Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1032-2018

for

Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD)

from

Veridos GmbH - Identity Solutions by G+D BDR

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1032-2018 (*)

Digital signature: Secure Signature Creation Devices (SSCD)

Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD)

from	Veridos GmbH - Identity Solutions by G+D BDR
PP Conformance:	EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation, 18 May 2013, BSI-CC-PP-0059-2009-MA-02 (**)
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

SOGIS IT SECURITY CERTIFIED

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 IT Product identified in this certificate is a compliant signature creation device according to Article 30(3) and a compliant seal creation device according to Article 39(2) of eIDAS Regulation (Regulation No 910/2014 of THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014) if the operational conditions as outlined in this certification report are followed.

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
recognition for components
up to EAL 2 only

Bonn, 18 December 2018

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

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

This page is intentionally left blank.

Contents

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

- 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: 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 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 Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD) has undergone the certification procedure at BSI.

The evaluation of the product Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD) was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 17 December 2018. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

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

The product was developed by: cv cryptovision 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 te 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 18 December 2018 is valid until 17 December 2023. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
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 Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD) 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] cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen
Deutschland

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 a Java Card applet configuration providing a Secure Signature Creation Device (SSCD) with Key generation. The TOE is named *Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD)*. It consists of an applet configuration *ePasslet3.0/SSCD* provided by the *Veridos Suite v3.0 – cryptovision ePasslet Suite* for secure signature creation devices with PIN and PACE (Password Authenticated Connection Establishment) authentication (PACE only for contactless variant), the corresponding guidance documents, the underlying operating system with the crypto library and the hardware platform.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation, 18 May 2013, BSI-CC-PP-0059-2009-MA-02 [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 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. 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
TSF_Access	Access Control
TSF_Admin	Administration
TSF_Secret	Secret key management
TSF_Crypto	Cryptographic operations
TSF_SecureMessaging	Secure Messaging
TSF_Auth	Authentication protocols
TSF_Integrity	Integrity protection
TSF_OS	Javacard OS Security Functionalities

Table 1: TOE Security Functionalities

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

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.

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:

Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW+ SW	Veridos eDoc Suite v3.0 – cryptovision ePasslet Suite on platform SmartCafe Expert 7.0 C3	3.0	The delivery is performed with sealed boxes by courier. The delivery process is included in the evaluation of the underlying smartcard OS.
2	DOC	Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing a Secure Signature Creation Device application with on-chip key generation (SSCD Type 3) and supporting PKI utilization - Operational Guidance (AGD_OPE) [10]	3.0.19	The delivery process is included in the evaluation of the underlying smartcard OS. Signed and encrypted Email delivery using PGP RSA 2048 bit is used.
3	DOC	Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card Applet Suite providing Electronic ID Documents applications - Guidance Manual [11]	3.0.11	
4	DOC	Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing a Secure Signature Creation Device application with on-chip key generation (SSCD Type 3) and supporting PKI utilization - Preparation Guidance (AGD_PRE) [12]	3.0.25	
5	DOC	Preparative Procedures Sm@rtCafé® Expert 7.0 C3 [13]	3.6	
6	DOC	Operational User Guidance Sm@rtCafé® Expert 7.0 C3 [14]	5.2	

Table 2: Deliverables of the TOE

The composite TOE consists of the underlying hardware platform, the SmartCafe Expert 7.0 C3 operating system including the crypto library and the Veridos eDoc Suite v3.0 – cryptovision ePasslet Suite in applet configuration ePasslet3.0/SSCD. First, the generated applet suite and the guidance are delivered by encrypted e-mail from the development to the production site. Either the SmartCafe operating system with the applet is integrated into the ordered IC by the IC manufacturer, or the smartcard embedded software developer, here Giesecke+Devrient Mobile Security GmbH (G+D), loads the SW part with the flash loader. Afterwards the composite TOE is delivered in the sense of Common Criteria. Thereby the delivery process is the same for the composite product as the delivery process covered by the certified SmartCafe Expert 7.0 C3 platform. The ST [22] and the guidance [14] of the platform outline the delivery procedure. The product is delivered within sealed boxes by courier and is additionally secured by the hardware and operating system security mechanisms. The TOE guidance is delivered in electronic form (encrypted and signed) according to defined mailing procedures by G+D. The delivery in sense of CC is fully covered by the underlying platform certification of the SmartCafe Expert 7.0 C3.

