
C001 Certification Report

[CB-4-RPT-QCCS]-C001

**DERMALOG Fingerprint PAD Kit LF10, Part No. 8004-0009-00,
DermalogBPLF10Plugin: 1.7.2.2126,
DermalogFakeFingerDetectionLF10Plugin: 1.4.0.2125,
DermalogFourprintSegmentation2: 1.18.1.2126,
DermalogAuditLogger: 1.1.3.1827**

Report

Compliance and Data Protection Department

22.09.2021

v2.0

Public



Document Authorization

This page detail may intentionally be removed or hidden when publicly published or shared

DOCUMENT TITLE: C001 Certification Report

DOCUMENT REFERENCE: [CB-4-PCD-QCCS]-C001

ISSUE: v2.0

DATE: 22.09.2021

PREPARED BY:



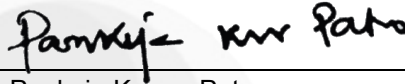
I.D Safairis Bin Amat Noor

Certifier, QCCS, CDP Dept.
MoTC, Qatar

22.09.2021

Date

REVIEWED BY:



Pankaja Kumar Patro

Quality Manager, QCCS, CDP Dept.
MoTC, Qatar

23.09.2021

Date

RECOMMENDED BY:



Ashraf Ali Ismael

Scheme Manager, QCCS, CDP Dept.
MoTC, Qatar

26.09.2021

Date

APPROVED BY:



Eng. Dana Yousif Al-Abdulla

Scheme Director, QCCS, CDP Dept.
MoTC, Qatar

30.09.2021

Date

FOREWORD

The Qatar Common Criteria Scheme (QCCS) Certification Body (CB) has been established to increase Qatar's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Qatar information security products.

The QCCS is operated by Ministry of Transport and Communications (MoTC) and provides a model for licensed Evaluation Bodies (or Evaluation Security Facility) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognized standards. The results of these evaluations are certified by Qatar Common Criteria Scheme Unit, a unit established within Compliance and Data Protection (CDP) Department, MoTC.

By awarding a Common Criteria certificate, the QCCS CB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation; Certificate ID: QCCS-CERT-C001-001-2021, and the Security Target (Ref [5]). The certification report, Certificate of product evaluation and security target are posted on the CDP Department website at and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement) subject to being authorized member of CCRA.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

DISCLAIMER / LEGAL RIGHTS

Compliance and Data Protection (CDP) Department of Ministry of Transport and Communications (MOTC) has designed and created this publication, titled “C001 Certification Report” - v2.0 - Public, product name DERMALOG Fingerprint PAD Kit LF10, Part No. 8004-0009-00, DermalogBPLF10Plugin: 1.7.2.2126, DermalogFakeFingerDetectionLF10Plugin: 1.4.0.2125, DermalogFourprintSegmentation2: 1.18.1.2126, DermalogAuditLogger: 1.1.3.1827, as the outcome of evaluation and certification under the Qatar Common Criteria Scheme Certification Body.

CDP is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge MOTC and CDP as the source and owner of the “Certification Report”.

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the CDP and MOTC. CDP and MOTC shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from CDP and MOTC shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Qatar Common Criteria Scheme (QCCS) using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (Ref [2]).

This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Qatar Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by MoTC or by any other organization that recognizes or gives effect to this certification report and its associated certificate, and no warranty of the IT product by MoTC or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

LEGAL MANDATE(S)

Article 18 of the Emiri Decree no (4) for the Year 2016 setting the mandate of Ministry of Transport and Communications (hereinafter referred to as “MOTC”) provides that MOTC has the authority to regulate and develop the sector of Information and Communications Technology in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual’s life and community and build knowledge-based society and digital economy.

Based on Cabinet decision (26) for the year 2018, the Compliance & Data Protection Department (herein referred to as CPD) is entrusted by the Ministry of Transport and Communications (MOTC) as the competent authority, responsible for determining, in the public interest, the technical competence and integrity of organizations such as those offering assessments, testing and compliance services and the Issuance of Certifications those seeking certificates of compliance within the State of Qatar.

