Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1036-2019

for

MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892)

from

MaskTech International GmbH

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1036-2019 (*)

Secure Signature Creation Device (SSCD)

MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892)

from	MaskTech International GmbH
PP Conformance:	EN 419211-2:2013 (BSI-CC-PP-0059-2009-MA-02), EN 419211-4:2013 (BSI-CC-PP-0071-2012-MA-01), EN 419211-5:2013 (BSI-CC-PP-0072-2012-MA-01)(**)
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

SOGIS
Recognition Agreement

Common Criteria

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

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

(**) "The IT Product identified in this certificate fulfils PP EN 419211-2:2013, PP EN 419211-4:2013 as well as PP EN 419211-5:2013 and is therefore a compliant signature creation device according to Article 30(3.(a)) (“Certification of qualified electronic signature creation devices”, 3.(a)) of eIDAS Regulation (Regulation No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014).

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

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 23 July 2019

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

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....13
3. Security Policy....14
4. Assumptions and Clarification of Scope....14
5. Architectural Information....15
6. Documentation....16
7. IT Product Testing....16
8. Evaluated Configuration....17
9. Results of the Evaluation....19
10. Obligations and Notes for the Usage of the TOE....21
11. Security Target....21
12. Regulation specific aspects (eIDAS, QES)....21
13. Definitions....23
14. Bibliography....25

C. Excerpts from the Criteria....29

D. Annexes....30

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

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

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

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

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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.

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

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 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 MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1001-2018. Specific results from the evaluation process BSI-DSZ-CC-1001-2018 were re-used.

The evaluation of the product MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892) was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 12 July 2019. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: MaskTech International GmbH.

The product was developed by: MaskTech International GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 23 July 2019 is valid until 22 July 2024. Validity can be re-newed by re-certification.

[6] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
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 MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892) has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] MaskTech International GmbH
Nordostpark 45
90411 Nürnberg

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 product MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892) provided by MaskTech International GmbH and based on the dual interface smart card IC SLE78CLFX400VPHM/BPHM/7PHM (M7892) including Libraries for RSA and EC (Infineon Technologies AG).

The TOE is a combination of hardware and software configured to securely create, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole life cycle as to be used in a signature creation process solely by its signatory. The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature.

The TOE provides the following functions:

- PACE function (mutual authentication and Secure Messaging);
- Chip Authentication Version 1 (Proof of authenticity, establishment of trusted channel between terminal and card);
- Terminal Authentication Version 1 (Restriction of service provisions to authorized Signature Creation Applications and Certificate Generation Applications)
- Protection function in transport (protection against attacks during transport before issuing the TOE); and
- Tamper resistance (protection against confidential information leak due to physical attacks).

The Security Target [6] and [7] is the basis for this certification. It is based on the following certified Protection Profiles:

- Protection profiles for secure signature creation device – Part 2: Device with key generation, CEN/ISSS, EN 419211-2:2013, 2016-06-30, BSI-CC-PP-0059-2009-MA-02 [9]
- Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, CEN/ISSS, EN 419211-4:2013, 2016-06-30, BSI-CC-PP-0071-2012-MA-01 [10]
- Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, CEN/ISSS, EN 419211-5:2013, 2016-06-30, BSI-CC-PP-0072-2012-MA-01 [11]

Password Authenticated Connection Establishment (PACE) including PACE Chip Authentication Mapping and Extended Access Control Version 1 (EACv1) (i.e. Chip Authentication Version 1 (CAv1) and Terminal Authentication Version 1 (TAv1)) functionality to provide a secure authentication protocol and a secure channel for the communication with authorized terminals in usage/operational phase has been added to the ST. This implies extensions, which are adapted from protection profiles PP-0056-V2 [18], PP-0068-V2 [19] and PP-0086 [20]. These extensions were evaluated in the course of this certification procedure.

