DERMALOG

Security Target DERMALOG Fingerprint PAD Kit LF10

DERMALOG Identification Systems Contact Details
www.dermalog.de
Corporate Headquarter
DERMALOG Identification Systems GmbH,
Mittelweg 120
20148 Hamburg Germany
Tel: +49 (0) 40 41 32 27 0
Fax: +49 (0) 40 41 32 27 89
info@dermalog.de

1 ST Introduction

1.1 Introduction

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 DERMALOG Fingerprint PAD Kit LF10 – the TOE described in this Security Target – provides a countermeasure against those 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 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.

This Security Target has been developed based on and it claims strict conformance to the requirements from the

> *Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies FSDPP_OSP v1.7 ([PP]).*

Please note that [PP] and other documents often mix the terms "presentation attack detection" and "spoof detection". While all other documents in the course of this evaluation, refer to the term "presentation attack detection" (which is state of the art), the use of the term "spoof" could not be avoided for this Security Target as this term is heavily used in the underlying Protection Profile. It is important to mention that both terms are used as synonyms in this document.

1.2 ST Reference

Title	Security Target DERMALOG Fingerprint PAD Kit LF10
Version	2.7
Date	26.02.2020
Certification-ID	BSI-DSZ-CC-1042
Author	Manuela Tiedemann, DERMALOG GmbH, Nils Tekampe, konfidas GmbH

Table 1: ST Reference

1.3 TOE Reference

TOE name	DERMALOG Fingerprint PAD Kit LF10
Hardware Version LF10	Part No. 8004-0009-00
Software Version	• DermalogBPLF10Plugin: 1.3.8.1935 • DermalogFakeFingerDetectionLF10Plugin: 1.3.3.1925 • DermalogFourprintSegmentation2 1.14.0.1919 • DermalogAuditLogger: 1.1.3.1827

Guidance Documents	• DERMALOG Guidance Addendum Dermalog Fingerprint PAD Kit LF10, Version 1.9 (as a PDF document) • DermalogBPLF10Plugin.chm. This file with some additional information is installed by the installer into the path %PROGRAMFILES%\DERMALOG\MultiScannerSDK CommonCriteria 11.0\doc\DermalogBPLF10Plugin\ DermalogBPLF10Plugin .chm[1] (SHA-256: 0B40999446BEBF78AD5FC5B2AD09081CCCA3856390FD6E9CF2 3D44BD287DB240) • DERMALOG Fingerprint Scanner LF10 User Guide, Version 3.3 (as a PDF document)

Table 2: TOE Reference

1.4 TOE Overview

Biometric systems that work based on fingerprints are often subject to a well-known and easy kind of attack: Attackers can use artefact fingerprints (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 TOE described in this Security Target is the DERMALOG Fingerprint PAD Kit LF10. The DERMALOG Fingerprint PAD Kit LF10 is a fingerprint sensor (plus its related software and guidance documentation) and 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:

- **Presentation Attack Detection:** The TOE can be used to determine whether a fingerprint that is presented to the sensor of the TOE is genuine or an artefact.
- **Logging (i.e. audit)**: 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.
- **Management:** The TOE provides management functionality to manage its core functionality.
- **Residual Information Protection:** The TOE ensures that the content of all memory is securely deleted before the memory is released.

For more information on the security functionality and the method of use of the TOE, please refer to chapter 7.

Summarizing, the TOE comprises the complete sensor device, its firmware, the software that is implementing the presentation attack detection and other security functions and its related guidance documentation.

[1] Please note that this description assumes that the 32bit version of the TOE is used if the Operating System is a 32bit version and the 64bit version of the TOE is used if the OS is in 64bit. In the case that the 32bit version of the TOE would be installed under a 64bit OS, the %PROGRAMFILES%\ system variable would resolve to the wrong folder.

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. Further, the TOE does not comprise the PC nor the Operating System that is used to operate the software part of the TOE. For more information on the structure of the TOE and its boundaries, please refer to chapter 1.5.

1.5 TOE DESCRIPTION

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.

It shall be noted that 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.

1.5.1 Components of the TOE

The following figure visualizes the TOE demarcation and shows the major components of the TOE.

