Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0368-2006

for

Philips P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software

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

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0368-2006

Philips P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software

from

Philips Semiconductors GmbH
Business Line Identification

Common Criteria Arrangement for components up to EAL4

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, EAL4 / augmented by** ADV_IMP.2 (Development - Implementation of the TSF), ALC_DVS.2 (Life cycle support - Sufficiency of security measures), ATE_DPT.2 (Testing - Low-level design), 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, 13. March 2006

The Vice President of the Federal Office
for Information Security

Hange L.S.

IT Security Certified

SOGIS - MRA

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 (AIS 34)

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 Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 22 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, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

This evaluation contains the components ADV_IMP.2 (Implementation of the TSF), ALC_DVS.2 (Life cycle support - Sufficiency of security measures), ATE_DPT.2 (Testing - Low-level design), AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states), AVA_VLA.4 (Vulnerability assessment - Highly resistant) that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4-components of these assurance families are relevant.

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 P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0296-2006. For this evaluation specific results from the evaluation process based on BSI-DSZ-CC-0296-2006 were re-used.

The evaluation of the product Philips P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software 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, 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 13. March 2006.

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-26 and D1 to D-4.

The product Philips P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software 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 +49 228 9582-111.

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) and subject of the Security Target (ST) [6] and [7] is the Philips P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software.

The evaluation of the TOE was conducted as a composition evaluation making use of the platform evaluation results of the CC evaluation of the underlying semiconductor.

Therefore, the Target of Evaluation (TOE) consists of a hardware part and a software part. The hardware part consists of the Philips P5CC036V1D Secure Smart Card Controller with IC Dedicated Software stored in the Test-ROM that is not accessible in the System Mode or the User Mode after Phase 3. There is dedicated documentation regarding the hardware. The additional IC Dedicated Support Software “Secured Crypto Library on the P5CC036V1D” consists of a software library and associated documentation. The Secured Crypto Library provides cryptographic functions that can be operated on the hardware platform as described in the Security Target lite [7].

Therefore, the TOE comprises the following components:

- Integrated Circuit (IC) "Philips P5CC036V1D with specific IC Dedicated Software Secure Smart Card Controller" provided by Philips Semiconductors GmbH (separately certified under the ID: BSI-DSZ-CC-0293-2005 [11])
- Secured Crypto Library on the P5CC036V1D.

The Hardware Security Target [10] contains an introduction about the SmartMX hardware TOE that is considered in this composite evaluation. The P5CC036V1D covers IC Dedicated Software stored in the ROM provided with the SmartMX hardware platform.

The IC Dedicated Support Software “Secured Crypto Library on the P5CC036V1D“ is a cryptographic library which provides a set of cryptographic functions that can be used by a Smartcard Embedded Software. The cryptographic library consists of several binary packages that must be linked to the Smartcard Embedded Software. The Philips SmartMX smart card processor P5CC036V1D provides the computing platform and the cryptographic support by means of co-processors for the Secured Crypto Library on the P5CC036V1D. The used parts of the Secured Crypto Library on the P5CC036V1D are linked to the Smartcard Embedded Software during the development process and implemented with the Smartcard Embedded Software in the User ROM.

The TOE can be described by using the following three layers:

1. The Protection Profile “Smartcard IC Platform Protection Profile (SSVG-PP), Version 1.0, July 2001; reference BSI-PP-0002-2001” [9] describes general requirements for smart card controllers and their support software. It is a

common basis for smart card platform evaluations and defines the minimum requirements to the TOE hardware and the associated functionality.

2. The Hardware Security Target [10] defines the functionality of the platform provided by the P5CC036V1D Smart Card Controller. It comprises the specific hardware features of this platform.
3. The Secured Crypto Library on the P5CC036V1D provides additional functionality to the developer of Smartcard Embedded Software. It is a supplement of the basic cryptographic features provided by the hardware platform. The Crypto Library on SmartMX implements cryptographic algorithms with countermeasures against the attacks described in this Security Target using the co-processors of the P5CC036V1D to provide a software programming interface for the developer of the Smartcard Embedded Software.