The TOE can be identified in accordance with the described processes in [6] and [12]. After the delivery the TOE can be identified by the command response sequence as outlined in [6] and [12], verifying the configuration and the life cycle of the underlying platform OS, as well as the CPLC-Data.

After instantiation of the applet it can be selected and the version of the applet can be verified, as well as the internal version numbers, see [12].There are two software versions with different internal version numbers that fall under this certification. Details regarding the identification of the two versions are described in [12].

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:

- Cryptographic Support,
- User Data Protection,
- Identification and Authentication,
- Security Management, and
- Protection of the TSF.

Specific details concerning the above mentioned security policies can be found in Chapter 6.2 of the Security Target [6].

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:

- OE.SVD_Auth,
- OE.CGA_QCert,
- OE.SSCD_Prov_Service,
- OE.HID_VAD,
- OE.DTBS_Intend,
- OE.DTBS_Protect,
- OE.Signatory,
- OE.APPLET,
- OE.VERIFICATION, and

- OE.CODE-EVIDENCE.

Details can be found in the Security Target [6], chapter 4.3 and in the guidance documents.

5. Architectural Information

The composite TOE is a Java Card applet based on a certified Java Card platform that comprises eight subsystems, listed with a short description in the following itemization:

- Platform: Represents the parts of the underlying hardware platform of the composite TOE, which interacts with the application in regards of control, including the creation and selection of applet instance and the internal life cycle control.
- Operating System: Represents the operating system of the underlying SCE platform of the composite TOE, which is used by the applications to realize the functionality. It also comprises the underlying cryptographic library.
- Configuration Manager: Provides services for applet creation and configuration. This subsystem is called by the platform subsystem each time an application is instantiated.
- Event Manager: Handles events from internal subsystems and from the underlying platform and calls other subsystems interfaces to process these events.
- Command Processor: Provides the main interface to the platform by passing through APDU commands from the terminal to the applet. The subsystem decides if specific APDUs have to be handled by the application and ensures their execution by the responsible applet. It also provides access controlled execution of commands covering all applet commands.
- Secure Messaging Manager: Handles the secure channel between the application and the terminal in accordance with the specified cryptographic mechanisms and key sizes. The responsibility for secure messaging includes the verification of MAC, unwrapping messages and security mechanisms for secure messaging.
- File System Manager: Provides an interface for file and object access and management by a representation of the existing elements.
- State Manager: Handles the internal state of the application and provides update functionality and access to the current DF, EF, KO, security environment, and the authentication status of the terminal and the challenge.

For details concerning the CC evaluation of the Java Card platform see the evaluation documentation under the Certification ID BSI-DSZ-CC-1028-2017-MA-01 [15, 16, 19, 20].

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

Developer's Test according to ATE_FUN

The developer’s testing effort is summarised as follows:

TOE configurations tested:

The tests were performed with the composite smart card product ePasslet3.0/SSCD on G&D OS SmartCafe Expert 7.0 C3, in the one configuration in scope of the certification.

Developer’s testing approach:

The developer considered the following aspects when designing his test approach:

- Tests to cover all actions defined in the functional specification,
- Good case and bad case tests for each command defined in the functional specification and executable on the TOE,
- Access rules tests as part of the requirements on TSF data,
- Tests covering all TSF subsystems in the TOE design.

Verdict for the activity:

All test cases in each test suite were run successfully on this TOE version. The developer’s testing results demonstrate that the TOE operates as expected.

Evaluator Tests

Independent Testing according to ATE_IND

The evaluator’s testing effort is described as follows, outlining the testing approach, configuration, depth and results.

Test Approach and Set-up:

The TOE consists of the ePasslet3.0/SSCD application installed on SmartCafe Expert 7.0 C3 OS. The APDU tests were performed using standard PCSC readers, a standard PC, test software provided by the developer as well as evaluator’s test software. Further, for some tests, i.e. fuzzing, B0 card readers (supporting also raw communication) were used.

The selected tests cover tests of the TSFI related to:

- Identification and Authentication (interfaces of different authentication mechanisms),
- Protection against interference, logical tampering and bypass (disturbance of interface execution),
- Secure Messaging (test of interface commands using secure messaging),
- Preparative procedures, performed by the evaluator according to the guidance documentation [11] and [12].