The product also contains an MRTD application, which is not part of the TOE, but subject to BSI-DSZ-CC-1033 (see [24]) and BSI-DSZ-CC-1034 (see [25]).

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [7], chapter 8.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
F.IC_CL	This Security Function covers the security functions of the hardware (IC).
F.Access_Control	This TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access.
F.Identification_Authentication	This function provides identification/authentication of user roles.
F.Management	Provides management capabilities during development, usage/preparation and usage/operational phases to set file layout, security attributes, and writing of data groups.
F.Crypto	This function provides the implementation or, if the functionality of the cryptographic library (F.IC_CL) is used, the high-level interface to cryptographic functions.
F.Verification	TOE internal functions ensure correct operation by implementing internal hardware test routines.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [7], chapter 10.1.

The assets to be protected by the TOE are defined in the Security Target [6] and [7], chapter 5.1. 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] and [7], chapter 5.

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

The vulnerability assessment results as stated within this certificate do not include a rating for the 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:

MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892) An IC module including the necessary basic software (OS) and SSCD application (file system)		
		1. Hardware Platform Infineon Technologies AG SLE78CLFX400VPHM/BPHM/7PHM (M7892), dual interface Smartcard IC (BSI-DSZ-CC-0891-V3 [16]) using the derivatives with sales code: • SLE78CLFX400VPHM • SLE78CLFX400BPHM and • SLE78CLFX4007PMH	M7892 Design Steps D11 and G12 FW: 78.015.18.2 Crypto libraries: RSA2048/4096 v2.07.003, EC v2.07.003	SW is implemented in NVM memory; chip is initialised and tested before delivery to Personalisation Agent. Delivery type: The OS and application software flashed on the IC Platform
		2. TOE Embedded Software IC Embedded Software (the operating system MTCOS Pro 2.5, implemented in NVM of the IC)	MTCOS Pro Version 2.5, Build date 2018-11-22 Short ROM Codes: MTE1: SLE78CLFX400VPHM without OS MT10T12: SLE78CLFX400VPHM incl. MTCOS MT10T12B: SLE78CLFX400BPHM incl. MTCOS MT10T12S: SLE78CLFX4007PHM incl. MTCOS	
		3. TOE Embedded Applications IC Embedded Software / Part Application Software (containing the SSCD Application implemented in the NVM of the IC with the file system)	MTCOS Pro 2.5 SSCD	
2	DOC	1. User Guidance MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892)	Version 1.3, 03.07.2019 [13]	Password protected Secure Webserver
		2. Guidance for Initialization and Pre-personalization MTCOS Pro 2.5 / SLE78CLFX400VPHM/BPHM/7PHM (M7892) Supporting Document – Initialization/Pre-personalization	Version 1.3, 03.07.2019 [14]	
		3. Manual MTCOS 2.5 on IFX SLE78C(L)FX40xxPH(M)	Version 1.2, 10.01.2019 [15]	

Table 2: Deliverables of the TOE

For TOEs distributed by Infineon Technologies AG the Short ROM Codes are generated on order.

Delivery of sensitive electronic data is performed PGP encrypted via email. The guidance documentation can be obtained by password-protected download from the MaskTech International GmbH website (http://www.masktech.com).

Flash image production: The Developer transfers the flash image (HEX file) to the secure webserver of the Manufacturer via an SSL-protected web access.

TOE for Personalisation: Chip card hardware is securely shipped to the Personalisation Agent.

For the customer to be able to check the correct delivery visually, a delivery note together with the hardware stating the product type and certification reference number is provided. However, the most important check is done implicitly by means of the personalisation keys. The Personalisation Agent must perform a MUTUAL AUTHENTICATE command to authenticate himself against the key. The response of the chip to the command must be verified, either by using Secure Messaging, which is strongly recommended, or by an explicit verification. Because the personalisation keys are derived from the production key provided by MaskTech International GmbH and can only be set after authentication against this production key, the personalisation keys will work only with the correct hardware. Therefore, by being able to perform personalisation successfully, the customer has implicitly checked that the hardware part of the delivery is correct.