The hardware part of the TOE is not described here in detail. For more details please read the Hardware Security Target [10].

The IT product Philips P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software was evaluated by T-Systems GEI GmbH, Prüfstelle für IT-Sicherheit. The evaluation was completed on 03. February 2006. The T-Systems GEI GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[7] recognised by BSI.

The concept for composition as outlined in CC Supporting Document [4, AIS 36] was used.

The sponsor, vendor, and distributor is

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

This certification is a re-certification of the composition TOE with crypto library certified under the certification ID “BSI-DSZ-CC-0296” (see [27]). The only change is an additional augmentation of the EAL level (ATE_DPT.1 augmented to ATE_DPT.2). The TOE itself remains completely the same in both processes. The additional augmentation has only an effect on the documention relevant for the evaluation.

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 Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented). The following table shows the augmented assurance components.

[7] Information Technology Security Evaluation Facility

Requirement	Identifier
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+: ADV_IMP.2	Development – Implementation of the TSF
+: ALC_DVS.2	Life cycle support – Sufficiency of security measures
+: ATE_DPT.2	Testing - Low-level design
+: AVA_MSU.3	Vulnerability assessment - Analysis and testing for insecure states
+: AVA_VLA.4	Vulnerability assessment - Highly resistant

Table 1: Augmented assurance components

1.2 Functionality

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

The following SFRs are taken from CC part 2:

Security Functional Requirement	Addressed issue
FAU	**Security audit**
FAU_SAS.1	Audit storage
FCS	**Cryptographic support**
FCS_COP.1[DES]	Cryptographic operation (DES)
FCS_COP.1[SW-DES]	Cryptographic operation (TDES)
FCS_COP.1 [RSA]	Cryptographic operation (RSA)
FCS_COP.1.1[SHA-1]	Cryptographic operation (SHA-1)
FCS_CKM.1.1	Cryptographic key generation
FCS_RND.1	Quality metric for random numbers (hardware (true) RNG)
FCS_RND.2	Random number generation (software (pseudo) RNG)
FDP	**User data protection**
FDP_ACC.1[MEM]	Subset access control
FDP_ACC.1[SFR]	Subset access control
FDP_ACF.1[MEM]	Security Attribute based access control
FDP_ACF.1[SFR]	Security Attribute based access control
FDP_IFC.1	Subset information flow control
FDP_ITT.1	Basic internal transfer protection
FDP_ITT.1 [COPY]	Basic internal TSF data transfer

Security Functional Requirement	Addressed issue
	protection
FDP_RIP.1	Subset residual information protection
FMT	**Security Management**
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FMT_MSA.1[MEM]	Management of security attributes
FMT_MSA.1[SFR]	Management of security attributes
FMT_MSA.3[MEM]	Static attribute initialisation
FMT_MSA.3[SFR]	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FPT	**Protection of the TOE Security Functions**
FPT_FLS.1	Failure with preservation of secure state
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_ITT.1 [COPY]	Basic internal TSF data transfer protection
FPT_PHP.3	Resistance to physical attack
FPT_SEP.1	TSF domain separation
FPT_TST.2	Subset TOE security testing
FRU	**Resource Utilistaion**
FRU_FLT.2	Limited fault tolerance

Table 2: SFRs for the TOE taken from CC Part 2

Only the titles of the Security Functional Requirements are provided. For more details please refer to the Security Target Lite [7], chapter 5, and the Security Target Lite [10] of the hardware platform.

Chapter 5 of the ST Lite [7] also gives information if the SFRs are defined and described in the protection profile, in the ST of the hardware, or in the ST of the composition product.

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

TOE Security Function	Addressed issue
F.RNG	Hardware Random Number Generator
F.HW_DES	Hardware Triple-DES Co-processor
F.OPC	Control of Operating Conditions
F.PHY	Protection against Physical Manipulation

TOE Security Function	Addressed issue
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 3: TOE Security Functions of the IC part of the TOE

Only the titles of the TOE Security Functions are provided. For more details please read the Security Target Lite of the hardware platform [10], chapter 6.