The choice of the subset of interfaces used for testing has been done according to the following approach:

- Augmentation of developer testing for interfaces and supplementation of developer testing strategy for interfaces are both used for setting up test cases,
- Besides augmentation and supplementation of developer’s tests the tests are also selected by the complexity and the susceptibility to vulnerabilities of interfaces and related functionality,

- Since the developer has tested all interfaces and the rigour of developer testing of the interfaces is sufficient, the evaluator found that all TSFI have been suitably tested. The evaluator had no doubt that an interface is not properly implemented,
- The APDU interfaces are essential for the TOE and therefore in the focus of testing,
- Implicit testing was sufficiently included in developer testing because preparative steps were performed and described for nearly each test case,
- The selection process is based on evaluation experience of the evaluation body. Therefore all TOE security functionality is included within the subset. All cryptographic functionality is provided by the platform and was sufficiently tested during platform evaluation,
- Specific tests were conducted that were aligned during online and offline meetings with the certification body.

Configuration:

The TOE was tested in the one configuration in scope of the certification. The keys and personalization data used in the test configuration were provided by the developer.

Test Results:

The test reports for the APDU tests are automatically generated by the test tool used. The test results are logged.

The test logs and the test documentation include details and comments on the test configuration, on the test equipment used, on the used command structure and the expected results. The test prerequisites, test steps, and expected results adequately test the related TSFI, and they are consistent with the descriptions of the TSFI in the functional specification.

The test results have not shown any deviations between the expected test results and the actual test results.

Penetration Testing according to AVA_VAN

Overview:

The penetration testing was performed at the site of the evaluation body TÜViT in the evaluator’s test environment with the evaluator’s test equipment. The samples were provided by the sponsor and by the developer. The test samples were configured and parametrized by the evaluator according to the guidance documentation. The one configuration of the TOE being intended to be covered by the current evaluation was tested. The overall result is that no deviations were found between the expected result and the actual result of the tests. Moreover, no attack scenario with an attack potential of High was actually successful.

Penetration testing approach:

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment created within vulnerability analysis evaluation report, the evaluator created attack scenarios for the penetration tests, where the evaluator is of the opinion that the vulnerabilities could be exploitable. While doing so, the evaluator also considered all aspects of the security architecture of the TOE being not covered by the functional developer tests.

The source code reviews of the provided implementation representation accompanied the development of test cases and were used to find test input. The code inspection supported testing activity by enabling the evaluator to verify implementation aspects that could hardly be covered by test cases.

The primary focus for devising penetration tests was to cover all potential vulnerabilities identified as applicable in the TOE's operational environment for which an appropriate test set was devised.

TOE test configurations:

The tests were performed with the one configuration of the TOE it is delivered in to the personalization agent and as stated in the security target.

Verdict for the sub-activity:

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 of High was actually successful in the TOE's operational environment as defined in the security target provided that all measures required by the developer are applied.

Summary of Test Results and Effectiveness Analysis

The test results yielded 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] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

There is only one configuration of the TOE. For all tests the TOE is configured and parametrized, if necessary, according to the guidance documents. The ePasslet3.0/SSCD TOE configuration is generated out of the applet suite and loaded in the underlying certified OS platform SmartCafe Expert 7.0 C3. The ePasslet3.0/SSCD applet needs to be created according to the guidelines given in [11] and [12].

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) *Application of CC to Integrated Circuits,*

(ii) *Attack Methods for Smartcards and Similar Devices,*

(iii) *Application of Attack Potential to Smartcards,*

(iv) *Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6,*

(v) *Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations,*

(vi) *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 [15, 16, 17, 18, 19. 20, 21]) have been applied in the TOE evaluation.*

(see [4], AIS 26, 33, 34, 36, 46).

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

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

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

The evaluation has confirmed:

- PP Conformance: EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation, 18 May 2013, BSI-CC-PP-0059-2009-MA-02 [8]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

The cryptographic algorithms outlined in Table 4, Annex C (except PACEv2) are implemented in the Java Card Platform SmartCafe Expert 7.0 C3 that is part of the TOE and on which the Java Card applet configuration providing a Secure Signature Creation Device (SSCD) with Key generation is set up. Except for the PACEv2-implementation the security evaluation of the implementation of all other cryptographic algorithms depicted in Table 4 was performed in the framework of the certification of the Java Card Platform SmartCafe Expert 7.0 C3 (refer to the Certification Report [15][16] and related Security Target [25]). The TOE and its specific applet rely on the correct (i.e. standard-conform) and secure implementation of these cryptographic algorithms.

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.

