamburg.

The certification is concluded with

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

This work was completed by the BSI on 18 June 2003.

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-20.

The product Philips Smart Card Controller P16WX064V0C 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 GmbH, Business Line Identification, Stresemannallee 101, P.O. Box 54 02 40, D-22502 Hamburg, Germany

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 P16WX064V0C"*. 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 and non-volatile memories (5152 Bytes RAM, 128 KBytes User-ROM, 64 KBytes EEPROM), a Triple-DES and FameX co-processor and a Random number generator. Also two 16-bit Timers, an Interrupt Module, a Memory Management Unit, an UART and an USB interface. 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-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 a 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 Protection Profile BSI-PP-0002-2001 [9]. With reference to this Protection Profile, the smart card product life cycle is described in seven phases and the development, production and operational user environment are described and referenced to these phases. The assumptions, threats and objectives defined in this Protection Profile are used.

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 and are contained in BSI-PP-0002-2001:

Security Functional Requirement	**Identifier**	Source from PP or added in ST
FCS	**Cryptographic support**	
FCS_COP.1	Cryptographic operation	ST
FDP	**User data protection**	
FDP_ACC.1 [MEM, SFR]	Subset access control	ST
FDP_ACF.1 [MEM, SFR]	Security Attribute based access control	ST

FDP_IFC.1	Failure with preservation of secure state	PP
FDP_ITT.1	Basic internal TSF data transfer protection	PP
FPT	**Protection of the TOE Security Functions**	
FPT_FLS.1	Failure with preservation of secure state	PP
FPT_ITT.1	Basic internal TSF data transfer protection	PP
FPT_PHP.3	Resistance to physical attack	PP
FPT_SEP.1	TSF domain separation	PP
FRU	**Resource utilisation**	
FRU_FLT.2	Limited fault tolerance	PP
FMT	**Security Management**	**ST**
FMT_MSA.3 [MEM, SFR]	Static attribute initialisation	ST
FMT_MSA.1 [MEM, SFR]	Management of security attributes	ST
FMT_SMF.1	Specification of Management Functions	ST

Table 1: SFRs taken from CC Part 2

The following CC part 2 extended SFRs are defined.

Security Functional Requirement	**Identifier**	Source from PP or added in ST
FAU	**Security audit**	
FAU_SAS.1	Audit storage	PP
FCS	**Cryptographic support**	
FCS_RND.1	Quality metric for random numbers	PP
FMT	**Security management**	
FMT_LIM.1	Limited capabilities	PP
FMT_LIM.2	Limited availability	PP
FRU	**Resource utilisation**	
FRU_VRC.1	Simple value range check	ST

Table 2: SFRs CC part 2 extended.

The security functions (SF) of the TOE are applicable to the phases 4 to 7. All security functions (SF) of the TOE are applicable from TOE delivery at the end of phase 3 or 4 (depending on when TOE delivery takes place in a specific case) to phase 7. It is not possible to switch back to the Test Mode once the Application Mode is activated.

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.HW_DEA: Triple-DES Co-Processor

The TOE provides the Triple Data Encryption Algorithm (TDEA) of the Data Encryption Standard (DES) [12]. F.HW_DEA is a modular basic cryptographic function which provides the TDEA algorithm as defined by FIPS PUB 46-3 [13] 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. 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.

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 it controls the program execution. Therefore the proper operation of the Random Number Generator, the Triple-DES co-processor and the arithmetic co-processor (FameX) that may be used for cryptographic operations can be ensured within the specified limits [9]. Before delivery the mode-switch is set to application mode. In application 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

The function F.PHY protects the TOE against manipulation of (i) the hardware, (ii) the IC Dedicated Test Software in the ROM, (iii) the Smartcard Embedded Software in the ROM and the EEPROM, (iv) the application data in the EEPROM and RAM, (v) the configuration data in the security row, (vi) the control of the TOE mode and (vii) the OTP-area. It also protects User Data or TSF data against disclosure by physical probing when stored or while being processed by the TOE.

F.LOG Protection against Reconstruction of the TOE internal Information

The function F.LOG implements measures to limit or eliminate the information that might be contained in the shape and amplitude of signals or in the time between events found by measuring such signals. This comprises the power consumption and signals on the other pads that are not intended by the terminal or the Smartcard Embedded Software. Thereby this security function prevents the disclosure of User Data or TSF data stored and/or processed in the Smartcard IC through the measurement of the power consumption and subsequent complex signal

processing. The protection of the TOE comprises different features within the design that support the other security functions. The Triple-DES co-processor includes special features to prevent SPA/DPA analysis of shape and amplitude of the power consumption and ensures the same calculation time for all operations.