TOE Security Function	Addressed issue
F.RNG_Access	Software generation of random numbers and test functionality for hardware RNG
F.DES	DES and TDES encryption and decryption in ECB, “outer” CBC and CBC-MAC mode
F.RSA	RSA and RSA-CRT algorithms (DFA-resistant and non-resistant variants)
F.RSA_KeyGen	Key generation for the RSA (both modes RSA and RSA-CRT)
F.SHA-1	Computation of secure hash algorithm SHA-1
F.LOG	Extends the F.LOG of hardware part of the TOE and provides in addition protection against side channel attacks and forced leakage attacks for the additional functionality F.DES, F.RSA, F.RSA_KeyGen, F-SHA.1
F.COPY	Provides means to copy of data resistant to side channel attacks
F.Object_Reuse	Clears memory areas used by the crypto library after the usage

Table 4: TOE Security Functions of the IC dedicated SW part of the TOE

Only the titles of the TOE Security Functions are provided. For more details please read the Security Target Lite [7], chapter 6.

1.3 Strength of Function

The TOE‘s strength of functions is rated ‘high’ (SOF-high) for those functions, identified in the Security Target lite [7], chapter 6.1.9, 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).

1.4 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 [6]:

Name	Definition
T.Leak-Inherent	Inherent Information Leakage
T.Phys-Probing	Physical Probing
T.Malfunction	Malfunction due to Environmental Stress
T.Phys-Manipulation	Physical Manipulation
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

Table 5: Threats for the TOE

In comparison to the threats outlined in the Security Target of the hardware [10], the scope of the threat T.RND is extended to include both the deficiency of hardware random numbers and the deficiency of software random numbers.

The Organisational Security Policies for the TOE are defined as:

Name	Definition
P.Process-TOE	Protection during TOE Development and Production
P.Add-Components	Additional Specific Security Components
P.Add-Func	Additional Specific Security Functionality

Table 6: OSPs

Since the Security Target claims conformance to the Protection Profile [9], the policy P.Process-TOE (Protection during TOE Development and Production) of the Protection Profile is applied in the Security Target.

One additional Organisational Security Policy is defined in the hardware Security Target. The Policy P.Add-Components (Additional Specific Security Components) is defined for Triple-DES encryption and decryption, Area based Memory Access Control, Special Function Register Access Control, and memory separation for different software parts.

One additional Organisational Security Policy is provided by the Crypto Library for use by the Smardcard Embedded Software. The Policy P.Add-Func (Additional Specific Security Functionality) is defined for Triple-DES encryption and decryption, RSA and RSA-CRT algorithm, RSA key generation, SHA-1 Hash Algorithm, access to the RNG (implementation of a software RNG and tests for the hardware RNG), secure copy routine, protection of residual information, and resistance against side channel attacks.

For more details please refer to the Security Target lite [7], chapters 3.3 and 3.4.

1.5 Special configuration requirements

The IC Dedicated Support Software as part of the TOE provides an interface between the smart card hardware (P5CC036V1D) and a smart card operating system or smart card application for the usage of the cryptographic functions provided by the TOE. It uses the specific functionality of the hardware to provide these cryptographic services.

The considered configuration of the Secured Crypto Library on the P5CC036V1D assumes that the crypto library is executed in System Mode. In addition the following Compiler Options are required:

- Memory Model: Large
- Code ROM size: huge

The Embedded Software developer has to be aware that no restrictions regarding the access to the memory and to Special Function Registers are available in the System Mode.

For performance reasons, specific checks on the input data have to be performed by the Smartcard Embedded Software before the crypto library is called. Details are described in the User Guidance [12] - [17].

These crypto functions are supplied as a library rather than as a monolithic program and hence a user of the library may include those functions he requires – it is not necessary to include all cryptographic functions of the library in every Smartcard Embedded Software. Details are described in the User Guidance [12].

In addition to the above, 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.