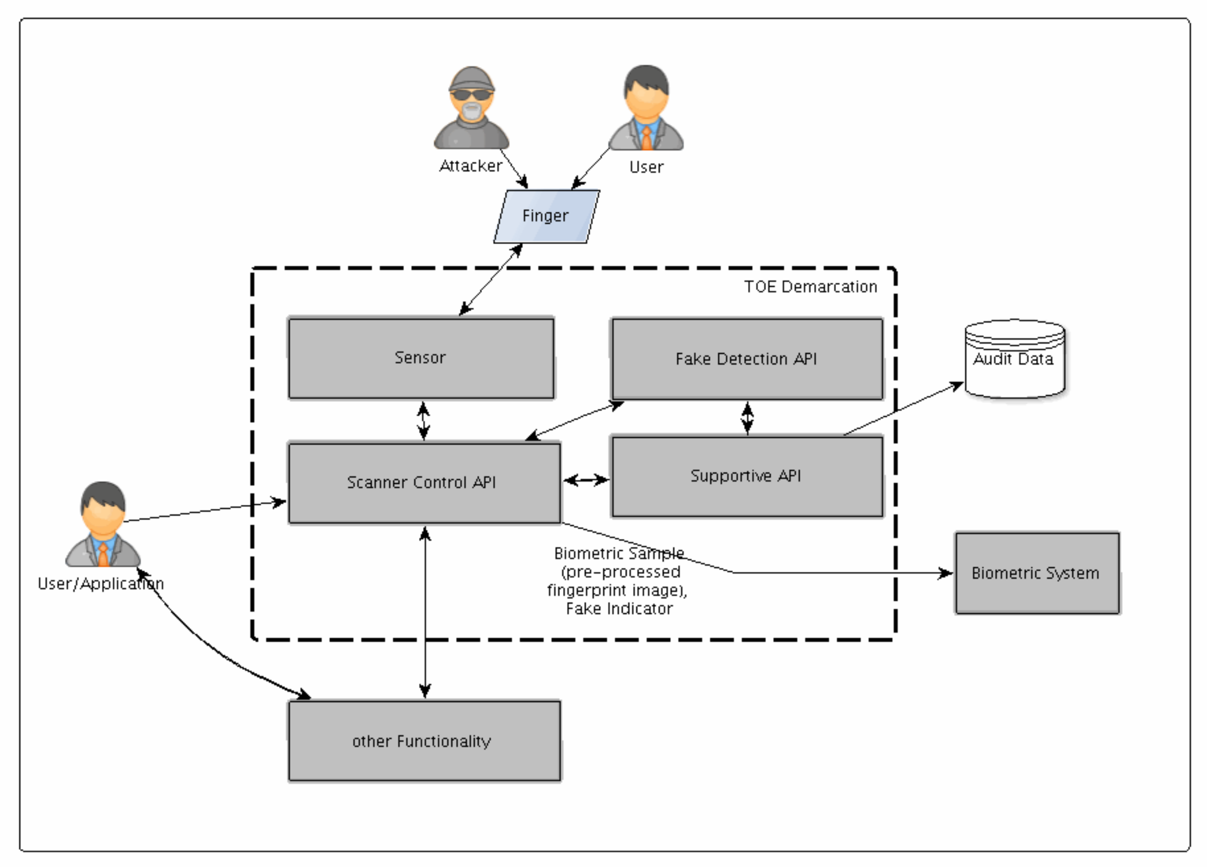


FIGURE 1: TOE DEMARCATION AND MAJOR COMPONENTS

In detail, the TOE comprises the following components:

Name	Type	Description
Sensor	Hardware	The LF10 capture device for producing the image of one or multiple fingerprints and images using reflexive light at different wave lengths for spoof detection. The sensor is connected to a host system via USB 2.0 interface.
Scanner Control API	Software	The Scanner Control API implements all functionality that invokes sensor communication.
Supportive API	Software	The supportive API comprises functionality that is relevant but not in the primary focus. This includes segmentation functions for the four-finger sensor and logging functionality.
FakeDetection API	Software	A set of DLLs written in Visual C++ that implement the core functionality of the TOE. Specifically, the presentation attack detection functionality is implemented in these DLL.

Guidance Documentation	Guidance Documentation for the TOE.

Table 3: TOE components

It should be noted that the DERMALOG product platform comprises significantly more functionality and components than the pure TOE (denoted by the box "other functionality" in Figure 1) and that a user would usually interact with the TOE via other parts of the product platform.

The delivery of the hardware of the TOE is performed in a secure delivery process to the customer. The certified software is exclusively distributed via the DERMALOG support portal that can be reached under https://support.dermalog.com/. Customer support will supply each customer with dedicated login credentials that allow a secure download of the software parts of the TOE and its guidance documentation.

Please note that the installer for the TOE and its guidance documents carry a digital signature that allow a verification of the authenticity before the actual installation. The signature is created by the use of a certificate that has been issued to DERMALOG by a trustworthy Certification Authority.

