Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0990-V2-2017

for

SLS 32TLC00xS(M) CIPURSE™ 4move, V1.0.2

from

Infineon Technologies AG

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-0990-V2-2017 (*)

Smart Cards and similar devices: Operation Systems and Applications

SLS 32TLC00xS(M) CIPURSE™ 4move
V1.0.2

from	Infineon Technologies AG
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

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 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 2 only

Bonn, 22 November 2017

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

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

This page is intentionally left blank.

Contents

A. Certification....6

1. Preliminary Remarks....6
2. Specifications of the Certification Procedure....6
3. Recognition Agreements....7
4. Performance of Evaluation and Certification....8
5. Validity of the Certification Result....8
6. Publication....9

B. Certification Results....10

1. Executive Summary....11
2. Identification of the TOE....12
3. Security Policy....13
4. Assumptions and Clarification of Scope....13
5. Architectural Information....13
6. Documentation....13
7. IT Product Testing....14
8. Evaluated Configuration....16
9. Results of the Evaluation....17
10. Obligations and Notes for the Usage of the TOE....18
11. Security Target....18
12. Definitions....18
13. Bibliography....20

C. Excerpts from the Criteria....22

D. Annexes....23

A. Certification

1. Preliminary Remarks

Under the BSIG1 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 03 March 2005, Bundesgesetzblatt I p. 519

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

- 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.sogisportal.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: 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 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. 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 SLS 32TLC00xS(M) CIPURSE™ 4move, V1.0.2 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0990-2016. Specific results from the evaluation process BSI-DSZ-CC-0990-2016 were re-used.

The evaluation of the product SLS 32TLC00xS(M) CIPURSE™ 4move, V1.0.2 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 16 November 2017. 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: Infineon Technologies AG.

The product was developed by: Infineon Technologies AG.

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 22 November 2017 is valid until 21 November 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

[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 SLS 32TLC00xS(M) CIPURSE™ 4move, V1.0.2 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] Infineon Technologies AG
Am Campeon 1-12
85579 Neubiberg

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the SLS 32TLC00xS(M) CIPURSE™4move V1.0.2. It is a smartcard device based on the Infineon M7791 B12 and G11 hardware with a file system oriented operating system, which supports contact-less communication according to ISO/IEC 14443-3 and ISO/IEC 14443-4. The device contains a software part compliant to CIPURSE™ V2, which provides a file system according to ISO/IEC 7816-4 with flexible access rights, a mutual authentication method (3-pass as per ISO/IEC 9798-2) using AES with a terminal and secure messaging which provides integrity protection and confidentiality of the communication (AES-MAC or AES-encryption).

The TOE may also contain a Mifare compatible system, whose data is also accessible by the CIPURSE4move software, to support migration from Mifare to CIPURSE™ V2. The TOE is targeted to contact-less ticketing and payment applications compliant to CIPURSE™ V2.

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

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level 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], chapter 6.2. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functionality	Addressed issue
SF.Authenticate	The TOE provides a three-way cryptographic challenge-and-response mechanism. After successfully performing this challenge-and-response mechanism the TOE enters a secure state. During the authentication a session key is generated by the TOE, which is used to subsequently derive keys for secure messaging activities. The authentication is finished, once a MAC'ed response of the TOE is verified by the terminal.
SF.SM	The TOE supports secure messaging for integrity and confidentiality with AES-MAC and AES-encryption, using proprietary secure messaging APDU format (denoted as SM-APDU format).
SF.Access	The TOE provides flexible access rights and secure messaging rules for each file. Up to 8 keys can be configured per application.
SF.Command-Atomicity	The TOE provides a mechanism for tearing-safe command execution. This mechanism ensures that all changes to the data stored on the TOE are successfully performed or no data changed in case of command execution interruption.
SF.NoTrace	During anti-collision the UID can be retrieved. The TOE can be configured such, that a randomized UID is provided instead of a fixed UID.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. 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] chapter 3.2 and 3.4.