For other recommendations please read chapter 10 of this Report.

1.6 Assumptions about the operating environment

Since the Security Target claims conformance to the Protection Profile [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 assumptions are assumed in the Security Target of the HW chip:

- 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).

The following additional assumption is assumed in the Security Target of the composition [7]:

Operational preconditions (A.Preconditions):

- In case that resistance of the SHA-1 implementation against side channel attacks is required, the Smartcard Embedded Software developer shall ensure that the necessary operational preconditions are met.
- For the RSA-CRT there exist two algorithms. Only one of them provides built-in resistance against DFA attacks. When using the second algorithm, it is assumed that the user of the Secured Crypto Library on the P5CC036V1D first analyses and decides whether DFA attacks are applicable in the specific field of application, and that he implements effective DFA countermeasures on his own, if necessary.

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 Federal Office for Information Security (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 Target of Evaluation (TOE) is called:

Philips P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
1	Hard-ware	Philips P5CC036V1D Secure Smart Card Controller	V1D	T503D.gds 2_20040915	wafer (dice include reference T503D)
2	Soft-ware	Test ROM Software (the IC Dedicated Test Software)	1.4	August 16th, 2004	Test ROM on the chip (tmfos.lst, V1.4)
3	Soft-ware	Boot ROM Software (boot.asm, part of the IC Dedicated Support Software)	1.7	March 9th, 2004	Test ROM on the chip (tmfos.lst, V1.4)
4	Docu-ment	Data Sheet: SmartMX - P5CC036, [18]	3.3	27.06.2005	electronic document
5	Docu-ment	Instruction Set SmartMX-Family, [19]	1.0	09.05.2003	electronic document
6	Docu-ment	Guidance, Delivery and Operation Manual: P5CC036V1D, [20]	1.0	23.03.2005	electronic document
7	Soft-ware	Secured Crypto Library on the P5CC036V1D Pseudo Random Number Generator	2.0	n/a (cf. MD5 checksum)	binary library file(s) plus the required header file(s), on CD or electronically
8	Soft-ware	Secured Crypto Library on the P5CC036V1D Secured DES Library	1.0	n/a (cf. MD5 checksum)	binary library file(s) plus the required header file(s), on CD or electronically
9	Soft-ware	Secured Crypto Library on the P5CC036V1D Secured RSA Library	2.0	n/a (cf. MD5 checksum)	binary library file(s) plus the required header file(s), on CD or electronically
10	Soft-ware	Secured Crypto Library on the P5CC036V1D Secured RSA Key Generation Library	2.0	n/a (cf. MD5 checksum)	binary library file(s) plus the required header file(s), on CD or electronically
11	Soft-ware	Secured Crypto Library on the P5CC036V1D SHA-1 Library	2.0	n/a (cf. MD5 checksum)	binary library file(s) plus the required header file(s), on CD or electronically

No	Type	Identifier	Release	Date	Form of Delivery
12	Document	Secured Crypto Library on the P5CC036V1D, User Guidance [12]	2.0	23.11.2005	printed on paper, or electronically with the crypto library
13	Document	User Guidance: Crypto Library on SmartMX – Pseudo Random Number Generator and Chi-Squared Test Library [13]	3.0	23.11.2005	printed on paper, or electronically with the crypto library
14	Document	User Guidance: Crypto Library on SmartMX – Secured DES Library [14]	2.0	23.11.2005	printed on paper, or electronically with the crypto library
15	Document	User Guidance: Crypto Library on SmartMX – SHA-1 Library [15]	3.0	23.11.2005	printed on paper, or electronically with the crypto library
16	Document	User Guidance: Crypto Library on SmartMX – Secured RSA Library [16]	3.0	23.11.2005	printed on paper, or electronically with the crypto library
17	Document	User Guidance: Crypto Library on SmartMX – Secured RSA Key Generation Library [17]	3.0	23.11.2005	printed on paper, or electronically with the crypto library
18	Document	Software Delivery Description, Secured DES Library, [21]	1.0	23.11.2005	electronically with the crypto library
19	Document	Software Delivery Description, SHA-1 Library, [22]	1.0	23.11.2005	electronically with the crypto library
20	Document	Software Delivery Description, Secured Random Number Library, [23]	1.0	23.11.2005	electronically with the crypto library
21	Document	Software Delivery Description, Secured RSA Library, [24]	1.0	23.11.2005	electronically with the crypto library
22	Document	Software Delivery Description, Secured RSA Key Generation Library, [25]	1.0	23.11.2005	electronically with the crypto library

