Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0592-2010

for

Smart card reader SPR332 firmware version 6.01

from

SCM Microsystems GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0592-2010

class 2 smart card reader

Smart card reader SPR332
firmware version 6.01

from	SCM Microsystems GmbH
PP Conformance:	None
Functionality:	Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 and AVA_VLA.4.

Common Criteria
Recognition
Arrangement
for components up to
EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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.

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.

Bonn, 19 February 2010
For the Federal Office for Information Security

IT
Security
Certified

SOGIS - MRA

Bernd Kowalski L.S.
Head of Department

This page is intentionally left blank.

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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 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

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

This evaluation contains the components AVA_MSU.3 and AVA_VAN.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 SPR332, firmware version 6.01 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0394-2006.

The evaluation of the product smart card reader SPR332, firmware version 6.01 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 15 December 2009. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: SCM Microsystems GmbH

The product was developed by: SCM Microsystems GmbH

[6] Information Technology Security Evaluation Facility

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. 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 and in the Security Target.

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.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product smart card reader SPR332, firmware version 6.01 has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] SCM Microsystems GmbH
Oskar-Messter-Straße 13
85737 Ismaning

This page is intentionally left blank.

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.

1 Executive Summary

The Target of Evaluation (TOE) is the smart card reader SPR332 with the firmware version 6.01. It is a universal smart card reader with a keypad unit, which in whole builds the TOE. The keypad comprises the numeric keys “0” to “9” as well as the keys “Clear” (yellow), “Confirmation” (green) and “Cancel” (red). The enclosure of the smart card reader is sealed with a security seal so that any attempts to manipulate the hardware are made obvious to the user.

The TOE works with all smart card transmission protocols compliant to ISO 7816 (T=0, T=1) and EMV2004 [17]. Data transmission protocols for memory cards (I2C, 2-wire, 3-wire protocol) are also supported.

The reader can be used at all host systems that contain an USB interface. On the host side the application interfaces are made available as CT-API and PC/SC, which can be used for all types of smart cards.

The smart card reader realises secure PIN entry functionality over its keypad, whereas the PIN data are only redirected to the connected smart card, but do not leave the TOE in direction to the host computer. The application receives only a signal that one of the numeric keys was pressed, but not which key.

If a host application sends one of the commands listed in table 1 to an inserted smart cards the smart card reader SPR332 switches into the secure PIN entry mode, which is indicated to the user by the LEDs. Non-supported instruction bytes will be rejected with a qualified error message:

Command	Standard	Instruction byte
VERIFY	ISO/IEC 7816-4	INS=0x20
CHANGE REFERENCE DATA	ISO/IEC 7816-8	INS=0x24
ENABLE VERIFICATION REQUIREMENT	ISO/IEC 7816-8	INS=0x28
DISABLE VERIFICATION REQUIREMENT	ISO/IEC 7816-8	INS=0x26
RESET RETRY COUNTER	ISO/IEC 7816-8	INS=0x2C
UNBLOCK APPLICATION	EMV2004	INS=0x18

table 1: Supported instruction bytes

Therefore the smart card reader as a class 2 reader is able to capture identification data (PIN) and to transmit it to a secure signature creation device (signature smart card). Moreover, the TOE is used for the transmission of the hash value from the application to the signature card and for the end around carry of the signature from the card to the signature creation application on the host system. Thus, the TOE can be used as a component for the creation of electronic signatures in accordance with SigG [9] and SigV [10].

For future use the firmware of the smart card reader can be replaced. A new version of the firmware must be digitally signed by the SCM. During the upload of the new firmware into the memory of the TOE the electronic signature is verified. If the signature is not valid, the device cannot communicate with a smart card until a correct signed firmware version is installed.

The smart card reader SPR332 is suitable both for office and private use. The TOE offers protection against attackers with a high attack potential whereas the assumptions especially with respect to the operational environment must be fulfilled.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL3 augmented by ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 and AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

The Security Target does not contain any Security Functional Requirements (SFR) relevant for the IT-Environment.

