Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0363-2006

for

Smart card reader SPR532
Firmware version 5.09

from

SCM Microsystems 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

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0363-2006

Smart card reader SPR532
Firmware version 5.09

from

SCM Microsystems 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 the advice of the Certification Body for components beyond EAL4 for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL3 augmented by** ADO_DEL.2 – Detection of modification ADV_IMP.1 – Subset of the implementation of the TSF ADV_LLD.1 – Descriptive low-level design ALC_TAT.1 – Well-defined development tools AVA_MSU.3 – Analysis and testing for insecure states AVA_VLA.4 – 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, December 22nd 2006

The President of the Federal Office
for Information Security

Dr. Helmbrecht 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 9582-5455 - 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 2.3[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 AVA_MSU.3 and AVA_VLA.4 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 smart card reader SPR532, firmware version 5.09 has undergone the certification procedure at BSI.

The evaluation of the product smart card reader SPR532, firmware version 5.09 was conducted by TÜV Informationstechnik GmbH. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

SCM Microsystems GmbH
Oskar-Messter-Str. 13
85737 Ismaning, Germany

The certification is concluded with

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

This work was completed by the BSI on December 22nd 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-20.

The product smart card reader SPR532, firmware version 5.09 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] SCM Microsystems
Oskar-Messter-Str. 13
85737 Ismaning, Germany

B Certification Results

The following results represent a summary of

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

Contents of the certification results

1 Executive Summary

The SPR532 smart card reader represents universal smart card reader devices, which can communicate with processor cards compliant to ISO 7816 [14] (T=0, T=1) and EMV2004 [15] through different application interfaces (CT-API [16], PC/SC [17]). Data transmission protocols for memory cards (I^2C, 2-wire, 3-wire protocol) are also supported.

SPR532 readers have a keypad with silicone keys in order to guarantee a secure PIN entry. The reader recognizes the commands sent by the host (typically a PC) to the smart card and inserts the numbers entered over the keypad as a PIN into the appropriate places of the command. Only the fact that a numeric key was pressed is communicated to the host. The PIN never leaves the reader towards the host.

The SPR532 smart card reader family offers the possibility to update the firmware in a secure manner in order to be prepared for future requirements. This functionality can also be used to update the firmware of already delivered smart card readers SPR532 to the new functionality incorporated in the firmware version 5.09 without bying new hardware. The mechanism consists of a digital signature of the firmware that is verfied by the smart card reader SPR532 before the new firmware is stored in the EEPROM. The verification of the signature with the asymmetrical RSA algorithm and a bit length of 1024 guarantees the integrity and authenticity of the firmware during the upload of the firmware into the smart card reader. The manufacturer SCM Microsystems ensures the secure generation and administration for the production of the necessary secure signature key. SCM guarantees that each new version of the TOE receives a new version number and is clearly identifiable by means of this number.

SPR532 smart card readers are usable in many market segments because of their multi-functionality. As class 2 readers the SPR532 readers also allow to enter identification data (PIN) and convey it securely to secure signature creation devices (smart cards with dedicated signature application) according to §2 number 10 SigG [8]. Therefore the readers can also be used for applications in accordance with the signature law and signature regulation. Moreover, they can be used for the transmission of the hash value from the application to the signature card and for the provision of a signature from the card for use in signature applications. Thus, they represent a partial component for signature applications, which require a security confirmation to be able to be used for qualified electronic signatures under §2 number 3 SigG [8]. For the use of the TOE in accordance with SigG and SigV [9], only signature applications and smart cards can be used that were evaluated and confirmed in the SigG context. The web pages of the Bundesnetzagentur list the evaluated and confirmed products (see www.bundesnetzagentur.de).

SPR532 smart card readers fulfill the special requirements under §15 paragraph 2 number 1a (no disclosure or storage of identification data) and paragraph 4 (recognizability of security-relevant changes) to SigV [9].

The IT product smart card reader SPR532, firmware version 5.09 was evaluated by TÜV Informationstechnik GmbH. The evaluation was completed on 24 October 2006. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, and vendor and distributor is

SCM Microsystems GmbH
Oskar-Messter-Str. 13
85737 Ismaning, Germany

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 EAL3 augmented. The following table shows the augmented assurance components.