This Report has been prepared to take into consideration the current applicable laws of the State of Qatar. If a conflict arises between this document and the laws of Qatar, the latter shall take precedence. Any such term shall, to that extent be omitted from this Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments, in that case, shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

Executive Summary

DERMALOG Fingerprint PAD Kit LF10 from DERMALOG Identification Systems GmbH is the Target of Evaluation (TOE), claiming strict conformance to the security assurance requirements stated in section 7.2 of *Fingerprint Spoof Detection Protection Profile based on Organizational Security Policies FSDPP_OSP v1.7* (Ref [7]).

The TOE is capable of classifying whether a finger that is presented to the sensor of the TOE, is actually a real finger presented by a genuine user (in a so-called Bona Fide attempt) or whether an artefact is presented (a so-called artefact presentation or presentation attack).

The TOE does not comprise any functionality for biometric recognition or enrolment. The functionality for Presentation Attack Detection works without any enrolment functionality and biometric functionality – such as enrolment, verification and identification – is out of scope for this evaluation.

The DERMALOG Fingerprint PAD Kit LF10 consisting of:

- fingerprint sensor (Part No. 8004-0009-00)
- software -
 - DermalogBPLF10Plugin: 1.7.2.2126,
 - DermalogFakeFingerDetectionLF10Plugin: 1.4.0.2125,
 - DermalogFourprintSegmentation2: 1.18.1.2126
 - DermalogAuditLogger: 1.1.3.1827

The TOE provides the following main security functionality:

- Presentation Attack Detection
- Security Audit
- Security Management
- Residual Information Protection

The evaluation was performed by TÜV Informationstechnik GmbH - Evaluation Body for IT Security and completed by Evaluation Technical Report (Ref [6]) submission on 16th September 2021.

This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Qatar Common Criteria Scheme requirements (Ref [4])

The Qatar Common Criteria Certification Body (QCCS CB) declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates (Ref [1]).

It is the responsibility of user to ensure that the TOE meet their requirements. It is recommended that a potential user of the TOE to refer to the Security Target (Ref [5]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

1	Introduction	10
1.1	TOE Description	10
1.2	TOE Identification	11
1.3	Security Policy	13
1.4	TOE Architecture	13
1.4.1	Logical and Physical Boundaries	14
1.5	Assumptions and Clarification of Scope	14
1.6	Evaluated Configuration	15
1.7	Delivery Procedures	15
1.8	Documentation	15
2	Evaluation	16
2.1	Evaluation Analysis Activities	16
2.1.1	Life-cycle support	16
2.1.2	Development	16
2.1.3	Guidance documents	17
2.1.4	IT Product Testing	17
3	Result of the Evaluation	18
3.1	Assurance Level Information	19
3.2	Recommendation	19
4	References	20
5	Terms and abbreviations	21
5.1	Terms	21
5.2	Abbreviations	23
6	Template History	24
7	Document Change Log	24

1 Introduction

1.1 TOE Description

Biometric systems that work based on fingerprints are often subject to a well-known and easy kind of attack: Attackers can use artefacts (e.g.; fingers built out of gummy or silicone, also known as spoofs) that carry the characteristics of a known user in order to get recognized by a biometric system. As an alternative, a user of a biometric system may use artefacts in order to disguise their identity.

The Target of Evaluation (TOE) is DERMALOG Fingerprint PAD Kit LF10 consisting of hardware and software stated in section 1.2, Table 2 of this document.

The DERMALOG Fingerprint PAD Kit LF10 is a fingerprint sensor (plus its related software and guidance documentation) which provides a countermeasure against the aforementioned attacks. It is capable of classifying whether a finger that is presented to the sensor of the TOE, is actually a real finger presented by a genuine user (in a so-called Bona Fide attempt) or whether an artefact is presented (a so-called artefact presentation or presentation attack).

