# Certification Report

**Bundesamt für Sicherheit in der Informationstechnik**

## BSI-DSZ-CC-0294-2006

for

## Philips P541G072V0P (JCOP 41 v2.2)

from

## IBM Deutschland Entwicklung GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5455, Infoline +49 (0)3018 9582-111

**Deutsches IT-Sicherheitszertifikat**

erteilt vom
**Bundesamt für Sicherheit in der Informationstechnik**

BSI
Bundesamt für Sicherheit
in der Informationstechnik

## BSI-DSZ-CC-0294-2006

Smartcard with Java Card Platform

## Philips P541G072V0P (JCOP 41 v2.2)

from

## IBM Deutschland Entwicklung GmbH

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, Version 2.3* (ISO/IEC 15408:2005) 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 2.3 (ISO/IEC 15408:2005)*.

**Evaluation Results:**

| | |
|---|---|
| Functionality: | **Product specific Security Target**<br>**Common Criteria Part 2 extended** |
| Assurance Package: | **Common Criteria Part 3 conformant**<br>**EAL 4 augmented with**<br>ADV_IMP.2 (Implementation of the TSF) and<br>ALC_DVS.2 (Sufficiency of security measures) |

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, 31. August 2006

The Vice President of the Federal Office
for Information Security

IT Security Certified

Hange L.S. SOGIS - MRA

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 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

[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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

# 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) and ALC_DVS.2 (Sufficiency of security measures) 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 P541G072V0P (JCOP 41 v2.2) has undergone the certification procedure at BSI.

The evaluation of the product Philips P541G072V0P (JCOP 41 v2.2) was conducted by TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit. The TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor and vendor is IBM Deutschland Entwicklung GmbH, Schoenaicher Strasse 220, 71032 Böblingen, the distributor is Philips Semiconductor GmbH, Stresemannallee 101, 22529 Hamburg.

The certification is concluded with

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

This work was completed by the BSI on 31. August 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.

The product Philips P541G072V0P (JCOP 41 v2.2) 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.

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] IBM Deutschland Entwicklung GmbH
Schoenaicher Strasse 220
71032 Böblingen

# B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

# Contents of the certification results

# 1 Executive Summary

The target of evaluation (TOE) is the Java Card Philips P541G072V0P (JCOP 41 v2.2), and consists of:

- Smart Card Platform SCP (hardware platform and hardware abstraction layer)
- Embedded software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager), and
- native MIFARE application (physically present, but not within the logical scope because for this TOE the minor configuration option of the hardware “MIFARE Emulation = A” is mandatory, i. e. MIFARE interface disabled.)

The software for the application layer (Java applets) is not part of the TOE.

The physical scope is defined by the hardware platform Philips P5CT072V0P which is certified under registration number BSI-DSZ-CC-0348-2006 on the level EAL5 augmented by ALC_DVS.2, AVA_MSU.3, and AVA_VLA.4 (see Hardware Security Target [11] and certification report [10].

The logical scope of the TOE is comprised of

- different communication protocols: ISO 7816 T=1 direct convention, ISO 7816 T=0 direct convention, ISO 7816 T=1 inverse convention, ISO 7816 T=0 inverse convention, ISO 14443 T=CL (contact-less)[8].
- cryptographic algorithms and functionality: 3DES (112 and 168 bit keys) for en-/decryption (CBC and ECB) and signature (MAC) generation and verification, RSA (1024 up to 2368 bits keys) for en-/decryption and signature generation and verification, AES (Advanced Encryption Standard) with key length of 128, 192, and 256 Bit for en-/decryption (CBC and ECB), SHA-1 hash algorithm, random number generation according to class K3 of AIS 20 [4]
- JavaCard 2.2.1 functionality: Garbage Collection fully implemented with complete memory reclamation incl. compactification
- GlobalPlatform 2.1.1 functionality: CVM Management (Global PIN) fully implemented: all described APDU and API interfaces for this feature are present, Secure Channel Protocol (SCP01, and SCP02) is supported
- functionality as defined in the JCSPP [9] minimal configuration (i. e. no post-issuance installation and deletion of applets, packages and objects, no RMI, no logical channels, no on-card byte code verification), and
- card manager functionality for pre-issuance loading and management of packages and applets.

[8] Communication via the USB interface was not part of the evaluation

Byte code verification and applets are not part of the TOE.