Table 7: Deliverables of the TOE

The hardware part of the TOE is identified as Philips P5CC036V1D with specific IC Dedicated Software 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. The nameplate T503D is specific for the SSMC (Singapore) production site as outlined in the guidance documentation of the chip. This nameplate identifies Version V1D of the hardware. For identification of the P5CC036V1D, the Device Coding Bytes stored in the EEPROM can be used. The value “0E” hex in Device Coding Byte DC2 identifies the chip P5CC036V1D. For more details about the hardware identification please read [11].

To ensure that the customer receives this evaluated version, the delivery procedures described in [20] 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 generator. Additionally, a combination of software and hardware parts of the TOE implement several cryptographic functions to be used by the smart card embedded software.

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 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 a composition evaluation of the present TOE and the future operating system and smart card application is important. Within the present 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 future 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 of this report.

The evaluation results are applicable for chips from the IC fabrication SSMC in Singapore indicated by the nameplate (on-chip identifier) T503D.

The Security Target of the composition [7] also specifies an assumption that defines the operational preconditions that a Smartcard Embedded Software developer and user of the Secured Crypto Library on the P5CC036V1D has to fulfil (A.Preconditions, see also chapter 1.6 of this report).

5 Architectural Information

The TOE is called “Philips P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software.” It is a composite TOE, consisting of the hardware “Philips SmartMX P5CC036V1D Secure Smart Card Controller,” which is used as the evaluated platform, and the “Secured Crypto Library on the P5CC036V1D,” which is built upon this platform.

The hardware covers the IC Dedicated Software stored in the ROM provided with the SmartMX hardware platform.

The IC Dedicated Support Software “Secured Crypto Library on the P5CC036V1D“ is a cryptographic library which provides a set of cryptographic functions that can be used by the Smartcard Embedded Software. The cryptographic library consists of several binary packages that must be linked to the Smartcard Embedded Software. The Philips SmartMX smart card processor P5CC036V1D provides the computing platform and the cryptographic support by means of co-processors for the Secured Crypto Library on the P5CC036V1D. The used parts of the Secured Crypto Library on the P5CC036V1D are linked to the Smartcard Embedded Software during the development process and implemented with the Smartcard Embedded Software in the User ROM.

The additional IC Dedicated Support Software “Secured Crypto Library on the P5CC036V1D“ is part of the present composite TOE. It provides cryptographic support for the Philips P5CC036V1D smart card processor. The IC Dedicated Support Software as part of the TOE provides an interface between the smart card hardware and a future smart card operating system or smart card application that use the cryptographic functions provided by the TOE. The IC Dedicated Support Software uses the specific functionality of the hardware to provide these cryptographic services.

6 Documentation

The following documentation is provided with the product by the developer to the customer (see also table 7 of this report):