Requirement	Identifier
EAL3	TOE evaluation: methodically designed, tested, and reviewed
+: ADO_DEL.2	Delivery and operation. – Detection of modification
+: ADV_IMP.1	Development - Subset of the implementation of the TSF
+: ADV_LLD.1	Development - Descriptive low-level design
+: ALC_TAT.1	Life cycle support - Well-defined development tools
+: AVA_MSU.3	Vulnerability Assessment - Analysis and testing for insecure states
+: AVA_VLA.4	Vulnerability Assessment - Highly resistant

Table 1: Assurance components and EAL-augmentation

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.

[8] Information Technology Security Evaluation Facility

The following SFRs are taken from CC part 2:

Security Functional Requirement	Addressed issue
FCS	**Cryptographic support**
FCS_COP.1	Cryptographic operation
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_RIP.2	Subset residual information protection
FTA	**TOE access**
FTA_TAB.1	Default TOE access banners
FPT	**Protection of the TOE Security Functions**
FPT_PHP.1	Passive detection of physical attack

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

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

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

TOE Security Function	Addressed issue
SF.PINCMD	The firmware in the reader checks the commands sent to the reader by means of the command structure compliant to the USB smart card reader specification. If commands for Verification or Modification of the PIN are recognized and if the command, which has to be forwarded to the smart card, contains one of the following instruction bytes: • VERIFY (ISO/IEC 7816-4): INS=0x20 • CHANGE REFERENCE DATA (ISO/IEC 7816-4): INS=0x24 • ENABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4): INS=0x28 • DISABLE VERIFICATION REQUIREMENT (ISO/IEC 7816-4): INS=0x26 • RESET RETRY COUNTER (ISO/IEC 7816-4): INS=0x2C • UNBLOCK APPLICATION (EMV2004): INS=0x18 it will be switched into the mode for secure PIN entry over the integrated keypad. The RS232 version of the reader emulates the protocol, which is specified for the USB smart card reader, so for both host interface versions an identical data stream will be processed by the security functions. The security function SF.PINCMD recognizes the command for PIN entry, sent by the host software, and inserts the PIN data

TOE Security Function	Addressed issue
	entered over the keypad to the corresponding place in the command to the smart card. As well, only the fact that one of the numeric keys is pressed is reported to the host. During the PIN entry the corresponding LEDs display the mode of secure PIN entry. The exchange of the PIN takes place only between smart card and TOE over the card reader interface. This interface is inside the TOE and from manipulation protected by the security seal.
SF.CLMEM	The memory area for the PIN data will be reworked after transfer of the command to the smart card, after removing the card, after cancellation by the user, after a timeout during PIN entry, during switch on process and after defined reset commands from the host.
SF.SECDOWN	The verification of a signature of the firmware with the asymmetric RSA algorithm and a bit length of 1024 guarantees the integrity and authenticity of the firmware during loading of a new firmware into the smart card reader. The hash value over those firmware, which will be loaded, is determined based on the algorithm SHA-1 with a length by 160 bits. The verification of the integrity and authenticity takes place in the TOE via comparison of the determined hash value and the hash value as a component of the decoded signature. The public key for this operation is stored in the TOE.
Security measure	The housing is sealed by means of a falsification secure security sticker, which will be destroyed during removal and thus can be used only once. Thus the user can recognize by the condition of the safety seal that no manipulations at the hardware were made.

Table 3: Security Functions of the TOE

For more details please refer to the Security Target [6], chapter 6.1 and 6.2.

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

The values that must be protected are identification data (PIN) of the user as well as the firmware and hardware of the smart card reader itself.

Those assets are threatened by an attacker with high attack potential. The following threads are identified in the Security Target:

Thread	Summary
T.REVEAL	The attacker could try to intercept the communication between host and smart card and/or smart card reader over a Trojan horse (virus), if the PIN is entered into the host equipment. Or the attacker could try to attain a PIN code outside of the commands planned for it.
T.STORE	Storing identification data in the TOE also poses a danger of attack because these data could be obtained from the TOE by an attacker, if the attacker came into the possession of the TOE and would have the technical facility.
T.DOWNLOAD	By manipulations during the download, a modified or unauthorized firmware could be loaded into the reader, which could contain capabilities for uncovering the PIN.
T.SEAL	By manipulation of the seal and following manipulation of the hardware after opening the reader the attacker can intercept the communication between reader and smart card.