The FameX co-processor provides measures to prevent timing attacks on basic modular function. The calculation time of one modular operation depends on the lengths of the operands but not on the value of the operands. The FameX does not realise an algorithm on its own specific countermeasures against leakage must be implemented by the smart card embedded software related to the realised cryptographic algorithm.

Additional features that can be configured by the Smartcard Embedded Software comprise (i) the secure DCDC-converter that can be used to smooth the power consumption and (ii) several clock configurations that can be used to prevent the possibility to synchronise the internal operation with the external clock or to synchronise with the characteristics of the power consumption that can be used as trigger signal to support leakage attacks (DPA or timing attacks) The behaviour of F.LOG is supported by different features realised in the functions F.OPC and F.PHY.

F.COMP: Protection of Mode Control

The function F.COMP provides a control of the TOE mode for (i) Test Mode and (ii) Application Mode. This includes the protection of electronic fuses stored in a protected memory area. In addition F.COMP provides a write once memory area. All bits in this area can only be set once. The control of the TOE mode prevents the use of features implemented in the TOE that are used during production/test and that are disabled before the delivery of the TOE. The initial TOE mode is the Test Mode. F.COMP limits the capabilities of the test functions and provides test personnel during Phase 3 with the capability to store the identification and/or pre-personalisation data and/or supplements of the Smartcard Embedded Software in the EEPROM. The implemented control of the TOE mode ensures that in the Test Mode (i) allows to execute the IC Dedicated Test Software and (ii) prevents to execute the Smartcard Embedded Software. In the Application Mode the TOE (i) allows to execute the Smartcard Embedded Software and (ii) prevents to execute the IC Dedicated Test Software. The protection of electronic fuses ensures the secure storage of configuration- and calibration data stored in the Test Mode. The TOE allows to change the TOE mode only one time from the Test Mode into the Application Mode. The TOE prevents to change the TOE mode from the Application Mode into the Test Mode.

F.MEM_ACC: Access control for code and data memory

The function F.MEM_ACC is designed in a way that dedicated software routines of a smartcard operating system (Smartcard Embedded Software) can be used to configure the memory management units for

code and data. Memory access is based on virtual addresses that are mapped to physical addresses. The CPU uses virtual addresses, physical addresses are used to access the memories. The Memory Management Units perform the translation from virtual to physical addresses. The access control is performed by the definition of memory areas with related access rights. The access control for the Code Memory Areas can be configured with the granularity of (i) read, (ii) write, (iii) execute and (iv) enable/disable. The access control for the Data Memory Areas can be configured with the granularity of (i) read, (ii) write and (iii) enable/disable. The memory management provides the possibility to define different independent windows that provide access to a memory area. Every window has its own set of Code Memory Area Attributes or Data Memory Area Attributes that define the memory location and limitation as well as the access rights. Access violations and accesses outside the boundary of the physical implemented memory range are notified by raising an exception.

F.SFR_ACC: Access control for Special Function Registers (SFRs)

The function F.SFR_ACC realises the access control to the Special Function Registers and the switch between the System Mode, the Meta Mode and the Application mode. The actual mode of operation is set in the Program Status Word. Access to the Special Function Register is granted or not depending on the Mode of Operation (System Mode, Meta Mode, Application mode). The System Mode and the Meta Mode are mainly the same. They provide access to all Special Function Registers including the Data MMU, the cryptographic co-processors, I/O interfaces and the configuration of the hardware. Exceptions are the Special Function Registers of the Code MMU and the System Configuration Register that are only writable in the System Mode. The configuration of the Code MMU is readable in the Meta Mode but cannot be changed in this mode of operation. In the Application mode only the Special Function Registers related to General CPU Functions are accessible and specific Special Function Registers that can be used for the value range check.

F.RANGE_CHK: Range checking for certain registers

The security function F.RANGE_CHK provides range checking for certain registers (CPU internal and Special Function Register). The range checking comprises checking against a lower and an upper bound.

