Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0537-2009

for

Sm@rtCafe Expert
Version 5.0

from

Giesecke & Devrient 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-0537-2009

Java Card

Sm@rtCafe Expert
Version 5.0

from	Giesecke & Devrient GmbH
PP Conformance:	Java Card System Protection Profile, Version 1.0b, Standard 2.2 Configuration, August 2003: DCSSI-PP/ 0305
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ADV_IMP.2 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 and guidance specific for the technology of the product 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, 17 December 2009
For the Federal Office for Information Security

IT Security Certified
SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

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 ADV_IMP.2 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 SmartCafe Expert Version 5.0 has undergone the certification procedure at BSI.

The evaluation of the product SmartCafe Expert Version 5.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 26 October 2009. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Giesecke & Devrient GmbH

The product was developed by: Giesecke & Devrient 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 SmartCafe Expert Version 5.0 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] Giesecke & Devrient GmbH
Prinzregentenstrasse 159
Postfach 800729
81607 München

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 Java Card SmartCafe Expert V5.0.

Parts of the TOE are the Java Card Runtime Environment (JCRE), the Java Card Virtual Machine (JCVM), the Java Card API, the Card Manager and the Smart Card Platform.

The final product contains Java and no native applications. However, there are vendor-specific libraries present on the card that are available to applets. These libraries contain native code and are not part of the TOE.

The Java Card SmartCafe Expert V5.0 is intended to transform a smart card into a platform capable of executing applications written in a subset of the Java programming language. The intended use of a Java Card platform is to provide a framework for implementing IC independent applications conceived to safely coexist and interact with other applications into a single smart card.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Java Card System Protection Profile, Version 1.0b, Standard 2.2 Configuration, August 2003: DCSSI-PP/0305 [10].

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 EAL 4 augmented by ADV_IMP.2 and AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 5.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6] and [9], chapter 5.3.

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

TOE Security Function	Addressed issue
SF.TRANSACTION	This security function ensures the rollback process. It provides assurance in the Java objects update in EEPROM.
SF.ACCESS_CONTROL	This security function is in charge of access control for the TOE. It is in charge of the FIREWALL access control SFP and the JCVM information flow control SFP
SF.CRYPTO	This security function controls all the operations related to the cryptographic key management and cryptographic operations.
SF.INTEGRITY	This security function provides a means to check the integrity of checksummed data stored in EEPROM.
SF.SECURITY	This security function ensures a secure state of information, the non-observability of operations on it and the unavailability of previous information content upon deallocation/allocation.
SF.APPLET	This security function ensures the secure loading of a package or installing of an applet and the secure deletion of applets and/or packages.
SF.RMI	This security function ensures secure remote method invocation features, which provides a new protocol of communication between the terminal and the applets.

TOE Security Function	Addressed issue
SF.CARRIER	This security function ensures secure downloading of applications on the card.
SF.CARDMANAGER	This security function ensures the security for the card manager.

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] and [9], chapter 6.1.

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6] and [9], chapter 6.1 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 assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.2. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 3.4 – 3.6.

This certification covers the following configurations of the TOE:

- Configuration 1: NXP P5CD040V0B (BSI-DSZ-CC-0404-2007),
- Configuration 2: NXP P5CD080V0B (BSI-DSZ-CC-0410-2007),
- Configuration 3: NXP P5CD144V0B (BSI-DSZ-CC-0411-2007).

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:

SmartCafe Expert Version 5.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Chip modules NXP P5CD040/080/144V0B	See [13], [14] and [15]	Modules implanted in plastic cards
2	SW	SmartCafe Expert V5.0 OS	5.0	Stored in the ROM of the chip
3	DOC	User and Administrator Guidance SmartCafe Expert V5.0 [11]	1.3	PDF-file

Table 2: Deliverables of the TOE

The TOE ROM code on the IC and additional mask keys are delivered to the initialisation site. The initialisation file is then securely loaded on the Smart Card at the initialisation site. The initialisation and the personalisation process are out of scope of this evaluation.

The hardware product can be identified from the ATR emitted by the product after reset. The EEPROM image data can be identified by the file name:

Chip Type	EEPROM Image file
P5CD040	V102-SF-4CC-CD040-036-004-CR-211-ENC.mot
P5CD080	V202-SF-4CC-CD080-036-004-CR-211-ENC.mot
P5CD144	V302-SF-4CC-CD144-036-004-CR-211-ENC.mot

Table 3: Identification of the EEPROM Image file

The product transmits a message, the ATR, immediately after it was powered up over its contacts, when triggered by activating the reset contact or after it was 'selected' in the standardized protocol for establishing contact-less communication. During product completion the ATR is the same in all cases and identifies the hardware component of the product:

Chip Type	ATR
P5CD040	3B F9 18 00 00 80 31 FE 45 53 46 2D 34 43 43 2D 30 31 CB
P5CD080	3B F9 18 00 00 80 31 FE 45 53 46 2D 34 43 43 2D 30 31 CB
P5CD144	3B F9 18 00 00 80 31 FE 45 53 46 2D 34 43 43 2D 30 31 CB

Table 4: ATR identifying product in completion process

In order to get the version of the TOE, the CPLC (Card Production Life Cycle) data could be read from the card by the GET DATA command.