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

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:

SLS 32TLC00xS(M) CIPURSE™ 4move, V1.0.2

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Infineon M7791	B12 / G11	IC package
2	SW	CardOS	V1.0.2	Loaded in protected part of Flash EEPROM of the hardware
3	DOC	CIPURSE™V2 Operation and Interface Specification [9a]	2.0 (2013-12-20)	Hardcopy or pdf file
4	DOC	CIPURSE™V2 Operation and Interface Specification R2.0 Errata and Precision List [9b]	1.0 (2014-09-18)	Hardcopy or pdf file
5	DOC	CIPURSE™V2 CIPURSE™ S Profile Specification [9c]	2.0 (2013-12-20)	Hardcopy or pdf file
6	DOC	CIPURSE™V2 Cryptographic Protocol [9d]	1.0 (2012-09-28)	Hardcopy or pdf file
7	DOC	CIPURSE™V2 Cryptographic Protocol R1.0 Errata and Precision List [9e]	1.0 (2014-09-18)	Hardcopy or pdf file
8	DOC	CIPURSE™4move, SLS 32TLC004S(M) / SLS 32TLC002S(M), Datasheet [9f]	2.2 (2017-09-04)	Hardcopy or pdf file
9	DOC	CIPURSE™4move, SLS 32TLC004S(M), SLS 32TLC002S(M), Personalization Manual [9g]	1.2 (2015-12-01)	Hardcopy or pdf file
10	DOC	CIPURSE™ PICC, Chip Identification Guide [9h]	1.1 (2016-07-08)	Hardcopy or pdf file
11	DOC	CIPURSE™4move, SLS 32TLC00xS(M) V1.0.2, Release Notes [9i]	1.1 (2017-10-10)	Hardcopy or pdf file

Table 2: Deliverables of the TOE

The delivery to the customer (personalization agent) is an external delivery. The TOE is delivered from one of the distribution centers DHL Singapore, IFX Wuxi, K&N

Großostheim, K&N Hayward. The delivery procedures are covered by the platform certificate.

The user can clearly identify the TOE by the information in the predefined file EF.ID_INFO and the Chip Identification Data. The corresponding information is given to him in [9f] and [9h]. Thereby, the exact and clear identification of any product with its exact configuration of this TOE is given.

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:

- Role based access control
- Tearing-safe command execution
- No traceability
- Encryption and Decryption
- Mutual Authentication and Secure messaging
- Key generation and destruction

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- Secure Authentication Data: The operational environment is responsible to keep externally generated keys which are downloaded to the TOE confidentially.
- Terminal-Support: The terminal ensures integrity and confidentiality by verifying data and following the minimum communication level defined by the TOE.

Details can be found in the Security Target [6], chapter 4.1.

5. Architectural Information

The TOE consists of the following subsystems:

- CIPURSE™ engine, which handles all CIPURSE™relevant operations such as access right control, authentication and handling of secure messaging and the file system.
- Communication interface, which implements the functionality of the contact-less communication protocol and manages the incoming and outgoing communication streams.

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. Description of the evaluated TOE configuration

The ST [6] identifies different configurations of the SLS 32TLC00xS(M) CIPURSE™4move V1.0.2.

In accordance with the following sections 7.2, 7.3 and 7.4, the developer and evaluator tested the TOE in these configurations in which the TOE is delivered and which is described in chapter 8.

For the tests performed by the evaluator in the process of the current evaluation both platforms M7791 B12 and M7791 G11 were used. The software version was FF.00.03 which is identical to the final version V1.0.2 of the TOE except the version number, where FF indicates the development version.

7.2. Developer Tests

The developers' testing effort can be summarized as follows.

TOE test configuration:

The tests are performed with the TOE configuration consistent with the Security Target [6].

Developer's testing approach:

- All TSF and related security mechanisms, subsystems and modules are tested in order to assure complete coverage of all SFR.
- Different classes of tests are performed to test the TOE in a sufficient manner:
  - Functional tests,
  - Stress tests,
  - Performance tests,
  - Tearing tests.