The TOE provides the following main security functionality:

- **SF.PAD:** Presentation Attack Detection (FPT.SPOD): The TOE can be used to determine whether a fingerprint that is presented to the sensor of the TOE is genuine or an artefact.
- **SF.AUDIT:** Logging (i.e.; audit) (FAU.GEN.1): The TOE supports logging on different log levels. Log levels are: ERROR, INFO, WARNING, VERBOSE and DEBUG. Each level of audit has a dedicated set of events that are associated with that level. The levels are ordered as follows: ERROR, WARNING, INFO, VERBOSE, DEBUG. Higher levels of audit include all events of the lower levels. Please note that the level ERROR and WARNING will not log the required information that are defined in the [PP] and must therefore not be used for the certified version.
- **SF.SM:** Management (FMT_SMF.1 and FMT_MTD.3): The TOE provides security management functionality to manage its core functionality.
- **SF.RIP:** Residual Information Protection (FDP_RIP.2): The TOE ensures that the content of all memory is securely deleted before the memory is released.

For more information on security functionality and the method of use of the TOE refer to the Security Target (Ref [5]), section 7.

The functional concept of the TOE bases on an optical sensor device combined with a dedicated set of algorithms implemented in software. The TOE is able to record images of up to four fingerprints that are presented to the sensor at the same time.

The TOE in general supports multiple modes to acquire fingerprints. In this context, specifically the plain mode can be distinguished from the rolled mode. The actual mode that is used by the TOE is determined by the API call.

It is important to note that the mode for rolled fingerprints has been developed with a supervised scenario in mind. For this reason, this mode is not enforcing Presentation Attack Detection and must not be used in the context of the certified configuration.

The optical sensor of the TOE utilizes a multi-phase illumination that bases on a set of diodes. When a finger or an artefact is placed on the sensor device, it is not only illuminated and captured using the standard wavelength that a fingerprint sensor would normally use but is additionally exposed to a range of visible and invisible illumination.

This way, the sensor part of the TOE produces a set of typical images of the fingerprint or artefact. These images are then processed by the software part of the TOE to decide whether the sensor has actually been presented with a genuine fingerprint or an artefact.

The TOE comprises components as stated in the TOE Architecture section 1.4 of this document.

The assets to be protected by the TOE are defined in the Security Target (Ref [5]), section 4.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions and Organizational Security Policies. This is outlined in the Security Target (Ref [5]), chapter 4.3 and 4.5.

1.2 TOE Identification

The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Certification Scheme	Qatar Common Criteria Scheme
Project Identifier	C001
TOE Name	DERMALOG Fingerprint PAD Kit LF10
TOE Version	Part No. 8004-0009-00, DermalogBPLF10Plugin: 1.7.2.2126, DermalogFakeFingerDetectionLF10Plugin: 1.4.0.2125, DermalogFourprintSegmentation2 1.18.1.2126, DermalogAuditLogger: 1.1.3.1827

Security Target Title	DERMALOG Fingerprint PAD Kit LF10 - Security Target
Security Target Version	3.6
Security Target Date	31 st August 2021
Assurance Level	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
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP), Version 1.7, 27 November 2009, BSI-CC-PP-0062-2010 (Ref [7])
Common Criteria Conformance	PP conformant Common Criteria Part 2 extended
Sponsor and Developer	DERMALOG Identification Systems GmbH Mittelweg 120, 20148 Hamburg, Germany
Evaluation Facility	TÜV Informationstechnik GmbH – Evaluation Body for IT Security Langemarckstr. 20, 45141 Essen, Germany

Table 2: Deliverables of the TOE

No	Type	Identifier	Release/Version	Form of Delivery
1	Hardware	LF10 hardware	Part No. 8004-0009-00	Parcel Mail
2	Software	DermalogBPLF10Plugin	1.7.2.2126	Download from support portal (Ref [11])
3	Software	DermalogFakeFingerDetectionLF10Plugin	1.4.0.2125	
4	Software	DermalogFourprintSegmentation2	1.18.1.2126	
5	Software	DermalogAuditLogger	1.1.3.1827	
6	Document	DERMALOG Fingerprint Scanner LF10 User Guide (Ref a))		
7	Document	DERMALOG Guidance Addendum DERMALOG Fingerprint PAD Kit LF10 (Ref b))		
8	Document	DermalogBPLF10Plugin (Ref c))		

In order to verify the integrity of the software, the administrator has to ensure

- that the download of the installer for the SDK is only obtained via the support portal and via a secure https connection,
- that the digital signature of the installer and the PDF documents is valid.