Table 4: Threats to the TOE

Organisational policies are not formulated in the Security Target.

1.5 Special configuration requirements

The results of the evaluation are valid for the following version of the TOE:

smart card reader SPR532, firmware version 5.09.

The necessary information regarding the installation and start-up of the TOE are provided in the user guidance [11] and [10]. The upload of a firmware version into a smart card reader SPR532 other than 5.10 is not a matter of configuration but a change of the TOE that is not in the scope of this evaluation and certificate.

1.6 Assumptions about the operating environment

The SPR532 smart card readers are suitable both for office and for private use. Due to their multi-functionality, the readers can support additional uses beyond signature applications, such as secure home banking. In general, the end user is informed about his or her responsibility during the use of the TOE. In detail, the following assumptions are mentioned in the Security Target [6, chapter 3.1]:

Assumption	Summary
A_USER.VERSION	Regular check of the version of the software.
A_USER.UNOBSERV	Unobserved input of the PIN.

Assumption	Summary
A_USER.KEYPAD	Usage of the integrated keypad to enter the authentication data.
A_USER.LED	Verification of LEDs while entering the PIN.
A_USER.SEAL	Observation of the security seal.
A_USER.STORE	Communication of rules for the handling of PIN and smart card.
A_USER.USAGE	Responsible usage of the TOE in the designated environment.
A_USER.ISO_EMV	Usage of smart cards that are compliant to the ISO [14] – and EMV [15] - Standard.
A_USER.FWLOAD	Download of certified firmware only.
A_USER.SIG_APP	Application of the TOE for qualified electronic signatures only together with evaluated and confirmed signature application components.

Table 5: Assumptions about the operational environment of the TOE

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:

smart card reader SPR532, firmware version 5.09

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Smart card reader SPR532 with serial RS232 and USB cable connector	Part number 904712	packed in a blister foil bag
2	SW	Firmware	5.09	• together with the hardware • on the installation CD-ROM (see below) • download from http://scmmicro.com/security/pcs_product_drivers.html
3	DOC	User manual (english)	1.22	pdf-document or printed form

No	Type	Identifier	Release	Form of Delivery
4	DOC	Bedienungsanleitung (german)	1.21	pdf-document or printed form
5	DOC	SPR532 DLL API Document	1.5	pdf-document
6	DOC/SW	Installation CD including the software to check the version number of the firmware and to conduct the firmware download		CD-ROM

Table 6: Deliverables of the TOE

The content of the installation CD (no. 6 in Table 6) apart from the items 2, 3, and 4 mentioned in Table 6 is not part of the evaluation and thus not included in this certificate.

2.1 Delivery of the firmware including the hardware

Every reader is packed seperately in a blister foil bag that is closed with a yellow sticker. From the production site the readers are delivered in bulk cartons either directly to the customer or to subcontractors of the vendor. The subcontractors arrange the single readers into end user packages according to the requirements of the customer. Each end user package will contain at least the installation CD including the deliverables 2, 3 and 4 listed in Table 6. The deliverable no. 5 in Table 6 is only intended for application developers. This document is available upon request from the vendor.

The end user can clearly identify the TOE by the part number 904712 printed on the bottom label of the TOE. Furthermore, the bottom label shows the id of the certification procedure (BSI-DSZ-CC-0363) that allows the end user to retrieve the certification report from the web-pages of BSI. The next figure shows an example of the label with the part number encircled.

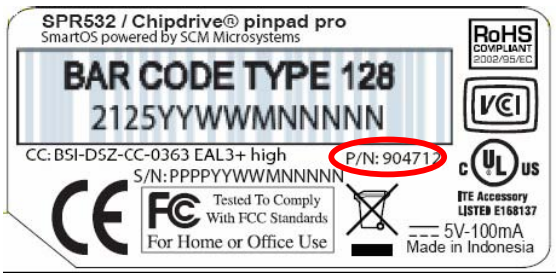

Figure 1: Example of bottom label

2.2 Delivery of the firmware without hardware

In addition to the delivery of the TOE including the hardware it is possible to download the new firmware version alone together with the Windows tools (USB, RS232) for the firmware update from the internet side

http://scmmicro.com/security/pcs_product_drivers.html. In this case, the items 2, 3, and 4 of Table 6 belong to the TOE.