The TOE was evaluated against the claims of the Security Target [5] by T-Systems GEI GmbH. The evaluation was completed on June 12th, 2003. The evaluation facility of T-Systems GEI GmbH is an evaluation facility recognised by BSI (ITSEF)[8].

[8] Information Technology Security Evaluation Facility

The sponsor, vendor and distributor is Philips Semiconductors GmbH, Business Line Identification, Stresemannallee 101, P.O. Box 54 02 40, D-22502 Hamburg.

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Part 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
+: 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

Table 4: 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].

1.2 Strength of Function

The TOE‘s strength of functions is rated ‘high’ (SOF-high) for those functions, identified in the Security Target, chapter 6.1, SOF Claim. 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 are specified in the BSI-PP-0002-2001 [9] and mentioned in the Security Target. Considering the Application Notes 10 and 11 of [9] there are no additional high-level security concerns or additional new threats defined in the Security Target.

Since the Security Target claims conformance to BSI-PP-0002-2001, the policy P.Process-TOE (Protection during TOE Development and Production) of the Protection Profile is applied in the Security Target. Because there is a specific security component which is not derived from threats the developer must apply the Policy P.Add-Components (Additional Specific Security Components), which is defined in the Security Target.

1.4 Special configuration requirements

The TOE has two different operating modes, *Application 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 organised in a way that excludes all possibilities of physical manipulation of the TOE. There are no special security measures for the start-up of the TOE besides the requirement that the controller has to be used under the well-defined operating conditions and that the requirements on the software have to be applied as described in the user documentation [10].

1.5 Assumptions about the operating environment

Since the Security Target claims conformance to the Protection Profile BSI-PP-0002-2001, the assumptions defined in section 3.2 of the Protection Profile are valid for the Security Target of this TOE.

Additional assumptions are chosen in the Security Target (see [5], chapter 3.2).

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 version P16WX064V0C:

No	Type	Identifier	Release	Date	Form of Delivery
1	HW	Philips P16WX064V0C Secure 16-bit Smart Card Controller	V0C	C013C.gds2_20020926(GDS2 File)	Wafer (dice include reference C013C)
2	SW	Test ROM Software *(the IC dedicated software)*	2.1	03.09.2001	Test ROM on the chip (Testrom_0s_xsa_080801.lst)

No	Type	Identifier	Release	Date	Form of Delivery
3	DOC	Data Sheet P16WX064 SmartXA-Family, Secure 16-bit Smart Card Controller	3.1	November 29th,.2002	electronic document [11]
4	DOC	Instruction Set P16WX064 SmartXA-Family, Secure 16-bit Smart Card Controller	3.0	July 23th, 2002	electronic document [16]
5	DOC	Guidance, Delivery and Operation Manual of the P16WX064V0C [10]	1.2	12.06.2003	electronic document [10]

Table 5: Deliverables of the TOE version P16WX064V0C

Note that item 2 in table 5 ist not delivered as asingle piece, but included in the Test ROM part of the chip. The TOE is identified by P16WX064V0C. A so called nameplate (on-chip identifier) is coded in a metal mask onto the chip during production and can be checked by the customer, too. The nameplate for the waferfab in Nijmegen, NL (MOS4YOU) is C013C.

This code is specific for the MOS4YOU (Nijmegen, The Netherlands) production site 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, against access for code and data memory and against abuse of functionality. Hence the TOE shall:

- maintain the integrity and the confidentiality of data stored in the memory of the TOE and

- maintain the integrity, the correct operation and the confidentiality of security functions (security mechanisms and associated functions) provided by the TOE.

4 Assumptions and Clarification of Scope

The smart card operating system and the application software stored in the User ROM and in the EEPROM are not part of the TOE. The code in the Test ROM of the TOE (IC dedicated software) is used by the manufacturer of the smart card to check the functionality of the chips.

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 memory 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.

Within this evaluation of the TOE several aspects were specifically considered to support a composite evaluation of the TOE together with an embedded smart card application software (i.e. smart card operating system and application). This was necessary as Philips Semiconductors is the TOE developer and manufacturer and responsible for specific aspects of handling the embedded smart card application software in its development and production environment. For those aspects refer to chapter 9 of this report.

The full evaluation results are applicable for chips from MOS4YOU (Nijmegen, The Netherlands) indicated by the namplate C013C.