The TOE offers a function that allows checking the version information of the TOE components. This function is called FFDGetVersionA and its use can be learned from the sample application that is distributed with the TOE software.

The sensor component carries version information on the sticker on its backside. It is important that this version information (in form of the Part No.) is checked to match the value listed in Table 1, section 1.2 of this document.

1.3 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.

1.4 TOE Architecture

The TOE consists of four subsystems identified as follows:

- Scanner control API,
- Supportive API,
- Presentation attack detection API,
- Scanner

All sub-systems have been declared as SFR-enforcing sub-systems and together implement the TOE Security Functionality.

Scanner Control API: The scanner Control API forms the complete software interface and offers all functionality of the TOE to the application that utilizes the services of the TOE.

Supportive API: The supportive API supports the other subsystems but does not implement any functionality completely. This subsystem writes audit data into the log file.

Presentation Attack Detection API: The presentation attack detection API implements the presentation attack detection. The subsystem analyses images of fingerprints and returns information on how likely these images show a presentation attack.

Scanner: The subsystem scanner consists of all hardware of the TOE.

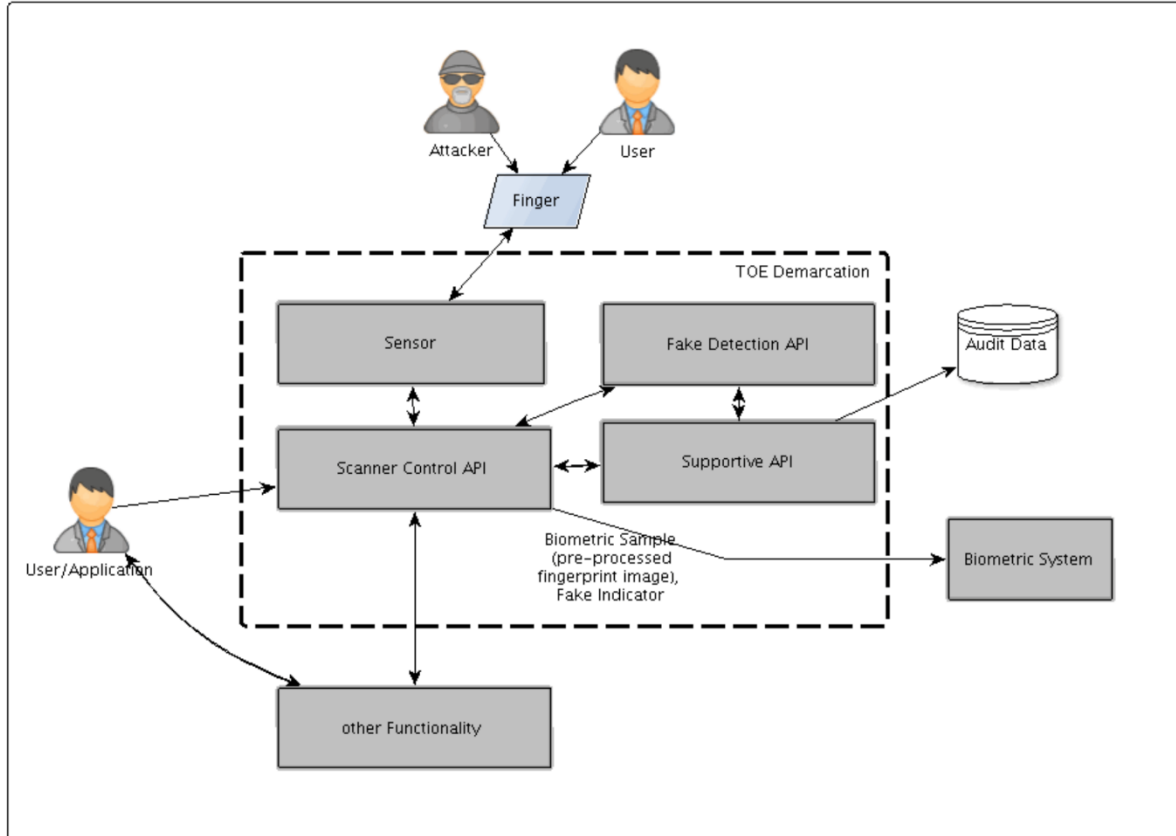


Figure 1: TOE demarcation and major components

1.4.1 Logical and Physical Boundaries

The logical and physical boundaries of the TOE can be defined by the functionality it provides and the sensor part of the TOE as stated in Security Target (Ref [5]) section 2.5.3 and 2.5.4.