The evaluation was performed as a composite evaluation according to AIS 36 and therefore relies on the platform certifications of the used platform (certification ID BSI-DSZ-CC-1028-2017-MA01) [15, 16, 19, 20].

The composite TOE takes care of the recommendations and requirements imposed by the guidance documentation and ETR for composition of the underlying platform to be resistant against attackers with attack potential high.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The table in annex C of part D of this report 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. Regulation specific aspects (eIDAS, QES)

The IT Product identified in this certificate fulfils

- PP EN 419211-2:2013 (Protection profiles for secure signature creation device - Part 2: Device with key generation (BSI-CC-PP-0059-2009-MA-02))

This Protection Profile is taken from the list of standards identified in COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016, Annex, for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

Therefore, the IT-product certified is technically suitable to be a compliant signature creation device according to Article 30(3) and a compliant seal creation device according to Article 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 and to fulfil the requirements laid down in Article 29(1), Article 39(1) and Annex II provided that the following operational conditions are followed:

- The obligations and notes for the usage of the TOE have to be followed as outlined in chapter 10 of this report.
- The trust service provider has to follow the operational requirements from the regulation as relevant for a compliant signature creation device and a compliant seal creation device as well as to follow all related obligations from its supervisory body.
- For the creation of qualified electronic signatures or qualified electronic seals the product has to use the cryptographic algorithms in accordance with the SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms [26] which are depicted in Table 3. Please note that digital signature creation with RSA is only certified with the key sizes 2048, 2304, 2560, 2816, 3072, 3328, 3584, 3840, and 4096 bit and SHA-224, SHA-256, SHA-384, and SHA-512 with the exception of the following specific combinations: 3072 bit and SHA-384, 3328 bit and SHA-512, 3584 bit and SHA-512 (see ST [6,7], Table 4 in Annex C, and corresponding guidance documentation [10, 11, 12]).
- The trust service provider shall consider the results of the certification and the operational conditions listed above within the system risk management process for the product usage. Specifically, the evolution of limitations of cryptographic algorithms and parameters[7] as well as the evolution of attack methods related to the product or to the type of product has to be considered e.g. by a regular re-assessment of the TOE assurance.

No.	Cryptographic Mechanism	Key Size in Bits	Acceptability Deadline according to [26] as of today
1	RSA PKCS#1 v1.5 [27, 28, 29]	Modulus length = 2048, 2304, 2560, 2816, 3072, 3328, 3584, 3840, 4096	31. December 2022
2	RSA PSS (PKCS#1 v2.1) [27, 28, 29]	Modulus length = 2048, 2304, 2560, 2816	31. December 2024
3	RSA PSS (PKCS#1 v2.1) [27, 28, 29]	Modulus length = 3072, 3328, 3584, 3840, 4096	None
4	ECDSA [30, 31]	ECC Key sizes corresponding to the used elliptic curve brainpoolP{256, 384, 512}r1 [32] secp{256, 384, 521}r1 [30, Appendix D.1.2]	None
5	SHA-2, hash length (bits) = 224 [33, 34]	-	31. December 2022
6	SHA-2, hash length (bits) = 256, 384, 512 [33, 34]	-	None

Table 3: Cryptographic algorithms of the TOE in accordance with [26]

[7] Future updates of the catalogue [26] may shorten or extending the acceptance time frame. This may need actions for the usage of the product to be taken.

Out of this, the compliance of the QSCD / QSealCD is confirmed under the conditions mentioned above within the following categories:

- Components and procedures for the generation of signature resp. seal creation data
- Components and procedures for the storage of signature resp. seal creation data
- Components and procedures for the processing of signature resp. seal creation data

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
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
CGA	Certificate generation application
CPLC	Card production life cycle
cPP	Collaborative Protection Profile
DES	Data Encryption Standard; symmetric block cipher algorithm
DTBS/R	Data to be signed or a unique representation thereof
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
eIDAS	electronic IDentification, Authentication and trust Services
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MAC	Message Authentication Code
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
QES	Qualified electronic signature
RAD	Reference authentication data
SAR	Security Assurance Requirement
SCA	Signature creation application
SCD	Signature creation data

SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SM	Secure Messaging
SSCD	Secure Signature Creation Device
ST	Security Target
SVD	Signature verification data
TOE	Target of Evaluation
TSF	TOE Security Functionality
VAD	Verification authentication data

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.

