Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1042-2020

for

DERMALOG Fingerprint PAD Kit LF10

LF10, Part-No. 8004-0009-00
DermalogBPLF10Plugin, V 1.3.8.1935
DermalogFakeFingerDetectionLF10Plugin, V 1.3.3.1925
DermalogFourprintSegmentation2 V 1.14.0.1919
DermalogAuditLogger, V 1.1.3.1827

from

DERMALOG Identification Systems 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-1042-2020 (*)

Presentation Attack Detection System

DERMALOG Fingerprint PAD Kit LF10

Hardware:	LF10, Part-No. 8004-0009-00
Software:	DermalogBPLF10Plugin, V 1.3.8.1935 DermalogFakeFingerDetectionLF10Plugin, V 1.3.3.1925 DermalogFourprintSegmentation2, V 1.14.0.1919 DermalogAuditLogger, V 1.1.3.1827
from	DERMALOG Identification Systems GmbH
PP Conformance:	Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7, 27 November 2009, BSI-CC-PP-0062-2010
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ALC_FLR.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2

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 and TOE type specific methodology 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.

Common Criteria
Recognition Arrangement

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, 17 March 2020

For the Federal Office for Information Security

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

Bernd Kowalski
Head of Division

L.S.

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the 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 3 March 2005, Bundesgesetzblatt I, p. 519

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

3. Recognition Agreements

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

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

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

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

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

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

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

3.2. International Recognition of CC – Certificates (CCRA)

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

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under CCRA-2014 for all assurance components selected.

[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 DERMALOG Fingerprint PAD Kit LF10 has undergone the certification procedure at BSI.

The evaluation of the product DERMALOG Fingerprint PAD Kit LF10 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 27 February 2020. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is:
DERMALOG Identification Systems GmbH.

The product was developed by: DERMALOG Identification Systems 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 17 March 2020 is valid until 16 March 2025. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

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

[5] Information Technology Security Evaluation Facility

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

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product DERMALOG Fingerprint PAD Kit LF10 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] DERMALOG Identification Systems GmbH
Mittelweg 120
20148 Hamburg
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 the DERMALOG Fingerprint PAD Kit LF10 consisting of a fingerprint sensor (LF10, Part-No. 8004-0009-00) and PC software (Dermalog BPLF10Plugin, V 1.3.8.1935, DermalogFakeFingerDetectionLF10Plugin, V 1.3.3.1925, DermalogFourprintSegmentation2, V 1.14.0.1919, DermalogAuditLogger, V 1.1.3.1827).

Its core functionality is classifying whether a finger that is presented to the sensor, is actually a real finger presented by a genuine user or whether an artefact is presented (a so-called artefact presentation or presentation attack).

The Security Target [6] is the basis for this certification. It is based on the certified Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7, 27 November 2009, BSI-CC-PP-0062-2010 [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 ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ALC_FLR.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2.
This explicitly defined assurance package is based on EAL 2, but the AVA_VAN component is completely omitted. It was defined in the PP to focus on application cases for which it is sufficient to determine whether the Security Functionality claimed by a TOE is working correctly without performing a dedicated vulnerability assessment.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2 and one of them is newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
SF.AUDIT	Security Audit
SF.RIP	Residual Information Protection
SF.SM	Security Management
SF.PAD	Presentation Attack Detection (PAD)

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 3.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.3 and 3.5.

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

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:

DERMALOG Fingerprint PAD Kit LF10

It consists a fingerprint sensor (LF10, Part-No. 8004-0009-00) and PC software (DermalogBPLF10Plugin, V 1.3.8.1935, DermalogFakeFingerDetectionLF10Plugin, V 1.3.3.1925, DermalogFourprintSegmentation2, V 1.14.0.1919, DermalogAuditLogger, V 1.1.3.1827).

The following table outlines the TOE deliverables:

No	Type	Identifier	Release/Version	Form of Delivery
1	HW	LF10 hardware	Part No. 8004-0009-00	Parcel mail
2	SW	DermalogBPLF10Plugin	1.3.8.1935	Download from support portal
3	SW	DermalogFakeFingerDetectionLF10Plugin	1.3.3.1925	Download from support portal
4	SW	DermalogFourprintSegmentation2	1.14.0.1919	Download from support portal
5	SW	DermalogAuditLogger	1.1.3.1827	Download from support portal
6	DOC	DERMALOG Guidance Addendum Dermalog Fingerprint PAD Kit LF10 [12]	1.9	Download from support portal
7	DOC	DERMALOG Fingerprint Scanner LF10 User Guide [13]	3.3	Download from support portal
8	DOC	DermalogBPLF10Plugin [14]	SHA-256-Hash: 0B40999446BEBF78AD5FC5B2AD09081CCCA3856390FD6E9CF23D44BD287DB240	Download from support portal

Table 2: Deliverables of the TOE

The delivery of the hardware part (fingerprint sensor) is performed via parcel mail including tracking information. The delivery process starts at the premises of the manufacturer and is directed directly to the end customer.
As soon as the box arrives at the premises of the customer, the administrator of the device (who received the guidance documentation via an independent channel, namely the support portal) is advised to perform an integrity check of the sensor which includes an inspection of the body of the sensor for any visible manipulations and a check of the seal that is placed on the bottom of the device.

The TOE software parts and the guidance documentation can be downloaded from the access controlled support portal of the developer via https connection. The binaries of the TOE are delivered as part of the installer of the DERMALOGMultiScannerSDK. The integrity check of the software and the guidance documentation is performed using digital signatures.

The TOE software offers a function that allows checking the version information of the TOE components. This function is called FFDGetVersionA and its use is described in the guidance documentation [12].

