Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1092-2020

for

Sm@rtCafé® Expert 7.0 EAL 6+ C1

from

Veridos GmbH - Identity Solutions by Giesecke+Devrient and Bundesdruckerei

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-1092-2020 (*)

Smart card with a Java Card operating system

Sm@rtCafé® Expert 7.0 EAL 6+ C1

from	Veridos GmbH - Identity Solutions by Giesecke+Devrient and Bundesdruckerei
PP Conformance:	Java Card Protection Profile - Open Configuration, December 2017, Version 3.0.5, BSI-CC-PP-0099-2017
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1

SOGIS
Recognition Agreement

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 (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 5.

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.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

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, 29 May 2020

For the Federal Office for Information Security

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

Sandro Amendola L.S.
Head of Division

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.

Contents

A. Certification

1. 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.

2. 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[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- 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[4] [1] also published as ISO/IEC 15408.

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

2 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

3 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 3 March 2005, Bundesgesetzblatt I, p. 519

- 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]

3. 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.

3.1. European Recognition of 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.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. 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 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.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

3.2. 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 current list of signatory nations and approved certification schemes can be seen on the website: https://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 related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

4. 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 EAL 6+, C1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1028-2017. Specific results from the evaluation process BSI-DSZ-CC-1028-2017 were re-used.

The evaluation of the product Sm@rtCafé® Expert 7.0 EAL 6+, C1 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 25 May 2020. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Veridos GmbH - Identity Solutions by Giesecke+Devrient and Bundesdruckerei.

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.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is 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 components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

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-assessment or 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 would 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 29 May 2020 is valid until 28 May 2025. 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

[5] Information Technology Security Evaluation Facility

Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

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.

6. Publication

The product Sm@rtCafé® Expert 7.0 EAL 6+, C1 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[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Veridos GmbH - Identity Solutions by Giesecke+Devrient and Bundesdruckerei
Prinzregentenstraße 159,
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 EAL 6+ C1 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. Since a post-issuance installation of applets is possible, the TOE corresponds to an open configuration, as defined in [8]. 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.

The TOE is based on the Integrated Circuit (IC) M5073 G11 [14] (Certification ID BSI-DSZ-CC-0951-V4-2019). The TOE comprises the underlying hardware IC, the operating system including the G+D crypto library and according TOE guidance documents.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Java Card Protection Profile - Open Configuration, December 2017, Version 3.0.5, BSI-CC-PP-0099-2017 [8].

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 6 augmented by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 7. 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 ([JCRE304], Section 7) for updating persistent data in flash memory.
SF.ACCESS_CONTROL	This security function provides 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 installing of an applet by S.CAD

TOE Security Functionality	Addressed issue
	and the secure deletion of applets and/or packages by S.ADEL.
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 [9], chapter 4.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], 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 [9], 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 EAL 6+, C1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
	HW+ SW	ICC including the software part of the TOE	Sm@rtCafé® Expert 7.0 EAL 6+ C1	Sealed boxes by courier to Composite Product Integrator. The delivery is covered by the certification of the site certifications.
	DOC	Preparative Guidance Sm@rtCafé® Expert 7.0 EAL 6+ C1 [12]	2.1	Via email PGP RSA 2048 bit to Composite Product Integrator.
	DOC	Operative GuidanceSm@rtCafé® Expert 7.0 EAL 6+ C1 [13]	3.6	Via email PGP RSA 2048 bit to Composite Product Integrator.

Table 2: Deliverables of the TOE

The TOE delivery takes place after IC Packaging so that the evaluation process is limited to Phases 1 to 4 as defined in [8]. The TOE is delivered to the Composite Product Integrator (CPI), which is responsible for sending the 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 TOE can be used in two different configurations:

- Config 1: TOE is fully compliant to the GlobalPlatform Card Common Implementation Configuration [17], and
- Config 2: TOE is fully compliant to the GlobalPlatform Card ID Configuration [18].
  The TOE itself and the different TOE configurations can be identified through the GET DATA and the GET STATUS APDU command responses (listed in the tables below):

TOE Configuration	GET DATA Response (80 CA 00 C8 06)
Config 1	C8 04 7A 7D 36 C7
Config 2	C8 04 22 BF 6D BC

Table 3: TOE configuration identification by GET DATA response

TOE Configuration	GET STATUS Response (80 F2 80 00 02 4F 00)
Config 1	08 A0 00 00 00 03 00 00 00 0F 9E
Config 2	08 A0 00 00 01 51 00 00 00 0F 9E

Table 4: TOE configuration identification by GET STATUS response

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 Path / Channels.