- Data Sheet: SmartMX - P5CC036, 3.3, 27.06.2005 [18]
- Instruction Set SmartMX-Family, 1.0, 09.05.2003 [19]
- Guidance, Delivery and Operation Manual: P5CC036V1D, 1.0, 23.03.2005 [20]
- Secured Crypto Library on the P5CC036V1D, User Guidance 2.0, 23.11.2005 [12]
- User Guidance: Crypto Library on SmartMX – Pseudo Random Number Generator and Chi-Squared Test Library, 3.0, 23.11.2005 [13]
- User Guidance: Crypto Library on SmartMX – Secured DES Library, 2.0, 23.11.2005 [14]
- User Guidance: Crypto Library on SmartMX – SHA-1 Library, 3.0, 23.11.2005 [15]
- User Guidance: Crypto Library on SmartMX – Secured RSA Library, 3.0, 23.11.2005 [16]
- User Guidance: Crypto Library on SmartMX – Secured RSA Key Generation Library, 3.0, 23.11.2005 [17]
- Software Delivery Description, Secured DES Library, 1.0, 23.11.2005 [21]
- Software Delivery Description, SHA-1 Library, 1.0, 23.11.2005 [22]
- Software Delivery Description, Secured Random Number Library, 1.0, 23.11.2005 [23]
- Software Delivery Description, Secured RSA Library, 1.0, 23.11.2005 [24]
- Software Delivery Description, Secured RSA Key Generation Library, 1.0, 23.11.2005 [25]

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 the hardware computing platform with a crypto library that provides cryptographic support. The documents will be used by the customer to implement the software (operating system / application software) and to integrate the required parts of the Secured Crypto Library.

The ETR-lite of this evaluation will be available for a future composite evaluation on the base of this TOE. It is intended to provide the results of this evaluation in a way that meets the requirements for a composite evaluation as defined in AIS 36 [4].

7 IT Product Testing

For Information on testing of the IC part of the TOE, please read the Certification Report BSI-DSZ-CC-0293-2005 [11].

Developer Tests:

Tests on functionality and memory leakage have been performed by the developer to the farthest possible extend using specialised automatic test software.

The TOE consists of a Secured Crypto Library on the P5CC036V1D as IC dedicated Software. Therefore the test environment is based on a smart card reader connected to a PC.

The performed Test Sequences describe real test scenarios. In a test sequence all necessary commands are collected to build up the special environment of the test case, the preparation for the particular function call is done and the particular function is called in conjunction with the expected return code.

The testing concentrates on the interfaces, the subsystems, and the modules of the TOE security functions as identified and described in the functional specification, the high level design and the low level design. The functions are called with different parameters and different sets of option bits. In addition, many standard tests from NIST are used showing the correctness of the implemented algorithms.

Manual checks which cannot be performed in an automated manner are described with sufficient detail to cover all aspects of the security functions, this includes tests with an emulation of the hardware to cover the low level interfaces of the Secured Crypto Library.

Independent evaluator tests:

The evaluators repeated a carefully chosen subset of the automatic developer tests using the same test environment and test tools as the developer. The evaluators have also done additional testing for all security functions.

The developer provided many tests for each TSF. These tests have been verified and extended by the evaluators in an appropriate manner. The tests produced the expected results. This verified the correct implementation of the TSFs in the TOE. The independent testing performed by the evaluators additionally confirmed that all the TOE's security functions behave as specified in the Security Target [6] and as detailed in the developer's functional specification.

To verify and reject possible vulnerabilities, the evaluators performed penetration tests. Therefore, they took all security functions into consideration. Intensive penetration testing was performed to consider the physical tampering of the TOE using highly sophisticated equipment and expertise know how. In addition non-invasive attacks like side channel analysis and fault analysis were performed during the vulnerability tests. During the evaluator's penetration testing the TOE operated as specified. The TOE withstood the penetration

efforts of attackers with high attack potential in the intended environment for the TOE.

8 Evaluated Configuration

The TOE is a composite TOE, consisting of the hardware “Philips SmartMX P5CC036V1D Secure Smart Card Controller”, which is used as the evaluated platform and the “Secured Crypto Library on the P5CC036V1D”, which is built upon this platform.

The considered configuration of the Secured Crypto Library on the P5CC036V1D assumes that the crypto library is executed in System Mode.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all 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 [4, AIS 34]).

As the evaluation of the TOE was conducted as a composition evaluation, the ETR [8] includes also the evaluation results of the composite evaluation activities in accordance with CC Supporting Document, ETR-lite for Composition: Annex A Composite smart card evaluation [4, AIS 36].

