Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0227-2004

for

Philips P5CT072V0M and P5CC072V0M
Secure Smart Card Controller

from

Philips Semiconductors GmbH
Business Line Identification

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

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0227-2004

Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller

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/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

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 German Federal Office for Information Security (BSI) 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, 16 September 2004

The President of the Federal Office
for Information Security

Common Criteria

Dr. Helmbrecht L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 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 Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security 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 Federal Office for Information Security (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 Federal Office for Information Security (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

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

---

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Federal Office for Information Security (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 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, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003.

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 products Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller have undergone the certification procedure at BSI.

The evaluation of the products Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller was conducted by T-Systems GEI GmbH, Prüfstelle für IT-Sicherheit. The T-Systems GEI GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, and vendor and distributor is:

Philips Semiconductors GmbH
Business Line Identification
P.O. Box 54 02 40
D-22502 Hamburg, Germany

The certification is concluded with

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

This work was completed by the BSI on 16 September 2004.

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-28 and D1 to D4.

The products Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller have 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 +49 228 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, 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) are the Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller. They provide a hardware platform for a smart card to run smart card applications executed by a smart card operating system.

The TOE is manufactured in the IC fabrication SSMC in Singapore (see part D, Annex A) indicated by the nameplate (on-chip identifier) T023M.

The TOE is the Philips chip P5CT072V0M resp. P5CC072V0M composed of a processing unit, security components, I/O ports, volatile and non-volatile memories (4608 Bytes RAM, 160 KBytes Application-ROM, 72 KBytes EEPROM), a Triple-DES, an AES and a FameXE co-processor and a Random number generator. Also two 16-bit Timers, an Interrupt Module, a Memory Management Unit, an UART for ISO 7816 Interface, a USB interface and an ISO 14443 contactless interface are implemented.

The USB interface and the ISO 14443 contactless interface can be deactivated before TOE delivery if requested by the customer. In this configuration the TOE has the product name P5CC072V0M.

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 Application-ROM and in the EEPROM are not part of the TOE.

The IC Dedicated Support Software consists of two parts: the Boot ROM Software being executed after each reset of the TOE and the Mifare Operating System. The Mifare Operating System software is disabled if the TOE is configured as P5CC072V0M.

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 IT products Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller were evaluated against the claims of the Security Target [6] by T-Systems GEI GmbH, Prüfstelle für IT-Sicherheit. The evaluation was completed

on 6 August 2004. The T-Systems GEI GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[8] recognised by BSI.

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

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 1: 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 Functionality

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	Source from PP or added in ST
FCS	**Cryptographic support**	
FCS_COP.1 [DES]	Cryptographic operation	ST
FCS_COP.1 [AES]	Cryptographic operation	ST
FDP	**User data protection**	
FDP_ACC.1 [MEM]	Subset access control	ST

[8] Information Technology Security Evaluation Facility

Security Functional Requirement	Identifier	Source from PP or added in ST
FDP_ACC.1 [SFR][9]	Subset access control	ST
FDP_ACF.1 [MEM]	Security Attribute based access control	ST
FDP_ACF.1 [SFR]	Security Attribute based access control	ST
FDP_IFC.1	Subset information flow control	PP
FDP_ITT.1	Basic internal transfer protection	PP
FMT	**Security Management**	
FMT_MSA.1 [MEM]	Management of security attributes	ST
FMT_MSA.1 [SFR]	Management of security attributes	ST
FMT_MSA.3 [MEM]	Static attribute initialisation	ST
FMT_MSA.3 [SFR]	Static attribute initialisation	ST
FMT_SMF.1	Specification of management functions (see also [4, AIS 32, Int065])	ST
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

Table 2: 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

[9] [SFR] here means Special Function Register

Security Functional Requirement	Identifier	Source from PP or added in ST
FMT	**Security management**	
FMT_LIM.1	Limited capabilities	PP
FMT_LIM.2	Limited availability	PP

Table 3: SFRs CC part 2 extended.