1.5.2 Minimum System Requirements

The following table identifies the Minimum System Requirements for the operation of the TOE

CPU	Intel Core i3 (2nd Gen) / 2 GHz core
System Memory	512 MB
Free Disk Space	approx. 200 MB
Operating System	Windows 7 or later
Interfaces	USB 2.0 high-speed, data rate approx. 24 MB/s

Table 4: Minimum system requirements

The hardware part of the TOE needs certain environmental conditions in order to work properly. The following tables provide more specific information:

The following table describes device specifications for the LF10 sensor device and its operational conditions.

Light source	Near-infrared, red and green light-emitting diodes (LEDs)
Operating temperature	0 °C to +50 °C (32 °F to 122 °F)
Humidity range	humidity 5 – 95 % non-condensing

Table 4.2: Device Specifications LF10

The following chapters introduce the logical and physical scope of the TOE in more detail.

1.5.3 Logical Boundary

The logical boundaries of the TOE can be defined by the functionality that it provides:

- **Presentation Attack detection:** the TOE detects whether a presented fingerprint is an artefact or genuine. The result of this operation is passed on to the user (which itself is usually an application) so that it can be considered during the rest of the biometric process.

- **Management:** the TOE provides functionality to manage its relevant parameters.
- **Residual Information Protection:** in order to prevent the leakage of information the TOE deletes relevant information if not longer in use and before releasing any memory.
- **Logging (i.e. audit):** the TOE produces audit events for security relevant events and writes audit logs to a file.

The following functionalities on the other hand have to be provided by the environment to support the secure operation of the TOE:

- **Access control:** the environment provides access control for the presentation attack detection parameters, and any software parts of the TOE. To perform access control, the environment maintains roles for an user and an administrator and ensures their identification and authentication.
- **Transmission / Storage:** the environment provides a secure communication and storage for data where security relevant data is transferred to or from the TOE.
- **Auditing**: the environment may provide additional audit functionalities. In any case, it provides reliable time stamps for logging, storage for the audit logs that are produced by the TOE and mechanisms for review of audit logs.

1.5.4 Physical Boundary

The TOE physical boundary can be readily defined for the sensor part of the TOE. The following figures show the sensor device of the TOE (i.e. the LF10) and its physical dimensions:

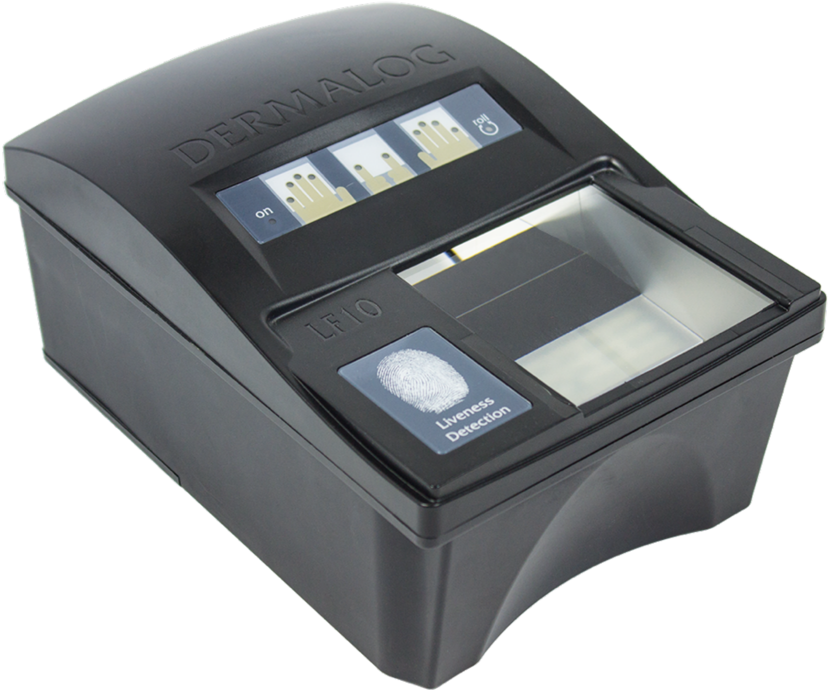


Figure 2: LF10 sensor device

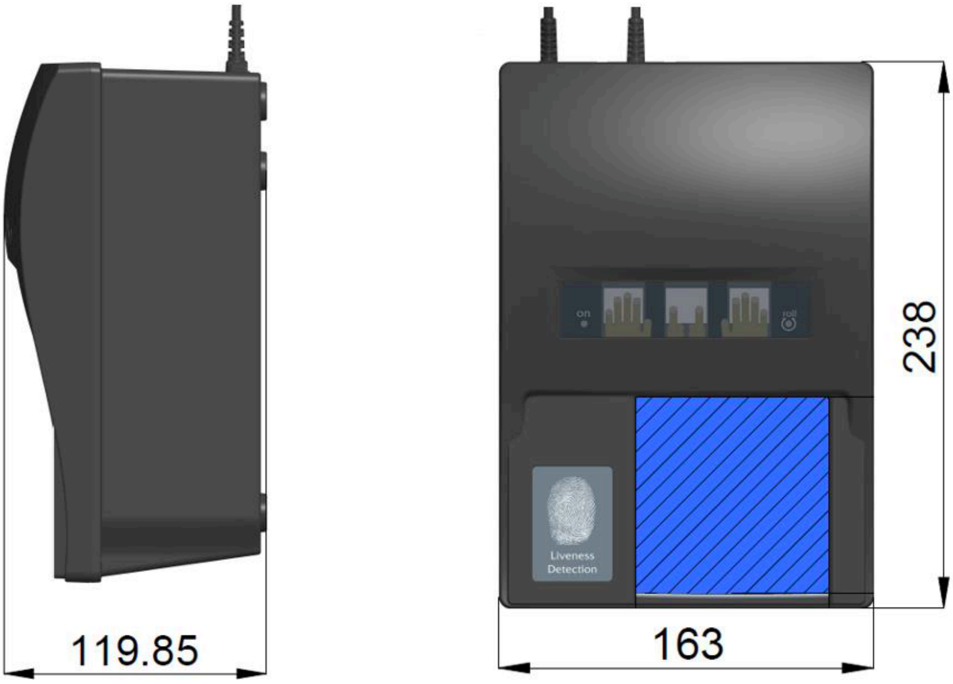


Figure 3: Physical dimensions of the LF10 (I)

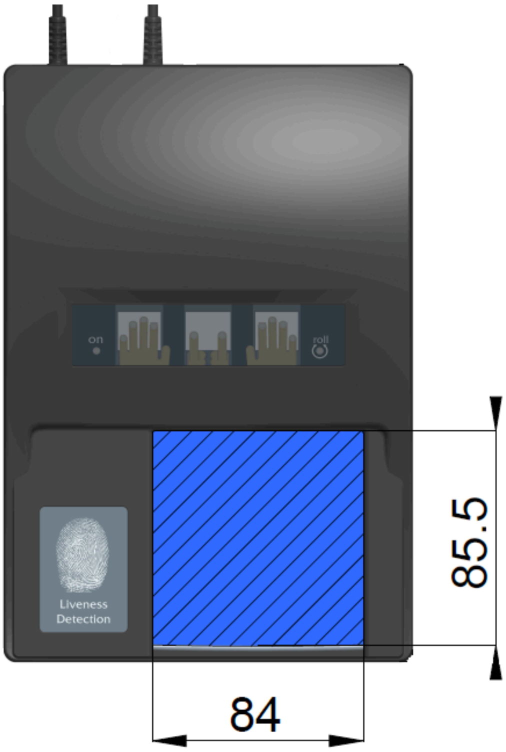


Figure 4: Physical dimensions of the LF10 (II)

The sensor device is connected to a host PC via a USB 2.0 cable following the [USB2.0] specification. This cable is also part of the TOE.

On the PC side, the TOE only comprises software as outlined in the previous chapters. Thus, it does not have any physical boundary.

In addition to the components that have been mentioned in the paragraphs before, the guidance documentation is also considered being part of the TOE.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target (ST) and the TOE claim conformance to Common Criteria version v3.1, Revision 5 Part 1 [CCPart1], Part 2 [CCPart2] and Part 3 [CCPart3].

Conformance of this ST is claimed for:

- **Common Criteria part 2 extended and**
- **Common Criteria part 3 conformant.**

2.2 PP Claim

This ST claims strict conformance to [PP].

2.3 Package Claim

This ST claims to be compliant to the assurance package as defined in [PP].

2.4 Conformance Rationale

The TOE as described in this ST is a product that allows spoof detection for fingerprints. It therewith falls directly into the classes of TOEs that are defined by [PP].

In chapter 1.2 [PP] states:

The scope of this Protection Profile is to describe the functionality of a biometric spoof detection system in terms of [CC] and to define functional and assurance requirements for the evaluation of such systems. Chapter 2 gives a more detailed overview about the design of the TOE and its boundaries.

In chapter 1.4 this ST describes:

The DERMALOG Fingerprint PAD Kit LF10 is a fingerprint sensor (plus its related software and guidance documentation) and 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). Correspondence should therewith be obvious.