The TOE identifier consist of three parts of the CLPC data. The three parts are, IC Fabricator, IC Type and the Release Level .

The GET DATA command has the following APDU format:

CLA	INS	P1	P2	Lc
´80´	´CA´	\`9F\`	\`7F\`	\`2D\`

Table 5: GET DATA command

TOE ID			
CHIP Type	IC Fabricator	IC Type	Release Level
P5CD040	47 90	50 38	50 01
P5CD080	47 90	50 40	50 01
P5CD144	47 90	50 43	50 01

Table 6: TOE identifier

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: Identification of subjects, correct operation, control of the availability of resources, control of the sharing of data container, restriction of the execution of native code, re-allocation of memory, cleaning of data container after the execution of an application, access control to memory, alarm after detection of a potential security violation, execution of operations, encryption of sensitive data, secure management of PIN objects, secure installation of applets, secure loading of packages, secure deletion of applets and packages, references to objects, restrictive remote access, recovery to a consistent and secure state, quality of random numbers, protection against disclosure of user data and TSF data.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies 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:

- Native code shall be conform to the TOE as stated in OE.NATIVE
- No applet loaded post-issuance shall contain native methods as stated in OE.APPLET.
- All the bytecodes shall be verified as stated in OE.VERIFICATION

Details can be found in the Security Target [6] and [9] chapter 4.2.

5 Architectural Information

The TOE consists of the 5 components:

- Java Card API (JC-API)
- Java Card Runtime Environment (JCRE)
- Java Card Virtual Machine (JCVM)
- Card Manager (CM)
- Smart Card Platform (SCP)

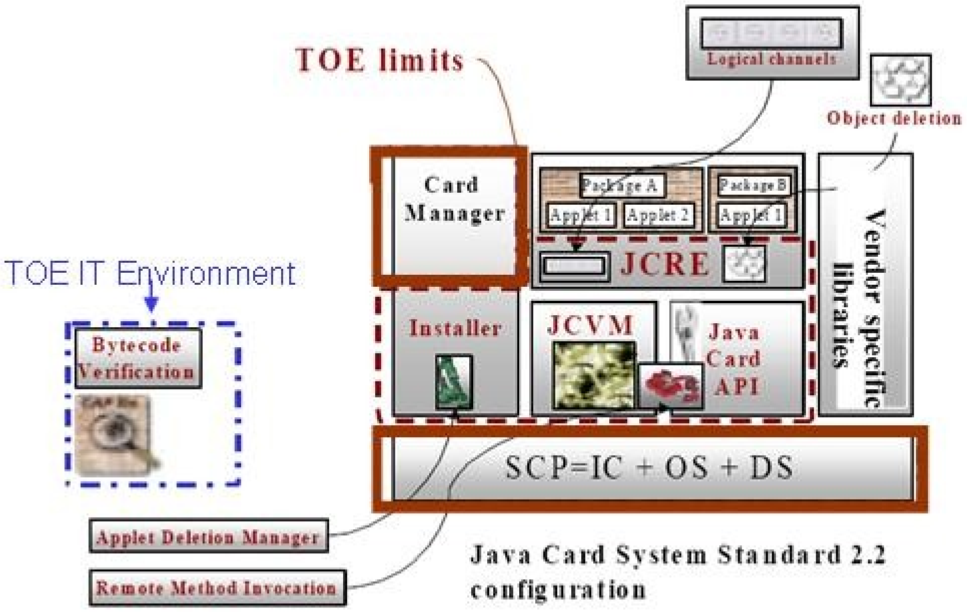

Figure 1 TOE Limits (dotted and straight red line): SCP (Smart Card Platform), IC (Integrated Circuit), OS (Chip Operating System), DS (Chip Dedicated Software). Contrary to the Java Card System Standard 2.2 configuration native Applications are not part of the product except vendor-specific libraries.

6 Documentation

The evaluated documentation as outlined in table 2 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 TOE configurations tested

The tests are performed with the composite smart card product. The physical format of the test configuration for TOE testing is either

- a card which is usable for all directly testable requirements, which are tested through System Tests. Each of these system tests has one or more Java Card applets that are contained in one or more Java packages. Note, that applets are not part of the TOE and therefore out of scope. The hardware platform was always the NXP P5CD144V0B.
- an emulator which is required for test cases that could not be tested directly. All indirectly testable requirements are tested through Module Tests.