Further checks can be done using the GET CHIP ID or GET CHIP INFORMATION command. They return the chip identifier respectively additional information about the platform, the operating system and the patch level. Whether the chip contains the correct file system layout can be verified by checking the product identifier stored in the file EF.KVC (see [13] appendix C).

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: The TOE implements physical and logical security functionality in order to protect user data stored and operated on the smart card when used in a hostile environment. Due to the nature of its intended application, the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives. Specific details concerning the above mentioned security policies can be found in [6] and [7], sec. 6.3.

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: Authenticity of the SVD
- OE.CGA_Qcert: Generation of qualified certificates
- OE.HID_VAD: Protection of the VAD

- OE.DTBS_Intend: SCA sends data intended to be signed
- OE.DTBS_Protect: SCA protects the data intended to be signed
- OE.Signatory: Security obligation of the signatory
- OE.Dev_Prov_Service: Authentic SSCD provided by SSCD-Provisioning Service
- OE.CGA_SSCD_Auth: Pre-initialization of the TOE for SSCD authentication
- OE.CGA_TC_SVD_Imp: CGA trusted channel for SVD import
- OE.HID_TC_VAD_Exp: Trusted channel of HID for VAD export
- OE.SCA_TC_DTBS_Exp: Trusted channel of SCA for DTBS export

Details can be found in the Security Target [6] and [7], chapter 6.2.

5. Architectural Information

The TOE is a composite product. It is composed from an Integrated Circuit SLE78CLFX400VPHM/BPHM/7PHM (M7892), IC Dedicated Software including Test and Support Software, IC Embedded Software (Operating System) and the SSCD Application. While the IC Embedded Software contains the operating system MTCOS Pro V2.5, the NVM contains the SSCD application.

As all these parts of the software are running inside the IC, the external interface of the TOE to its environment can be defined as the external interface of this IC, the Infineon Technologies AG SLE78CLFX400VPHM/BPHM/7PHM (M7892), dual interface Smartcard IC (BSI-DSZ-CC-0891-V3 [16], [17]). The TOE uses three derivatives of SLE78CLFX400VPHM/BPHM/7PHM (M7892) with the sales code:

- SLE78CLFX400VPHM
- SLE78CLFX400BPHM and
- SLE78CLFX4007PHM

These derivatives differ only in the antenna capacity of the module. This difference is not security relevant, thus all three derivatives are taken as one configuration. The chip and cryptographic library are certified according to CC EAL6 augmented compliant to the Protection Profile BSI-CC-PP-0084-2014. For details concerning the CC evaluation of the Infineon IC and its cryptographic libraries see the evaluation documentation under the Certification ID BSI-DSZ-CC-0891-V3-2018 [16], [17].

The security functions of the TOE are enforced by the following subsystems:

Subsystem	**TSF supported**
Application Data	SP.Access_Control, SP.Identification_Authentication
Operation System Kernel	SP.Access_Control, SP.Crypto, SP.Identification_Authentication, SP.Management, SP.Verification
HAL	SP.IC_CL, SP.Crypto, SP.Identification_Authentication, SP.Verification
Hardware	SP.IC_CL

Table 3: Subsystems enforcing TSF

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. Developer Test concept

Test Configuration

Suitable samples were chosen from the described configurations (chapter 8) to test all security functions.

Testing approach

Each security function is covered by at least one test case. Additionally, test cases exist for all subsystems identified in the TOE design. The tests performed can be categorized into two groups: tests with the real card and tests with the emulator. The latter are used for situations that cannot be achieved in a real card's life.

Amount of developer testing performed

The test cases are dedicated to the demonstration of the proper implementation of all security functions, card commands and operating system functionalities. For all commands resp. functionality, test cases are specified in order to demonstrate the expected behaviour including error cases.

Testing Results

All test cases were executed successfully and matched the expected result.