The life-cycle for this Java Card is shown in the following table. It is based on the general smart card life-cycle defined in the smart card hardware platform protection profile [12] and has been adapted to Java Card specifics.

| Phase | Name | Description |
|---|---|---|
| 1 | Smartcard Embedded Software Development | The **Smartcard Embedded Software Developer** is in charge of smartcard embedded software development including the development of Java applets and specification of IC pre-personalization requirements, though the actual data for IC pre-personalization come from phase 6 (or phase 4 or 5). |
| 2 | IC Development | The **IC Designer** designs the IC, develops IC Dedicated Software, provides information, software or tools to the Smartcard Embedded Software Developer, and receives the smartcard embedded software from the developer, through trusted delivery and verification procedures.<br>From the IC design, IC Dedicated Software and Smartcard Embedded Software, the IC Designer constructs the smartcard IC database, necessary for the IC photomask fabrication. |
| 3 | IC Manufacturing and Testing | The **IC Manufacturer** is responsible for producing the IC through three main steps: IC manufacturing, IC testing, and IC prepersonalization.<br>The IC Mask Manufacturer generates the masks for the IC manufacturing based upon an output from the smartcard IC database. |
| 4 | IC Packaging and Testing | The **IC Packaging Manufacturer** is responsible for IC packaging and testing. |
| 5 | Smartcard Product Finishing Process | The **Smartcard Product Manufacturer** is responsible for smartcard product finishing process including applet loading and testing. |
| 6 | Smartcard Personalization | The **Personalizer** is responsible for smartcard (including applet) personalization and final tests. Other smartcard embedded software may be loaded onto the chip at the personalization process |
| 7 | Smartcard Endusage | The **Smartcard Issuer** is responsible for smartcard product delivery to the smartcard end-user, and the end of life process. |

Table 1: TOE life cycle

The evaluation process is limited to phases 1 to 4, while delivery is either at the end of phase 3 or 4 (see also Hardware Security Target [11]).

The applet development is outside the scope of this evaluation. Applets with patch code can be loaded in phase 3 only. Normal applet loading is only possible in phases 5 or 6, i. e. no post-issuance loading of applets.

The IT product Philips P541G072V0P (JCOP 41 v2.2) was evaluated by TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit. The evaluation was completed on 11. July 2006. The TÜV Informationstechnik GmbH, Prüfstelle IT-Sicherheit is an evaluation facility (ITSEF)[9] recognised by BSI.

The sponsor and vendor is IBM Deutschland Entwicklung GmbH, the distributor is Philips Semiconductor GmbH.

## 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 EAL 4 + (Evaluation Assurance Level augmented). The following table shows the augmented assurance components.

| **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 |

Table 2: Assurance components and EAL-augmentation

## 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** | **Addressed issue** |
|---|---|
| **Firewall Policy** | |
| **FDP** | **User data protection** |
| FDP_ACC.2/Firewall | Complete access control |
| FDP_ACF.1/Firewall | Security attribute based access control |
| FDP_IFC.1/JCVM | Subset Information flow control |
| FDP_IFF.1/JCVM | Simple security attributes |
| FDP_RIP.1/Objects | Subset residual information protection |
| **FMT** | **Security Management** |
| FMT_MSA.1/JCRE | Management of security attributes |
| FMT_MSA.2/JCRE | Secure security attributes |
| FMT_MSA.3/Firewall | Static attribute initialization |
| FMT_SMR.1/JCRE | Security roles |
| **FPT** | **Protection of the TSF** |

[9] Information Technology Security Evaluation Facility

| **Security Functional Requirement** | **Addressed issue** |
|---|---|
| FPT_SEP.1 | TSF domain separation |
| **Application programming Interface** | |
| **FCS** | **Cryptographic support** |
| FCS_CKM.1 | Cryptographic key generation |
| FCS_CKM.2 | Cryptographic key distribution |
| FCS_CKM.3 | Cryptographic key access |
| FCS_CKM.4 | Cryptographic key destruction |
| FCS_COP.1/Triple DES | Cryptographic operation |
| FCS_COP.1/AES | Cryptographic operation |
| FCS_COP.1/RSAChiper | Cryptographic operation |
| FCS_COP.1/MAC | Cryptographic operation |
| FCS_COP.1/RSASignatureISO9796 | Cryptographic operation |
| FCS_COP.1/RSASignaturePKCS#1 | Cryptographic operation |
| FCS_COP.1/SHA-1 | Cryptographic operation |
| **FDP** | **User data protection** |
| FDP_RIP.1/APDU | Subset residual information protection |
| FDP_RIP.1/bArray | Subset residual information protection |
| FDP_RIP.1/Transient | Subset residual information protection |
| FDP_RIP.1/Abort | Subset residual information protection |
| FDP_RIP.1Keys | Subset residual information protection |
| FDP_ROL.1/Firewall | Basic rollback |
| **Card Security Management** | |
| **FAU** | **Security audit** |
| FAU_ARP.1/JCS | Security alarms |
| **FDP** | **User data protection** |
| FDP_SDI.2 | Stored data integrity monitoring and action |
| **FPT** | **Protection of the TSF** |
| FPT_RVM.1 | Non-bypassability of the TSF |
| FPT_FLS.1/JCS | Failure with preservation of secure state |
| FPT_TST.1 | TSF testing |
| **FPR** | **Privacy** |
| FPR_UNO.1 | Unobservability |
| **AID Management** | |
| **FMT** | **Security Management** |
| FMT_MTD.1/JCRE | Management of TSF data |