Note: Only the titles of the Security Functional Requirements are provided. For more details please refer to the Security Target [7], chapter 5.1.1.

These Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Functions	Description
F.RNG	Random Number Generator
F.HW_DES	Triple-DES Co-Processor
F.HW_AES	AES Co-Processor
F.OPC	Control of Operating Conditions
F.PHY	Protection against Physical Manipulation
F.LOG	Logical Protection
F.COMP	Protection of Mode Control
F.MEM_ACC	Memory Access Control
F.SFR_ACC	Special Function Register Access Control

Table 4: TOE Security Functions

F.RNG: Random Number Generator

The random number generator continuously produces random numbers with a length of one byte. 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). The TSF provides a hardware test functionality that can be used by the Smart Card Embedded Software to detect faults in the hardware implementing the random number generator.

F.HW_DES: Triple-DES Co-Processor

The TOE provides the Triple Data Encryption Algorithm (TDEA) of the Data Encryption Standard (DES). F.HW_DES 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.

F.HW_AES: AES Co-processor

The TOE provides the Advanced Encryption Standard (AES) algorithm of the Advanced Encryption Standard. F.HW_AES is a modular basic cryptographic function which provides the AES algorithm as defined by FIPS PUB 197 [18] by means of a hardware co-processor and supports the AES algorithm with three different key lengths of 128, 192 or 256 bit.

F.OPC: Control of Operating Conditions

The function F.OPC ensures the correct operation of the TOE (functions offered by the micro controller including the standard CPU as well as the Triple-DES co-processor, AES co-processor, the arithmetic co-processor, the memories, registers, I/O interface and the other system peripherals) during the execution of the IC Dedicated Support Software and Smart Card Embedded Software. This includes all specific security features of the TOE which are able to provide an active response.

F.OPC filters the power supply and the clock input. 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. In addition, light sensors are provided to detect specific attacks and the specific range of the stack pointer is controlled.

Before TOE delivery the Test Mode is disabled. In all other modes except the Test Mode the TOE enables the sensors automatically when operated. Furthermore the TOE prevents that the Smart Card Embedded Software 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 Software in the ROM, (iii) the Smart Card Embedded Software in the ROM and the EEPROM, (iv) the application data in the EEPROM and RAM including the configuration data in the security row. It also protects User Data or TSF data against disclosure by physical probing when stored or while being processed by the TOE.

F.LOG: Logical Protection

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 Smart Card Embedded Software. Thereby this security function prevents the disclosure of User Data or TSF data stored and/or processed in the smart card 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 that the calculation time is independent from any key and plain/cipher text.

The AES co-processor includes special features to prevent SPA/DPA analysis of shape and amplitude of the power consumption and ensures that the calculation time is with respect to the key length independent from any plain/cipher text.

The FameXE co-processor provides measures to prevent timing attacks on basic modular function. In addition special features are included to provide limitations of the capability for the analysis of shape and amplitude of the power consumption. Of course the FameXE does not realise an algorithm on its own and algorithm-specific leakage countermeasures have to be added for the FameXE.

Additional features that can be configured by the Smartcard Embedded Software comprise (i) the FameXE HIGHSEC mode and (ii) several clock configurations to support resistance against leakage 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 CPU mode for (i) Boot Mode, (ii) Test Mode and (iii) Mifare Mode. This includes the protection of electronic fuses stored in a protected memory area, the so-called “Security Row”, and the possibility to store initialisation or pre-personalisation data in the so-called “FabKey Area”.

The control of the CPU mode according to Boot Mode, Test Mode and Mifare Mode prevents the abuse of test functions after TOE delivery. Additionally it also ensures that features used at boot time to configure the TOE can not be abused.

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 Smart Card Embedded Software in the EEPROM. The security function F.COMP maintains the security domain for its own execution that protects it from interference and tampering by untrusted subjects both in the Test Mode and in the other modes. It also enforces the separation between the security domains of subjects regarding the IC Dedicated Software and the Smart Card Embedded Software.

