Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1028-2017

for

Sm@rtCafé® Expert 7.0 C3

from

Veridos GmbH - Identity Solutions by G&D BDR

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-1028-2017 (*)

Sm@rtCafé® Expert 7.0 C3

from	Veridos GmbH - Identity Solutions by G&D BDR
PP Conformance:	Java Card Protection Profile - Open Configuration, Version 3.0, May 2012, ANSSI-CC-PP-2010/03-M01
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

SOGIS
Recognition Agreement

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 4.

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.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 8 September 2017

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - 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

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:

- Act on the Federal Office for Information Security[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1. European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

[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 Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[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 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogisportal.eu.

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

This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: 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 by the nations listed above.

This certificate is recognized according to the rules of CCRA-2014, i.e. up to and including CC part 3 EAL 2 components. The evaluation contained the components ADV_FSP.5, ADV_IMP.1, ADV_INT.2, ADV_TDS.4, ALC_CMC.4, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2, ATE_COV.2, ATE_DPT.3, AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the CCRA-2014, for mutual recognition the EAL 2 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 Sm@rtCafé® Expert 7.0 C3 has undergone the certification procedure at BSI.

The evaluation of the product Sm@rtCafé® Expert 7.0 C3 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 6 September 2017. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant and sponsor is: Veridos GmbH - Identity Solutions by G&D BDR.

The product was developed by: Giesecke+Devrient Mobile Security GmbH.

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, as specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report or in the CC itself.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 8 September 2017 is valid until 7 September 2022. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[6] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

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 Sm@rtCafé® Expert 7.0 C3 has been included in the BSI list of 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] Veridos GmbH - Identity Solutions by G&D BDR
Truderinger Straße 15
81677 München

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), the Sm@rtCafé® Expert 7.0 C3 described in the Security Target, is a dual-interface, contact based or a pure contactless smart card with a Java Card operating system (OS). The TOE is a multi-purpose Java Card platform where applets of different kind can be installed. Pre- or post-issued applets are not part of the TOE. The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Java Card Protection Profile - Open Configuration, Version 3.0, May 2012, ANSSI-CC-PP-2010/03-M01 [8] (strict conformance). The Remote Method Invocation (RMIG) package and the External memory (EMG) package as defined in the Protection Profil as optional packages are not part of the TOE. The TOE was subject to a composite evaluation according AIS 36 [4].

Since a post-issuance installation of applets is possible, the TOE corresponds to an open configuration, as defined in the Protection Profile [8]. The platform is the Integrated Circuit (IC) M5073 G11 (certification ID BSI-DSZ-CC-0951-2015 including the re-assessment BSI-DSZ-CC-0951-2015-RA-01) manufactured by Infineon ([14] to [18]). Depending on the installed applets, the entire product (consisting of the TOE plus applets) can be used as a government card (like an ID card or a passport), a payment card, a signature card and for other purposes.

Sm@rtCafé® Expert 7.0 C3 is a follow-up TOE of the Sm@rtCafé® Expert 7.0 C1 (certification ID BSI-DSZ-CC-0868-2014, BSI-DSZ-CC-0868-2014-MA-01).

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 5 augmented by ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [7], chapter 8. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
SF.TRANSACTION	This security function provides atomic transactions according to the Java Card Transaction and Atomicity mechanism with commit and rollback capability for updating persistent data in flash memory.
SF.ACCESS_CONTROL	This security function provides 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 check-summed data stored in flash memory.
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.
SF.APPLET	This security function ensures the secure loading of a package or installation of an applet by S.CAD (see [8]) and the secure deletion of applets and/or packages by S.ADEL (see [8]).

TOE Security Functionality	Addressed issue
SF.CARRIER	This security function ensures secure downloading of applications on the card.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [7], chapter 9.

The assets to be protected by the TOE are defined in the Security Target [6] and [7], chapter 5. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [7], chapter 5.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

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:

Sm@rtCafé® Expert 7.0 C3

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW+SW	ICC including the software part of the TOE	Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries, symmetric crypto library v2.02.010 and with specific IC dedicated software (firmware) with Sm@rtCafé® Expert 7.0 C3	Sealed boxes by courier to Composite Product Integrator.
2	DOC	Preparative Guidance Sm@rtCafé® Expert 7.0 C3	3.6	Via email
3	DOC	Operative Guidance Sm@rtCafé® Expert 7.0 C3	5.2	Via email

Table 2: Deliverables of the TOE

According to the Security Target chapter 2.4.1 the life cycle of the TOE consists of 7 phases:

- Phase 1: IC Embedded Software Development
- Phase 2: IC Development
- Phase 3: IC Manufacturing
- Phase 4: IC Packaging
- Phase 5: Composite Product Integration
- Phase 6: Personalisation
- Phase 7: Operational Usage

The TOE delivery takes place after Phase 4 so that the evaluation process is limited to Phases 1 to 4. The TOE is delivered to the Composite Product Integrator (CPI), which is responsible for sending the SCP02/SCP03 authentication keys to be integrated into the TOE previous to the TOE production. I.e. the CPI delivers the (Card Manager) Master Key to the TOE embedded SW development G&D site from which the card individual keys are derived before the TOE is delivered.