| **Security Functional Requirement** | **Addressed issue** |
|---|---|
| FMT_MTD.3 | Secure TSF data |
| **FIA** | **Identification and authentication** |
| FIA_ATD.1/AID | User attribute definition |
| FIA_UID.2/ATD | User identification before any action |
| FIA_USB.1 | User-subject binding |
| **SCPG Security Functional Requirements** | |
| **FPT** | **Protection of the TSF** |
| FPT_AMT.1/SCP | Abstract machine testing |
| FPT_FLS.1/SCP | Failure with preservation of secure state |
| FPT_PHP.3/SCP | Resistance to physical attack |
| FPT_RVM.1/SCP | Non-bypassability of the TSF |
| **FRU** | **Resource utilization** |
| FRU_FLT.2/SCP | Limited fault tolerance |
| FPT_SEP.1/SCP | TSF domain separation |
| **CMGRG Security Functional Requirements** | |
| FDP_ACC.1/CMGR | Subset access control |
| FDP_ACF.1/CMGR | Security attribute based access control |
| **FMT** | **Security Management** |
| FMT_MSA.1/CMGR | Management of security attributes |
| FMT_MSA.3/CMGR | Static attribute initialization |
| FMT_SMR.1/CMGR | Security roles |
| **FIA** | **Identification and authentication** |
| FIA_UID.1/CMGR | Timing of identification |
| **Further Functional Requirements not contained in [9]** | |
| **FDP** | **User data protection** |
| FDP_ETC.1 | Export of user data without security attributes |
| FDP_ITC.1 | Import of user data without security attributes |
| **FIA** | **Identification and authentication** |
| FIA_AFL.1/PIN | Authentication failure handling |
| FIA_AFL.1/CMGR | Authentication failure handling |
| FIA_UAU.1 | Timing of authentication |
| FIA_UAU.3/CMGR | Unforgeable authentication |

| **Security Functional Requirement** | **Addressed issue** |
|---|---|
| FIA_UAU.4/CMGR | Single-use authentication mechanisms |
| **FTP** | **Trusted path/channels** |
| FTP_ITC.1/CMGR | Inter-TSF trusted channel |
| **FAU** | **Security audit** |
| FAU_SAA.1 | Potential violation analysis |
| **FMT** | **Security Management** |
| FMT_SMF.1 | Specification of Management Functions |

Table 3: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

| **Security Functional Requirement** | **Addressed issue** |
|---|---|
| **FMT** | **Security Management** |
| FMT_LIM.1 | Limited capabilities |
| FMT_LIM.2 | Limited availability |
| **FCS** | **Cryptographic support** |
| FCS_RND.1 | Quality Metric for random numbers |
| **FPT** | **Protection of the TSF** |
| FPT_EMSEC.1 | TOE Emanation |

**Table 4: SFRs for the TOE, CC part 2 extended**

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.1.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

| **Security Functional Requirement** | **Addressed issue** |
|---|---|
| **Byte Code Verification** | |
| **FDP** | **User data protection** |
| FDP_IFC.2/BCV | Complete information flow control |
| FDP_IFF.2/BCV | Hierarchical security attributes |
| **FMT** | **Security Management** |
| FMT_MSA.1/BCV | Management of security attributes |
| FMT_MSA.2/BCV | Secure security attributes |
| FMT_MSA.3/BCV | Static attribute initialization |
| FMT_SMR.1/BCV | Security roles |
| **FRU** | **Resource utilization** |
| FRU_RSA.1/BCV | Maximum quotas |

| Security Functional Requirement | Addressed issue |
|---|---|
| **Trusted Channel** | |
| **FTP** | **Trusted path/channels** |
| FTP_ITC.1/ENV | Inter-TSF trusted channel – none |

**Table 5: SFRs for the IT-Environment**

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.3.

In addition there is a security requirement defined for the Non-IT Environment, R.ICManufacturer (IC Design, manufacturing and testing), which is related to the need for confidentiality and integrity of the Smart Card Native Operating System manufacturing (see ST chapter 5.4).

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

| TOE Security Function | Addressed issue |
|---|---|
| SF.AccessControl | enforces the access control |
| SF.Audit | Audit functionality |
| SF.CryptoKey | Cryptographic key management |
| SF.CryptoOperation | Cryptographic operation |
| SF.I&A | Identification and authentication |
| SF.SecureManagement | Secure management of TOE resources |
| SF.PIN | PIN management |
| SF.Transaction | Transaction management |
| SF.Hardware | TSF of the underlying IC |

**Table 6: TOE security functions**

For more details please refer to the Security Target [6], chapter 6.

## 1.3 Strength of Function

The TOE’s strength of functions is claimed ‘high’ (SOF-high) for specific functions as indicated in the Security Target [6], chapter 6.1.

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). For details see chapter 9 of this report.

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

Assets are divided in primary and secondary assets. As primary assets User Data and TSF Data are further refined. The TOE objective is to protect the primary assets, during usage phase. In order to protect these primary assets, information and tools used for the development and manufacturing of the Smart Card, need to be protected. These information and tools are called secondary assets.