The TOE 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 instruction bytes mentioned in table 1, it will be switched into the mode for secure PIN entry over the integrated keypad. The security function SF.PINCMD recognizes the command for PIN entry sent by the host software and inserts the PIN data entered over the keypad into 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 protected from manipulation 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 the start-up process of the device 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 2048 bits guarantees the integrity and authenticity of a new firmware version that may be loaded into the smart card reader in future. The hash value over this new firmware is calculated by means of the algorithm SHA-256 with a length of 256 bits. The verification of the integrity and authenticity takes place in the TOE via comparison of the determined hash value and the hash value decoded from the signature. The public key for this operation is stored in the TOE.
Security measure	The enclosure is sealed by means of a falsification secure security sticker, which will be destroyed during removal. Thus the user can recognize by the condition

TOE Security Function	Addressed issue
	of the safety seal that no manipulations at the hardware were made.

table 2: TOE Security Functions

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

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6], chapter 1 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). For details see chapter 9 of this report.

The TOE Security Environment is defined in terms of Assumptions and Threats. This is outlined in the Security Target [6], chapter 3.

This certification covers the following TOE: smart card reader SPR332 with the firmware version 6.01 that can be identified by the part number 905127. For details refer to chapter 2 and 8.

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 SPR332 firmware version 6.01

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	smart card reader SPR332 with firmware and USB connector.	firmware version 6.01, smart card reader part number 905127	bulk shipment in a carton.
2	SW	setup program for software installation on PC (for Windows 2000 – Windows 7)	1.00	CD-ROM
3	DOC	Class 2 Smart Card Reader SPR332 User Manual	1.44	PDF-document on CD-ROM or printed document
4	DOC	Klasse-2-Chipkarten-Leser SPR332 Bedienungsanleitung	1.44	PDF-document on CD-ROM or printed document
5	DOC	SPR532 DLL API Document	1.5	PDF-document
6	SW	fw601_check.exe	6.01	Executable on the CD-ROM

No	Type	Identifier	Release	Form of Delivery
7	SW	Driver software for the SPR 332 smart card reader for the operating systems Windows 2000 - Windows 7		CD-ROM
		PC/SC driver	4.45	
		CT-API driver	2.63	

table 3: Deliverables of the TOE

The deliverables no. 2, 6 and 7 in table 3 are not part of the evaluation and thus not included in this certificate.

Every smart card reader is packed separately 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 3. The deliverable no. 5 in table 3 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 905127 and the certification id (BSI-DSZ-CC-0592) printed on the bottom label of the TOE. The next figure shows an example of the label with the part number and certification id encircled.

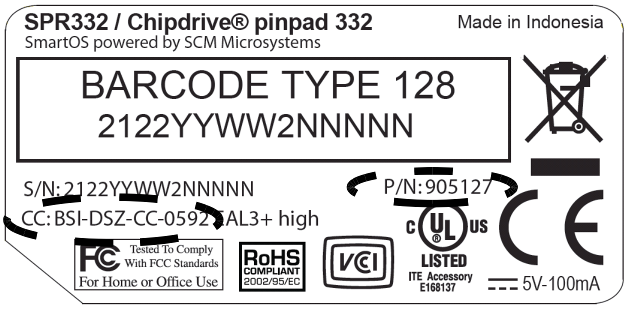
SPR332 / Chipdrive® pinpad 332
Made in Indonesia
SmartOS powered by SCM Microsystems
BARCODE TYPE 128
2122YYWW2NNNNN
S/N:2122YYWW2NNNNN
P/N:905127
CC: BSI-DSZ-CC-0592 EAL3+ high
Tested To Comply With FCC Standards
For Home or Office Use
RoHS COMPLIANT 2002/95/EC
LISTED
ITE Accessory E168137
5V-100mA

Figure 1: bottom label of the TOE

Furthermore, the user should verify the firmware version to ensure that the smart card reader is always operating with the certified firmware (6.01). To check the firmware version, the user has to use the "fw601_check.exe" utility provided together with the TOE by SCM on the CD ROM (item no. 6 in table 3). The user has to run the program directly from the CD-ROM to ensure that the application has not been modified. In case the "fw601_check.exe" utility indicates a deviation of the firmware version (i.e. a different version than 6.01), the configuration of the smart card reader is different to the configuration covered by this certificate and may have been manipulated. The user should contact the developer to find out more about the status and authenticity of the firmware. Without a certified and approved firmware version the TOE must not be used for applications following the German signature law (SigG).