The Composite Product Integrator has to verify that he has received the correct versions of the TOE documentation. The correctness of the TOE can be verified by checking the GET DATA APDU command response. The TOE can be used in two different configurations:

- Configuration 1: TOE is fully compliant to the GlobalPlatform Card Common Implementation Configuration
- Configuration 2: TOE is fully compliant to the GlobalPlatform Card ID Configuration

The TOE and the different TOE configurations can be identified through the GET DATA and the GET STATUS APDU command responses (see table 3 and table 4):

TOE Configuration	**Type GET DATA Response (80 CA 00 C8 06), see [13] 4.1.7**
Configuration 1	C8 04 8D 89 E8 6F
Configuration 2	C8 04 22 8C 1E 60

Table 3: TOE configuration identification by GET DATA response status

TOE Configuration	**GET STATUS Response (80 F2 80 00 02 4F 00), see [13] 4.1.8**
Configuration 1	08 A0 00 00 00 03 00 00 00 0F 9E
Configuration 2	08 A0 00 00 01 51 00 00 00 0F 9E

Table 4: TOE configuration identification by GET STATUS response status

In order to verify that the user receives a certified TOE in the certified configuration, the TOE can be identified using the means described in the guidance [13] chapter 7.

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:

- Security Audit,
- Communication,
- Cryptographic Support,

- User Data Protection,
- Identification and Authentication,
- Security Management,
- Privacy,
- Protection of the TSF, and
- Trusted Channels.

The Security Policy of the TOE as a dual-interface, contact based or a pure contactless smart card with a Java Card operating system is to provide basic security functionalities to be used by the smart card applications thus providing an overall smart card system security.

The TOE implements physical and logical security functionality in order to protect user data stored and operated on the smartcard when used in a hostile environment. Hence the TOE maintains integrity and confidentiality of code and data stored in its memories and the different CPU modes with the related capabilities for configuration and memory access and for integrity, the correct operation and the confidentiality of security functionality provided by the TOE. Therefore the TOEs policy is to protect against malfunction, leakage, physical manipulation and probing. Besides, the TOE's life-cycle is supported as well as the user Identification whereas the abuse of functionality is prevented. Furthermore, random number generation as well as specific cryptographic services are being provided to be securely used by the smartcard embedded software.

Specific details concerning the above mentioned security policies can be found in section 8 of the Security Target [6] and [7].

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 and measures to be taken by the TOE environment, the user or the risk manager.

In particular the following security objectives for the environment have to be followed and considered (Security Target [6] and [7], chapter 6.2):

- OE.APPLET: No applet loaded post-issuance shall contain native methods.
- OE.VERIFICATION: All the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. See #.VERIFICATION in the PP [8] chapter 4.4 for details. Additionally, the applet shall follow all the recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform.

  Application Note: Constraints to maintain the isolation property of the platform are provided by the platform developer in application development guidance. The constraints apply to all application code loaded in the platform (described in [13] chapter 3.1.5, "Recommendations for maintaining the isolation property of the platform").
- OE.CODE-EVIDENCE: For application code loaded pre-issuance, evaluated technical measures implemented by the TOE or audited organizational measures must ensure

that loaded application has not been changed since the code verifications required in OE.VERIFICATION.

For application code loaded post-issuance and verified off-card according to the requirements of OE.VERIFICATION, the verification authority shall provide digital evidence to the TOE that the application code has not been modified after the code verification and that he is the actor who performed code verification.

For application code loaded post-issuance and partially or entirely verified on-card, technical measures must ensure that the verification required in OE.VERIFICATION is performed. On-card bytecode verifier is out of the scope of this Security Target.

Application Note: For application code loaded post-issuance and verified off-card, the integrity and authenticity evidence is achieved by electronic signature of the application code, after code verification, by the actor who performed verification.

Details can be found in the user guidance [12] and [13] chapters 5.1 and 5.2.

5. Architectural Information

The global structure of the TOE is as shown in the Security Target [6], [7] Figure 1. The TOE design reflects the abstract structure of the TOE as a Java Card OS based on a certified HW IC. It follows this approach by defining subsystems and modules according to the realized functionalities of a Java Card OS composite product. The subsystems again are logically grouped together and compose four subsystems of the TOE: APDU, Application Programmers Interface, Virtual Machine, Hardware platform (composite evaluation).