- Primary assets: TOE including NOS (Native Operating System ) code, TSF data, as initialization data, configuration data, cryptographic keys, random numbers for key generation, and all data used by the TOE to execute its security functions. This includes also configuration of hardware specific security features; User Data, as application code (applets), specific sensitive application values, as well as application specific PIN and authentication data.
- Secondary assets: IC development and manufacturing related information, handled by the IC manufacturer during phase 2 and 3 as IC specification; IC dedicated software; NOS development related information handled by NOS developer during phase 1; TOE documentation exchanged between IC manufacturer and NOS developer as IC data sheet, IC user guidance, NOS mask related information; TOE documentation delivered to IC packaging or Smartcard product manufacturer as initialization data or other sensitive information for usage phase 4 to 7.

For more details on the definition of assets refer to the Security Target [6], chapter 3.1.1 and 3.1.2.

As subjects active components of the TOE that (essentially) act on behalf of users are considered. The main subjects of the TOE considered are the following ones taken from the JCSPP [9]:

- Packages used on the Java Card platform that act on behalf of the applet developer. These subjects are involved in the FIREWALL security policy and they should be understood as instances of the subject S.PACKAGE.
- The CardManager, can be considered a special instance of S.PACKAGE which implements the Open Platform specification. This package provides the functionality of a runtime environment running at the JCRE ‘system’ (privileged) context and for clarity is always represented by the subject S.PACKAGE(CM).
- The JCRE, which acts on behalf of the card issuer. This subject is involved in several of the security policies defined in this document and is always represented by the subject S.JCRE.

The threats are partly taken from JCSPP [9] and others are specifically defined.

The following threats are not taken from JCSPP:

Threats on TOE environment:

- T.DEV_IC on theft, modification, disclosure of information related to IC development and manufacturing. This includes disclosure/modification of the NOS code by the IC manufacturer. This threat addresses the information handled by the IC manufacturer in the IC development and manufacturing environment (phases 2 and 3).

- T.DEV_NOS on theft, modification, or disclosure of NOS related information during NOS development. This threat addresses the information handled by the NOS Developer during phase 1.
- T.DEL_IC_NOS on theft, modification, disclosure of information related to IC or NOS during delivery between IC manufacturer and NOS Developer. This threat addresses the delivery process used for information exchange between the IC manufacturer and the NOS developer.
- T.DEL on theft, modification, disclosure of information related to TOE during delivery to IC packaging manufacturer or Smart Card manufacturer or personalization. This threat addresses the delivery process used for information transfer to IC packaging, Smart Card Manufacturer, or Personalizer.

The TOE is intended to protect itself against the following threats in the phases 4 to 7: Manipulation of User Data and of the Smart Card Native Operating System (while being executed/processed and while being stored in the TOE's memories) and Disclosure of User Data and of the Smart Card NOS (while being processed and while being stored in the TOE's memories). Therefore, the following threats are defined as so called software threats:

- T.ACCESS_DATA on unauthorized access to sensitive information stored in memories in order to disclose or to corrupt the TOE data (TSF and user data). This includes any consequences of bad or incorrect user authentication by the TOE.
- T.OS_OPERATE on modification of the correct NOS behaviour by unauthorized use of TOE or use of incorrect or unauthorized instructions or commands or sequence of commands, in order to obtain an unauthorized execution of the TOE code.
- T.OS_DECEIVE on Modification of the expected TOE configuration by unauthorized loading of code, unauthorized execution of code, unauthorized modification of code behaviour

The following threats are defined as so called environment threats on the complete TOE:

- T.LEAKAGE on exploitation of information which is leaked from the TOE during usage of the Smart Card in order to disclose the confidential primary assets.
- T.FAULT on causing a malfunction of TSF or of the Smart Card embedded NOS by applying environmental stress in order to (1) deactivate or modify security features or functions of the TOE or (2) deactivate or modify security functions of the Smart Card embedded NOS.

- The threat T.RND on random numbers is about Deficiency of Random Numbers

The following threats are taken from JCSPP:

- T.PHYSICAL on discloses or modification of the design of the TOE, its sensitive data (TSF and User Data) or application code or disabling of security features of the TOE.
- T.CONFID-JCS-CODE on executing an application without authorization to disclose the Java Card System code.
- T.CONFID-APPLI-DATA on executing an application without authorization to disclose data belonging to another application.
- T.CONFID-JCS-DATA on executing an application without authorization to disclose data belonging to the Java Card System.
- T.INTEG-APPLI-CODE on executing an application to alter (part of) its own or another application’s code.
- T.INTEG-JCS-CODE on executing an application to alter (part of) the Java Card System code.
- T.INTEG-APPLI-DATA on executing an application to alter (part of) another application’s data.
- T.INTEG-JCS-DATA on executing an application to alter (part of) Java Card System or API data.
- T.SID.1 on impersonating another application, or even the JCRE, in order to gain illegal access to some resources of the card or with respect to the end user or the terminal.
- T.SID.2 on modification of the identity of the privileged roles.
- T.EXE-CODE.1 on unauthorized execution of a method.
- T.EXE-CODE.2 on unauthorized execution of a method fragment or arbitrary data.
- T.NATIVE on trying to execute a native method to bypass some security function such as the firewall.
- T.RESOURCES on preventing correct operation of the Java Card System through consumption of some resources of the card:

A policy OSP.IC_ORG is defined on the need for procedures dealing with physical, personnel, organizational, technical measures for the confidentiality and integrity, of Smart Card Native Operating System and IC Manufacturer proprietary information in IC development and manufacturing and procedures to ensure confidentiality and integrity of information during exchange with the NOS developer.