F.MEM_ACC: Access control for code and data memory

F.MEM_ACC controls access of any subject (program code comprising processor instructions) to the memories of the TOE through the Memory Management Unit (MMU). Memory access is based on virtual addresses that are mapped to physical addresses. The CPU always uses virtual addresses. The Memory Management Unit performs the translation from virtual to physical addresses and the physical addresses are provided

from the MMU to the memory interfaces to access the memories. The access control is performed in two ways (i) Partition of the memories and (ii) Segmentation of the memory in the User Mode.

In addition F.MEM_ACC permanently checks whether the selected addresses are within the boundary of the physical implemented memory range. Access violations (i.e. access to forbidden memory addresses in User Mode) 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 controls access to the Special Function Registers and the switch between the CPU modes.

The TSF implements the access control to the Special Function Registers as specified in the Access Control Policy and the Security Functional Requirements FDP_ACC.1[SFR] and FDP_ACF.1[SFR].

F.SFR_ACC used information provided by F.MEM_ACC in order to determine access to the Special Function Registers related to hardware components. Access to all other Special Function Registers is pre-defined and cannot be changed.

Only two modes are available to the Smart Card Embedded Software, the System Mode and the User Mode. The combination of F.SFR_ACC and F.COMP ensures that the other CPU modes are not available for the Smart Card Embedded Software, but reserved for specific purposes fulfilled by the IC Dedicated Software. In addition F.MEM_ACC provides separation of the memories and access control information.

As the Test Mode is disabled before TOE delivery, all TOE Security Functions 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.

1.3 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) (see Chapter 9 of this report).

1.4 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.

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.

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) for Triple-DES encryption and decryption, AES encryption and decryption, Area based Memory Access Control, Memory separation for different software parts (including IC Dedicated Software and Smart Card Embedded Software) and Special Function Register Access Control.

Objectives are taken from the Protection Profile plus additional ones related to the additional policy.

1.5 Special configuration requirements

The Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller distinguish between five different CPU modes: Boot Mode, Test Mode, Mifare Mode, System Mode and User Mode.

As the TOE comprises the Mifare Operating System belonging to the Mifare Mode, this mode is disabled and is not accessible if the TOE is configured as P5CC072V0M. Nevertheless, the Mifare Mode is existent and security functionality with regard to the Mifare Mode is present in the TOE in this configuration, but in this case the TOE prevents that the Mifare Mode is activated and the related software is executed. Available for the developer of the Smart Card Embedded Software are the System Mode, the User Mode and in case of P5CT072V0M the Mifare Mode, too.

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, personalisation 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 [11] and chapter 10 of this report.

1.6 Assumptions about the operating environment

Since the Security Target claims conformance to the Protection Profile BSI-PP-0002-2001 [9], the assumptions defined in section 3.2 of the Protection Profile are valid for the Security Target of this TOE. 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 these assumptions from the PP:

The developer of the smart card 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 as defined for the specific application context 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.

Protection during packaging, finishing and personalisation (A.Process-Card) is assumed after TOE Delivery up to the end of phase 6, as well as during the delivery to phase 7.

The following additional assumption is assumed in the Security Target:

- Key-dependent functions shall be implemented (if applicable) in the smart card Embedded Software in a way that they are not susceptible to leakage attacks (A.Key-Function).
- The Smart Card Embedded Software must provide a function to check initialisation data. The data is defined by the customer and injected by the TOE Manufacturer into the non-volatile memory to provide the possibility for TOE identification and for traceability (A.Check-Init)

1.7 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 Philips P5CT072V0M or P5CC072V0M Secure Smart Card Controller:

No	Type	Identifier	Release	Date	Form of Delivery
1	HW	Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller (dice include reference T023M and specific EEPROM coding, see below)	V0M	T023M_plus.gds2_20040514 (GDS2 File)	Sawn Wafer or embedded in a chip card module
2	SW	Test ROM Software *(the IC dedicated test software)*	46	30 Jan. 2004	Included in Test ROM on the chip (tmfos_46.lst)
3	SW	Boot ROM Software (part of the IC Dedicated Support Software)	1.9	28 Jan. 2004	Included in Test ROM on the chip (tmfos_46.lst)
4	SW	Mifare Operating System (part of the IC Dedicated Support Software)	1.16	30 Jan. 2004	Included in Test ROM on the chip (tmfos_46.lst)[10]
5	DOC	Data Sheet, P5CT072, SmartMX, Secure Triple Interface Smart Card Controller	2.3	20 Feb. 2004	Electronic document [12]
		resp. Data Sheet, P5CC072, SmartMX, Secure Smart Card Controller	2.3	8 April 2004	Electronic document [20]
6	DOC	Instruction Set SmartMX-Family	1.0	9 May 2003	Electronic document [16]
7	DOC	Guidance, Delivery and Operation Manual for the P5CT072	1.3	28 March 2004	Electronic document [11]
8	DOC	Anomaly Sheet for P5CT072 V0M Product Behaviour	1.2	July 2004	Electronic document [17]

Table 5: Deliverables of the TOE for both, Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller

[10] Although the software is implemented on the chip it is deactivated and cannot be executed

The hardware part of the TOE is identified by Philips P5CT072V0M resp. P5CC072V0M Secure Smart Card Controller and their specific GDS-file. 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 T023M is specific for the SSMC (Singapore) production site as outlined in the guidance documentation [11]. This nameplate identifies Version V0M of the hardware, but does not identify specifically the TOE Philips P5CT072V0M resp. P5CC072V0M. For identification of a specific Philips P5CT072V0M or P5CC072V0M chip, the Device Coding Bytes stored in the EEPROM can be used (see [12, chapter 6.9.8] resp. [20, chapter 6.9.8):

- The value 11 hex in Device Coding Byte DC2 identifies the chip P5CT072
- The value 10 hex in Device Coding Byte DC2 identifies the chip P5CC072

Items 2, 3 and 4 in table 5 are not delivered as single pieces, but included in the Test ROM part of the chip. They are identified by their unique version numbers.

The delivery process from Philips to their customers (to phase 4 or phase 5 of the life cycle) guarantees, that the customer is aware of the exact versions of the different parts of the TOE as outlined above.

To ensure that the customer receives the evaluated version of the chip, either

- the customer collects the TOE himself at the Philips site Philips Semiconductors GmbH, Business Line Identification, Stresemannallee 101, 22529 Hamburg – Germany (see part D, annex A of this report) as a wafer or
- the customer collects the TOE himself at the Philips site, Philips Semiconductors (Thailand), 303 Chaengwattana Rd., Laksi Bangkok 10210, Thailand (see part D, annex A of this report) as a module or
- the TOE is sent by Philips to the customer protected by special ordering, secured transport and tracking measures. Additionally, a FabKey according to the defined FabKey-procedures has to be used to support the secure delivery and the identification of the TOE

as described [11].

TOE documentation is delivered either as hardcopy or as softcopy (encrypted) according to defined mailing procedures.

To ensure that the customer receives this evaluated version, the delivery procedures described in [11] have to be followed.

Defined procedures at the development and production sites guarantee that the right versions of the Test ROM Software, Boot ROM Software and Mifare Operating System are implemented into a specific ROM mask for a TOE IC.

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 symmetric cryptographic block cipher algorithms (Triple-DES and AES) 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), protection against physical probing, malfunctions, 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 before TOE Delivery. This was considered as part of the evaluation under the CC assurance aspects ALC for relevant procedures and under ATE for testing.