The TOE contains a functionality that can be used to update already delivered smart card readers SPR532 to new firmware version. This functionality consists of the mathematical verification of the signature of the firmware during the upload of a new version to guarantee the integrity and authenticity of the certified firmware. As the part number 904712 mentioned in Table 6 refers only to newly produced smart card readers SPR532 with the firmware 5.09, the part number of smart card readers to be updated to the new firmware version is typically different. The combination of the certified firmware version 5.09 with smart card readers labelled with the following part numbers is also included in this certificate:

- smart card reader SPR532 labelled with the part number 903391 and certified with the certification id TUVIT-DSZ-CC-9209

The information regarding the certification id and the part number is always printed on a bottom label of a smart card reader similar to the one shown in Figure 1. For details on the different deliverables refer to chapter 2.

3 Security Policy

The TOE is intended to be used for the application of qualified electronic signatures according to the German Signature Law ([8]). To apply a qualified electronic signature, a signatory must authenticate himself by possession of a secure signature creation device and knowledge of the signature PIN.

Consequently, the security policy of the TOE focusses on the protection of the firmware, the signature PIN and the integrity of the hardware.

The security objectives of the TOE are the non-proliferation of the PIN apart from passing it to the smart card, the integrity-protection of the firmware and the signalling of manipulation of the hardware.

4 Assumptions and Clarification of Scope

The assumptions already listed in Table 5 in a short form are presented here as an excerpt from the Security Target.

4.1 Usage assumptions

Assumption	Summary
A_USER.VERSION	It is assumed that the user verifies routinely with a software tooll provided by the manufacturer, whether the version number of the TOE agrees with the confirmed version, before use of the smart card reader.
A_USER.UNOBSERV	The user must enter his or her identification data unobserved.
A_USER.KEYPAD	It is assumed that the user enters his or her identification data using the keypad of the TOE.
A_USER.LED	While the PIN is being entered on the keypad of the reader, the status of the LED verifies that the mode of the secure PIN input is active.
A_USER.SEAL	The user routinely has to examine that the security seal is intact.
A_USER.STORE	The rules to the secure keeping and non-proliferation of the PIN are communicated to the user by the publisher of the smart card.
A_USER.USAGE	The TOE is laid out for use in private and office environments. In an office environment, the SPR532 smart card reader should be arranged in such a way that the usage is avoided by unauthorized users. That means that the smart card reader is set up in such a manner that its usage is possible for authorized persons only and that a working environment protected from manipulation attempts has to be guaranteed. An unobserved input of identification data (PIN) is to be ensured by suitable measures at the place of work.
A_USER.ISO_EMV	For applications requesting a secure PIN input the user has to use only processor smart cards compliant to ISO 7816 [14] or EMV [15].
A_USER.FWLOAD	The user may download firmware versions of the TOE from the Internet site of the manufacturer, the supplier or the distributor as well as from intranet sites of a company. It is assumed that it is clearly communicated during the download of the firmware from an external source, whether or not the firmware is CC certified. It is assumed that the user will download CC certified firmware versions only. It is assumed that the user knows that he or she will loose the CC certified and SigG/SigV confirmed status of the product, if he or she downloads any non CC certified firmware version to the TOE.

Table 7: Usage Assumptions

4.2 Environmental assumptions

Assumption	Summary
A_USER.SIG_APP	It is assumed that for the use of the TOE in accordance with SigG/SigV, only applications and smart cards that were evaluated and confirmed in the SigG context are used.

Table 8: Environmental assumptions

4.3 Clarification of scope

Threats that are only countered by settings in the IT-environment were not detected in course of the evaluation and thus not depicted in the Security Target. Nevertheless, the assumptions listed in Table 7 and Table 8 support the TOE to reach its security objectives and assist the security functions to counter the threats mentioned in chapter 1.4.

For a more detailed description of the security function, security functions and a rationale how the single threats are countered by the combination of assumptions and security functions see the Security Target [6].

5 Architectural Information

The TOE comprises hard- and software and is delivered either as a complete smart card reader or as a firmware version alone (see chapter 2). Apart from the security sealing the hardware does not provide any security relevant features and can be separated as follows:

- Microcontroller with internal volatile and non-volatile memory, USB-controller and smart card controller
- USB-interface or RS232-interface including cable and connector
- display unit consistings of LEDs in different colors
- smart card interface

The firmware that provides the main security functions is composed of different subsystems. These subsystems and their functionality are listed in the next table.