The security policy of the TOE, a smart card with a Java Card operating system (OS), is to provide basic security functionalities to be used by smart card applications, thus providing 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 numbers generation as well as specific cryptographic services are being provided to be securely used by the applications.

Specific details concerning the above mentioned security policies can be found in Section 8 of the Security Target [6] and [9]).

In the context of ADV_SPM.1, the security policies of the TOE were formally modelled. The security policies that were modelled comprise the Java Card firewall, the on-card package management and the secure package loading. The complete list of SFRs which are included in the SPM can be found in [6, 8.2]. SFRs which are not covered comprise only cryptographic functionality, unobservability, data exchange formats (FPT_TDC.1) and parts of self-testing.

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. Details can be found in the Security Target [6] and [9], chapter 4.4 as well as [12, 5.1] and [13, 3.1 / 5.1 / 5.2].

5. Architectural Information

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, and
- 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 2.2.1 [16].
	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 [JCAPI].
	Global Platform	Module Global Platform implements content management functions according [GP] and Chapter 11 of [JCRE304] to: • Load packages,

Subsystem	Module	Description
		• Install applets, • 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.
Virtual Machine	Bytecode Interpreter	Module Bytecode Interpreter implements Javacard Virtual Machine according [JCVM304]. This includes: • Bytecodes as defined in Chapter 7 of [JCVM304], • Exception Handling as defined in Chapter 7 of [JCVM304], • Firewall checks as defined in Chapter 6 of [JCRE304].
	Memory Management	Module Memory Management implements provides interface to copy data in memory providing tear save writing according [JCRE304].
HW	-	Assessed by evaluator as SFR-enforcing.

Table 5: Subsystems of the TOE

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 test configurations:

- Tests were performed with different TOE configurations, i.e. with different TOE interfaces (contact based and contactless) as well as with the TOE simulator (software based TOE simulation).
- The TOE has been tested in the configurations Configuration 1 and Configuration 2 representing the final TOE.
- Tests were done in different life-cycle phase (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 which is tested.

The evaluator determined that the used samples deviating from the final TOE configuration, including the simulated TOEs, represent exactly the TOE functionality

tested. I.e. this means that the test results done with modified TOE samples are valid and can be taken over as results for the final TOE.

7.2. 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, details in [7]): GlobalPlatform API, JavaCard API, G&D Proprietary API, Visa Openplatform API, Java Card Virtual Machine TSFI (a subset of the Java Card Virtual Machine (JCVM) Interface, i.e. all SFR relevant bytecodes), APDU Interface, and 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, Systemtests and Simulatortests (so-called Moduletests).

TOE configurations tested:

According to the security target the TOE can be used in two different configurations (see Chapter 8): All configurations can either be installed on a dual-interface, contact based chip or on a pure contactless smart card platform. 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, 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.

7.3. Evaluator Tests

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:
    1. Configuration 1, the configuration where all requirements can be applied.
    2. Configuration 2 with several restrictions
- Tests were done in different life-cycle phase (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 repeat the 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 JavaCard 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 focused on the APDU interface (based on the Global Platform specification [16]) and the API interface (which provides packages from JavaCard API, GlobalPlatform API and proprietary API).

During the evaluator's TSF subset testing the TOE was operated as specified. No unexpected behaviour was observed, particularly related to different TOE configurations.

7.4. Penetration Testing according to AVA_VAN

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 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 ST. 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 [6] an [9] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE, the composite smartcard product Sm@rtCafé® Expert 7.0 EAL 6+ C1 was tested in both possible configurations in scope of the certification:

- Config 1: TOE is fully compliant to the GlobalPlatform Card Common Implementation Configuration [17], and
- Config 2: TOE is fully compliant to the GlobalPlatform Card ID Configuration [18].