The TOE is delivered as a hardware unit at the end of the chip manufacturing process (phase 3 of the life cycle defined) or at the end of the IC packaging into modules (phase 4 of the life cycle defined). At these specific points in time the ROM part of the operating system software is already stored in the ROM of the chip and the test mode is completely 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 GmbH Business Line Identification 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 9.2 of this report.

The full evaluation results are applicable for chips from the IC fabrication SSMC in Singapore indicated by the nameplate (on-chip identifier) T023M.

5 Architectural Information

The Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller are integrated circuits (IC) providing a hardware platform to a smart card operating system and Smart Card Embedded Software. A top level block diagram including an overview 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 P5CT072V0M and P5CC072V0M Secure Smart Card Controller can be found in the Data Sheet, P5CT072, SmartMX, Secure Triple Interface Smart Card Controller [12] resp. Data Sheet, P5CC072, SmartMX, Secure Smart Card Controller [20] and Instruction Set SmartMX-Family [16].

For the implementation of the TOE Security Functions basically the components 8-bit CPU, Special Function Registers, Triple-DES Co-Processor, AES Co-Processor, FameXE Co-Processor, Random Number Generator (RNG), Power Module with Security Sensors and Filters are used. The CPU is equipped with a Memory Management Unit and provides different CPU modes in order to separate different applications running on the TOE. Security measures for physical protection are realised within the layout of the whole circuitry.

The Special Function Registers provide the interface to the security functions of the TOE.

The Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller provide different levels of access control to the SFR with the different CPU modes and additional – configurable – access control to Special Function Registers in the least-privileged CPU Mode, the User Mode.

The FameXE does not provide a cryptographic algorithm itself. The modular arithmetic functions are suitable to implement different asymmetric cryptographic algorithms.

The TOE executes the IC Dedicated Support Software (Boot Software) during the start up to configure and initialise the hardware. This software is executed in the Boot Mode that is not accessible after the start up is finished.

For the P5CT072V0M, the Mifare Operating System supports the functions to exchange data in the contactless mode with other Mifare components. The Mifare Operating System is executed in the Mifare Mode to ensure a strict separation between IC Dedicated Support Software and Smart Card Embedded Software. Based on the partitioning of the memories the Mifare Operating System is not able to access the Smart Card Embedded Software and the data stored in the EEPROM area that is not reserved for the Mifare Operating System. In the same way the access to the program and the data of the Mifare Operating System is denied for the Smart Card Embedded Software. A limited memory area for the data exchange (between Smart Card Embedded Software and Mifare Operating System) and the access to components of the hardware (by the Mifare Operating System) must be configured by the Smart Card Embedded Software.

6 Documentation

The following documentation is provided with the product by the developer to the customer for secure usage of the TOE in accordance with the Security Target:

For both, Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller

- The Guidance, Delivery and Operation Manual [11],
- Instruction set [16]
- The ETR-lite [10] and
- Anomaly Sheet [17]

For Philips P5CT072V0M resp. P5CC072V0M Secure Smart Card Controller

- The Data Sheet [12] for the P5CT072V0M
- The Data Sheet [20] for the P5CC072V0M

Additional guidance as outlined in chapter 10 of this report has to be followed.

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 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 can be divided into the following categories:

1. technology development tests as the earliest tests to check the technology against the specification and to get the technology parameters used in simulations of the circuitry;
2. tests which are performed in a simulation environment with different tools for the analogue parts and for the digital parts of the TOE;
3. regression tests which are performed for the IC Dedicated Test Software and for the IC Dedicated Support Software on emulator versions of the TOE and within a software simulation of chip in special hardware;
4. characterisation and verification tests to release the TOE to production:
   - used to determine the behaviour of the chip with respect to different operating conditions and varied process parameters
   - special verification tests for Security Functions which were done with samples of the TOE and which include also layout tests by automatic means and optical control, in order to verify statements concerning the layout;
5. functional production tests, which are done for every chip to check its correct functionality as a last step of the production process (phase 3 or phase 4 depending on the TOE delivery form).