5 Architectural Information

The Philips P16WX064V0C smart card controller is an integrated circuit (IC) providing a hardware platform for a smart card operating system and smart card application software. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target. The complete hardware description and the complete instruction set of the Philips P16WX064V0C smart card controller [16] is to be found in the Data Sheet, P16WX064, Version 3.1 [11].

For the implementation of the TOE Security Functions basically the components 16-bit CPU, Special Function Registers, Triple-DES and FameX Co-Processors,

Random Number Generator (RNG), Memory Management Unit for access control, Power Module with Security Sensors and Security Logic and a Clock Filter are used. Security measures for physical protection are realised 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],
- Instruction set [16]
- The Data Sheet [11] and
- The ETR-lite [8]

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], [11] and [16] will be used by the customer to implement the software (operating system / application software) which will use the TOE.

The ETR-lite is intended to provide the results of the platform evaluation for the TOE in a way that meets the requirements for a composite evaluation as defined in AIS 36 [4].

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) characterisation 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 MOS4YOU production site 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 developer‘s 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 (V0C) 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 P16WX064V0C with the nameplates C013C. There is only one configuration of the TOE [15] (all TSF are active and usable). All information on 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, *application 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 *application mode*. For all evaluation activities performed in *test mode,* there was a rationale why the results are valid for the *application mode*, too.

9 Results of the Evaluation

9.1 Evaluation of the TOE

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

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 smart card IC specific methodology the guidance documents (i) *Joint Interpretation Library - The application of CC to Integrated Circuits,* (ii) *Joint Interpretation Library - Integrated Circuit Hardware Evaluation Methodology* and (iii*) Functionality classes and evaluation methodology for physical random number generators and (iv) ETR-lite – for Composition and ETR-lilte – for composition: Annex A Composite smartcard evaluation: Recommended best practice* (see [4]: AIS 25, AIS 26, AIS 31 and AIS 36) 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 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	PASS
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
Descriptive low-level design	ADV_LLD.1	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: low-level 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 channel 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

Table 6: Verdicts for the assurance components

The evaluation has shown that the TOE fulfils 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 TOE security function F.HW_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 full evaluation results are applicable for chips from MOS4YOU (Nijmegen, The Netherlands), indicated by the nameplate C013C.

For specific evaluation results regarding the development and production environment see annex A in part D of this report.

The results of the evaluation are only applicable to the Philips Smart Card Controller P16WX064V0C. The validity can be extended to new versions and releases of the product or chips from other production and manufacturing sites, 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.

9.2 Additional Evaluation Results

- The evaluation confirmed specific results of a previous smart card IC evaluation regarding assurance aspects for the development and production environment. This is outlined in part D of this report, annex A.
- To support a composite evaluation of the TOE together with a specific smart card embedded software additional evaluator actions were performed during the TOE evaluation. The results are documented in ETR-Lite [8] according to [4] AIS 36. Therefore, the interface between the smart card embedded software developer and the developer of the TOE was examined in detail. These composition related actions comprised the following tasks:
  - Examination of the integration of the embedded software in the configuration management system of the IC manufacturer for the TOE.

    This comprises the handling of the ROM-code, the related acceptance and verification procedures with the customer and the assignment to a unique commercial type identifier as well as the handling of different ROM-code masks for the same smart card IC.
  - Examination of consistency of delivery and pre-personalisation procedures.

    This comprises the handling of the Fabkey and pre-personalisation data with respect to the physical, technical and organisational measures to protect these data as well as the procedures to ensure the correct configuration of the TOE. In addition, the production test related to customer specific items including the integrity check of the customer ROM-code and the personalisation process, were checked.
  - Examination of the separation based on the unique commercial type identifier and the related test and delivery procedures.

- Examination, that Philips Semiconductors has implemented procedures to provide a customer product related configuration list based on the general configuration list provided for the evaluation of the TOE supplemented by the customer specific items including ROM-mask labelling, specific development tools for embedded software development and related customer specific deliveries and the corresponding verification data generated by Philips to be sent to customer. In the course of the TOE evaluation a specific customer product related configuration list was checked [15].
- Examination of aspects relevant for the user guidance documentation of the TOE to use the TOE for a product composition.

10 Evaluator Comments/Recommendations

1. The operational documentation guidance [10], Data sheet [11] and Instruction set [16] contain 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 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 according to AIS 36.

11 Annexes

Annex A: Evaluation results regarding the development and production environment. (see part D of this report)

12 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document. It is a sanitized version of the complete Security Target [5] used for the evaluation performed.