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 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 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] have been applied in the TOE evaluation.

(vi) Cryptographic Algorithms and Random Number Generators (see [4], AIS 46)

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

For RNG assessment the scheme interpretations AIS 20 and AIS 31 were 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 6 package including the class ASE as defined in the CC (see also part C of this report)
- The component ALC_FLR.1 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1028-2017, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the following areas:

- The assurance level for evaluation was increased to EAL6 augmented with ALC_FLR.1.
- Improvements and strengthening of countermeasures for ECC, RSA and the secure SHA-2 were applied.
- A few smaller EC key lengths were removed from the TOE scope (160 and 192 bit curves).
- Some bugfixes and improvements were applied, such as an RSA signature creation bugfix and a corrected check for limitation on fields in a class instance.

The evaluation has confirmed:

- PP Conformance: Java Card Protection Profile - Open Configuration, December 2017, Version 3.0.5, BSI-CC-PP-0099-2017 [8]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 6 augmented by ALC_FLR.1

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 implementation of the ECC scalar multiplication shows a reduced remaining rest entropy for the secret scalar that lies below the general security level given for the respective elliptic curve. This should be taken into account for applets that are set up and running on the TOE.

The tables in annex C of part D of this report give an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of table 8 with '*no*' achieves a security level of lower than 100 Bits (in general context) only. An explicit validity period is not given.

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, too.

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, e.g. the Embedded Software 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].

At the point in time when evaluation and certification results are reused there might be an update of the document "ETR for composite evaluation" available. Therefore, the certified products list on the BSI website has to be checked for latest information on reassessments, recertifications or maintenance result available for the product.

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. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AID	Application identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
AIS	Application Notes and Interpretations of the Scheme
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
CAP	Converted Applet
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DES	Data Encryption Standard
DLC	Giesecke & Devrient Dienstleistungscenter
EAL	Evaluation Assurance Level
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
OS	Operating System
PIN	Personal Identification Number
PGP	Pretty Good Privacy
PP	Protection Profile

RAM	Random Access memory
ROM	Read-Only Memory
PP	Protection Profile
RSA	Rivest, Shamir and Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TRex	TTCN-3 Refactoring and Metrics Tool
TSF	TOE Security Functionality

13.2. 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.

Java Card System - The Java Card System consists of the JCRE (JCVM +API). GlobalPlatform defines the Card Manager, which includes the Installer and the Applet Deletion Manager, which are also part of the TOE.

JCRE - The Java Card runtime environment consists of the Java Card virtual machine, the Java Card API, and its associated native methods. This notion concerns all those dynamic features that are specific to the execution of a Java program in a smart card, like applet lifetime, applet isolation and object sharing, transient objects, the transaction mechanism, and so on.

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.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://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[7] 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 BSI-DSZ-CC-1092-2020, Version 4.6, 15.04.2020, Security Target Sm@rtCafé® Expert 7.0 EAL 6+ C1, Giesecke+Devrient Mobile Security GmbH (confidential document)

[7] 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 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- 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 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- 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

[7] Evaluation Technical Report BSI-DSZ-CC-1092-2020 Sm@rtCafé® Expert 7.0 EAL 6+ C1, Version 6, 25.05.2020, TÜV Informationstechnik GmbH (confidential document)

[8] Java Card Protection Profile - Open Configuration, December 2017, Version 3.0.5, BSI-CC-PP-0099-2017, Oracle Corporation

[9] Security Target BSI-DSZ-CC-1092-2020, Version 4.7, 18.05.2020, Security Target Lite Sm@rtCafé® Expert 7.0 EAL 6+ C1, Giesecke+Devrient Mobile Security GmbH (sanitised public document)

[10] Evaluation Technical Report for Composite Evaluation according to AIS 36 for Sm@rtCafé® Expert 7.0 EAL 6+ C1, Version 6, 25.05.2020, BSI-DSZ-CC-1092-2020, TÜViT GmbH (confidential document)

[11] Configuration list for the TOE, Version 1.5, 18.05.2020, Giesecke+Devrient Mobile Security GmbH (confidential document)