[PP] requires strict conformance which is claimed by this Security Target.

3 Security Problem Definition

The SPD as defined in this chapter has been reproduced from [PP] for a better readability. No changes have been made to the text from [PP].

3.1 External entities

The following external entities interact with the TOE:

Entity	Description
TOE administrator:	The TOE administrator is authorized to perform administrative TOE operations and able to use the administrative functions of the TOE. The administrator is also responsible for the installation and maintenance of the TOE. Depending on the concrete implementation of a TOE there may be more than one administrator and consequently also more than one administrative role.
User:	A person who uses a biometric system that is protected by the TOE to get enrolled, identified or verified and is therefore checked by the biometric spoof detection system.

Table 5: external entities

3.2 Assets

The following assets are defined in the context of this Protection Profile.

Asset	Description
Primary assets:	The primary assets do not belong to the TOE itself. The primary scope of the biometric spoof detection system is the protection of the biometric system behind it. As such any asset that is protected by the biometric system can be considered being a primary asset for the TOE. Formally, the decision that is taken by the TOE (fake/no fake) can be considered being the primary asset.
Secondary assets:	Secondary assets (i.e. TSF data) are information which are used by the TOE to provide its core services and which consequently will need to be protected. The following assets should be explicitly mentioned for the TOE: • **Spoof detection parameters (SDP)**: These (configuration) data include the settings necessary to detect a spoofed biometric characteristic, e. g., temperature limits, general threshold settings, typical movement patterns. These parameters may be specific for a claimed identity. The parameters are partly produced during development of the TOE but may be adjusted during installation, maintenance and enrollment. The integrity and confidentiality of these parameters will have to be protected. • **Spoofing evidence (SE):** This data is acquired by the capture device and/or separated dedicated sensor devices for the purpose of spoof detection. The TOE decides about a finger being a fake or not based on this data. The integrity and confidentiality of this data have to be protected.

	• **Log data (AD):** This data comprises the audit information that is generated by the TOE. The integrity, confidentiality and authenticity of the information has to be protected.

Table 6: Assets

3.3 Assumptions

Assumption	Description
A.BIO	The spoof detection system addressed in this Protection Profile is a protection mechanism against spoofing attacks. The biometric system that is protected by the TOE therefore ensures that all threats that are not related to spoof detection are appropriately handled. Further, the biometric system ensures that the functionality of the TOE is invoked/used in order to protected the biometric system against spoof attacks. It is also assumed that the fingerprint sample that is acquired by the capture devices belongs to the fingerprint that is used for spoof detection.

Table 7: Assumption

3.4 Threats

No threats have been defined in the Security Problem Definition of this PP[2] as it is solely based on organizational security policies.

[2] Strictly speaking this would mean “ST” instead of “PP” but the text from [PP] has been taken without any change.

3.5 Organizational Security Policies

OSP	Description
OSP.SPOOF_DETECTION	The TOE shall be able to detect whether a presented fingerprint is spoofed or genuine. The spoof detection shall be adequate to detect all artificial biometric characteristics listed and described in [Toolbox].
OSP.RESIDUAL	The TOE shall ensure that no residual or unprotected security relevant data remain in memory after operations are completed.
OSP.MANAGEMENT	The TOE shall provide the necessary management functionality for the modification of security relevant parameters for TOE administrators. Only secure values shall be used for such parameters.
OSP.AUDIT	In order to • generate statistics that can be used to adjust the parameters for better quality (maintenance), • trace modification, and • trace possible attacks, the TOE shall record security-relevant events.

Table 8: OSP

4 Security Objectives

The chapters containing the security objectives for the TOE and the environment have been reproduced from [PP] for a better readability. No changes have been made to the text from [PP].

4.1 Security Objectives for the TOE

Objective	Description
O.SPOOF_DETECTION	The TOE shall be able to detect whether a presented fingerprint is spoofed or genuine. The spoofing evidence may be extracted from the data provided by the same sensor that is used to acquire the biometric characteristic for recognition (by the biometric system in the environment), or it may be retrieved using sensors which are solely dedicated to spoof detection.
O.AUDIT	The TOE shall produce audit records at least for the following security relevant events: • A use of the TOE where a faked fingerprint has been detected • A use of the TOE where a genuine fingerprint has been detected • Every use of a management function • All parameters modified by the management functions
O.RESIDUAL	The TOE shall ensure that no residual or unprotected security relevant data remain in memory after operations are completed.
O.MANAGEMENT	The TOE shall provide the necessary management functionality for the modification of security relevant parameters to TOE administrators only.