3 Security Policy

The TOE is intended to be used for the application of qualified electronic signatures according to the German Signature Law [9]. 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 defined in the Security Target and some aspects of Threats are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- Adequate behaviour of the user. The user must pay attention to enter the PIN for the creation of qualified electronic signatures unobserved by means of the keypad of the smart card reader. In this case the LEDs must signal that device resides in the secure PIN-entry mode. Furthermore the user must not disclose his PIN and use a smart card that supports the corresponding protocols.
- The user should control the firmware version installed on the device. For this purpose he should start the tool “fw601_check.exe” from the CD-ROM that is delivered along with the hardware.
- The smart card reader SPR 332 must only be used in an environment where access to the device is only possible for trustworthy personal. This means that it is intended for private use or in offices where the access to is strictly controlled.

Details especially for the behaviour of the user can be found in the Security Target [6], chapter 4.

5 Architectural Information

The TOE comprises hard- and software and is delivered as a complete smart card reader (see table 3). 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 including cable and connector
- display unit consisting of LEDs in different colours
- 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. This subsystem helps to connect the host level commands through the USB bus with the secure download and the CCID subsystems.
CCID SUBSYSTEM	This subsystem shall process the CCID messages received from the USB subsystems. This subsystem dispatches the messages to SmartOS or Secure PIN management subsystems, based on the received message and updates the error/status/data returned by the other subsystems to the caller. Also this subsystem implements functions that manage the reader specifics for the host interface subsystems.
SMARTOS SUBSYSTEM	This subsystem implements functions that manage the smart card specifics for the host interface subsystems like USB Functions that provide methods for card power control, card reset and submitting APDUs. This subsystem connects with the secure pinpad and CCID subsystems.
SECUREPINPAD SUBSYSTEM	This subsystem implements the SF.PINCMD and SF.CLMEM security functions as derived from the Security Target of this product. This subsystem shall process the Verify and Modify CCID PIN entry messages. It shall handle the user PIN entry, formatting of the PIN to the appropriate PIN format type selected and dispatches the APDU to the SmartOS subsystem. The response received from SmartOS is returned back to the CCID command-processing subsystem.
SECUREDOWNLOAD SUBSYSTEM	This subsystem mainly implements the SF.SECDOWN security function as defined in the ST of this product. This subsystem shall implement functions that involve processing of USB DFU class requests and to successfully perform the DFU operation. When the DFU detach command is received, the USB subsystem aborts any pending operation and hands over control to this subsystem to start the DFU process. Moreover, the purpose of this subsystem is to verify the functional firmware to be downloaded using a SHA-256 digest encrypted with the 2048-bit RSA Key as signature.

table 4: Subsystems of the firmware software

6 Documentation

The evaluated documentation as outlined in table 3 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

7.1 Developer Tests

For the test the TOE was attached to different IBM-compatible PC-Systems. The developer's tests were conducted with the goal to confirm that the TOE meets the security functional requirements. The developer's strategy was to test the TOE against the specification of all security enforcing functions detailed in the functional specification and in the high-level design. The manufacturer presented corresponding test objectives and specified suitable tests for each of the security functions

- SF.PINCMD

- SF.CLMEM
- SF.SECDOWN.

The tests reported in the testing documentation completely cover the security functions of the TOE defined in the functional specification and the Security Target.

The manufacturer tested the TSF on the level of the subsystems mapping them to the related test cases and thus confirmed their correct functioning. Tests were conducted not only for all security functions but also for all subsystems and, moreover, all modules of the TOE. In doing so, the tests ensured that all external interfaces of the TOE and all internal interfaces between the subsystems were tested.

The test results obtained for all of the performed tests turned out to be as expected. No errors or other flaws occurred with regard to the security functionality, the interfaces and the TOE subsystems. Consequently, the test results demonstrate that the behaviour of the security functions are as specified.

7.2 Evaluator's Tests

The evaluator's testing strategy was to test the functionality of the TOE as described in the Security Targets [6]. The subset of tests was sampled so that the TOE security functions (TSF) with the external interfaces specified in the functional specification and subsystems from the architectural design documents were covered.

The test environment for the independent testing was equivalent to that used for the developer's tests. This includes a subset of the software tools used by the developer to perform the tests.

The results of the independent evaluator tests including the repeated developer tests confirm the TOE functionality as described in the Security Target, the functional specification and the high level design. All the actual test results were consistent with the corresponding expected results and there resulted no hints to any errors.