[12] Preparative Procedures Sm@rtCafé® Expert Expert 7.0 EAL 6+ C1 Version 2.1 , 15.04.2020, Giesecke+Devrient Mobile Security GmbH

[13] Operational User Guidance Sm@rtCafé® Expert 7.0 EAL 6+ C1, Version 3.6, 01.04.2020, Giesecke+Devrient Mobile Security GmbH

[14] Certification Report BSI-DSZ-CC-0951-V4-2019 for Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008 or v2.07.003, EC v2.03.008 or v2.07.003, SHA-2 v1.01 and Toolbox v2.03.008 or v2.07.003 libraries, symmetric crypto library v2.02.010, as well as with specific IC dedicated firmware, including the Flash Loader enhanced by the Mutual Authentication Extension (MAE) from Infineon Technologies AG, 18.12.2019, BSI

[15] ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-0951-V4-2019, Version 2, 2019-12-10, “Evaluation Technical Report for Composite Evaluation (ETR Comp)”, TÜV Informationstechnik GmbH (confidential document)

[16] GlobalPlatform Card Specification Version 2.2.1, January 2011

[17] GlobalPlatform Card Common Implementation Configuration, Version 1.0, February 2014.

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

[19] Certification Report BSI-DSZ-CC-S-0127-2019 for BSI-DSZ-CC-S-0127-2019 for Giesecke+Devrient Mobile Security Development Center Germany of Giesecke+Devrient Mobile Security GmbH, 13.12.2019, BSI

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

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: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1092-2020

Evaluation results regarding development and production environment

The IT product Sm@rtCafé® Expert 7.0 EAL 6+, C1 (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 29 May 2020, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.3) are fulfilled for the development and production sites of the TOE listed below:

Name of site / Company name	Address	Type of site	Date of last audit	New audit / reused audit / n.r.
Giesecke+Devrient Mobile Security Development Center Germany(DCG)	Prinzregenten-str. 159, 81677 Munich, Germany	SW Development (including documentation) / Testing	2019-07-23/24	Covered by site certification: BSI-DSZ-CC-S-0127-2019

Table 6: Relevant development sites

Related to the composite TOE the HW Infineon sites are also in scope of this TOE certification. Those sites are covered by the underlying HW IC certification BSI-DSZ-CC-0951-V4-2019 [14] and also comprise the delivery.

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.

Annex C of Certification Report BSI-DSZ-CC-1092-2020

Overview and rating of cryptographic functionalities implemented in the TOE

Table 7 gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. 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) only.

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Cryptographic Primitives	ECDH	The implemented ECDH key agreement is reduced to scalar multiplication, checking for the resulting point whether it lies on the curve and differs from the base point. The Elliptic curve parameters, the secret scalar and the public key of the other party are provided from outside and not under control of the TOE. It is in responsibility of the user to implement the full ECDH key agreement procedure compliant to the referenced standard [ISO11770-3]. ECDH provides an elliptic curve Generic Mapping according to [TR-03111] Chapter 4.4.1.	Key sizes corresponding to the used elliptic curve secp{224, 256, 384, 521}r1 [SEC2], brainpoolP{224, 256, 320, 384, 512}r1 and brainpoolP{224, 256, 320, 384, 512}r1[RFC 5639].	Yes	FCS_COP.1.1/ECDH
2	Cryptographic Primitives	SHA-1	[FIPS180-4] (SHA)	None	No	FCS_COP.1.1/HASH
3	Cryptographic Primitives	SHA-{224, 256, 384, 512}	[FIPS180-4] (SHA)	None	Yes	FCS_COP.1.1/HASH