For each subsystem, the TOE design breaks its structure further down into modules. However, this does not include the Hardware subsystem, since it is already covered by the underlying hardware certification. The following table shows the modules and subsystems, which are all classified as SFR-enforcing, defined by the TOE design:

Subsystem	Module	Description
APDU	Applet	The module Applet contains Issuer Security Domain applet and Security Domain applet according GlobalPlatform Card Specification [18].
	Dispatcher	The module Dispatcher implements Transport Management including protocols T=0, T=1 (ISO7816) and T=CL (ISO14443). Thus it receives all APDU commands provided by CAD via APDU interface.
Application Programmers Interface	Javacard	Module Javacard implements all functions required by Java Card API Specification.
	Global Platform	Module Global Platform implements content management functions according to GP [20] and chapter 11 of the Java Card Runtime Environment (JCRE) Specification to load packages, install applets and delete applets and packages. Content on card and additional information is managed in Registry as defined in GP. Additionally it defines interfaces which enable applets to provide and use the further services.

Subsystem	Module	Description
Virtual Machine	Bytecode Interpreter	Module Bytecode Interpreter implements Javacard Virtual Machine according to the Java Card Virtual Machine (JCVM) Specification. This includes: bytecodes as defined in chapter 7 of the JCVM Specification, Exception Handling as defined in chapter 7 of the JCVM Specification, Firewall checks as defined in chapter 6 of the JCRE Specification.
	Memory Management	Module Memory Management implements interfaces to copy data in memory providing tear save writing according the JCRE Specification.
HW	-	See platform certificate [14], [15], [18]

Table 5: Subsystems of the TOE

For detail on the versions of the specification JCRE and JCVM please refer to the Security Target.

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

The TOE, the composite smartcard product Sm@rtCafé® Expert 7.0 C3, was tested in Configuration 1 and Configuration 2 (see chapter 8) in scope of the certification.

TOE test configurations:

- Tests were performed with different TOE configurations, i.e. with different TOE interfaces (contactless, contact based) as well as with the TOE simulator (software based TOE simulation).
- The TOE has been tested in the configurations Configuration 1 and Configuration 2 (see chapter 8).
- Tests were done in different life-cycle phases (e.g. Global Platform life cycle states SECURED, OP_READY, etc.).
- Tests were additionally performed with samples that had the re-flash and reset life-cycle ability for prevention of increased amount of broken samples during testing.
- Penetration tests were performed with special samples reduced/modified to the functionality to test.

Developer's Test according to ATE_FUN

Test approach:

According to the description of the TSFI in the Functional Specification, the following kinds of APIs and TSFI were tested (not all parts of the packages or interfaces are implemented):

- GlobalPlatform API (Package org.globalplatform),
- Java Card API (Packages javacard.security, javacardx.crypto, javacard.framework and javacardx.apdu),
- G&D Proprietary API,
- Java Card Virtual Machine TSFI (a subset of the Java Card Virtual Machine (JCVM) Interface, i.e. all SFR relevant bytecodes),
- APDU Interface,
- Electrical Interface.

Therefrom the following TSFI are defined: API, JCVM Interface, APDU Interface and Electrical Interface.

Test environment:

Generally, two kinds of tests are differentiated, system tests and simulator tests (so called module tests). Employed test tools are:

- Test tool JCTS (Java Card Test Suite): Based on a proprietary script language JCB to send APDU sequences to the card.
- Test tool TRex is a test framework which runs together with Eclipse and is used for system tests.
- Test tool ATX2 (Automated Test Execution) is a tool which coordinates the test execution of defined test procedures for JCB and TRex tests.
- Simulator tests: Not all requirements can be tested directly with system tests on a real card. In this case the requirement will be tested by a module test (simulator tests). These test cases are designed to be run on the Keil µVision simulator. The interaction between Eclipse IDE and the Keil µVision simulator is fully automated.

TOE configurations tested:

According to the Security Target the TOE can be used in two different configurations (see chapter 8). All configurations have been tested whereby the Configuration 1 is the configuration where all requirements can be applied. Due to some restrictions in Configuration 2 (certain aspects of GP are not implemented) several tests were skipped during the testing activity of Configuration 2.

Test results:

The tests mainly run automatically and perform all test steps including installation of test applets, test scripting, result checking and clean-up procedures. Test documentation including test case description, tests steps, expected and actual results are partially generated automatically. Actual results and details from test execution from module testing can be gained from prepared logs. ATE_COV and ATE_DPT were taken into account and all mappings to interfaces and modules of the TOE are covered by the tests.

Verdict for the activity:

The testing approach covers all TSFI as described in the Functional Specification and all subsystems and modules of the TOE design adequately. All configurations as described in the Security Target are covered. All test results collected in the test reports are as expected and in accordance with the TOE design and the desired TOE functionality.