Subsystem	Description
USB SUBSYSTEM	This subsystem manages and implements all functions relating to the processing of the standard USB commands, and the host specific secure and non-secure commands.
RS232 SUBSYSTEM	This subsystem manages and implements all functions relating to the processing of the host specific secure and non-secure commands.
CCID SUBSYSTEM	This subsystem shall process the CCID messages received from the USB/RS232 subsystems.
SMARTOS SUBSYSTEM	This subsystem implements functions that manage the smart card specifics for the host interface subsystems like USB, RS232.
SECUREPINPAD SUBSYSTEM	This subsystem processes different CCID messages. It handles the user PIN entry, formatting of the PIN to the appropriate PIN format type selected and dispatches accordingly.

Subsystem	Description
SECUREDOWNLOAD SUBSYSTEM	This subsystem mainly implements the SF3 SECDOWNLOAD security function.

Table 9: Architectural description of the firmware

6 Documentation

The following documentation is provided for the end customer:

- “Klasse-2-Chipkarten-Leser SPR532 Bedienungsanleitung”, version 1.21, 03/04/2006
- “Class 2 Smart Card Reader SPR532 User Manual”, version 1.22, 03/22/2006
- SPR532 DLL API Documentation, version 1.5, 04/25/2006

Other documentation relevant for this certification procedure is listed in chapter 14.

7 IT Product Testing

7.1 Developer tests

The manufacturer tests were executed with smart card readers SPR532 with the part number (P/N) 904712 and 903391 and the firmware version 5.09 as defined in the Security Target [6].

For the tests the TOE is operated at an IBM compatible PC system with a 32 bit Microsoft Windows operating system. In accordance with the test strategy of the manufacturer the scheduled functional tests are to show the compliance of the TOE with the security functions described in the functional specification.

The tests were executed and documented related to the security functions. A test plan was created that includes the following items for every test:

- The goal of the single test
- The expected test result
- The description how to execute the tests
- The actual test result.

As the test coverage analysis is proving, the manufacturer tested the TOE systematically on the level of the security functionalities from the functional specification and the subsystems of the high level design.

The manufacturer specified functional tests for every security function. For all tests, the expected test results matched with the actual results. No faults were

discovered and no differences occurred concerning the described security functionality. Consequently all security functions were tested successfully.

7.2 Evaluator tests

Independent testing of the evaluators was performed with the smart card readers SPR532 with the part number 904712 and 903391 in combination with the firmware version 5.09. For the tests the TOE was operated at an IBM compatible laptop with a 32 bit Microsoft Windows operating system.

In accordance with the test strategy of the evaluator the scheduled independent tests of the TOE are to show the fulfillment of the functional security requirements in accordance with the Security Target and the compliance with the described security functionality in the functional specification. Furthermore all subsystems and interfaces are to be included in the tests in accordance with the high level design.

For every test a test plan is created with the test goal, the used test configuration, the described method of testing, the expected test results and the actual test results.

The Evaluator selected and tested a sample from the manufacturer tests of the security functions of the TOE. The sample of the Evaluator covers all security functions of the TOE and considered the characteristics in accordance with the functional specification. These test cases address both the normal process of the secure pin entry and different kinds of fault situation.

The actual results matched with the expected results. No faults were discovered and no differences occurred concerning the described security functionality. All security functions could consequently be tested successfully.

7.3 Penetration tests

The evaluators searched for vulnerabilities by means of manufacturer documents and test reports as well as the guidelines mentioned in the CEM [2] and AIS 34 [4]. The evaluator also examined the security measure sealing of the TOE with regard to the attachment and positioning of the seals for vulnerabilities. By conducting the tests identified in the test concept the evaluators examined the complete and correct implementation of the security functions and searched for hidden functions or further commands.

During penetration testing the security functions of the TOE worked as specified. Furthermore the penetration tests showed that it was not possible to remove the security sealing without destroying it. Any vulnerabilities detected by the evaluators were not exploitable in the intended environment. According to the misuse analysis, no insecure state was detected.

8 Evaluated Configuration

The tests of the developer and the evaluator were conducted with devices equal to those that can be purchased by the end user.