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
4	Cryptographic Primitives	3-DES in ECB mode: encryption and decryption	[SP800-67] Chapter 3.3.1 and 3.3.2 (3DES), [SP800-38A] Chapter 6.1 (ECB), [ISO9797-1] padding method M1 Chapter 6.3.1 and M2 Chapter 6.3.2 and [PKCS5] Appendix B.2.5	|k|=112, 168	No	FCS_COP.1.1/3DES
5	Cryptographic Primitives	3-DES in CBC mode: encryption and decryption	[SP800-67] Chapter 3.3.1 and 3.3.2 (3DES), [SP800-38A] chapter 6.2 (CBC), [ISO9797-1] padding method M1 Chapter 6.3.1 and M2 Chapter 6.3.2 and [PKCS5] Appendix B.2.5	|k|=112	No	FCS_COP.1.1/3DES
6	Cryptographic Primitives	3-DES in CBC mode: encryption and decryption	[SP800-67] Chapter 3.3.1 and 3.3.2 (3DES), [SP800-38A] Chapter 6.2 (CBC), [ISO9797-1] padding method M1 Chapter 6.3.1 and M2 Chapter 6.3.2 and [PKCS5] Appendix B.2.5	|k|=168	Yes	FCS_COP.1.1/3DES
7	Cryptographic Primitives	3DES in CBC-MAC and Retail-MAC mode: generation and verification	[SP800-67] Chapter 3.3.1 and 3.3.2 (3DES), [ISO9797-1] Chapter 7.2 and 7.4 (CBC-MAC, Retail-MAC)	|k|=112	No	FCS_COP.1.1/MAC-DES

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
8	Cryptographic Primitives	3DES in CBC-MAC: generation and verification	[SP800-67] Chapter 3.3.1 and 3.3.2 (3DES), [ISO9797-1] Chapter 7.2 (CBC-MAC)	|k|=168	No	FCS_COP.1.1/MAC-DES
9	Cryptographic Primitives	3DES in Retail-MAC mode: generation and verification	[SP800-67] Chapter 3.3.1 and 3.3.2 (3DES), [ISO9797-1] Chapter 7.4 (Retail-MAC)	|k|=168	Yes	FCS_COP.1.1/MAC-DES
10	Cryptographic Primitives	AES in ECB mode: encryption and decryption	[FIPS 197] (AES), [SP800-38A] Chapter 6.1 (ECB), [ISO9797-1] padding method M1 Chapter 6.3.1 and M2 Chapter 6.3.2 and [PKCS5] Appendix B.2.5	|k|=128, 192, 256	No	FCS_COP.1.1/AES
11	Cryptographic Primitives	AES in CBC mode: encryption and decryption in CBC mode	[FIPS 197] (AES), [SP800-38A] Chapter 6.2 (CBC), [ISO9797-1] padding method M1 Chapter 6.3.1 and M2 Chapter 6.3.2 and [PKCS5] Appendix B.2.5	|k|=128, 192, 256	Yes	FCS_COP.1.1/AES
12	Cryptographic Primitives	AES in CMAC mode: generation and verification	[FIPS 197] (AES), [SP800-38B] (CMAC)	|k|=128, 192, 256	Yes	FCS_COP.1.1/CMAC-AES
13	Cryptographic Primitives	AES in CBC-MAC mode: generation and verification	[FIPS 197] (AES), [ISO9797-1] Chapter 7.2 (CBC-MAC)	|k|=128, 192, 256	No	FCS_COP.1.1/MAC-AES
14	Cryptographic Primitives	RSA encryption and decryption with encoding (RSAES-PKCS1-v1_5) and without encoding (RSADP, RSAEP)	[PKCS #1] Chapter 7.2 (RSA) with encoding and without encoding Chapter 5.1.1 for RSAEP, Chapter 5.1.2 for RSADP	512, 736, 768, 896, 1024, 1280, 1536	No	FCS_COP.1.1/RSA-ENC, FCS_COP.1.1/RSA-DEC