The ETR [8] builds up on the ETR-lite for Composition documents of the evaluations of the underlying hardware "Philips SmartMX P5CC036V1D Secure Smart Card Controller " (see [11]).

For smart card IC specific methodology the CC supporting documents or Joint Interpretation Library documents

- The Application of CC to Integrated Circuits
- Application of Attack Potential to Smartcards
- Integrated Circuit Hardware Evaluation Methodology and

(see [4]: AIS 25 and AIS 26), AIS 31 (Functionality classes and evaluation methodology for physical random number generators) and AIS 20 (Functionality classes and evaluation methodology for deterministic 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 EAL4 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
Problem tracking CM coverage	ACM_SCP.2	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
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Sufficiency of security measures	ALC_DVS.2	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	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

Assurance classes and components		Verdict
Vulnerability assessment	CC Class AVA	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 8: Verdicts for the assurance components

This certification is a re-certification of the composition TOE with crypto library certified under the certification ID “BSI-DSZ-CC-0296” (see [27]). The only change is an additional augmentation of the EAL level (ATE_DPT.1 augmented to ATE_DPT.2). The TOE itself remains completely the same in both processes. The additional augmentation has only an effect on the documention relevant for the evaluation.

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, EAL4 augmented by ADV_IMP.2, ALC_DVS.2, ATE_DPT.2, AVA_MSU.3, and AVA_VLA.4,
- the TOE fulfils the claimed strength of function SOF-high for the functions as outlined in chapter 1.3.
  This applies to F.LOG, F.RSA, F.RNG, and F.RNG_Access.
  Therefore the scheme interpretations AIS 20, 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 functions F.RSA, F.RSA_KeyGen, F.HW_DES, and F.DES.

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 P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software as outlined in this report and that is produced and initialised in an environment that was subject to an audit in the cause of the evaluation.

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The operational documentation (refer to chapter 6 of this report) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [6] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents.

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. Therefore, the document ETR-lite [26] was generated according to AIS 36 [4]. That document lists the results of additional evaluator actions performed to support a composite evaluation of the TOE together with a specific smart card embedded software.

Based on the life cycle model only the delivery of the TOE at the end of phase 4 is relevant. Nevertheless the interaction between phase 1 and phase 2 are also important and they are taken into account. During the evaluation dedicated tasks were performed to examine the interface between the Smartcard Embedded Software developer and the developer of the smartcard IC. These composition related actions cover the following tasks:

- The integration of the Smartcard Embedded Software in the IC manufacturer configuration management system.

  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 smartcard IC.

  This comprises also the handling of 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 are checked.

- The configuration of the TOE (mask coded bits assembled with the ROM code and different configuration pattern for the EEPROM loaded at the end of the wafer tests) according to the configuration issues described in the Security Target (refer to [10]).

- Consistency check and verification for the ROM code delivery and the data of the pre-personalisation procedures between Philips and the customer.

In addition, the separation based on the unique commercial type identifier according to test and delivery was also subject of the evaluation.

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])
DES	Data Encryption Standard; symmetric block cipher algorithm
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
GDS	Graphic Design System; Image file format used for integrated circuit masks
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NIST	National Institute of Standards & Technology
PP	Protection Profile
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, Adelmann – a public key encryption algorithm
SF	Security Function

SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SOF	Strength of Function
SSMC	Systems on Silicon Manufacturing Co. Pte. Ltd., Singapore
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.

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) as relevant for the TOE.

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

[6] Philips Semiconductors Evaluation Documentation: Secured Crypto Library on the P5CC036V1D - Security Target, Revision 2.2.0, 27.01.2006 (confidential document)

[7] Philips Semiconductors Evaluation Documentation: Secured Crypto Library on the P5CC036V1D- Security Target Lite, Version 2.2.0, 30.01.2006

[8] Evaluation Technical Report; BSI-DSZ-CC-0368; Version 1.2; Feb 9th, 2006 (confidential document)

[9] Bundesamt für Sicherheit in der Informationstechnik (BSI): Smartcard IC Platform Protection Profile (SSVG-PP), Version 1.0, July 2001; registered and certified by (BSI) under the reference BSI-PP-0002-2001