7.2. Evaluator Tests

Independent Testing according to ATE_IND

Test Configuration

Suitable samples were chosen from the described configurations (chapter 8) to test all security functions.

Testing approach

The tests performed can be categorized into two groups: tests with the real card and tests with the emulator. The latter are used for situations that cannot be achieved in a real card's life. From all existing file system setups, a representative subset of setups was chosen for evaluator testing. For the chosen setups the evaluators conducted all test cases of the developer’s test suite for non-interactive tests using the test equipment provided by the developer. The evaluators decided to focus their own independent tests on tests with real cards, but emulator tests were also conducted. For these tests the evaluators derived some test ideas from the developer tests under consideration of the described security functionality. Furthermore, the evaluators used fuzz testing to determine the correct implementation of the TOE.

Testing Results

All test cases developed by the evaluator were executed successfully and ended up with the expected result.

All repeated developer tests have been conducted successfully and all the actual test results were as the expected ones (as gained by the developer). For the test results of the emulator tests the evaluator repeated the emulator tests executed by the developer. The repetition of the emulator tests showed that the test results are consistent. Fuzz testing did not reveal any flaws in the TOE's implementation.

Penetration Testing according to AVA_VAN

Penetration testing approach

The penetration testing was performed using the test environment of the evaluation facility. All relevant information as well as evaluation documentation was taken into account for the analysis by the evaluators. For the penetration analysis the evaluator analysed the CC deliverables for potential vulnerabilities already during the evaluation work for the corresponding aspects. The evaluators found no exploitable vulnerabilities in the evaluation deliverables. The evaluator used the potential vulnerabilities from the JIL document as the leads for further investigations. All possible attack methods against an authentic operational TOE were analysed. Thereby the results and experience of the ISCI working group consolidated in the corresponding document were taken into account.

Testing Results

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential *High* was actually successful in the TOE's operational environment as defined in [6][7] provided that all measures required by the developer are applied. Potential vulnerabilities cannot be exploited during the phases development, manufacturing and personalisation.

8. Evaluated Configuration

This certification covers the following TOE:

MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892) consisting of:

- Operating system and a file system in the context of the SSCD application with the Infineon Technologies AG MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892) chip; software completely contained in NVM
- File system layout according to the selected configuration (see table 4 and user guidance [13])
- User guidance [13] and [14],
- Product Manual [16].

The IC embedded software consists of the operating system MTCOS Pro V2.5 and an application layer containing the SSCD application.

The product is provided in 8 available configurations. These differ in the provided key set and the requirement for Terminal Authentication Version 1 for the communication between the TOE and the Signature Creation Application (SCA) or the Certificate Generation Application (CGA), respectively. Some configurations include an additional decryption key. The decryption key and the corresponding security functionality are not in the scope of this

certification. The configurations, that are in the scope of this certification are depicted in table 4:

No	Configuration-ID	Signature key	Decryption key	Terminal Authentication required
1	RSA-PSS	key-set-1	-	no
2	RSA-PSS-ta	key-set-1	-	yes
3	RSA-PSS-dec	key-set-1	key-dec	no
4	EC	key-set-2	-	no
5	EC-ta	key-set-2	-	yes
6	EC-dec	key-set-2	key-dec	no
7	RSA-raw-dec	key-set-3	key-dec	no
8	RSA-raw-dec-ta	key-set-3	key-dec	yes

Table 4: Product configurations and corresponding file system layouts

The key sets provided for digital signature and decryption are listed in the user guidance table 3.6 (see [13]).

The product also contains an MRTD application, which is not part of the TOE, but subject to BSI-DSZ-CC-1033-2019 (see [24]) and BSI-DSZ-CC-1034-2019 (see [25]). The MRTD application has 20 available configurations (for details see [24] and [25]), which, combined with the 8 available configurations of the SSCD application leads to a total of 45 available configurations (see table 5).