1.5 Assumptions and Clarification of Scope

This section summarizes the security aspects of the environment/configuration in which IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the TOE which has defined in the Security Target (Ref [5]).

The Assumptions defined in the Security Target and some aspects of Organizational 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:

- a) The TOE shall be integrated into the overall application/biometric system in a way that the functionality of the TOE is invoked every time that the biometric system is used. Additionally, all kinds of attacks (except Presentation Attacks) against the biometric system that is protected by the TOE have to be countered by other means.
- b) The TOE and its components have to be physically protected against unauthorized access or modification in a controlled office environment.
- c) The administrator shall be well trained and non-hostile.
- d) The administrator shall take responsibility to ensure that the platform provides functionality required by the security objective.

1.6 Evaluated Configuration

This certification covers only one configuration of the TOE. It consists of the Hardware and Software parts as indicated in section 1.2 of this document. Furthermore, the TOE has to be operated using FFD_Mode 0 and FFD_Threshold 50. As described in the guidance documentation (Ref [9]), the plain finger mode has to be used.

1.7 Delivery Procedures

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 and the software. The integrity check of the software and documentation is performed using digital signatures of the SDK and the documents itself, while the integrity check of the hardware 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.

1.8 Documentation

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

- a) DERMALOG Fingerprint Scanner LF10 User Guide, version 3.9, 27th June 2021 - DERMALOG-Fingerprint-Scanner-LF10-User-Guide-Version-3.9.signed.pdf

- b) DERMALOG Guidance Addendum DERMALOG Fingerprint PAD Kit LF10, version 2.5, 11th August 2021 - DERMALOG_AGD_ADD_LF10_V2.5.signed.pdf
- c) DermalogBPLF10Plugin.chm (SHA-256: 702F 0A0C 834A 39B8 29B5 71BA 6C4D AF00 9A88 DE97 9457 1D9A DB6F 48B9 E467 A67D) as part of the software installers in support portal <https://support.dermalog.com>

2 Evaluation

The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level stated in section 1.2 of this document. The evaluation body have performed the evaluation steps following to the scheme requirement (Ref [4]).

2.1 Evaluation Analysis Activities

The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).

The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

2.1.3 Guidance documents

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

All developer tests in the context of the evaluation were conducted using the final version of the TOE. The TOE has been configured using mode 0 (FFD_Mode 0) and PAD threshold of 50 (FFD_Threshold 50) 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 (Ref [10]). In total, the developer created 145 fake artefacts and applied each artefact at least 20 times to the TOE. The test results showed that no faked finger was detected as a real finger in any attempt.

In overall, 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

2.1.4.1 Independent Functional Testing

All evaluator tests in the context of the evaluation were conducted using the final version of the TOE. The TOE was configured using mode 0 (FFD_Mode 0) and PAD threshold of 50 (FFD_Threshold 50) 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. Such approach had been chosen 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 63 fake artefacts of various materials according to the requirements of the Toolbox documentation (Ref [10]). The evaluator carried out more than 1500 attempts to spoof the TOE with these artefacts.

All tests were passed successfully.

2.1.4.2 Penetration Testing

No penetration tests have been formed since no AVA_VAN component is part of the evaluation.

2.1.4.3 Testing Results

Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. The TOE passed all developer and evaluation body tests.

3 Result of the Evaluation

After due consideration during the oversight of the execution of the evaluation and submission of the Evaluation Technical Report (Ref [6]), the Qatar Common Criteria Scheme Certification Body (QCCS CB) certifies the evaluation of DERMALOG Fingerprint PAD Kit LF10 performed by TÜV Informationstechnik GmbH – Evaluation Body for IT Security (TÜViT).