Independent Testing according to ATE_IND

Approach for independent testing:

- Examination of developer's testing amount, depth and coverage analysis and of the developer's test goals 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 at the Evaluation Body with the TOE developer test environment and additional Evaluation Body test equipment using tests applets, test scripts and simulation tools.

TOE test configurations:

- Tests were performed with different TOE configurations, i.e. with different TOE interfaces (contactless, contact based) as well as with the TOE simulator.
- The TOE has been tested in the following configurations:
  - Configuration 1, the configuration where all requirements can be applied.
  - Configuration 2 with several restrictions
- Tests were done in different life-cycle phases (e.g. Global Platform life cycle states SECURED, OP_READY, etc.).

The test samples provided by the developer for repeating developer's tests and for setting up evaluator created tests are not identical to final delivered TOE cards. These samples were brought in the state and configuration as desired.

Subset size chosen:

During sample testing the evaluator chose to repZertReporteat all developer functional tests. During independent testing the evaluator used test applets and test scripts to invoke and test functionality given by the API and APDU interfaces.

Interfaces tested:

The selection criteria for the interfaces of the composed subset consider simply the security functionality that is available from these interfaces. Focus was laid upon interfaces that are in particular security sensitive for Java Card platform, such as firewall mechanisms, atomic transactions, PIN mechanisms or key handling. The tested subset comprises the APDU and the API interfaces available to users. While the physical IC interface relies on the platform certification, the independent testing focussed on the APDU interface (based on the Global Platform specification) and the API interface (which provides packages from Java Card API, Global Platform API and G&D proprietary API classes).

Verdict for the activity:

During the evaluator's TSF subset testing the TOE was operated as specified. No unexpected behaviour was observed, particularly related to different TOE configurations. The evaluator verified the developer's test results by executing all of the developer's tests and verifying the test log files for successful execution.

Penetration Testing according to AVA_VAN

The TOE in different configurations being intended to be covered by the current evaluation was tested.

Penetration testing approach:

Based on a list of potential vulnerabilities applicable to the TOE in its operational environment the evaluators devised the attack scenarios for penetration tests. The aspects of the security architecture described in ADV_ARC were considered for penetration testing as well as all other evaluation evidence. Source code reviews of the provided implementation representation accompanied the development of test cases and were used to find input for penetration testing. The code inspection also supported the testing activities because they enabled the evaluator to verify implementation aspects that could hardly be covered by test cases.

In addition the evaluator applied tests and performed code reviews during the evaluation activity of composition tests to verify the implementation of the requirements imposed by the ETR for Composition and the guidance of the underlying platform. This ensured confidence in the security of the TOE as a whole.

TOE test configurations:

The evaluators used TOE samples for testing that were configured according to the Security Target. The tests were performed in different test scenarios:

- TOE smart cards tested using specialized test tools for smart cards, Java cards and for LFI testing.
- A simulator was used for test cases, which were not possible to perform with a real smart card TOE, e.g. memory manipulation.
- Different life-cycles and life-cycle management were tested.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential high was actually successful in the TOE's operational environment as defined in Security Target [6] and [7] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- Configuration 1: TOE is fully compliant to the GlobalPlatform Card Common Implementation Configuration
- Configuration 2: TOE is fully compliant to the GlobalPlatform Card ID Configuration

All configurations can either be installed on a dual-interface, contact-based or on a pure contactless smart card platform.

The user can identify the specific TOE configuration by the TOE response to a specific APDU, specified in the Operative Guidance Sm@rtCafé® Expert 7.0 C3. The TOE does not use the cryptographic libraries of the hardware platform, but provides cryptographic services by the G&D crypto library and enhanced G&D proprietary APIs. The Biometric API is not part of the TOE and can be part of the product or not.

The different configurations can be differentiated through the GET DATA APDU command response status and the GET STATUS APDU command response status. Therefore the configurations 1 and 2 are distinguishable.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [9] 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 EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The TOE was subject to a composite evaluation according AIS 36 [4]. The platform certificate for the Integrated Circuit (IC) M5073 G11, certification ID BSI-DSZ-CC-0951-2015 including BSI-DSZ-CC-0951-2015-RA-01, was used ([14] to [18]).

The following guidance specific for the technology was used:

(i) Security Architecture requirements (ADV_ARC) for smart cards and similar devices (see [4], AIS 25),

(ii) The application of CC to integrated circuits (see [4], AIS 25),

(iii) Application of Attack Potential to Smartcards (see [4], AIS 26),

(iv) Certification of "open" smart card products (see [4], AIS 36),

(v) Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on hardware [14], [15], [16]) have been applied in the TOE evaluation.

(vi) Informationen zur Evaluierung von kryptographischen Algorithmen (see [4], AIS 46).