## 1.5 Special configuration requirements

The evaluation process is limited to phases 1 to 4, while delivery is either in phase 3 or 4. The administrator guidance includes all information for prepersonalization including ROM mask configuration via FabKey (phase 3) and for smart card finishing and personalizing including applet loading (phases 3, 5, 6).

## 1.6 Assumptions about the operating environment

The assumptions are defined for the different phases of the TOE life cycle:

- Assumption A.DLV_PROTECT on the TOE delivery process (phases 4 to 7) to guarantee the control of the TOE delivery and storage process and conformance to its objectives.
- Assumption A.TEST_OPERATE on phases 4 to 6 for security procedures to maintain confidentiality and integrity of the TOE and of its manufacturing and test data and on appropriate functionality testing of the TOE.
- Assumption A.USE_DIAG on phase 7 for the usage of secure communication protocols offered by TOE.
- Assumption A.USE_KEYS on phase 7 for confidentiality and integrity of keys.
- Assumptions used from JCSPP [9] are:
- A.NATIVE on conformance of native code with the TOE not to violate the security policies and objectives.
- A.NO-DELETION related to phase 7 for impossibility of deletion of installed applets (or packages).
- A.NO-INSTALL related to phase 7 for impossibility of post-issuance installation of applets.
- A.VERIFICATION related to phases 1-6 that all the bytecodes are verified at least once before the loading.

For more details please refer to the Security Target [6], chapter 3.3.

## 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 P541G072V0P (JCOP 41 v2.2)**

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| 1 | HW / SW | Philips P541G072VOP (JCOP 41 v2.2)<br>Chip including ROM mask and EEPROM patch | Mask ID: 0x24<br>Mask name: PH522D<br>Patch ID: 0x04 | Sawn Wafer or embedded into specific module package (see [11] |
| 2 | DOC | User Guidance Philips P541G072V0P (JCOP 41 v2.2) Secure Smart Card Controller [13], | Version 1.6, 31. March 2006 | Electronic PDF document, encrypted and signed |
| 3 | DOC | Administrator Guidance Philips P541G072V0P (JCOP 41 v2.2) Secure Smart Card Controller [14], | Version 1.5, 06. June 2006 | Electronic PDF document, encrypted and signed |

**Table 7: Deliverables of the TOE**

The Philips P541G072VOP (JCOP 41 v2.2) includes the hardware chip P5CT072V0P. It can be identified by the administrator in phases 3-5 by determination of Device Coding Byte DC2 as outlined in [10]. The value 11 hex in Device Coding Byte DC2 identifies the chip P5CT072. For that, the administrator sends either APDU 'DFB0FFDC04' (possessing the ADMIN_ROOTKEY) or encrypted APDU '0020000008D2C8FCD61B6C8CF0' (using Transport Key, related to Fabkey-ID=1B) to the TOE. In both cases he will receive '410711009000' indicating P5CT072 as HW platform.

In addition the customer can use the so called nameplate (on-chip code on the surface of the chip) to make sure that the evaluated version of the chip has been delivered. This on-chip code is printed onto the chip during production. This code also corresponds to the version of the chip and can therefore be used to check it. The nameplate for the waferfab in Singapore (SSMC) is T023P where (i)'T' identifies the waferfab, (ii)'023' identifies the P5CT072 (and its possible configurations) and (iii) where 'P' identifies the version V0P.

The delivered HW/SW at the end of phase 3 or 4 is protected by applying the Philips Fabkey-procedure.

# 3 Security Policy

The TOE is the composition of an IC, IC Dedicated Software and Smart Card Embedded Software and is intended to be used as a Java Card platform and to be equipped with Java applets conformant to the Java Card standard.

The Java Card virtual machine (JCVM) is responsible for ensuring language-level security. The basic runtime security feature imposed by the JCRE enforces isolation of applets using an applet firewall. It prevents objects created by one applet from being used by another applet without explicit sharing. This prevents unauthorized access to the fields and methods of class instances, as well as the length and contents of arrays.

The applet firewall is considered as the most important security feature. It enables complete isolation between applets or controlled communication through additional mechanisms that allow them to share objects when needed. The JCVM should ensure that the only way for applets to access any resources are either through the JCRE or through the Java Card API (or other vendor-specific APIs).

The Card Manager is responsible for the management of applets in the card. No post-issuance loading and deletion of applets is allowed for the present TOE.

The platform also provides cryptographic algorithms and functionality for 3DES, AES, RSA and SHA-1.

# 4 Assumptions and Clarification of Scope

For assumptions see chapter 1.6 above.

The TOE provides a secure operating platform in case the assumptions, guidance and obligations are fulfilled. The scope of the TOE does not include any applet and thus it can not implement a specific card issuer or end user security policy by itself. A card issuer or end user security policy and the functionality of applets needs to be examined when specific applets are considered to be loaded onto this platform. Specific APIs were not part of the TSF (see below).