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
15	Cryptographic Primitives	RSA encryption and decryption with encoding (RSAES-PKCS1-v1_5) and without encoding (RSADP, RSAEP)	[PKCS #1] Chapter 7.2 (RSA) with encoding and without encoding Chapter 5.1.1 for RSAEP, Chapter 5.1.2 for RSADP	1984, 2048	Yes	FCS_COP.1.1/RSA-ENC, FCS_COP.1.1/RSA-DEC
16	Cryptographic Primitives	RSA-CRT decryption with encoding (RSAES-PKCS1-v1_5) and without encoding (RSADP)	[PKCS #1] Chapter 7.2 (RSA) with encoding and without encoding Chapter 5.1.2 for RSADP	512, 736, 768, 896, 1024, 1280, 1536	No	FCS_COP.1.1/RSA-CRT-DEC
17	Cryptographic Primitives	RSA-CRT decryption with encoding (RSAES-PKCS1-v1_5) and without encoding (RSADP)	[PKCS #1] Chapter 7.2 (RSA) with encoding and without encoding Chapter 5.1.2 for RSADP	1984, 2048, 4096	Yes	FCS_COP.1.1/RSA-CRT-DEC
18	Cryptographic Primitives	RSA signature generation according scheme 1 of [ISO9796-2] Chapter 8 and [PKCS #1] (RSASSA-PKCS1-v15) Chapter 8 using SHA-{1}	[PKCS #1] Chapter 8.2 (RSA) [ISO9796-2] Scheme 1 [FIPS180-4] (SHA)	512, 736, 768, 896, 1024, 1280, 1536, 1984, 2048	No	FCS_COP.1.1/RSA-SIGN
19	Cryptographic Primitives	RSA signature generation according scheme 1 of [ISO9796-2] Chapter 8 and [PKCS #1] (RSASSA-PKCS1-v15) Chapter 8 using SHA-{224, 256, 384, 512}	[PKCS #1] Chapter 8.2 (RSA) [ISO9796-2] Scheme 1 [FIPS180-4] (SHA)	512, 736, 768, 896, 1024, 1280, 1536	No	FCS_COP.1.1/RSA-SIGN

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
20	Cryptographic Primitives	RSA signature generation according scheme 1 of [ISO9796-2] Chapter 8 and [PKCS #1] (RSASSA-PKCS1-v15) Chapter 8 using SHA-{224, 256, 384, 512}	[PKCS #1] Chapter 8.2 (RSA) [ISO9796-2] Scheme 1 [FIPS180-4] (SHA)	1984, 2048	Yes	FCS_COP.1.1/RSA-SIGN
21	Cryptographic Primitives	RSA-CRT signature generation with encoding scheme 1 of [ISO9796-2] Chapter 8 and [PKCS #1] (RSASSA-PKCS1-v15) Chapter 8 using SHA-1	[PKCS #1] Chapter 8.2 (RSA) [ISO9796-2] Scheme 1 [FIPS180-4] (SHA)	512, 736, 768, 896, 1024, 1280, 1536, 1984, 2048, 4096	No	FCS_COP.1.1/RSA-CRT-SIGN
22	Cryptographic Primitives	RSA-CRT signature generation according scheme 1 of [ISO9796-2] Chapter 8 and [PKCS #1] (RSASSA-PKCS1-v15) Chapter 8 using SHA-{224, 256, 384, 512}	[PKCS #1] Chapter 8.2 (RSA) [ISO9796-2] Scheme 1 [FIPS180-4] (SHA)	512, 736, 768, 896, 1024, 1280, 1536	No	FCS_COP.1.1/RSA-CRT-SIGN
23	Cryptographic Primitives	RSA-CRT signature generation according scheme 1 of [ISO9796-2] Chapter 8 and [PKCS #1] (RSASSA-PKCS1-v15) Chapter 8 using SHA-{224, 256, 384, 512}	[PKCS #1] Chapter 8.2 (RSA) [ISO9796-2] Scheme 1 [FIPS180-4] (SHA)	1984, 2048, 4096	Yes	FCS_COP.1.1/RSA-CRT-SIGN