Amount of developer testing performed:

- The tests are performed on security mechanisms, subsystem and module level.
- The developer has tested all security mechanisms and TSFI.
- The developer has tested all the TSF subsystems and modules against the TOE design and against the security architecture description.

TOE security functionality tested:

- SF.Authenticate,
- SF.SM,
- SF.Access,
- SF.Command-Atomicity,
- SF.NoTrace.

Overall developer testing results:

- The TOE has passed all tests defined in the developer’s test plan.
- The developer’s testing results demonstrate that the TSF behave as specified.
- The developer’s testing results demonstrate that the TOE behaves as expected.

7.3. Independent Evaluator Tests

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 facility with the evaluation facility test equipment using test scripts.

TOE test configurations:

- Tests were performed with the TOE SLS 32TLC00xS(M) CIPURSE™4move V1.0.2. The TOE configuration was consistent to the configuration described in ST [6].

Subset size chosen:

- During sample testing the evaluator chose to sample the developer functional tests at the evaluation facility. Because of the enormous amount of functional developer tests, only some of the tests were repeated.
- During independent testing the evaluator prepared own test scripts to invoke and test functionality of the TOE. Further penetration testing was done for AVA_VAN aspects. This includes the penetration with laser fault injection attacks and leakage attacks.

Interfaces tested:

- The evaluator included all TSFI into the testing subset.

Developer’s tests repeated:

- The evaluator has re-implemented and performed a subset of developer’s test cases including at least one test case for each TOE Security Feature described in ST [6].
- Additional developer’s test cases were implemented and performed with different file attributes and command parameters compared to the attributes and parameters used by the developer.

Verdict for the activity:

- During the evaluator’s TSF subset testing the TOE operated as specified.
- The results of the developer tests, which have been repeated by the evaluator, matched the results of the developer.
- The results of the specified and conducted independent evaluator tests confirm the TOE functionality as described in Security Target, Functional Specification, and TOE Design. The TSF and interfaces were found to behave as specified.
- Overall the TSF have been tested against the Functional Specification, the TOE Design and the Security Architecture Description. The tests demonstrate that the TSF performs as specified.

7.4. Penetration Testing

Overview:

- The penetration testing was performed using the test environment of the evaluation facility.
- All configurations of the TOE being intended to be covered by the current evaluation were considered for testing.
- The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential high was actually successful.

Penetration testing approach:

- Systematic search for potential vulnerabilities and known attacks in public domain sources, use of a list of vulnerabilities, and from a methodical analysis of the evaluation documents.
- Analysis why these potential vulnerabilities are unexploitable in the intended environment of the TOE.
- If the rationale is suspect in the opinion of the evaluator penetration tests are devised.
- Even if the rational is convincing in the opinion of the evaluator, penetration tests are devised for some vulnerabilities.

TOE test configurations:

- The evaluators used TOE samples for testing that were configured according to the ST [6]. The configurations that were created for testing constitute a reasonable subset of possible configurations that are allowed according to the configurations as defined in ST [6].

Verdict for the sub-activity:

- The evaluator has performed penetration testing based on the systematic search for potential vulnerabilities and known attacks in public domain sources and from the methodical analysis of the evaluation documents.
- During the evaluator’s penetration testing of potential vulnerabilities the TOE operated as specified.
- All potential vulnerabilities are not exploitable in the intended environment for the TOE.
- The TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The Security Target [6] identifies different configurations of the SLS 32TLC00xS(M) CIPURSE™4move concerning the RFI input capacity, the maximum system frequency. Hence the TOE can be delivered with different RFI input capacities and different maximum system frequencies. Depending on these blocking configuration of the SLS 32TLC00xS(M) CIPURSE™4move product different features are available for the user as described in ST [6], chapter 1.4 and especially in table 1.

The hardware can be either M7791 B12 or M7791 G11. The only difference between these two variants is the production site (wafer fab), the functionality is identical.