The sensor components carry version information on the sticker on their back side. It is important that this version information (in form of the Part No.) is checked to match the values listed in table 2 above.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: security audit, residual information protection, security management and presentation attack detection.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of 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: Well trained and trustworthy TOE administrators, physical protection of the TOE, supporting mechanisms provided by the underlying platform and invocation of the TOE's Security Functionality by the protected biometric system. Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The TOE consists of a HW-subsystem (Scanner) and three SW-subsystems (Scanner Control API, Supportive API, Presentation Attack Detection API). All four subsystems together implement the TOE Security Functionality.

The Scanner subsystem provides the interface to the user and captures the fingerprint of the user.

The Presentation Attack Detection API subsystem implements the core functionality of the TOE, i.e. the presentation attack detection. This subsystem analyses images of fingerprints and returns information on how likely these images show a presentation attack.

The Scanner Control API subsystem implements all functionality that invokes sensor communication and provides the interface between the TOE SW parts and the sensor. This subsystem is also responsible for the final decision on PAD, i.e. it compares the calculated value by the Presentation Attack Detection API subsystem with the threshold setting and converts it into a binary value.

The Supportive API subsystem implements parts of the TOE's audit functionality and provides the interface to the external audit storage. It also provides the functionality to segment fingerprint images into images of single fingerprints out of an image that contains up to four fingerprints.

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. Functional Developer Testing

All developer tests in the context of the evaluation were conducted using the final version of the TOE. The TOE was configured using a PAD threshold of 50 and mode 0 for all tests. The tests of the audit and management functionality were performed with log level verbose.

The developer used two simple test tools to test the management, audit and residual information protection functionality.

The testing of the PAD functionality (according to FPT_SPOD.1) was conducted by creating fake fingers from different materials according to the requirements from the Toolbox documentation [10]. In total, the developer created 145 artifacts and applied each artifact at least 20 times to the TOE. The test results showed that no faked finger was detected as a real finger in any attempt.

All in all, the developer tested the TOE systematically at the level of TSFI as given in the Functional Specification. The developer thereby followed the strategy to cover all TSFI.

All tests were passed successfully.

7.2. Independent Evaluator Testing

All evaluator tests in the context of the evaluation were conducted using the final version of the TOE. The TOE was configured using a PAD threshold of 50 and mode 0 for all tests (except for the tests where the management of those parameters was tested).

The evaluator repeated all developer tests, except the test of the presentation attack detection, in order to verify the adequateness of the tests conducted with the developer test tools.

The evaluator further developed a set of own manual test cases for functional testing. Thereby he had chosen the approach to cover the functional areas presentation attack detection, audit and management. This approach extends the one used for the developer tests. Full TSFI coverage is provided in both approaches. The evaluator devised and performed 2 functional tests and 3 other tests.

For testing the presentation attack detection, the evaluator created and tested 65 artifacts of various materials according to the requirements of the Toolbox documentation [10]. The evaluator carried out more than 1350 attempts to spoof the TOE with these artifacts.

All tests were passed successfully.

8. Evaluated Configuration

This certification covers only one configuration of the TOE. It consists of the HW and SW parts as indicated in chapter 2. Furthermore the TOE has to be operated using FFD_Mode 0 and FFD_Threshold 50. As described in the guidance [12], chapter 5.3, the plain finger mode has to be used.

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, extended by guidance specific for the technology of the product.

The following guidance specific for the technology was used:

(i) Fingerprint Spoof Detection Evaluation Guidance [9]

(ii) Toolbox documentation [10].

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

- All components claimed in the Security Target [6], chapter 6.2 and defined in the CC (see also part C of this report).

The evaluation has confirmed:

- PP Conformance: Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7, 27 November 2009, BSI-CC-PP-0062-2010 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ALC_FLR.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The TOE does not include cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

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.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

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

12. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PAD	Presentation Attack Detection
PP	Protection Profile
SAR	Security Assurance Requirement
SDK	Software Development Kit
SFP	Security Function Policy

SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

12.2. Glossary

Artefact - Artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

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

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.

Fake - Synonym for artefact

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

Presentation Attack - Presenting an artefact to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

Presentation Attack Detection - Automated process of detecting a presentation attack

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.

Spoof Detection - Synonym for presentation attack detection

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

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

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

13. Bibliography

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

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

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

[6] Security Target BSI-DSZ-CC-1042-2020, Version 2.7, 26 February 2020, Security Target DERMALOG Fingerprint PAD Kit LF10, DERMALOG Identification Systems GmbH

[7] Evaluation Technical Report, Version 2, 26 February 2020, TÜV Informationstechnik GmbH (confidential document)

[8] Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7, 27 November 2009, BSI-CC-PP-0062-2010

[9] Fingerprint Spoof Detection Evaluation Guidance, Version 2.1, 18 December 2009

[10] Toolbox022017, February 2017, BSI

[11] Configuration list for the TOE: List of references DERMALOG Fingerprint PAD Kit LF10, Version 2.0, 26 February 2020, DERMALOG Identification Systems GmbH (confidential document)

[12] DERMALOG Guidance Addendum DERMALOG Fingerprint PAD Kit LF10, Version 1.9, 25 February 2020, DERMALOG Identification Systems GmbH

[13] DERMALOG Fingerprint Scanner LF10 User Guide, Version 3.3, 05 September 2019, DERMALOG Identification Systems GmbH

[14] DermalogBPLF10Plugin.chm (identified via hashsum, cmp. table 2) DERMALOG Identification Systems GmbH

[7] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

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 detailed 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.

Note: End of report