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
24	Cryptographic Primitives	RSA signature verification according scheme 1 of [ISO9796-2] Chapter 8 and [PKCS #1] (RSASSA-PKCS1-v15) Chapter 8 using SHA-{1, 224, 256, 384, 512}	Scheme 1 of [ISO9796-2] Chapter 8, [PKCS #1] Chapter 8.2 (RSA) [FIPS180-4] (SHA)	512, 736, 768, 896, 1024, 1280, 1536	No	FCS_COP.1.1/RSA-VERI
25	Cryptographic Primitives	RSA signature verification according scheme 1 of [ISO9796-2] Chapter 8 and [PKCS #1] (RSASSA-PKCS1-v15) Chapter 8 using SHA-1	Scheme 1 of [ISO9796-2] Chapter 8, [PKCS #1] Chapter 8.2 (RSA) [FIPS180-4] (SHA)	1984, 2048	No	FCS_COP.1.1/RSA-VERI
26	Cryptographic Primitives	RSA signature verification according scheme 1 of [ISO9796-2] Chapter 8 and [PKCS #1] (RSASSA-PKCS1-v15) Chapter 8 using SHA-{224, 256, 384, 512}	Scheme 1 of [ISO9796-2] Chapter 8, [PKCS #1] Chapter 8.2 (RSA) [FIPS180-4] (SHA)	1984, 2048	Yes	FCS_COP.1.1/RSA-VERI
27	Cryptographic Primitives	ECDSA-FP signature generation and verification	[TR-03111] Chapter 4.2.1 (ECDSA)	Key sizes corresponding to the used elliptic curves secp{224,256, 384, 521}r1 [SEC2] and brainpoolP{224,256,320,384,512}r1 and brainpoolP{224,256,320,384,512}t1 [RFC 5639]	Yes	FCS_COP.1.1/ECDSA-SIGN, FCS_COP.1.1/ECDSA-VERI
28	Cryptographic Primitives	Determ. RNG DRG.4	[AIS20], [AIS31], CTR_DRBG as specified in [ISO18031, C.3.2]	N/A	Yes	FCS_RNG.1.1, FCS_RNG.1.2, [TR-02102]

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
29	Cryptographic Primitives	RSA Key generation	[FIPS186-4], Section B.3.3, Deviations of the above stated standard as described in [SPA/ DPA/DFA –RSA].	512, 736, 768, 896, 1024, 1280, 1536	No	FCS_CKM.1.1/RSA
30	Cryptographic Primitives	RSA Key generation	[FIPS186-4], Section B.3.3, Deviations of the above stated standard as described in [SPA/ DPA/DFA-RSA].	1984, 2048, 4096	Yes	FCS_CKM.1.1/RSA
31	Cryptographic Primitives	ECC Key generation	[SEC2], [RFC 5639] Section 3, [FIPS186-4], Section B.4.1, Deviations of the above stated standard as described in [ECC_key]	Key sizes corresponding to the used elliptic curves secp{224,256, 384, 521}r1 and brainpoolP{224,256,320,384,512}r1 and brainpoolP{224,256,320,384,512}t1	Yes	FCS_CKM.1.1/ECC
32	Cryptographic Primitives	AES Key generation	[FIPS 197] Chapter 3.1 and 5	|k|=128, 192, 256	Yes	FCS_CKM.1.1/AES
33	Cryptographic Primitives	3DES Key generation	[SP800-67] Chapter 3.3.1 and 3.3.2	|k|=112, 168	No, for key lengths of 112 bit; Yes, for key lengths of 168 bit.	FCS_CKM.1.1/3DES

Table 7: TOE cryptographic functionality (with Security Level)

The following table 8 gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated. An explicit validity period is not given.

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1	Authenticity	RSA signature verification using SHA-1 (RSASSA-PKCS1-v1_5)	[PKCS #1] Chapter 8.2, [FIPS180-4] (SHA)	1024, 1280, 1536, 1984, 2048	(DAP-Verification, [GP221], App. C.2, C.3, and C.6)	FCO_NRO.2.1/CM, and FCS_COP.1.1/RSA-VERI.