As the initialisation and the personalisation process are out of scope of this evaluation, the TOE was always tested in its usage phase.

7.2 Developer's Test according to ATE_FUN

Developer’s testing approach:

- All TSF as specified in the functional specification with related sub-functions and subsystems are tested in order to assure complete coverage.
- The overall approach is to test all testable statements stated in the functional specification including different aspects of the commands as security functional effects. Each TSP enforcing subsystem and internal interface of the high level design has tests mapped.
- Test procedures are implemented in accordance with functional specification and the high level design in order to verify the TOE’s compliance with its expected behaviour.
- All test cases were run successfully on this TOE version.

Amount of developer testing performed

The developer tested the nine TSF of the TOE

- with system and module tests, grouped into several logical and/or functional units, so called test packages.
- at the level of testable statements as given in the functional specification.
- at the level of the subsystems and interfaces as given in the high level design.

Overall developer testing results

- All testing strategies of the TSF passed all tests of individual test scenarios so that all TSF were successfully tested against the functional specification and the high level design.
- The developer’s testing results demonstrate that the TSF perform as specified.
- The developer’s testing results demonstrate that the TOE performs as expected.

7.3 Evaluator Tests according to ATE_IND

Approach

- Examination of developer’s testing amount, depth and coverage analysis and of the developer’s test goal and plan for identification of gaps.
- Examination whether the TOE in its intended environment, is operating as specified using iterations of developer’s tests.
- Independent testing was performed by the evaluator at the ITSEF with the TOE development environment using script based developer test tools with automated comparison of expected and actual test results
- The evaluator verified the developer’s test results by executing all tests in the developer’s test documentation and verifying the test log files for successful execution.

TOE test configurations

- TOE smart cards and test cards
- TOE test images tested on a hardware simulator

Subset size chosen

- During sample testing the evaluator chose to repeat all developer functional tests at the Evaluation Body for IT Security in Essen that cover all TSF.
- During independent testing the evaluator tested all TSF explicitly with evaluator tests including simulator test cases so that all TSF could be covered by at least one test case in order to confirm that the TOE operates as specified.

Security functions tested

- SF.TRANSACTION
- SF.ACCESS_CONTROL
- SF.CRYPTO
- SF.INTEGRITY
- SF.SECURITY
- SF.APPLET
- SF.RMI
- SF.CARRIER
- SF.CARDMANAGER

Verdict for the activity

- During the evaluator's TSF subset testing the TOE operated as specified.

7.4 Penetration Testing according to AVA_VLA

In the following the evaluator's penetration testing efforts are summarized according to [2].

Approach

- Examination of developer's vulnerability analysis and the developer's rationale for why the vulnerabilities are not exploitable in the intended environment of the TOE.
- Examination whether the TOE, in its intended environment, is susceptible to vulnerabilities not considered by the developer by considering current information regarding obvious public domain vulnerabilities.
- The evaluator performed penetration testing based on the developer vulnerability analysis. The penetration testing was performed at the ITSEF with the TOE development environment using script based developer test tools with automated comparison of expected and actual test results.

TOE test configurations

- TOE smart cards produced from TOE ROM mask
- TOE test images tested on a hardware emulator

Penetration testing performed

- Effectiveness of the TSF
- Secure use of the TOE

- Penetration tests of vulnerabilities identified by the developer

Security functions penetration tested

- SF.TRANSACTION
- SF.ACCESS_CONTROL
- SF.CRYPTO
- SF.INTEGRITY
- SF.SECURITY
- SF.APPLET
- SF.RMI
- SF.CARRIER
- SF.CARDMANAGER

Verdict for the sub-activity

- During the evaluator’s penetration testing based on the developer vulnerability analysis the TOE operated as specified.
- The vulnerabilities discussed in the developer vulnerability analysis are not exploitable in the intended environment for the TOE.
- The TOE is resistant to attackers with high attack potential in the intended environment for the TOE described in the developer vulnerability analysis.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

SmartCafe Expert Version 5.0

in the configuration as identified in chapter 2.

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 and guidance specific for the technology of the product [4] (AIS 34).

- The following guidance specific for the technology were used:
  - Functionality classes and evaluation methodology of deterministic random number generators
  - The Application of CC to Integrated Circuits

- Application of Attack Potential to Smart Cards
- Composite product evaluation for Smart Cards and similar devices
- Smartcard evaluation guidance

(see [4], AIS 20, AIS 25, AIS 26, AIS 36, AIS 37).

The ETR [7] builds up on the ETR-for-Composition document of the evaluation of the evaluation of the underlying platform certification [12][13][14] supplemented by a recent Re-Assessment [15][16][17].