The developer tests cover all Security Functions and all security mechanisms as identified in the functional specification and in the high and low level designs. Chips from IC fabrication SSMC in Singapore were used for tests.

The evaluators were able to repeat the tests of the developer either using the library of programs, tools and prepared chip samples 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. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections both in design data and on the final product.

The evaluation provides evidence that the actual version of the TOE provides the Security Functions as specified by the developer. 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 planned based on the analysis results and performed for the underlying mechanisms of Security Functions using bespoke equipment and expert know-how. The penetration tests considered both the physical tampering of the TOE and attacks which do not modify the TOE physically (i.e. side channel testing).

8 Evaluated Configuration

The TOE is identified by Philips P5CT072V0M and P5CC072V0M both with the nameplates T023M and specific EEPROM coding as outlined above.

There are two major configuration options, denoted by different product names. The product with the name P5CT072V0M is equipped with all three interfaces (ISO 7816, USB and contact-less). The product with the name P5CC072V0M is equipped only with the ISO 7816 interface. The USB and the contact-less interface are deactivated in this configuration.

Both major configurations of the TOE support further configuration options as outlined in the Security Target [6] chapter 2.2. All TSF are active and usable. Information on how to use the TOE and its security functions by the software is provided within the user documentation.

The Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller distinguish between five different CPU modes: Boot Mode, Test Mode, Mifare Mode, System Mode and User Mode.

As the TOE comprises the Mifare Operating System belonging to the Mifare Mode, this mode is disabled in the Philips P5CC072V0M and is not accessible.

As the TOE operates after delivery in System Mode or User Mode and the application software being executed on the TOE can not use the Test Mode, the evaluation was mainly performed in the System Mode and User Mode. For all evaluation activities performed in Test Mode, there was a rationale why the results are valid for the System Mode and User Mode, too.

9 Results of the Evaluation

9.1 Evaluation of the TOE

The Evaluation Technical Report (ETR) [8], was provided by the ITSEF T-Systems GEI GmbH, Prüfstelle für IT-Sicherheit, 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 co-ordination with the Certification Body (see [4, AIS 34]). For smart card IC specific methodology the CC supporting documents

(i) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smartcards and

(iii) ETR-lite – for Composition and
ETR-lite – for Composition: Annex A Composite smartcard evaluation: Recommended best practice

(see [4, AIS 25, AIS 26 and AIS 36]) and [4, AIS 31] (*Functionality classes and evaluation methodology for physical random number generators)* 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

Assurance classes and components		**Verdict**
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 is conform to the Smartcard IC Platform Protection Profile, BSI-PP-0002-2001 [9]
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL5 augmented by ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function:
  - F.RNG (random number generator), according to AIS 31 Functionality class P2 High,
  - F.LOG (Logical Protection) contributing to the leakage attacks especially for F.HW_DES (Triple-DES Co-processor) by SPA/DPA countermeasures.
  - F.LOG (Logical Protection) contributing to the leakage attacks especially for F.HW_AES (AES Co-processor) by SPA/DPA countermeasures together with the guidance given in Guidance, Delivery and Operation Manual [11].

  The scheme interpretations AIS 26 and AIS 31 (see [4]) were used.

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 holds for the TOE Security Function F.HW_DES (Triple-DES Co-processor) used for Triple-DES encryption and decryption and the TOE Security Function F.HW_AES (AES Co-processor) used for AES encryption and decryption.

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

The code in the Test ROM of the TOE (IC Dedicated Test Software) is used by the TOE manufacturer to check the chip function before TOE delivery. This was considered as part of the evaluation under the CC assurance aspects ALC for relevant procedures and under ATE for testing.

The full evaluation results are applicable for chips from the IC fabrication SSMC in Singapore (see part D, Annex A) indicated by the nameplate (on-chip identifier) T023M and the firmware and software versions as indicated in table 5.