13 Definitions

13.1 Acronyms

BSI Bundesamt für Sicherheit in der Informationstechnik

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
MMU	Memory Management Unit
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
TSS	TOE Summary Specification

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 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.

UART - Universal Asynchronous Receiver and Transmitter

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] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE, e.g.
AIS 25, for *Joint Interpretation Library – The application of CC to Integrated Circuits, Version 1.2, July 2002*
AIS 26, for: *Joint Interpretation Library - Integrated Circuit Hardware Evaluation Methodology, Version 1.3, April 2000*
AIS 31, for: Functionality classes and evaluation methodology of physical random number generators
AIS 36, for: *ETR-lite – for Composition, Version 1.1, July 2002 and ETR-lilte – for composition: Annex A Composite smartcard evaluation: Recommended best practice, Version 1.2, March 2002*

[5] Security Target BSI-DSZ-CC-0203, Version 1.1, January 24th, 2003, Evaluation of Philips P16WX064V0C Secure 16-bit Smart Card Controller, Philips Semiconductors (confidential document)

[6] Security Target Lite BSI-DSZ-CC-0203, Version 1.2, May 8th, 2003, Evaluation of Philips P16WX064V0C Secure 16-bit Smart Card Controller, Philips Semiconductors (sanitized public document)

[7] Evaluation Technical Report, Philips P16WX064V0C Secure 16-bit Smart Card Controller, Version 1.2, June 12th, 2003 (confidential document)

[8] ETR-lite for Composition, according AIS 36, Version 1.2, June 12th, 2003 (confidential document)

[9] Smart Card IC Platform Protection Profile, Version 1.0, July 2001, registered at the German Certification Body under number BSI-PP-0002-2001

[10] Guidance, Delivery and Operation Manual for the P16WX064V0C, BSI-DSZ-CC-0203, Philips Semiconductors, Version 1.2, June 6th, 2003 (confidential document)

[11] Data Sheet, 16WX064 SmartXA-Family Secure 16-bit Smart Card Controller, Product Specification, Philips Semiconductors, Revision 3.1, Doc. No.: 053531, November 29th, 2002 (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

[15] Configuration List of the P16WX064V0C, BSI-DSZ-CC-0203, Version 1.1, Philips Semiconductors, June 12th, 2003 (confidential document)

[16] Instruction set, 16WX064 SmartXA-Family Secure 16-bit Smart Card Controller, Product Specification, Philips Semiconductors, Revision 3.0, Doc. No.: 074630, July 23th, 2002

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 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 modelling	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.

This page is intentionally left blank.

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0203-2003

Evaluation results regarding development and production environment

The IT product, Philips Smart Card Controller P16WX064V0C (Target of Evaluation, TOE) 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 smart card specific guidance, for conformance to the Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC15408: 1999).

As a result of the TOE certification, dated 18 June 2003, the following results regarding the development and production environment apply. The Common Criteria assurance requirements

- **ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.3),**
- **ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1),**
- **ALC – Life cycle support (i.e. ALC_DVS.2, ALC_LCD.2, ALC_TAT.2),**

are fulfilled for the development and production sites of the TOE listed below ((a) – (e)):

(a) **Philips Semiconductors GmbH, Business Line Identification (BU ID), Georg-Heyken-Strasse 1, 21147 Hamburg, Germany**

(b) **Philips Semiconductors MOS4YOU, Gerstweg 2, 6534 AE Nijmegen, The Netherlands (production site)**

(c) **Philips Semiconductors GmbH, Philips IC Test Operation Hamburg (PICTOH), Stresemannallee 101, 22529 Hamburg, Germany**

(d) **Photronics (UK) Ltd., Trafford Wharf Road, Trafford Park, Manchester, M17 1PE, United Kingdom.**

(e) **Philips Semiconductors (Thailand), 303 Chaengwattana Rd., Laksi Bangkok 10210, Tailand**

The TOE produced at site b in (Nijmegen) is indicated by the nameplate C013C for MOS4YOU

For all sites listed above, the requirements have been specifically applied for each site and in accordance with the Security Target [5]. The evaluators verified, that the threats and the security objective for the life cycle phases 2, 3 and 4 up to delivery at the end of phase 3 or 4 as stated in the TOE Security Target [5] are fulfilled by the procedures of these sites.

This page is intentionally left blank.