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 Attackpotential to Smartcards (see [4], AIS 26),*

(iv) *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 [10], [11]) have been applied in the TOE evaluation.*

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

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.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0990-2016, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on:

- Additional functionality and fixes
- Optimization of security functionality

The evaluation has confirmed:

● PP Conformance:	None
● for the Functionality:	Product specific Security Target Common Criteria Part 2 conformant
● 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 5 presented in chapter 6.2.4 of the Security Target [6] 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.

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.

11. Security Target

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

12. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation

CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
I/O	Input/Output
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MAC	Message Authentication Code
PICC	Proximity Integrated Circuit Card
PP	Protection Profile
RFI	Radio-Frequency Identification
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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.

13. 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
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, 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[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-0990-V2-2017, Revision 1.3, 2017-11-09, SLS 32TLC00xS(M) CIPURSE™4move V1.0.2, Infineon Technologies AG

[7] Evaluation Technical Report, Version 5, 2017-11-09, Evaluation Technical Report Summary, TÜV Informationstechnik GmbH, (confidential document)

[8] Configuration list for the TOE (confidential documents)

a) Configuration item list, Version 1.0.2, 2017-04-28, Infineon Technologies AG

b) Development Tool List, 2017-03-15, Infineon Technologies AG

c) Document References, Version 0.4, 2017-10-11, Infineon Technologies AG

[9] Guidance documentation for the TOE

a) CIPURSE™V2 Operation and Interface Specification, Version 2.0, 2013-12-20

b) CIPURSE™V2 Operation and Interface Specification R2.0 Errata and Precision List, Version 1.0, 2014-09-18

c) CIPURSE™V2 CIPURSE™ S Profile Specification, Version 2.0, 2013-12-20

d) CIPURSE™V2 Cryptographic Protocol, Version 1.0, 2012-09-28

[7] specifically

- AIS 25, Version 9, 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 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results

e) CIPURSE™V2 Cryptographic Protocol R1.0 Errata and Precision List, Version 1.0, 2014-09-18

f) CIPURSE™4move, SLS 32TLC004S(M) / SLS 32TLC002S(M), Datasheet, Version 2.2, 2017-09-04

g) CIPURSE™4move, SLS 32TLC004S(M), SLS 32TLC002S(M), Personalization Manual, Version 1.2, 2015-12-01

h) CIPURSE™ PICC, Chip Identification Guide, Version 1.1, 2016-07-08

i) CIPURSE™4move, SLS 32TLC00xS(M) V1.0.2, Release Notes, Version 1.1, 2017-10-10

[10] Certification Report BSI-DSZ-CC-0963-V2-2017, Infineon smartcard IC (Security Controller) M7791 B12 and G11 with specific IC-dedicated firmware, 2017-02-22, Bundesamt für Sicherheit in der Informationstechnik

[11] ETR for composite evaluation according to AIS 36 for the Product M7791 B12 and G11, Version 1, 2017-01-24, TÜV Informationstechnik GmbH (confidential document)

[12] Certification Report BSI-DSZ-CC-0990-2016, SLS 32TLC00xS(M) CIPURSE™ 4move v1.00.00, Infineon Technologies AG, 2016-04-08, Bundesamt für Sicherheit in der Informationstechnik

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 http://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 B of Certification Report BSI-DSZ-CC-0990-V2-2017

Evaluation results regarding development and production environment

The IT product SLS 32TLC00xS(M) CIPURSE™ 4move, V1.0.2 (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 22 November 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) Augsburg – Infineon Technologies AG, Alter Postweg 101, 86159 Augsburg, Germany (Development)

b) Bangalore – Infineon Technologies India Pvt. Ltd., Kalyani Platina, Sy. No. 6 & 24, Kundanahalli Village, Krishnaraja Puram Hobli, Bangalore, India, 560066 (Development)

c) Graz – Infineon Technologies Austria AG, Development Center Graz, Babenbergstr. 10, 8020 Graz, Austria (Development)

d) Munich Infineon Technologies AG, Am Campeon 1-12, 85579 Neubiberg, Germany (Development)

For development and production sites regarding the platform please refer to the certification report BSI-DSZ-CC-0963-V2-2017 [10].

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]) are fulfilled by the procedures of these sites.

Note: End of report