(vii) Guidance for Smartcard Evaluation (see [4], AIS 37).

For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [10] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

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

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Java Card Protection Profile - Open Configuration, Version 3.0, May 2012, ANSSI-CC-PP-2010/03-M01 [8]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended

  for the Assurance: Common Criteria Part 3 conformant EAL 5 augmented by
  ALC_DVS.2 and AVA_VAN.5

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 strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities 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' (https://www.bsi.bund.de).

The table in annex C in part D of this report outlines the rating of the cryptographic mechanisms implemented in the TOE. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

Some security measures are partly implemented in this certified TOE, but require additional configuration or control or measures to be implemented by a product layer on top using the TOE. For this reason the TOE includes guidance documentation (see table 2) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [10].

11. Security Target

For the purpose of publishing, the Security Target [7] 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

AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
API	Application Programming Interface
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
CAD	Card Acceptance Device (card reader)
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CPI	Composite Product Integrator
cPP	Collaborative Protection Profile
DAP	Data Authentication pattern
DLC	Giesecke & Devrient Dienstleistungscenter
EAL	Evaluation Assurance Level
EMG	External memory package
ETR	Evaluation Technical Report
GD SDM	Giesecke & Devrient Secure DataManagement
GDC	Giesecke & Devrient Development Center
GDSK	Giesecke & Devrient Slovakia
GP	Global Platform
HW	Hardware
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JCB	proprietary script language to send APDU sequences to the card
JCRE	Java Card Runtime Environment
JCS	Java Card System
JCTS	Java Card Test Suite
JCVM	Java Card Virtual Machine
LFI	Laser Fault Injection
OS	Operating System
OSP	Organizational Security Policy

PIN	Personal Identification Number
PGP	Pretty Good Privacy
PP	Protection Profile
RMIG	Remote Method Invocation package
RSA	Rivest, Shamir and Adleman algorithm
SAR	Security Assurance Requirement
SCP	Secure Channel Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
SW	Software
TOE	Target of Evaluation
TRex	TTCN-3 Refactoring and Metrics Tool
TSF	TOE Security Functionality
TSFI	TSF Interface

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

Deterministic (RNG) - An RNG that produces random numbers by applying a deterministic algorithm to a randomly selected seed and, possibly, on additional external inputs.

Random number generator (RNG) - A group of components or an algorithm that outputs sequences of discrete values (usually represented as bit strings).

True RNG - A device or mechanism for which the output values depend on some unpredictable source (noise source, entropy source) that produces entropy.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target Sm@rtCafé® Expert 7.0 C3, Version 2.9, Date 16.08.17, BSI-DSZ-CC-1028-2017, Giesecke+Devrient Mobile Security GmbH (confidential document)

[7] Security Target Lite Sm@rtCafé® Expert 7.0 C3, Version 2.9, Date 16.08.17, BSI-DSZ-CC-1028-2017, Giesecke+Devrient Mobile Security GmbH (sanitized public document)

[8] Common Criteria Java Card Protection Profile - Open Configuration, Version 3.0, May 2012, ANSSI-CC-PP-2010/03-M01, Oracle Corporation

[8] specifically

- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren
- AIS 47, Version 1.1, Regelungen zu Site Certification

[9] Evaluation Technical Report for Sm@rtCafé® Expert 7.0 C3, Version 2, 2017-08-16, BSI-DSZ-CC-1028-2017, TÜViT GmbH (confidential document)

[10] Evaluation Technical Report for Composite Evaluation according to AIS 36 for Sm@rtCafé® Expert 7.0 C3, Version 3, 2017-08-16, BSI-DSZ-CC-1028-2017, TÜViT GmbH (confidential document)

[11] Configuration List SmartCafe Expert 7.0 C3, Version 2.2, 2017-07-18, Giesecke & Devrient GmbH (confidential document)

[12] Preparative procedures Sm@rtCafé® Expert 7.0 C3, Version 3.6, 10.08.17, Giesecke & Devrient GmbH

[13] Operational User Guidance Sm@rtCafé® Expert 7.0 C3, Version 5.2, 07.08.17, Giesecke & Devrient GmbH

[14] Certification Report – BSI-DSZ-CC-0951-2015 for Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, 2015-11-11, BSI.

[15] Assurance Continuity Reassessment Report, BSI-DSZ-CC-0951-2015-RA-01, Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, 2017-05-31, BSI.

[16] ETR FOR COMPOSITE EVALUATION (ETR-COMP), M5073 G11, BSI-DSZ-CC-0951, Version 4, 2017-05-18, TÜViT.

[17] SLx 70 Family Production and Personalization User's Manual, Revision 2015-04-01, Infineon Technologies AG.