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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012

Part 3: Security assurance components, Revision 4, September 2012 https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012, 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[8] https://www.bsi.bund.de/AIS

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

[6] Security Target BSI-DSZ-CC-1032-2018, Version 1.9, 2018-12-07, Veridos Suite v3.0 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key Generation (SSCD), cv cryptovision GmbH

[7] Evaluation Technical Report BSI-DSZ-CC-1032, Version 3, 2018-12-12, ETR Summary – Veridos Suite v3.0 - cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD) 3.0, TÜV Informationstechnik GmbH – Evaluation Body for IT Security (confidential document)

[8] EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation, 18 May 2013, BSI-CC-PP-0059-2009-MA-02

[9] Configuration list for the TOE, 2018-12-07, File 1032_SSCD_conflist-SCE.xls, cv cryptovision GmbH (confidential document)

[10] Guidance Document for the TOE: Veridos Suite v3.0 - cryptovision ePasslet Suite - Java Card applet configuration providing a Secure Signature Creation Device application with on-chip key generation (SSCD Type 3) and supporting PKI utilization - Operational Guidance (AGD_OPE), Version 3.0.19, 2018-12-07, cv cryptovision GmbH

[11] Guidance Document for the TOE: Veridos Suite v3.0 - cryptovision ePasslet Suite - Java Card Applet Suite providing Electronic ID Documents applications - Guidance Manual, Version 3.0.11, 2018-12-06, cv cryptovision GmbH

[8] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 26, Version 10, 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 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[12] Guidance Document for the TOE: Veridos Suite v3.0 - cryptovision ePasslet Suite - Java Card applet configuration providing a Secure Signature Creation Device application with on-chip key generation (SSCD Type 3) and supporting PKI utilization - Preparation Guidance (AGD_PRE), Version 3.0.25, 2018-12-07, cv cryptovision GmbH

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

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

[15] Certification Report BSI-DSZ-CC-1028-2017 for Sm@rtCafé® Expert 7.0 C3 from Veridos GmbH – Identity Solutions by G&D BDR, 2017-09-08, Bundesamt für Sicherheit in der Informationstechnik.

[16] Assurance Continuity Maintenance Report BSI-DSZ-CC-1028-2017-MA-01 Sm@rtCafé® Expert 7.0 C3 from Giesecke+Devrient Mobile Security GmbH, 2018-10-04, Bundesamt für Sicherheit in der Informationstechnik.

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

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

[19] Evaluation Technical Report for Composite Evaluation according to AIS 36 for Sm@rtCafé® Expert 7.0 C3, Version 3, 2017-08-16, BSI-DSZ-CC-1028-2017, TÜV Informationstechnik GmbH.

[20] Evaluation Technical Report for Composite Evaluation Addendum for Sm@rtCafé® Expert 7.0 C3, Version 1, 2018-07-18, BSI-DSZ-CC-1028-2017-MA-01, TÜV Informationstechnik GmbH.

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

[22] Security Target Lite Sm@rtCafé® Expert 7.0 C3, Version 2.9, Date 16.08.17, BSI-DSZ-CC-1028-2017, Giesecke & Devrient GmbH

[23] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[24] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016, laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

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

[26] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.1, June 2018

[27] J. Jonsson and B. Kaliski. Public-Key Cryptography Standard (PKCS) #1: RSA Cryptography Specifications Version 2.1. 2003.

[28] RSA Laboratories. PKCS #1 v2.2: RSA Cryptography Standard. 2012.

[29] ISO/IEC. ISO/IEC 9796-2:2010 – Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms. 2010.

[30] National Institute of Standards and Technology. FIPS PUB 186-4: Digital Signature Standard (DSS). 2013.

[31] ISO/IEC. ISO/IEC 14888-3:2006 – Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms. 2006.

[32] M. Lochter and J. Merkle. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. 2010.

[33] National Institute of Standards and Technology. FIPS PUB 180-4: Secure Hash Standard (SHS). 2012.

[34] ISO/IEC. ISO/IEC 10118-3:2004 – Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions. 2004.

[35] ICAO: ICAO Doc 9303, Part 1: Machine Readable Passports, Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability, Sixth Edition – 2006

[36] ICAO: Technical Report: Supplemental Access Control for Machine Readable Travel Documents, Version - 1.01, 11. November 2010.