# 5 Architectural Information

Security Target [6], chapter 2.1 provides a high level overview about the architecture of the TOE. This high level concept is implemented by subsystems of the TOE as summarized in the following:

API Mapping Layer:

- The API_JavaCard module provides the API interface according to the Java Card 2.2.1 Application Programming Interface, June 2002. The API includes runtime, communication and crypto functions. This module implements the functionality using the Java System Layer APIs or directly maps the methods to the native System Layer.
- The API_GP module provides the API interface according to the Global Platform Card Specification, Version 2.1.1, March 2003. The API includes card management and security functions. This module implements the functionality using the Java System Layer APIs or directly maps the methods to the native System Layer.

- The API_OP, API_BIO and API_Korean are not within the scope of the TSF.

Java System Layer:

- JS_CardManager: The card manager is a special application with system rights, which is responsible for the administration of the smart card. It provides services to JavaCard applets over API interfaces and services to off card entities over APDU interfaces. This includes authentication as well as loading, installing and deleting of JavaCard packages and applets.
- JS_System (Internal System API): The JS_System module provides the API interface to special internal native functions and various helper functions required for the implementation of the standard APIs and the CardManager application. It directly maps to the native S_System module in the System Layer. Additionally it defines the layout for ROM and EEPROM regions and a number of constants shared between the native and the Java layers.
- JS_JZ System (JZSystem API): It provides the low-level Java API interface for cryptographic functions. It is used for implementation of the standard cypto API and the Card Manager implementation. It directly maps to the native S_Crypto module in the System Layer.

System Layer:

- S_VM: The S_VM module provides the JavaCard bytecode interpreter as defined in the JavaCard Virtual Machine specification. This module implements the interpreter loop and all of the virtual machine's byte code instructions. It is used by the S_JCRE module to execute JavaCard applications or system library code.
- S_JCRE: The S_JCRE module implements the runtime behaviour required by the JavaCard Runtime Environment specification. This includes command processing, applet control and memory management.
- S_System: The S_System module provides the common (i.e., hardware-independent) glue between high-level Java API and lower-level HAL implementations. This includes parameter and bounds checks as well as parameter and return value conversions. Additionally it implements common utility functions (e.g.array copy) and hardware-independent run-time functionality.
- S_Crypto: The S_Crypto module provides the common (i.e. hardware-independent) glue between the JS_JZSystem module and the HAL_Crypto implementation. This includes parameter and bounds checks as well as parameters and return values conversions.

Hardware Abstraction Layer:

- HAL_Crypto: The HAL_Crypto module provides low-level cryptographic libraries. The library functions are performed by the micro controller or by dedicated crypto hardware like DES, AES or RSA co-processors. Hardware-specific details are hidden from upper layers.

- HAL_System: The HAL_System module provides low-level system runtime libraries. Hardware-specific details are hidden from upper layers.
- HAL_IO: The HAL_IO module provides low-level communication libraries. The library functions are performed by the micro controller or by dedicated communications hardware like serial UART for contact interface (ISO 7816) or radio transmitters for contactless interface (ISO 14443). Hardware-specific details are hidden from upper layers.

Hardware Layer:

- This layer implements certain security functionality. This is done by the certified hardware (part of the TOE). Information about the hardware platform can be taken from the Hardware Security Target [11] and certification report [10].

# 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:

- User Guidance Philips P541G072V0P (JCOP 41 v2.2) Secure Smart Card Controller, Version 1.6, 31. March 2006, IBM, [13],
- Administrator Guidance Philips P541G072V0P (JCOP 41 v2.2) Secure Smart Card Controller, Version 1.5, 06. June 2006, IBM, [14].

The Administrator Guidance addresses the prepersonalization including ROM mask configuration via FabKey (phase 3) and smart card finishing and personalizing including applet loading (phases 3, 5, 6). The User Guidance addresses the applet developer (phase 1).

# 7 IT Product Testing

The TOE has been tested using automated test tools together with automated comparison of expected and actual test results.

Developer’s testing approach:

The TOE has been tested as a composite product according to Java Card specifications by the main test suites used during integration, system, function and performance test: (i) JavaCard - TCK tests, (ii) GlobalPlatform (GP) - Offical GP test suites and (iii) VISA GlobalPlatform - Test suite. During development additional UNIT tests have been performed. This has been done with internal tools, test applet(s) and test script(s) on an emulator and on basis of the source code.

Therefore the developer’s approach of testing the TOE is that the required functions and supported options of the card are correctly implemented and work as expected. The developer also employs code reviews as an alternate testing approach for testing of internal mechanisms or implementation of external requirements.

The developer has tested the TOE systematically at the level of TSF functionality according to FSP and of the HLD subsystems. The developer's testing results demonstrate that the TSF performs as specified.

Independent Evaluator Testing according to ATE_IND:

The TOE under test was the composite smartcard TOE as defined in table 7. Two physical configurations were used for testing: (i) contactless only chip (embedded in card body) and (ii) chip with contact and contactless interface available (as SO28 chip). Since the tests of the developer are of the kind of exhaustive specification testing, the testing approach of the evaluator has been to rerun specific test suites of the TOE.