The validity can be extended to new versions and releases of the product or to 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

- 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 the ETR-lite [10] 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 GmbH, Business Line Identification has implemented procedures to provide a customer product related configuration list based on the configuration list [15] 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.

- 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 [11], Data Sheet [12] resp. Data Sheet [20], Instruction set [16] and Anomaly Sheet [17] 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), the ETR-lite for composition [10] resulting from this evaluation is of importance and shall be given to the succeeding evaluation according to AIS 36.

3. For the fulfilment of the Strength of Function "high" for the Random Number Generator according to [4, AIS31] the following guidance is to be followed in addition:

   The defined online tests of the random number generator must detect all possible defects of the random number generator that lead to a significantly reduced quality of the random numbers. Due to physical defects within the random number generator the quality of the random numbers can be reduced. The requirements are not associated with any attack since the components of the random number generator are sufficiently protected and controlled by the design. The attack potential for the manipulation of the random number generator is assessed with “High”.

   In case that the physical defect exists before the start-up of the chip it is always detected by the two test procedures described in the User Guidance (refer to section 4.1.3 in [11]).

   If the physical defect occurs during the operation of the chip a defect can detected by the FIPS PUB 140-2 tests (refer to section 4.1.3 in [11]) if this test method is implemented for the statistical tests by the Smart Card Embedded Software. This is independent from the considered failure and the internal status of the random number generator.

   If the physical defect occurs during the operation, there are circumstances where it is not detected by a "chi-squared test of goodness" (refer to section 4.1.3 in [11]) if this test method is

implemented for the statistical tests by the Smart Card Embedded Software. This is based on the asynchronous operation of the random number generator and depends on the kind of failure and the internal status of the random number generator.

The "chi-squared test of goodness" can be extended to detect all considered defects. In addition to the result of the "chi-squared test of goodness" it must be checked whether two or more of the possible sixteen 4 bit tuples do not occur in the tested sequence. In other words, if at least two of the f[i] values in the formula given in section 4.1.3 of [11] are zero, the test fails. If this check detects at least two missing 4 bit tuples the test must be considered as fail and a repetition is required. The repetition of the tests is described in section 4.1.4 of [11].

4. For guidance and limitations on how to use the Triple-DES co-processor resp. AES co-processor in the context of high resistance against SPA/DPA for both, Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller, see Guidance, Delivery and Operation Manual for the P5CT072 [11, section 4.2.3 for Triple-DES resp. section 4.3.2 for AES].

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 [7] of the Target of Evaluation (TOE) is provided within a separate document. It is a sanitised version of the complete Security Target [6] used for the evaluation performed.

13 Definitions

13.1 Acronyms

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security

CC Common Criteria for IT Security Evaluation (see [1])

CPU Central Processing Unit

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
UART	Universal Asynchronous Receiver and Transmitter

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.

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)

[4] Application Notes and Interpretations of the Scheme (AIS), Bundesamt für Sicherheit in der Informationstechnik, Bonn, as relevant for the TOE, specifically

- AIS 25, Version 2, 29 July 2002 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 1.2, July 2002
- AIS 26, Version 2, 6 August 2002 for: CC Supporting Document, - Application of Attack Potential to Smartcards, Version 1.1, July 2002
- AIS 31, Version 1, 25 Sept. 2001 for: Functionality classes and evaluation methodology of physical random number generators
- AIS 32, Version 1, 02 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungs-schema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 36, Version 1, 29 July 2002 for: CC Supporting Document, ETR-lite for Composition, Version 1.1, July 2002 and CC Supporting Document, ETR-lite for Composition: Annex A Composite smartcard evaluation, Version 1.2 March 2002

[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-0227, Version 1.2, 28 April 2004, Evaluation of Philips P5CT072V0M Secure Smart Card Controller, Philips Semiconductors (confidential document)