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 EAL 4 package as defined in the CC (see also part C of this report)
- The components ADV_IMP.2 and AVA_VLA.4 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Java Card System Protection Profile, Version 1.0b, Standard 2.2 Configuration, August 2003: DCSSI-PP/0305 [10]
- for the Functionality: PP conformant plus product specific extensions
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by ADV_IMP.2 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function: high
  - SF.CRYPTO (random number generation according to [AIS20] class K3)
  - SF.INTEGRITY

  In order to assess the Strength of Function of SF.CRYPTO the scheme interpretations AIS 20 (see [4]) were used.

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

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 rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for:

- the TOE Security Function SF.CRYPTO (3-DES, RSA, AES)

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic functions with a security level of 80 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore for these functions it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (www.bsi.bund.de).

The cryptographic functions: 2-key Triple DES (2TDES) and RSA 1024 provided by the TOE have got a security level of maximum 80 Bits (in general context).

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4])

12 Definitions

12.1 Acronyms

3DES	Triple-DES
AES	Advanced Encryption Standard
API	Application Programming Interface
ATR	Answer to Reset
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CM	Card Manager
CPLC	Card Production Life Cycle
DES	Data Encryption Standard
DS	Dedicated Software
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
G & D	Giesecke & Devrient GmbH
HW	Hardware
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JCRE	Java Card Runtime Environment
JCVM	Java Card Virtual Machine

OS	Operating System
PP	Protection Profile
ROM	Read Only Memory
SAR	Security Assurance Requirement
SCP	Smart Card Platform
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
SW	Software
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

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-CC-0537, Version 3.0, Status 27.08.2009, Security Target SmartCafe Expert V5.0, Giesecke & Devrient (confidential document)

[8] specifically

- AIS 20, Version 1, 2 December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 6, 7 May 2009, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 2, 24 October 2008, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document and CC Supporting Document

[7] Evaluation Technical Report, Version 2, Date: 2009-10-14, BSI-DSZ-CC-0537, TUVIT (confidential document)

[8] Configuration list for the TOE, Version 1.4, Date: 2009-08-27, Giesecke & Devrient (confidential document)

[9] Security Target BSI-DSZ-CC-0537, Version 1.0, Date: 27.10.2009, Security Target Lite SmartCafe Expert V5.0, Giesecke & Devrient (sanitised public document)

[10] Protection Profile Java Card System Protection Profile, Version 1.0b, Standard 2.2 Configuration, August 2003: DCSSI-PP/0305, Sun Microsystems Inc.

[11] User and Administrator Guidance SmartCafe Expert V5.0, Version 1.3, Date: 2009-07-14

[12] Certification Report BSI-DSZ-CC-0404-2007 for NXP Secure Smart Card Controller P5CD040V0B, P5CC040V0B, P5CD020V0B and P5CC021V0B each with specific IC Dedicated Software, V1.0, Bundesamt für Sicherheit in der Informationstechnik, 2007-07-05

[13] Certification Report BSI-DSZ-CC-0410-2007 for NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B and P5CC080V0B each with specific IC Dedicated Software, V1.0, Bundesamt für Sicherheit in der Informationstechnik, 2007-07-05

[14] Certification Report BSI-DSZ-CC-0411-2007 for NXP Secure Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software, V1.0, Bundesamt für Sicherheit in der Informationstechnik, 2007-07-05

[15] ETR for composition according to AIS36, NXP P5CD040V0B Secure Smart Card Controller, BSI-DSZ-CC-0404, Bundesamt für Sicherheit in der Informationstechnik, Version 1.3, June 23rd, 2009

[16] ETR for composition according to AIS36, NXP P5CD080V0B Secure Smart Card Controller, BSI-DSZ-CC-0410, Bundesamt für Sicherheit in der Informationstechnik, Version 1.2, June 23rd, 2009

[17] ETR for composition according to AIS36, NXP P5CD144V0B Secure Smart Card Controller, BSI-DSZ-CC-0411, Bundesamt für Sicherheit in der Informationstechnik, Version 1.2, June 23rd, 2009

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

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0537-2009

Evaluation results regarding development and production environment

The IT product SmartCafe Expert Version 5.0 (Target of Evaluation, TOE) 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 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

As a result of the TOE certification, dated 17 December 2009, the following results regarding the development and production environment apply. The Common Criteria Security Assurance Requirements

- ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),
- ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and
- ALC – Life cycle support (i.e. ALC_DVS.1, ALC_LCD.1, ALC_TAT.1),

are fulfilled for the development and production sites of the TOE listed below:

(a) Giesecke & Devrient, Zamdorferstrasse 88, 81677 Munich, Germany (development site)

(b) See certification reports BSI-DSZ-CC-0404-2007, BSI-DSZ-CC-0410-2007, BSI-DSZ-CC-0411-2007 for the development and production sites used as part of the composition

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the Threats, Security Objectives and Requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.