The evaluator has performed additional tests on top of and different from the developer's testing for all security functions using both physical configurations. The independent testing was performed using an equivalent set of test tools. During the evaluator's independent testing the TOE operated as specified.

Penetration Testing according to AVA_VLA

The penetration testing approach was based on developer's vulnerability analysis and based on the independent vulnerability assessment of the evaluator. The evaluators approach was to systematically search for potential vulnerabilities and for known attacks in public domain sources and the use of actual information from an international working group (ISCI). Analysis why vulnerabilities are unexploitable in the intended environment of the TOE were performed assuming low attack potential. To support and to verify the analysis specific penetration attacks were performed in the course of this evaluation.

During the evaluator's penetration testing the TOE operated as specified. All potential vulnerabilities are not exploitable with a low attack potential in the intended environment for the TOE. Therefore it is concluded that the TOE is resistant to attackers with low attack potential as claimed in the Security Target.

# 8 Evaluated Configuration

The TOE was evaluated in the configuration as outlined in table 7 and with the native MIFARE application physically present, but not within the logical scope because for this TOE the minor configuration option of the hardware “MIFARE Emulation = A” is mandatory, i. e. MIFARE interface disabled. The evaluated Philips P541G072VOP (JCOP 41 v2.2) includes the hardware chip P5CT072V0P as certified under the registration number BSI-DSZ-CC-0348-2006.

# 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]). 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]) were used and the scheme interpretation [4, AIS 20] (Functionality classes and evaluation methodology for deterministic random number generators) was used. The evaluation was performed as a composite evaluation process based on the concepts defined ([4, AIS 36]).

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 EAL 4 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.2 | PASS |
| Delivery and operation | CC Class ADO | PASS |

| Assurance classes and components | | Verdict |
|---|---|---|
| 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.2 | PASS |
| Semiformal high-level design | ADV_HLD.2 | PASS |
| Implementation of the TSF | ADV_IMP.2 | PASS |
| Descriptive low-level design | ADV_LLD.1 | PASS |
| Semiformal correspondence demonstration | ADV_RCR.1 | PASS |
| Formal 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 |
| Standardised life-cycle model | ALC_LCD.1 | PASS |
| Compliance with implementation standards | ALC_TAT.1 | PASS |
| Tests | CC Class ATE | PASS |
| Analysis of coverage | ATE_COV.2 | PASS |
| Testing: low-level design | ATE_DPT.1 | PASS |
| Functional testing | ATE_FUN.1 | PASS |
| Independent testing – sample | ATE_IND.2 | PASS |
| Vulnerability assessment | CC Class AVA | PASS |
| Validation of analysis | AVA_MSU.2 | PASS |
| Strength of TOE security function evaluation | AVA_SOF.1 | PASS |
| Independent vulnerability analysis | AVA_VLA.2 | PASS |

**Table 8: Verdicts for the assurance components**

The evaluation has shown that:

- 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 and ALC_DVS.2.

- The following TOE Security Functions fulfil the claimed Strength of Function SOF high: SF.AccessControl (aspect 1[10]), SF.CryptoOperation (aspects 7, 8), SF.I&A (aspects 1, 2), SF.SecureManagement (aspect 6), SF.PIN (aspects 1,2,3) and SF.Hardware as outlined in the hardware certification report [10]. The random number generator (SF.CryptoOperation aspect 7) was evaluated to fulfil [4, AIS 20] class K3 requirements with strength high.

  The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for SF.CryptoKey (aspect[11] 1, 2, 3) and SF.CryptoOperation (aspects 1 to 6) and for other usage of encryption and decryption within the TOE.

The results of the evaluation are only applicable to the Java Card Platform Philips P541G072V0P (JCOP 41 v2.2) as outlined in chapter 2 and chapter 8 of this report and produced in an evaluated site.

Regarding the development and production environment the sites listed in the hardware certification report [10] apply for the TOE. For TOE software development the IBM sites in Boeblingen and Zurich[12] were part of the evaluation process. Sites for the life cycle phases 5 (Smartcard Product Finishing Process) and 6 (Smartcard Personalization) were not part of the evaluation process.

The underlying hardware had been successfully evaluated by T-Systems GEI GmbH, Prüfstelle für IT-Sicherheit, an evaluation facility (ITSEF) recognised by BSI and, is certified under the ID BSI-DSZ-CC-0348-2006 (see [10]).

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 documents [13] and [14] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

[10] The *aspects* are those functionalities numbered within the description of the security function in the Security Target chapter 6.1.x

[11] The *aspects* are those functionalities numbered within the description of the security function in the Security Target chapter 6.1.x

[12] IBM Deutschland Entwicklung GmbH, Schoenaicher Str. 220, D-71032 Boeblingen
IBM Research GmbH, Zurich Research Laboratory, Säumerstrasse 4 / Postfach CH-8803 Rüschlikon, Switzerland

## 11 Annexes

None.