	As part of this management functionality the TOE shall only accept secure values for security relevant parameters to ensure the correct operation of the TOE.

Table 9: Security Objectives for the TOE

4.2 Security objectives for the operational environment

Objective	Description
OE.ADMINISTRATION	The TOE administrator is well trained and non hostile. They read the guidance documentation carefully, completely understands and applies it. The TOE administrator is responsible for the secure installation and maintenance of the TOE and its platform and oversees the biometric spoof detection system requirements. In particular, the administrator shall ensure that all environmental factors (e. g., lighting, electromagnetic fields) are within an acceptable range with respect to the used capture and sensor devices. The administrator assures that audit records of the TOE are regularly reviewed in order to detect and prevent attacks being performed against the TOE.
OE.PHYSICAL	It shall be ensured that the TOE and its components are physically protected against unauthorized access or modification. Physical access to the hardware that is used by the TOE is only allowed for authorized administrators. This does not have to cover the capture device that has to be accessible for every user.
OE.PLATFORM	The platform the TOE runs on shall provide the TOE with services necessary for its correct operation. Specifically the platform shall • identify and authenticate TOE administrators, • restrict to use the management functions of the TOE in order to query, modify, delete, and clear security parameters which are important for the operation of the TOE to TOE administrators, • provide access control for all secondary assets (spoof detection parameters, spoofing evidence, and audit data) and the software parts of the TOE, • provide a secure communication and storage of information where security relevant data is transferred to or from the TOE, • provide functionality for storage and review of audit information and ensure that only authorized administrators have access to the audit logs, • provide reliable time stamps that can be used by the TOE, and • be free of malware like viruses, trojan horses, and other malicious software.
OE.BIO	The spoof detection system described in this Protection Profile is a protection mechanism which ensures that spoofed fingerprints are rejected by the TOE. The TOE only addresses the detection of spoof attacks.

	The biometric system that is protected by the TOE shall therefore ensure that all threats that are not related to spoof detection are appropriately handled. Further, the biometric system shall ensure that the functionality of the TOE is invoked/used in order to protected the biometric system against spoof attacks.

Table 10: Security Objectives for the operational environment

4.3 Security Objectives rationale

Chapter 5.3 from [PP] applies without any changes.

5 Extended Component Definition

Chapter 6 from [PP] applies without any changes.

6 Security Requirements

6.1 Security Functional Requirements

This chapter contains the Security Functional Requirements (SFR) the TOE complies with. The SFRs have been taken from [PP] and only the allowed operations have been performed. Operations are marked as follows:

- Selection operations (used to select one or more options provided by the [CC] in stating a requirement.) are denoted by underlined text
- *Assignment operation* (used to assign a specific value to an unspecified parameter, such as the length of a password) are denoted by *italicized text*.
- No Refinements have been performed
- No Iterations have been performed.

Operations that have been completed by the ST author (and not yet by the [PP]) are additionally marked by a grey background.

The following table contains an overview of all SFRs that are used in this Security Target.

ID	SFR	Chapter
FAU_GEN.1	Audit Data Generation	6.1.1
FDP_RIP.2	Full Residual Information Protection	6.1.2
FMT_MTD.3	Secure TSF data	6.1.3
FMT_SMF.1	Specification of Management Functions	6.1.4
FPT_SPOD.1	Spoof Detection	6.1.5

Table 11: List of all SFR

6.1.1 Audit data generation (FAU_GEN.1)

ID	SFR
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [basic] level of audit; and c) [*modification of Spoof Detection Parameters, and* *d) [none]*].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*none*].
Hierarchical to:	No other components
Dependencies:	FPT_STM.1

Application Note

According to the chosen level of audit and the SFRs contained in this PP the TOE has to audit the following event per minimum:

- A use of the TOE where a faked fingerprint has been detected (FPT_SPOD.1)
- A use of the TOE where a genuine fingerprint has been detected (FPT_SPOD.1)
- Every use of a management function (FMT_SMF.1)
- All parameters rejected by the management functions (FMT_MTD.3 or FMT_SMF.1[3])

If useful in the context of a concrete technology the ST author should consider to audit additional information (e.g. a score or a claimed identity) together with the first two events.

Hint from the ST author

This application note has been considered during the development if the TOE. The required events are audited. See also Security Function SF.Audit in chapter 7.1.

[3] Please note that the term “or FMT_SMF.1” has been added compared to [PP].