This certificate extends only to the following tested and evaluated version of the TOE:

smart card reader SPR532, firmware version 5.09

The sites for the development of the firmware and the final assembly of the TOE constitute an integral part of this evaluation. Thus it is compulsory that the TOE is developed and manufactured by

- SCM Microsystems (India) Pvt. Ltd, Chennai, India and
- PT BESA Engineering, P. Batam, Indonesia.

9 Results of the Evaluation

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

The evaluation methodology CEM [2] was used for those components identical with EAL3+. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4, AIS 34]).

The verdicts for the CC, Part 3 assurance components (according to EAL3 augmented by ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4) 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
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
Authorisation controls	ACM_CAP.3	PASS
TOE CM coverage	ACM_SCP.1	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS

Assurance classes and components		Verdict
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Subset of the implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.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
Identification of security measures	ALC_DVS.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-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
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 10: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL3 augmented by ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 and AVA_VLA.4.

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

(i) the TOE Security Function SF.SECDOWN (SF.3)

The results of the evaluation are only applicable to the smart card reader SPR532, firmware version 5.09 (see chapter 2 for the identification of the TOE).

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 [10] - [12] contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition to that the Security Target [6] contains information that may be useful for the customer.

The security function SF.SECDOWN (SF.3) is based on the algorithms RSA-1024 and SHA-1 that the Bundesnetzagentur considers to be suitable for the creation of qualified electronic signatures. The algorithms must be replaced as soon as the chosen parameters or implemention reveal any vulnerability and are there therefore not suitable to guarantee the integrity and authenticity of the firmware anymore. According to the assessement of the Bundesnetzagentur [18] the algorithm RSA-1024 is valid until the end of 2007, and the hash function SHA-1 may be used only until the end of 2009 for the creation of qualified electronic signatures. At the latest if the validity period for one of these algorithms expires a replacement with stronger algorithms is recommended.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
CCID	Chip Card Interface Device
EAL	Evaluation Assurance Level
ICC	Integrated Chip Card
IT	Information Technology

PIN	Personal Identification Number
PP	Protection Profile
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

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.

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

[6] Security Target BSI-DSZ-0363-2006, Version 1.21, 06/06/2006, Security Target to reach the evaluation level Common Criteria EAL3+ for the class 2 smart card reader SPR532, SCM Microsystems

[7] Evaluation Technical Report, 1.4, 10/20/2006, CC Evaluation of SmartCardReader SPR532 (confidential document)

[8] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) in der Fassung vom 16.05.2001 (BGBl. volume 2001 part I No. 22 p. 876)

[9] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) in der Fassung vom 16.11.2001 (BGBl. volume 2001 part I No. 59 p. 3074)

[10] Klasse-2-Chipkarten-Leser SPR532 Bedienungsanleitung, Version 1.21, 03/04/2006, SCM Microsystems GmbH

[11] Class 2 Smart Card Reader SPR532 User Manual, Version 1.22, 03/23/2006, SCM Microsystems GmbH

[12] SPR532 DLL API Document, Version 1.5, 04/25/2006, SCM Microsystems GmbH

[13] Device Class Specification for USB Chip/Smart Card Interface Devices, Revision 1.00, March 20, 2001

[14] DIN ISO 7816 - 1 Identification cards - Integrated circuit(s) cards with contacts – Physical Characteristics

DIN ISO 7816 - 2 Identification cards - Integrated circuit(s) cards with contacts - Dimensions and locations of the contacts

DIN ISO 7816 - 3 Identification cards - Integrated circuit(s) cards with contacts - electrical characteristics and transmission protocols

DIN ISO 7816 - 4 Information technology - Identification cards - Integrated circuit(s) cards with contacts - Inter - industry commands for interchange

DIN ISO 7816 – 8 Identification cards – Integrated circuit(s) cards with contacts – Security related interindustry commands

[15] EMV 2000 Book 1 - Application independent ICC to Terminal Interface requirements, Version 4.0, December 2000

[16] Anwendungsunabhängiges CardTerminal Application Programming Interface (CT-API) für Chipkartenanwendungen, Revision 1.1, 10/14/1998

[17] Interoperability Specification for ICCs and Personal Computer Systems, PC/SCWorkgroup, Version 1.0, Dezember 1997

[18] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 02. Januar 2006, published 23. March 2006 in the Bundesanzeiger No. 58, S. 1913-1915

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.”