[7] Security Target Lite BSI-DSZ-CC-0227, Version 1.0, 14 May 2004, Evaluation of Philips P5CT072V0M Secure Smart Card Controller, Philips Semiconductors (sanitised public document)

[8] Evaluation Technical Report, Philips P5CT072V0M Secure Smart Card Controller, Version 1.0, 5 Aug. 2004 (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] ETR-lite for Composition, according to AIS 36, Version 1.0, 5 Aug. 2004 for Philips P5CT072V0M Secure Smart Card Controller (confidential document)

[11] Guidance, Delivery and Operation Manual for the P5CT072, BSI-DSZ-CC-0227, Version 1.3, Philips Semiconductors, 28 March 2004 (confidential document)

[12] Data Sheet, P5CT072, SmartMX, Secure Triple Interface Smart Card Controller, Preliminary Specification, Philips Semiconductors, Revision 2.3, 20 Feb. 2004 (confidential document)

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

[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, BSI-DSZ-CC-0227, Version 1.2, 24 June 2004, Evaluation of the Philips P5CT072V0M Secure Smart Card Controller, Philips Semiconductors, Business Line Identification (confidential document)

[16] Instruction Set SmartMX-Family, Secure Smart Card Controller, Objective Specification, Philips Semiconductors, Revision 1.0, 9 May 2003

[17] Anomaly Sheet for P5CT072 V0M Product Behaviour, Philips Semiconductors, Revision 1.2, Date July 2004

[18] FIPS PUB 197 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology, 26 Nov. 2001

[19] Order Entry Form, P5CC072, Release 1.8, 2004-04-06, Philips Semiconductors Hamburg

[20] Data Sheet, P5CC072, SmartMX, Secure Smart Card Controller, Preliminary Specification, Philips Semiconductors, Revision 2.3, 8 April 2004 (confidential document)

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

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

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

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

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 inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

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

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

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

Table 6.1 - Evaluation assurance level summary“

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

„Objectives

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

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

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

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

„Objectives

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

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

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

„Objectives

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

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

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

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous,

do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

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

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

„Objectives

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

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

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

„Objectives

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

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

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

„Objectives

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

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

AVA_SOF Strength of TOE security functions

„Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

„Objectives

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

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

„Application notes

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

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

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-0227-2004

Evaluation results regarding development and production environment

The IT products, Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller (Target of Evaluation, TOE) have 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) and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

As a result of the TOE certification, dated 16 September 2004, 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),**

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

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

(b) **Philips Semiconductors GmbH, Assembly and Test Organisation Hamburg Stresemannallee 101, 22529 Hamburg, Germany**

(c) **Philips Semiconductors (Thailand), 303 Chaengwattana Rd., Laksi Bangkok 10210, Thailand (assembly)**

(d) **Philips Semiconductors GmbH, Business Line Identification, Document Control Office, Mikron-Weg 1, 8101 Gratkorn, Austria**

(e) **Systems on Silicon Manufacturing Co. Pte. Ltd. 8 (SSMC), 70 Pasir Ris Drive 1, Singapore 519527, Singapore (semiconductor factory)**

(f) **Photronics Singapore Pte. Ltd., 6 Loyang Way 2, Loyang Industrial Park, Singapore 507099, Singapore (mask shop)**

(g) **Photronics Semiconductors Mask Corp. (PSMC), 1F, No.2, Li-Hsin Rd., Science-Based Industrial Park, Hsin-Chu City Taiwan R.O.C. (mask shop)**

The TOE is manufactured in the IC fabrication SSMC in Singapore indicated by the nameplate (on-chip identifier) T023M.

For all sites listed above, the requirements have been specifically applied for each site and in accordance with the Security Target BSI-DSZ-CC-0227, Version 1.2, 28 April 2004, Evaluation of Philips P5CT072V0M Secure Smart Card Controller [6]. The evaluators verified, that the threats are countered and the security objectives 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 are fulfilled by the procedures of these sites.

This page is intentionally left blank.