No	Configuration-ID	RSA-PSS	RSA-PSS-ta	RSA-PSS-dec	EC	EC-ta	EC-dec	RSA-raw-dec	RSA-raw-dec-ta	No SSCD
1	LayoutA-86-AA_RSA-SM_3DES	x	x	x						x
2	LayoutA-86-AA_RSA-SM_AES-128	x	x	x				x	x	x
3	LayoutA-86-AA_EC-SM_3DES				x	x	x			
4	LayoutA-86-AA_EC-SM_AES-128				x	x	x	x	x	
5	LayoutB-86-AA_RSA-SM_3DES	x	x							x
6	LayoutB-86-AA_RSA-SM_AES-128	x	x							x
7	LayoutB-86-AA_EC-SM_3DES				x	x				
8	LayoutB-86-AA_EC-SM_AES-128				x	x				
9	LayoutC-160-AA_RSA-SM_3DES									x
10	LayoutC-160-AA_RSA-SM_AES-128									x
11	LayoutC-160-AA_EC-SM_3DES									x

12	LayoutC-160-AA_EC-SM_AES-128									x
13	LayoutD-131-AA_RSA-SM_3DES				x	x				x
14	LayoutD-131-AA_RSA-SM_AES-128				x	x				x
15	LayoutG-160-AA_RSA-SM_3DES									x
16	LayoutG-160-AA_RSA-SM_AES-128									x
17	LayoutG-160-AA_EC-SM_3DES									x
18	LayoutG-160-AA_EC-SM_AES-128									x
19	Layout0-S									x
20	Layout0-L				x	x				

Table 5: MRTD / SSCD layout combinations

Further details are given in the User Guidance [13].

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [8] 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) Application of CC to Integrated Circuits, (see [4], AIS 25)

(iii) Attack Methods for Smartcards and Similar Devices,(see [4], AIS 26)

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

(v) Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6, (see [4], AIS 34)

(vi) Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations (see [4], AIS 46)

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

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

(ix) *Composite product evaluation for Smart Cards and similar devices (see [4], 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 [16, 17], have been applied in the TOE evaluation.*

For smart card specific methodology the scheme interpretations AIS 25, AIS 26 and AIS 36 were used (see [4]). For RNG assessment the scheme interpretations AIS 31 and AIS 20 were 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.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1001-2018, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on porting of the embedded software to the hardware M7892 by Infineon Technologies AG (certification-ID: BSI-DSZ-CC-0891-V3-2018) and on changes related to the used sites.

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,

  Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application, CEN / ISSS - Information Society Standardization System, 12 October 2013, BSI-CC-PP-0071-2012-MA-01,

  Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application, CEN / ISSS - Information Society Standardization System, 12 October 2013, BSI-CC-PP-0072-2012-MA-01 [9, 10, 11]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

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

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configurations 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 IC (certification ID BSI-DSZ-CC-0891-V3) [16], [17].

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 A.1 presented in chapter A of the Security Target 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 'Standard of Application / Security Level' of the table A.1 with 'Security Level < 100 bits' achieves a security level of lower than 100 Bits (in general context) only.

The table A.1 outlines the standard of application where its specific appropriateness is stated. An explicit validity period is not given. The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

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

12. Regulation specific aspects (eIDAS, QES)

In [21] the European Parliament and the Council of the European Union has codified the conceptional requirements for qualified electronic signature devices used in the European Union. This regulation is clarified in the Commission Implementing Decision [22]. In this decision the requirements are stated an electronic signature device must fulfil to be compliant to [21] (Article 1 and Annex).

The IT Product identified in this certificate fulfils

- Protection profiles for secure signature creation device – Part 2: Device with key generation, CEN/ISSS, EN 419211-2:2013, 2016-06-30, BSI-CC-PP-0059-2009-MA-02 [9],
- Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, CEN/ISSS, EN 419211-4:2013, 2016-06-30, BSI-CC-PP-0071-2012-MA-01 [10],

- Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, CEN/ISSS, EN 419211-5:2013, 2016-06-30, BSI-CC-PP-0072-2012-MA-01 [11].