6.1.2 Full residual information protection (FDP_RIP.2)

ID	SFR
FDP_RIP.2	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] all objects.
Hierarchical to:	FDP_RIP.1
Dependencies:	No dependencies

6.1.3 Secure TSF data (FMT_MTD.3)

ID	SFR
FMT_MTD.3.1	The TSF shall ensure that only secure values are accepted for [● *[threshold for spoof detection]* ● *[none[4]]*]
Hierarchical to:	No other components
Dependencies:	FMT_MTD.1

Application Note	The assignment in FMT_MTD.3.1 (list of all spoof detection parameters) represents the minimum of parameters for which the TOE has to ensure secure settings. The objective O.MANAGEMENT however requires that the TOE has to ensure secure values for all security relevant parameters. As the list of those parameters depends on the concrete technology the ST author shall add all security relevant parameters to this assignment.
Hint from the ST author	The parameter that can be managed for the spoof detection functionality of the TOE is the threshold setting that determines which score value an image of the finger has to be met in order to be rated as genuine. As such, these are the only parameters that had to be considered in FMT_MTD.3

[4] „none" has been chosen here in conformance with the text in [PP]

6.1.4 Specification of Management Functions (FMT_SMF.1)

ID	SFR
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [• *Setting the threshold for the spoof detection functionality,*].
Hierarchical to:	No other components
Dependencies:	No dependencies

Application Note The necessary management functions are highly depending on the necessary information for the core functionality as defined in FPT_SPOD.1. The ST author shall consider all relevant parameters and decide whether a management function will be necessary for each.

Hint from the ST author The ST author considered this application note and developed a relevant set of management functionality for the security functionality of the TOE.

6.1.5 Biometric Spoof Detection (FPT_SPOD.1)

ID	SFR
FPT_SPOD.1.1	The TSF shall be able to detect whether a presented [fingerprint] is spoofed or genuine.
FPT_SPOD.1.2	If a spoofed biometric characteristic is detected, the following action(s) shall be performed: • [*the function for spoof detection returns TRUE*]
FPT_SPOD.1.3	If a genuine biometric characteristic is detected, the following action(s) shall be performed: • [*the function for spoof detection returns FALSE*]
FPT_SPOD.1.4	Along with the feedback about spoof status of the presented biometric characteristic the TOE shall deliver the following information: • [*a score value between 0 (artefact) and 100 (genuine) indicating the strength of the decision*]
Hierarchical to:	No other components
Dependencies:	FMT_MTD.3 Secure TSF data FMT_SMF.1 Specification of Management Functions

Application Note [5]

Please note that any use of residual information that remains on a sensor device is considered being a spoofed characteristic in the context of this SFR.

In FPT_SPOD.1.4, the ST author should list all additional information that shall be delivered by the spoof detection functionality to the integrating biometric system. Such information could be an additional score value that represents the likelihood that the presented biometric characteristic is spoofed. However, the ST author should understand that such information is sensitive as an attacker could use it to improve his attacks. Such information shall not be visible to the user of the biometric system.

Hint from the ST author

The ST author considered this application note carefully as the TOE returns a score value along with its decision. However, as the TOE is to be embedded into an application, this does not directly mean that a user and therewith potentially an attacker has access to this information. Instead, it falls into the responsibility of the application to take care of this information. Relevant hints will be provided in the guidance documentation.

[5] Please note that the first paragraph oft he original Application Note from [PP] has been deleted.

6.2 Security Assurance Requirements

The following table identifies the Security Assurance Requirements (SAR) that apply to the TOE. The SAR are taken from [PP] without any modification. Due to the significance of the SAR for the rest of the evaluation process, the SAR are reproduced here instead of being referenced.

Class	SAR	Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic Design
Guidance Documentation	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-cycle-support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.1	Basic flaw remediation
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended component definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample

TABLE 12: LIST OF ALL SAR

6.3 Security Requirements Rationale

Chapter 7.3 from [PP] applies without any modification.

7 TOE Summary Specification

The TOE Summary Specification (TSS) in this Security Target defines a set of Security Functions that describe, how the TOE realizes the functionality as required by the SFRs. Those Security Functions are described in the following paragraphs. Each Security Function is also directly mapped to the Security Functional Requirement it fulfils.

7.1 SF. AUDIT (FAU_GEN.1)

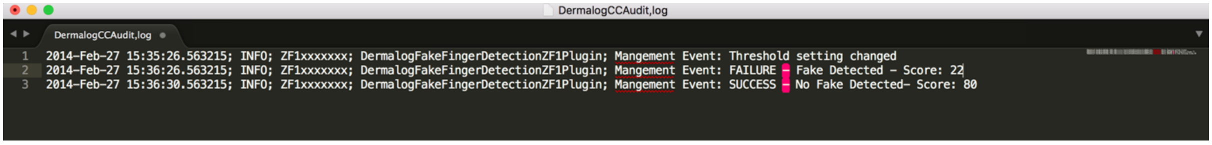
The TOE collects relevant audit information and stores it into a text file on disk. Please note that the TOE refers to this functionality as logging rather as audit (which is the wording used in Common Criteria).