[18] Security Target Lite M5073 G11 including optional Software Libraries RSA – EC – SHA-2 – Toolbox, Version 1.2, 2017-05-10, Infineon Technologies AG

[19] Technische Richtlinie BSI TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2014-01, 10.2.2014, BSI, https://www.bsi.bund.de/TR

[20] GlobalPlatform Card Specification Version 2.2.1, January 2011

[21] GlobalPlatform Card ID Configuration, Version 1.0 Member Release, December 2011, Document Reference: GPC_GUI_039

This page is intentionally left blank.

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“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 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC 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 augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 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.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 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 EAL 1 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.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 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 practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 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 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 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 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 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 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 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 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 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.

EAL 6 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 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 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 EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

Annex C: Rating of cryptographic mechanisms implemented in the TOE

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-1028-2017

Evaluation results regarding development and production environment

The IT product Sm@rtCafé® Expert 7.0 C3 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 8 September 2017, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2) are fulfilled for the development and production sites of the TOE listed below:

a) Giesecke+Devrient Mobile Security GmbH development site, Zamdorfer Straße 88, 81677 Munich, Germany and Prinzregentenstrasse 159, 81677 Munich, Germany (SW Development / Testing)

b) G&D production site Slovakia (GDSK), s.r.o., Dolné Hony 11, 94901 Nitra, Slovakia (Production / Delivery)

c) G&D Secure Data Management GmbH (GDSDM), Austraße 101b, 96465 Neustadt bei Coburg, Germany (Production / Delivery)

d) For development and production sites regarding the platform please refer to the certification reports BSI-DSZ-CC-0951-2015 [14], [15]

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 [7]) are fulfilled by the procedures of these sites.

Annex C of Certification Report BSI-DSZ-CC-1028-2017

Rating of cryptographic mechanisms implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 100 Bits	Comments
1.	Authenticity	RSA signature verification using SHA-1 (RSASSA-PKCS1-v1_5)	[RFC 3447] (RSA), [FIPS180-4] (SHA)	moduluslength= 1024 - 2048	No	FCO_NRO.2.1 /CM (DAP-Verification, [GP221, App. C.2 / C.3 / C.6])
2.	Authenticity	3DES in Retail-MAC mode using SHA-1	[FIPS 46-3] (3DES), [ISO9797-1] (Retail-MAC), [FIPS180-4] (SHA)	|k|=112	No	FCO_NRO.2.1 /CM (DAP-Verification [GP221, App. C.2 / C.3 / C.6])
3.	Authentication	3-DES in CBC mode	[FIPS 46-3] (3DES), [SP800-38A] (CBC)	|k|=112, |host-challenge|=64, |card-challenge| =48	No	[GP221, App. E.4.2]
4.	Authentication	KDF in counter mode with CMAC as PRF	[SP800-108] (KDF), [SP800-38B] (CMAC)	|k|=128, |host-challenge|= |card-challenge| =64	No[9]	[GP_ AM_D, 6.2.2.2 / 6.2.2.3 / 4.1.5]
5.	Key Agreement	3-DES in CBC mode with ICV=0	[FIPS 46-3] (3DES), [SP800-38A] (CBC)	|k|=112	No	[GP221], App. E.4.1
6.	Key Derivation	KDF in counter mode with CMAC as PRF	[SP 800-108] (KDF), [SP800-38B] (CMAC)	|k|=128	Yes	[GP_AM_D, 6.2.1]
7.	Key Agreement	ECDH	TR-03110 Part 2 chapters 3.2 and 3.3 [TR-3110, 3.2 / 3.3] TR-03116-2 chapter 3.2 [TR-03116, 3.2/3.3]	Key sizes corresponding to the used elliptic curve brainpool P{256, 320, 384, 512}r1 (RFC 5639),	Yes	-
8.	Confidentiality	3-DES in CBC mode	[FIPS 46-3] (3DES), [SP800-38A] (CBC)	|k|=112	No	[GP221, App. E.3.4/ E.4.2]
9.	Confidentiality	AES in CBC mode	[FIPS 197] (AES), [SP800-38A] (CBC)	|k|=128	Yes	[GP_AM_ D, 4.1.2 / 6.2.6 /