These Protection Profiles are 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 [22].

Furthermore the TOE must be certified using ISO/IEC 15408 and ISO/IEC 18045 in its 2008/2009 versions. The evaluation process of MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892) used the latest available version of Common Criteria [1] which is as used compatible to the ISO version cited in [22].

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 [23] which are depicted in Table 6.
- 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[8] 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 [23] as of today
1	RSA PKCS#1 v1.5 [26, 27, 28]	Modulus length = 2048-4096 (32-Bit steps)	31. December 2022
2	RSA PSS (PKCS#1 v2.1) [26, 27, 28]	Modulus length = 2048 – 2976 (32-Bit steps)	31. December 2024

[8] Future updates of the catalogue [23] may shorten or extending the acceptance time frame. This may need actions for the usage of the product to be taken.

No.	Cryptographic Mechanism	Key Size in Bits	Acceptability Deadline according to [23] as of today
3	RSA PSS (PKCS#1 v2.1) [26, 27, 28]	Modulus length = 3008 – 4096 (32-Bit steps)	None
4	ECDSA [29, 30]	ECC Key sizes corresponding to the used elliptic curve BrainpoolP{256, 384, 512}r1 [31] NIST P{256, 384, 521} [29, Appendix D.1.2]	None
5	SHA-2, hash length (bits) = 224 [32, 33]	-	31. December 2022
6	SHA-2, hash length (bits) = 256, 384, 512 [32, 33]	-	None

Table 6: Cryptographic algorithms of the TOE in accordance with [23]

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

BAC Basic Access Control

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

cPP Collaborative Protection Profile

DES Data Encryption Standard; symmetric block cipher algorithm

DTBS/R Data to be signed or a unique representation thereof

EAC	Extended Access Control
EAL	Evaluation Assurance Level
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
eIDAS	Electronic IDentification, Authentication and trust Services
ETR	Evaluation Technical Report
HEX	Hexadecimal
HW	Hardware
IFX	Infineon
ICAO	International Civil Aviation Organisation
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MAC	Message Authentication Code
MRTD	Machine Readable Travel Document
NVM	Non-Volatile Memory
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 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
https://www.commoncriteriaportal.org

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[9] 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-1036-2019 - Secure signature creation device with key generation MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892), Version 0.9, 03.07.2019, MaskTech International GmbH (confidential document)

[7] Security Target Lite BSI-DSZ-CC-1036-2019 - Secure signature creation device with key generation MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892), Version 1.3, 03.07.2019, MaskTech International GmbH (sanitised public document)

[8] Evaluation Technical Report BSI-DSZ-CC-1036, Version 1.8, 16.07.2019, Evaluation Technical Report (ETR), SRC Security Research & Consulting GmbH (confidential document)

[9] Protection profiles for secure signature creation device – Part 2: Device with key generation, CEN/ISSS, EN 419211-2:2013, 2016-06-30, BSI-CC-PP-0059-2009-MA-02

[10] Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, CEN/ISSS, EN 419211-4:2013, 2016-06-30, BSI-CC-PP-0071-2012-MA-01

[11] Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, CEN/ISSS, EN 419211-5:2013, 2016-06-30, BSI-CC-PP-0072-2012-MA-01

[12] Configuration List for MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892), Version 0.5, 03.07.2019, MaskTech International GmbH (confidential document)

[9] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[13] User Guidance: MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892), Version 1.3, 03.07.2019, MaskTech International GmbH

[14] Guidance for Initialization and Pre-personalization MTCOS Pro 2.5 / SLE78CLFX400VPHM/BPHM/7PHM (M7892) Supporting Document – Initialization/Pre-personalization, Version 1.3, 03.07.2019, MaskTech International GmbH