The EB, found that the TOE upholds the claims made in the Security Target (Ref [5]) and supporting documentations, and has met the requirements of the Common Criteria (CC) assurance level as stated in Table 1, section 1.2 of this document.

Certification does not guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

The TOE claims to be conformant to an assurance package based on EAL 2 augmented with ALC_FLR.1 (flaw-remediation) but without AVA_VAN.2 (vulnerability analysis). All of the SARs in Security Target (Ref [5]), section 7.2 have been found taken directly from FSDPP (Ref [7]) section 7.2 without any modifications.

The assurance level also provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behavior.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, however without penetration test have been done since no AVA_VAN component is part of the evaluation.

The assurance level also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

As outlined in Table 2, section 1.2 contains 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/her system risk management process. In order for the evolution of attack methods and techniques to be covered, the period of time until a re-assessment of the TOE is required should be defined 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 recertification. 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.

4 References

All CB references are listed in [CB-2-LST-DocRefList] Documentation Control Reference List.

- [1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014 – Ratified September 8, 2014.
- [2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
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
- [3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
- [4] QCCS CB Scheme Certification Procedure [CB-4-PCD-QCCS], v1.0, August 2020.
- [5] Fingerprint PAD Kit LF10 – Security Target, Version 3.6, 31 August 2021 - DERMALOG_SecurityTarget_LF10_V3.6.signed.pdf
- [6] Evaluation Technical Report Summary, Version 2, 16 September 2021 - C001_ETR_210916_v2.pdf
- [7] Fingerprint Spoof Detection Protection Profile based on Organizational Security Policies (FSDPP_OSP), Version 1.7, 27 November 2009, BSI-CC-PP-0062-2010
- [8] Fingerprint Spoof Detection Evaluation Guidance, Version 2.1, 18 December 2009
- [9] Fingerprint PAD Kit LF10 - Guidance Addendum, version 2.5, 11 August 2021 - DERMALOG_AGD_ADD_LF10_V2.5.signed.pdf
- [10] Toolbox022017, February 2017, BSI - Toolbox020217.xlsx
- [11] DERMALOG Support Portal: <https://support.dermalog.com>

5 Terms and abbreviations

The current manual uses terms as defined in ISO/IEC17065 and CCRA (Ref [1]).

5.1 Terms

Table 3: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An interpretation of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out certification and for overseeing the day-to-day operation of an Evaluation and Certification Scheme . Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and ISO/IEC 17065
Evaluation and Certification Scheme	The systematic organisation of the functions of evaluation and certification under the authority of a certification body in order to ensure that high standards of competence and impartiality are maintained, and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a national interpretation or a CC international interpretation .
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.

Term	Definition and Source
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the QCCS Scheme.
National Interpretation	An interpretation of the CC, CEM or QCCS Scheme rules that is applicable within the QCCS Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the QCCS Scheme. The sponsor may also be the developer.
Artefact	Artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns
Fake	Synonym for artefact
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.
Spoof Detection	Synonym for presentation attack detection
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.

5.2 Abbreviations

Acronym	Expanded Term
API	Application Programming Interface
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
EAL	Evaluation Assurance Level
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
QCCS	Qatar Common Criteria Scheme
ITSEF	Information Technology Security Evaluation Facility
EB	Evaluation Body (same function as ITSEF)
PAD	Presentation Attack Detection
PP	Protection Profile
SAR	Security Assurance Requirement
SDK	Software Development Kit
SFR	Security Functional Requirement
ST	Security Target
OSP	Organizational Security Policy
TOE	Target of Evaluation
ETR	Evaluation Technical Report
TSF	TOE Security Functionality
TSFI	TSF Interface

6 Template History

Version	Date	Comments	Author
1.0	2020/09/05	New - document template	MoTC

7 Document Change Log

Release	Date	Comments	Pages Affected
1.0	2021/09/15	Initial draft of certification report	All
2.0	2021/09/22	Applied amendment based on EB and QM review	3,4,6,7,10,12-14, 18,19,20

End of Document