## 12 Security Target

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

## 13 Definitions

### 13.1 Acronyms

| | |
|---|---|
| AID | Application identifier, an ISO-7816 data format used for unique identification of Java Card applications |
| APDU | Application Protocol Data Unit, an ISO 7816-4 defined communication format between the card and the off-card applications. |
| applet | The name is given to a Java Card technology-based user application |
| BCV | Byte Code Verifier (here off-card verifier) |
| BSI | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany |
| CC | Common Criteria for IT Security Evaluation |
| CM | Card Manger |
| EAL | Evaluation Assurance Level |
| EEPROM | Electrically Erasable Programmable ROM |
| ES | Embedded Software |
| HAL | Hardware Abstraction Layer |
| IC | Integrated Circuit |
| IT | Information Technology |
| JCRE | Java Card Runtime Environment |
| JCVM | Java Card Virtual Machine |
| NOS | Native Operating System |
| PP | Protection Profile |
| RAM | Random Access Memory |
| ROM | Read Only Memory |
| RTE | Runtime Environment |

| | |
|---|---|
| SCP | Smart Card Platform |
| SF | Security Function |
| SFP | Security Function Policy |
| SOF | Strength of Function |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSC | TSF Scope of Control |
| TSF | TOE Security Functions |
| TSP | TOE Security Policy |
| VM | Virtual Machine |

## 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 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE, specifically

- AIS 20: Functionality classes and evaluation methodology for deterministic random number generators AIS 20, Version 1, 2 December 1999
- 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 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 Philips P541G072V0P (JCOP 41, v2.2) Secure Smart Card Controller, Version 2.2, 25. March 2006, IBM Deutschland Entwicklung GmbH (confidential document)

[7] Security Target lite Philips P541G072V0P (JCOP 41, v2.2) Secure Smart Card Controller, Version 1.0, 21. August 2006, IBM Deutschland Entwicklung GmbH (sanitized public document)

[8] Evaluation Technical Report (ETR), Version 3, 10. July 2006, CC Evaluation of Philips P541G072V0P (JCOP 41 v2.2) (confidential document)

[9] Java Card System – Minimal Configuration Protection Profile (registered at DCSSI under registration number PP/0303) as part of Java Card System Protection Profile Collection, Version: 1.0b, August 2003

[10] Certification Report BSI-DSZ-CC-0348-2006 for Philips Secure Smart Card Controller P5CT072V0P, P5CC072V0P, P5CD072V0P and P5CD036V0P each with specific IC Dedicated Software from Philips Semiconductors GmbH Business Line Identification, Version 1.0, 28. March 2006, BSI

[11] Security Target Lite BSI-DSZ-CC-0348 Evaluation of the Philips P5CT072V0P, P5CC072V0P, P5CD072V0P and P5CD036V0P Secure Smart Card Controller, Version 1.2, 17. January 2006 Philips Semiconductors GmbH Business Line Identification

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

[13] User Guidance Philips P541G072V0P (JCOP 41 v2.2) Secure Smart Card Controller, Version 1.6, 31. March 2006, IBM

[14] Administrator Guidance Philips P541G072V0P (JCOP 41 v2.2) Secure Smart Card Controller, Version 1.5, 06. June 2006, IBM

This page is intentionally left blank.

# C Excerpts from the Criteria

CC Part1:

**Conformance results** (chapter 7.4)

„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 CC Part 2 (functional requirements), CC 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:

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

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

plus one of the following:

a) **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

b) **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC 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:

a) **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.

b) **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:

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

CC Part 3:

**Assurance categorisation** (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

| **Assurance Class** | **Assurance Family** |
|---|---|
| ACM: Configuration management | CM automation (ACM_AUT) |
| | CM capabilities (ACM_CAP) |
| | CM scope (ACM_SCP) |
| ADO: Delivery and operation | Delivery (ADO_DEL) |
| | Installation, generation and start-up (ADO_IGS) |
| 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) |
| AGD: Guidance documents | Administrator guidance (AGD_ADM) |
| | User guidance (AGD_USR) |
| ALC: Life cycle support | Development security (ALC_DVS) |
| | Flaw remediation (ALC_FLR) |
| | Life cycle definition (ALC_LCD) |
| | Tools and techniques (ALC_TAT) |
| ATE: Tests | Coverage (ATE_COV) |
| | Depth (ATE_DPT) |
| | Functional tests (ATE_FUN) |
| | Independent testing (ATE_IND) |
| AVA: Vulnerability assessment | Covert channel analysis (AVA_CCA) |
| | Misuse (AVA_MSU) |
| | Strength of TOE security functions (AVA_SOF) |
| | Vulnerability analysis (AVA_VLA) |

Table 1: Assurance family breakdown and mapping”

**Evaluation assurance levels** (chapter 11)

“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 CC 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 11.1)

“Table 6 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 7 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 standard 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: Evaluation assurance level summary”

**Evaluation assurance level 1 (EAL1) - functionally tested** (chapter 11.3)

“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 11.4)

“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 11.5)

“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 11.6)

“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 11.7)

“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 11.8)

“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 11.9)

“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 19.3)

“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 19.4)

"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 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”