[15] User Guidance: MTCOS MANUAL MTCOS 2.5 on IFX SLE78C(L)FX40xxPH(M), Version 1.2, 10.01.2019, MaskTech International GmbH

[16] Certification Report, BSI-DSZ-CC-0891-V3-2018 for Infineon Security Controller, M7892 Design Steps D11 and G12, with specific IC dedicated firmware and optional software from Infineon Technologies AG, 09.01.2018, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[17] ETR For Composite Evaluation (ETR COMP), Certification ID BSI-DSZ-CC-0891-V3, TOE M7892 G12 and D11, TÜV Informationstechnik GmbH - Evaluation Body for IT Security, Version 1, 29.11.2017

[18] BSI-CC-PP-0056-V2-2012, Common Criteria Protection Profile / Machine Readable Travel Document with ’ICAO Application’, Extended Access Control with PACE, BSI, Version 1.3.2, 2012-12-05

[19] BSI-CC-PP-0068-V2-2011, Common Criteria Protection Profile / Machine Readable Travel Document using Standard Inspection Procedure with PACE (ePass_PACE PP), BSI, Version 1.0, 2011-11-02

[20] BSI-CC-PP-0086-2015, Common Criteria Protection Profile / Electronic document implementing Extended Access Control Version 2 (EAC2) based on BSI TR-03110 (EAC2_PP), BSI, Version 1.01, 2015-05-20

[21] 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

[22] 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

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

[24] Certification Report BSI-DSZ-CC-1033-2019 for MTCOS Pro 2.5 EAC with PACE / SLE78CLFX400VPHM/BPHM/7PHM (M7892) from MaskTech International GmbH, 23 July 2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[25] Certification Report BSI-DSZ-CC-1034-2019 for MTCOS Pro 2.5 EAC with PACE / SLE78CLFX400VPHM/BPHM/7PHM (M7892) (BAC) from MaskTech International GmbH, 23 July 2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

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

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

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

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

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

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

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

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

C. Excerpts from the Criteria

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

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

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

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

Annex B of Certification Report BSI-DSZ-CC-1036-2019

Evaluation results regarding development and production environment

The IT product MTCOS Pro 2.5 SSCD / SLE78CLFX400VPHM/BPHM/7PHM (M7892) (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 23 July 2019, 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) MaskTech International GmbH, Nordostpark 45, 90411 Nuremberg, Germany (Development, Initialisation/Pre-personalisation)

b) SmarTrac Technology Ltd. 142 Moo, Hi-Tech Industrial Estate, Tambon Ban Laean, Amphor Bang-pa-in, 13160 Ayutthaya Thailand, BSI-DSZ-CC-S-0097-2017, Site Certificate valid until 26.12.2019 (Initialisation/Pre-personalisation)

c) HID Global Ireland, Teoranta Pairc Tionscail na Tullaigh, Baile na hAbhann Co. Galway, Ireland, BSI-DSZ-CC-S-0114-2018, Site Certificate valid until 18.09.2020 (Initialisation/Pre-personalisation)

d) HID Global Sdn. Bhd. No. 2, Jalan i-Park 1/1 Kawasan Perindustrian i-Park, Bandar Indahpura 81000 Kulai, Johor Malaysia, BSI-DSZ-CC-S-0085-2018, Site Certificate valid until 14.05.2020 (Initialisation/Pre-personalisation)

e) Gemalto AG, Hintere Bahnhofstrasse 12, CH-5001 Aarau Switzerland, BSI-DSZ-CC-S-0104-2018, Site Certificate valid until 05.06.2020 (Initialisation/Pre-personalisation)

f) For development and production sites regarding the platform at Infineon Technologies AG (headquarter), Am Campeon 1-12, 85579 Neubiberg, Germany, please refer to the certification report BSI-DSZ-CC-0891-V3-2018 [16] (IC Development, Initialisation/Pre-personalisation)

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [7]) are fulfilled by the procedures of these sites.

Note: End of report