[9]Because of challenge length

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 100 Bits	Comments
						6.2.7]
10.	Integrity	3DES in Retail-MAC mode	[FIPS 46-3] (3DES), [ISO9797-1] (Retail-MAC)	|k|=112	No	[GP221, App. E.4.4 (on unmodified and modified APDU) / E.4.5]
11.	Integrity	AES in CBC-MAC and CMAC mode truncated to 64 bits	[FIPS 197] (AES), [SP800-38B] (CMAC)	|k|=128	No[10]	[GP_AM_D, 6.2.4 / 6.2.5]
12.	Trusted Channel	SCP02	[GP221, App. E additionally cf. lines 3, 5, 7, 9]	-	No	[GP221, App. E, supported parameter 'i': 05,15,45,55]
13.	Trusted Channel	SCP03	[GP_AM_D additionally cf. lines 4, 6, 8, 10]	-	No[11]	[GP221, App. E, supported parameter 'i': 00,10,20,30, 60,70]
14.	Cryptographic Primitive	SHA-1	[FIPS180-4] (SHA)	None	No	-
15.	Cryptographic Primitive	SHA-{224, 256, 384, 512}	[FIPS180-4] (SHA)	None	Yes	-
16.	Cryptographic Primitive	3-DES in ECB mode	[FIPS 46-3] (3DES), [SP800-38A] (ECB), [ISO9797-1] padding method M1 and M2 and [PKCS5]	|k|=112, 168	No	-
17.	Cryptographic Primitive	3-DES in CBC mode	[FIPS 46-3] (3DES), [SP800-38A] (CBC), [ISO9797-1] padding method M1 and M2 and [PKCS5]	|k|=112	No	-
18.	Cryptographic Primitive	3-DES in CBC mode	[FIPS 46-3] (3DES), [SP800-38A] (CBC), [ISO9797-1] padding method M1 and M2 and [PKCS5]	|k|=168	Yes	-
19.	Cryptographic Primitive	3DES in CBC-MAC and Retail-MAC mode	[FIPS 46-3] (3DES), [ISO9797-1] (CBC-MAC, Retail-MAC)	|k|=112	No	-

[10]Because of truncation

[11]Only because of authentication and integrity

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 100 Bits	Comments
20.	Cryptographic Primitive	3DES in CBC-MAC and Retail-MAC mode	[FIPS 46-3] (3DES), [ISO9797-1] (CBC-MAC, Retail-MAC)	|k|=168	Yes	-
21.	Cryptographic Primitive	AES in ECB mode	[FIPS 197] (AES), [SP800-38A] (ECB), [ISO9797-1] padding method M1 and M2 and [PKCS5]	|k|=128, 192, 256	No	-
22.	Cryptographic Primitive	AES in CBC mode	[FIPS 197] (AES), [SP800-38A] (CBC), [ISO9797-1] padding method M1 and M2 and [PKCS5]	|k|=128, 192, 256	Yes	-
23.	Cryptographic Primitive	AES in CBC-MAC and CMAC mode	[FIPS 197] (AES), [ISO9797-1] (CBC-MAC), [SP800-38B] (CMAC)	|k|=128, 192, 256	Yes	-
24.	Cryptographic Primitive	RSA encryption and decryption with encoding (RSAES-PKCS1-v1_5) and without encoding (RSASP1,RSAVP1)	[RFC 3447] (RSA)	moduluslength= 512 - 1975	No	-
25.	Cryptographic Primitive	RSA encryption and decryption with encoding (RSAES-PKCS1-v1_5) and without encoding (RSASP1,RSAVP1)	[RFC 3447] (RSA)	moduluslength= 1976 - 2048	Yes	-
26.	Cryptographic Primitive	RSA-CRT decryption with encoding (RSAES-PKCS1-v1_5) and without encoding (RSASP1,RSAVP1)	[RFC 3447] (RSA)	moduluslength= 512 - 1975	No	-
27.	Cryptographic Primitive	RSA-CRT decryption with encoding (RSAES-PKCS1-v1_5) and without encoding (RSASP1,RSAVP1)	[RFC 3447] (RSA)	moduluslength= 1976 - 4096	Yes	-

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 100 Bits	Comments
28.	Cryptographic Primitive	RSA signature generation according scheme 1 of [ISO9796-2] chapter 8.2 and [RSA] (RSASSA-PKCS1-v15) chapter 8 using SHA-{1} and [RSASSA-PSS] and [RSA-SHA-RFC2409]	[RFC 3447] (RSA), [FIPS180-4] (SHA)	moduluslength= 512 - 2048	No	-
29.	Cryptographic Primitive	RSA signature generation according scheme 1 of [ISO9796-2] chapter 8.2 and [RSA] (RSASSA-PKCS1-v15) chapter 8 using SHA-{224, 256, 384, 512} and [RSASSA-PSS] and [RSA-SHA-RFC2409]	[RFC 3447] (RSA), [FIPS180-4] (SHA)	moduluslength= 512 - 1975	No	-
30.	Cryptographic Primitive	RSA signature generation according scheme 1 of [ISO9796-2] chapter 8.2 and [RSA] (RSASSA-PKCS1-v15) chapter 8 using SHA-{224, 256, 384, 512} and [RSASSA-PSS] and [RSA-SHA-RFC2409]	[RFC 3447] (RSA), [FIPS180-4] (SHA)	moduluslength= 1976 - 2048	Yes	-
31.	Cryptographic Primitive	RSA-CRT signature generation with encoding scheme 1 of [ISO9796-2] chapter 8 and [RSA] (RSASSA-PKCS1-v15) chapter 8 using SHA-{1, 224, 256, 384, 512} and [RSASSA-PSS] and [RSA-SHA-RFC2409]	[RFC 3447] (RSA), [FIPS180-4] (SHA)	moduluslength= 512 - 1975	No	-