[37] BSI: TR-03110-1 - Advanced Security Mechanisms for Machine Readable Travel Documents. Part 1 - eMRTDs with BAC/PACEv2 and EACv1, v2.10 (20. March 2012)

[38] Anwendungshinweise und Interpretationen zum Schema (AIS); AIS 20, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[39] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001

[40] Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, NIST Special Publication 800-38B, National Institute of Standards and Technology, May 2005

[41] ISO/IEC 18013-3:2009 Information technology -- Personal identification -- ISO-compliant driving licence -- Part 3: Access control, authentication and integrity validation (2009)

[42] PKCS #1: "RSA Encryption Standard – An RSA Laboratories Technical Note", Version 2.1

[43] Technical Guideline TR-03111, "Elliptic Curve Cryptography", Version 2.0, BSI, 2012-06-28.

[44] Digital Signature Standard (DSS) - FIPS PUB 186-3, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, June, 2009

[45] National Institute of Standards and Technology. SP800-38A: Recommendation for Block Cipher Modes of Operation. 2001.

[46] Standards for efficient cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Research, September 20, 2000, Version 1.0

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 10.4
- 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 11
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16
- 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-1032-2018

Evaluation results regarding development and production environment

The IT product Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Secure Signature Creation Device with Key generation (SSCD) (Ta rget 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 18 December 2018, 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 and ALC_COMP.1) are fulfilled for the development and production sites of the TOE listed below:

a) cv cryptovision GmbH, Munscheidstr. 14, 45886 Gelsenkirchen, Germany (software development site)

b) Regarding the development and production sites of the platform, please refer to the certification reports BSI-DSZ-CC-1028-2017 / BSI-DSZ-CC-1028-2017-MA-01 [15, 16] and BSI-DSZ-CC-0951-2015 / BSI-DSZ-CC-0951-2015-RA-01 [17, 18]

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.

Annex C of Certification Report BSI-DSZ-CC-1032-2018

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Authenticity	RSA-signature generation (RSASSA-PSS and RSASSA-PKCS1-v1_5) without internal hash calculation, or with SHA-224, SHA-256, SHA-384 or SHA-512	PKCS#1 v2.1 [42] [33]	Modulus length= 2048 bit (without CRT) or 2048, 2304, 2560, 2816, 3072, 3328, 3584, 3840, 4096 bit (with CRT) with the exception of the following specific combinations: 3072 bit and SHA-384, 3328 bit and SHA-512, 3584 bit and SHA-512	Yes	-
2	Authenticity	ECDSA without internal hash calculation, or with SHA-224, SHA-256, SHA-384 or SHA-512	[43] [33]	ECC Key sizes corresponding to the used elliptic curve brainpoolP{160, 192, 224, 256, 320, 384, 512}r1 [32], brainpoolP{160, 192, 224, 256, 320, 384, 512}t1 [32], secp{160, 192, 224, 256, 384, 521}r1 [46] |k|= 160, 192, 224, 256, 320, 384, 512, 521 bit	Yes if |k| =224 bit or larger	-
3	Authenticated Key Agreement	PACE version 2 with AES	[37] (PACEv2)	ECC Key sizes corresponding to the used elliptic curve brainpoolP{160, 192, 224, 256, 320, 384, 512}r1 [32], brainpoolP{160, 192, 224, 256, 320, 384, 512}t1 [32], secp{160, 192, 224, 256, 384, 521}r1 [46]	Yes if |k| =224 bit or larger	Only in contactless variant

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
				AES with |k|=128, 192, 256 Length of the Nonce: 16 byte		
4	Authentication	Symmetric Authentication using AES	Standard equivalent to [41]	|k|=128, 192, 256 bit; Length of the Nonce: 8 byte	No	For personalization
5	Confidentiality	AES in CBC mode	[39] (AES), [45] (CBC), IV according to [35]	|k|=128, 192, 256	Yes	Secure Messaging
6	Integrity	AES in CMAC mode	[39] (AES), [40] (CMAC) IV according to [35]	|k|=128, 192, 256	Yes	Secure Messaging
7	Trusted Channel	Secure messaging in ENC_MAC mode establish during PACE	[37] [36]	Cf. Confidentiality/Integrity	Yes	Secure Messaging
8		Secure Messaging for personalization	[35] but with AES Standard equivalent to [41]	|k|=128, 192, 256	No	For personalization
9	Cryptographic primitive	Deterministic RNG DRG.4	[38]	-	Yes	-

Table 4: TOE cryptographic functionality

Note: End of report