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
2	Authenticity	3DES in Retail-MAC mode using SHA-1	[SP800-67] Chapter 3.3.1 and 3.3.2 (3DES), [ISO9797-1] Chapter 7.4 (Retail-MAC), [FIPS180-4] (SHA)	|k|=112	(DAP-Verification [GP221], App. C.2, C.3, and C.6)	FCO_NRO.2.1/CM, and FCS_COP.1.1/MAC-DES.
3	Authentication	3-DES in CBC mode	[SP800-67] Chapter 3.3.1 and 3.3.2 (3DES), [SP800-38A] Chapter 6.2.1 (CBC)	|k|=112, |host-challenge|=64, |card-challenge|=48	[GP221], App. E.4.2	FCS_COP.1.1/3DES.
4	Authentication	KDF in counter mode with CMAC as PRF	[SP 800-108] Chapter 5.1 (KDF), [SP800-38B] (CMAC), [FIPS 197] (AES)	|k|=128, |host-challenge|=|card-challenge|=64	[GP_AM_D], Section 6.2.2.2, 6.2.2.3, and 4.1.5	FCS_COP.1.1/CMAC-AES.
5	Key Agreement	3-DES in CBC mode with ICV=0	[SP800-67] Chapter 3.3.1 and 3.3.2 (3DES), [SP800-38A] Chapter 6.2 (CBC)	|k|=112	[GP221], App. E.4.1	FCS_COP.1.1/3DES.
6	Key Agreement	KDF in counter mode with CMAC as PRF	[SP 800-108] Chapter 5.1 (KDF), [SP800-38B] (CMAC), [FIPS 197] (AES)	|k|=128	[GP_AM_D], Section 6.2.1	FCS_COP.1.1/CMAC-AES.
7	Confidentiality	3-DES in CBC mode	[SP800-67] Chapter 3.3.1 and 3.3.2 (3DES), [SP800-38A] Chapter 6.2 (CBC)	|k|=112	[GP221], App. E.3.4, and E.4.2	FCS_COP.1.1/3DES.
8	Confidentiality	AES in CBC mode	[FIPS 197] Chapter 3.1 and 5 (AES), [SP800-38A] Chapter 6.2.1 (CBC)	|k|=128	[GP_AM_D], Section 4.1.2, 6.2.6, and 6.2.7	FCS_COP.1.1/AES.

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
9	Integrity	3DES in Retail-MAC mode	[SP800-67] Chapter 3.3.1 and 3.3.2 (3DES), [ISO9797-1] Chapter 7.4 (Retail-MAC)	|k|=112	[GP221], App. E.4.4 (on unmodified and modified APDU), and E.4.5	FCS_COP.1.1 /MAC-DES.
10	Integrity	AES in CBC-MAC and CMAC mode truncated to 64 bits	[FIPS 197] (AES), [ISO9797-1]) Chapter 7.2 (MAC), [SP800-38B] (CMAC)	|k|=128	[GP_AM_D], Section 6.2.4, and 6.2.5	FCS_COP.1.1 /MAC-AES, and FCS_COP.1.1 /CMAC-AES.
11	Trusted Channel	SCP02	[GP221], App. E additionally cf. lines 3, 5, 7, 9	-	[GP221], App. E, supported parameter 'i': 15,1A,55	FCS_COP.1.1 /3DES, FIA_UID.1/CM, FTP_ITC.1/CMGR, and FCS_COP.1.1 /MAC-DES.
12	Trusted Channel	SCP03	[GP_AM_D] additionally cf. lines 4, 6, 8, 10	-	[GP_AM_D], supported parameter 'i': b1 – b8	FCS_COP.1.1 /AES, FIA_UID.1/CM, FTP_ITC.1/CMGR, FCS_COP.1.1 /MAC-AES, and FCS_COP.1.1 /CMAC-AES.

Table 8: TOE cryptographic functionality (with Standard of Application)

Technical references related to Table 7 and 8:

[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.

[FIPS186-4] Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[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 —

[ISO9797-1] ISO/IEC 9797-1:2011: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher.

[ISO11770-3]ISO/IEC 11770-3, Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques, 2015-07-15.

[ISO18031] ISO/IEC 18031:2011, Information technology – Security techniques – Random bit generation, 2011-11

[PKCS #1] PKCS #1: RSA Cryptography Standard, Version 2.2, October 27, 2012, RSA Laboratories.

[PKCS5] PKCS #5: Password-Based Encryption Standard, Version 2.1.

[SEC2] Standards for efficient cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Research, January 27, 2010, Version 2.0.

[SP800-38A] Recommendation for Block Cipher Modes of Operation, NIST Special Publication 800-38A, December 2001.

[SP800-38B] Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, May 2005.

[SP800-67] NIST Special Publication 800-67 – Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher – Revised November 2017, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

[SP 800-108] NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), Lily Chen; Computer Security Division Information Technology Laboratory, October 2009.

[RFC5639] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, BSI and secunet, March 2010, ISSN 2070-1721.

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

[GP221] GlobalPlatform Card Specification Version 2.2.1, January 2011.

Note: End of report