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 100 Bits	Comments
32.	Cryptographic Primitive	RSA-CRT signature generation according scheme 1 of [ISO9796-2] chapter 8 and [RSA] (RSASSA-PKCS1-v15) chapter 8 using SHA-1 and [RSASSA-PSS] and [RSA-SHA-RFC2409]	[RFC 3447] (RSA), [FIPS180-4] (SHA)	moduluslength= 1976 - 4096	No	-
33.	Cryptographic Primitive	RSA-CRT signature generation according scheme 1 of [ISO9796-2] chapter 8 and [RSA] (RSASSA-PKCS1-v15) chapter 8 using SHA-{224, 256, 384, 512} and [RSASSA-PSS] and [RSA-SHA-RFC2409]	[RFC 3447] (RSA), [FIPS180-4] (SHA)	moduluslength= 1976 - 4096	Yes	-
34.	Cryptographic Primitive	RSA signature verification according scheme 1 of [ISO9796-2] chapter 8.2 and [RSA] (RSASSA-PKCS1-v15) chapter 8 using SHA-{1, 224, 256, 384, 512} and [RSASSA-PSS] and [RSA-SHA-RFC2409]	[RFC 3447] (RSA), [FIPS180-4] (SHA)	moduluslength= 512 - 1975	No	-
35.	Cryptographic Primitive	RSA signature verification according scheme 1 of [ISO9796-2] chapter 8.2 and [RSA] (RSASSA-PKCS1-v15) chapter 8 using SHA-1 and [RSASSA-PSS] and [RSA-SHA-RFC2409]	[RFC 3447] (RSA), [FIPS180-4] (SHA)	moduluslength= 1976 - 2048	No	-

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 100 Bits	Comments
36.	Cryptographic Primitive	RSA signature verification according scheme 1 of [ISO9796-2] chapter 8.2 and [RSA] (RSASSA-PKCS1-v15) chapter 8 using SHA-{224, 256, 384, 512} and [RSASSA-PSS] and [RSA-SHA-RFC2409]	[RFC 3447] (RSA), [FIPS180-4] (SHA)	moduluslength= 1976 - 2048	Yes	-
37.	Cryptographic Primitive	ECDSA signature generation and verification	[TR-03111] (ECDSA)	Key sizes corresponding to the used elliptic curves secp{160,192}r1 [SEC2] and brainpoolP{160, 192}r1] and brainpoolP{160, 192}t1 [RFC5639]	No	-
38.	Cryptographic Primitive	ECDSA signature generation and verification	[TR-03111] (ECDSA)	Key sizes corresponding to the used elliptic curves secp{224,256,320, 384, 521}r1 [SEC2] and brainpoolP{224, 256,320,384,512}r1 and brainpoolP{224, 256,320,384,512}t1 [RFC5639]	Yes	-

Table 6: TOE cryptographic functionality[12]

[12] Technical references related to Table 6

[TR-03111] Technical Guideline TR-03111 Elliptic Curve Cryptography, TR-03111, version 2.0, 28.06.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[FIPS46-3] Federal Information Processing Standards Publication 46-3: Data Encryption Standard (DES), U.S. Department of Commerce / National Institute of Standards and Technology, reaffirmed October 25th, 1999

[FIPS180-4] Federal Information Processing Standards Publication FIPS PUB 180-4, Secure Hash Standard (SHS), March 2012, Information Technology Laboratory National Institute of Standards and Technology.

[FIPS197] Federal Information Processing Standards Publication 197, November 26, 2001, Announcing the ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology. [ISO9796-2] ISO/IEC9796-2 Information technology — Security techniques —

Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms, Second edition 2002-10-0, ISO/IEC.

[ISO_9797-1] Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 1999-12, ISO/IEC. [RFC3447] RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, February 2003 — available at: http://www.rfc-base.org/rfc-3447.html

[RFC5639] RFC 5639 ECC Brainpool Standard Curves & Curve Generation, March 2010 — available at: http://tools.ietf.org/html/rfc5639

[GP] GlobalPlatform Card Specification Version 2.2.1, January 2011

[GP_AM_D] GlobalPlatform Card Technology, Secure Channel Protocol 03, Card Specification v 2.2 – Amendment D, Version 1.1, September 2009

[SP800-38A] NIST. Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Special Publication SP800-38A, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2001.

[SP800-38B] NIST. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication SP800-38B, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2005.