7.3 Penetration tests

The evaluator performed penetration tests based on the vulnerability analysis of the manufacturer and an independent search for vulnerabilities. The vulnerability analysis took the manufacturer documents, test reports as well as the guidelines mentioned in the CEM [2] and AIS 34 [4] in account. 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.

The evaluator confirms that misuse cannot lead to an insecure state of the TOE which cannot be recognized by the user. The penetration testing conducted confirms that the vulnerabilities identified are non-exploitable in the intended operational environment of the TOE. Thus, the TOE resists attackers with a high attack potential.

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 SPR332, firmware version 6.01

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
- OSI Electronics, P. Batam, Indonesia.

9 Results of the Evaluation

9.1 CC specific results

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 up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 [4] (AIS 34).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL3 package as defined in the CC (see also part C of this report)
- The components ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 and AVA_VLA.4 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0394-2006, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the implementation of new algorithms for the firmware signature as well as some adoptions to improve the compatibility of the smart card reader with several secure signature creation devices and banking cards.

The evaluation has confirmed:

● PP Conformance:	None
● for the Functionality:	Common Criteria Part 2 conformant
● for the Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3 and AVA_VLA.4.

- The following TOE Security Functions fulfil the claimed Strength of Function:
  high
  SF.SECDOWN

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The following cryptographic algorithms are used by the TOE to enforce its security policy:

- hash functions:

  SHA-256

- algorithms for the encryption and decryption:

  RSA-2048

This holds for the following security functions:

- SF.SECDOWN

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 9, Para. 4, Clause 2). According to regulations of the Federal Network Agency and the assessment of the BSI [20] the algorithms are considered to ensure a commensurate level of assurance for the signature of the firmware. The validity period for the assessment of each algorithm is mentioned in the official catalogue [11] and summarized in chapter 10.

10 Obligations and Notes for the Usage of the TOE

The operational documents as outlined in table 3 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, the following aspects need to be fulfilled when using the TOE:

- The Security Target [6] defines assumptions about user behaviour, place of installation, usage of smart cards, PIN handling and several other aspects. The user must make sure that these assumptions are met when using the TOE.

According to the catalogue of the Federal Network Agency the cryptographic algorithms used for the signature of the firmware are considered to be appropriate for the creation even of qualified electronic signatures until the end of 2015. Therefore the security function SF.SECDOWN is expected to provide the necessary level of assurance in the integrity of the firmware at least until the end of 2015.

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
DFU	Device Firmware Upgrade
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
ICC	Integrated Chip Card
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
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
USB	Universal Serial Bus

12.2 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.

13 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.[8]

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

[6] Security Target BSI-DSZ-0592-2010, Version 1.35, 2009-08-26, Security Target to reach the evaluation level Common Criteria EAL3+ for the class 2 smart card reader SPR332 Title, SCM Microsystems GmbH

[7] Evaluation Technical Report, Version 5, 2009-12-15, EVALUATION TECHNICAL REPORT (ETR), TÜV Informationstechnik GmbH (confidential document)

[8] Configuration list for the TOE, Version 3.10, 2009-08-28, Configuration Item Record (confidential document)

[9] Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179) (SigG)

[10] Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631) (SigV)

[11] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 17. November 2008, published 27. January 2009 in the Bundesanzeiger Nr. 13, Seite 346

[12] Klasse-2-Chipkarten-Leser SPR332 Bedienungsanleitung, Version 1.44, 2009-0825, SCM Microsystems GmbH

[13] Class 2 Smart Card Reader SPR332 User Manual, Version 1.44, 2009-0825, SCM Microsystems GmbH

[14] SPR532 DLL API Document, Version 1.5, 2006-04-25, SCM Microsystems GmbH

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

[16] 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

[8] specifically

- AIS 34, Version 2, 24 October 2008, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

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

[17] EMV 2000 Book 1 - Application independent ICC to Terminal Interface requirements, Version 4.1, Juni 2004

[18] Anwendungsunabhängiges Card Terminal Application Programming Interface (CT-API) für Chipkartenanwendungen, Revision 1.1.1, 2001-06-07

[19] Interoperability Specification for ICCs and Personal Computer Systems, PC/SC Workgroup, Version 2.0, April 2005

[20] BSI - Technische Richtlinie Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 1.0, 20.06.2008

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:

- **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.
- **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:

- **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.
- **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:

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

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

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

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	**Assurance Family**
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	**Assurance Family**
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

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.”

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.