[10] Philips Semiconductors Documentation: Hardware Security Target Lite - Evaluation of the Philips P5CC036V1D, Secure Smart Card Controller, Version 1.0, 13.05.2005

[11] Certification Report BSI-DSZ-CC-0293-2005 for Philips P5CC036V1D and P5CC009V1D with specific IC Dedicated Software Secure Smart Card Controller from Philips Semiconductors GmbH, Business Line Identification, Bundesamt für Sicherheit in der Informationstechnik (BSI), 19.08.2005

[12] Philips Semiconductors User Guidance: Secured Crypto Library on the P5CC036V1D, User Guidance, Revision 2.0, November 23rd, 2005

[13] Philips Semiconductors User Guidance: Crypto Library on SmartMX – Pseudo Random Number Generator & Chi-Squared Test Library, User Guidance, Revision 3.0, November 23rd, 2005

[14] Philips Semiconductors User Guidance: Crypto Library on SmartMX – Secured DES Library, User Guidance, Revision 2.0, November 23rd, 2005

[15] Philips Semiconductors User Guidance: Crypto Library on SmartMX – SHA-1 Library, User Guidance, Revision 3.0, November 23rd, 2005

[16] Philips Semiconductors User Guidance: Crypto Library on SmartMX – Secured RSA Library, User Guidance, Revision 3.0, November 23rd, 2005

[17] Philips Semiconductors User Guidance: Crypto Library on SmartMX – Secured RSA Key Generation Library, User Guidance, Revision 3.0, November 23rd, 2005

[18] Philips Semiconductors Data Sheet: SmartMX - P5CC036 Secure Smart Card Controller, Revision 3.3, 27.06.2005, Document-ID 081733

[19] Philips Semiconductors Documentation: Instruction Set SmartMX-Family, Secure Smart Card Controller, Objective Specification, Revision 1.0, May 9th, 2003, Document Number: 084110

[20] Philips Semiconductors Guidance, Delivery and Operation Manual: P5CC036V1D - Evaluation of Philips P5CC036V1D - Secure Smart Card Controller, Revision 1.0, 23.03.2005

[21] Software Delivery Description, Secured DES Library, Delivery Module Contents, Revision 1.0, 23 November 2005, Doc.No 117110

[22] Software Delivery Description, SHA-1 Library, Delivery Module Contents, Revision 1.0, 23 November 2005, Doc.No 117510

[23] Software Delivery Description, Secured Random Number Library, Delivery Module Contents, Revision 1.0, 23 November 2005, Doc.No 117410

[24] Software Delivery Description, Secured RSA Library, Delivery Module Contents, Revision 1.0, 23 November 2005, Doc.No 117210

[25] Software Delivery Description, Secured RSA Key Generation Library, Delivery Module Contents, Revision 1.0, 23 November 2005, Doc.No 117310

[26] ETR-lite for composition according to AIS36 as summary of the Evaluation Technical Report; BSI-DSZ-CC-0368; Version 1.2; Feb 8th, 2006 (confidential document)

[27] Certification Report BSI-DSZ-CC-0296-2006 for Philips P5CC036V1D Secure Smart Card Controller with Cryptographic Libraryas IC Dedicated Support Software from Philips Semiconductors GmbH, Business Line Identification, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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: Assurance family breakdown and map

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 3: 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.“

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0368-2006

Evaluation results regarding development and production environment

The IT product Philips P5CC036V1D Secure Smart Card Controller with Cryptographic Library as IC Dedicated Support Software (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) 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 13. March 2006, 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.2),**
- **ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and**
- **ALC – Life cycle support (i.e. ALC_DVS.2, ALC_LCD.1, ALC_TAT.1),**

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

(a) **Philips Semiconductors GmbH, Business Line Identification (BL 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) T503D.

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target BSI-DSZ-CC-0296, Revision 2.0.0, 23.11.2005, Secured Crypto Library on the P5CC036V1D [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.