The following events are captured by the TOE:

- Start-up and shutdown of the log functions,
- The result of every analysis whether a finger is an artefact or not,
- The use of every management function,
- All parameters rejected by the management function.

The audit log is stored into a flat file named DermalogCCAudit.log in the operational environment of the TOE. The folder where the log file is stored can be configured via SF.SM (see also chapter 7.3).

The following figure shows the overall structure of log entries in this file:



```
2014-Feb-27 15:35:26.563215; INFO; ZF1xxxxxxx; DermalogFakeFingerDetectionZF1Plugin; Mangement Event: Threshold setting changed
2014-Feb-27 15:36:26.563215; INFO; ZF1xxxxxxx; DermalogFakeFingerDetectionZF1Plugin; Mangement Event: FAILURE - Fake Detected - Score: 22
2014-Feb-27 15:36:30.563215; INFO; ZF1xxxxxxx; DermalogFakeFingerDetectionZF1Plugin; Mangement Event: SUCCESS - No Fake Detected- Score: 80
```

Figure 5: Example of log file

As one can see, the following information are recorded for each event:

- Date and Time of the event,
- the event itself,
- a type of the event (Management Event, Analysis Event),
- the library that caused the event,
- the outcome (SUCCESS or FAILURE) of the event (as part of the event text).

7.2 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.

As the TOE comprises hardware and software parts, the way in which this security function is implemented is diverse for the different kind of memory that the TOE uses.

The hardware of the sensor devices contains memory that is used as a buffer. This buffer stores the image of a fingerprint or a small part of it before the image is transmitted to the PC side of the TOE. The buffer is directly overwritten with the next image (or part of an image) after that so that it is ensured that the previous information is made unavailable. Specifically, the buffer is filled completely or with data of the same size and structure so that no residual information can be remaining. After the last image has been retrieved from the sensor devices, the TOE takes an empty image and transmits it. By the use of this empty image, any previous information that might still resided in the buffer is overwritten.

The software part of the TOE comprises of a set of Windows DLLs that are developed using Visual C++. Within these DLLs each class has a de-constructor that ensures that the content of the class is overwritten before the memory is released. The TOE does not save any temporary files to disc.

7.3 SF.SM: TOE Management (FMT_SMF.1 and FMT_MTD.3)

The management functionality is provided in form of a configuration file named CCConfig.ini that is stored in the folder <Program Files>\Dermalog\ComponentSystem. As an alternative location the configuration file can also be stored at the same location as the binaries of the TOE.

It is implemented as an INI file following the general specification from https://en.wikipedia.org/wiki/INI_file.

The ini file provides the management for the logging functionality of the TOE. The following settings can be made:

1. The type of logging (has to be set to "file" in order to be CC compliant)
2. The path where the audit logs will be stored
3. The threshold setting for Presentation Attack Detection.

The TOE will ensure that only secure values are accepted for the threshold setting that is used for SF.PAD. Specifically, that means that a threshold value will only be accepted if it is between 25 and 75. Please note however that the TOE shall only be operated using a value of 50 for this threshold as the TOE has only been tested at this threshold during certification.

7.4 SF.PAD: Presentation Attack Detection (FPT_SPOD.1)

This Security Function represents the core functionality of the TOE. The DERMALOG Fingerprint PAD Kit is able to distinguish whether a finger that is presented to the sensor device is a real human finger (in this case the attempt is referred to as a Bona Fide Presentation Attempt) or whether a Presentation Attack is carried out in which an artefact is presented to the sensor.

The functional concept of the TOE bases on an optical sensor device combined with a dedicated set of algorithms. 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 functionality of the TOE is contained in the FakeDetection module. This module (which is a Windows DLL) exposes the functionality that is used to determine whether an image that has been taken using the sensor device of the TOE actually shows a genuine finger or an artefact.

The function for presentation attack detection accepts the images of the finger as input and returns the decision, whether the image shows an artefact or not. The function returns TRUE, if an artefact has been detected and FALSE if a bona fide presentation has been detected.

Also, a score value between 0 (artefact) and 100 (genuine finger) is returned.

If multiple fingers are detected by the sensor, the TOE will analyze each finger separately and return the results for each finger. The overall result is set to TRUE (artefact detected) if at least one finger has been found to be an artefact.

The decision that is returned by the function, is calculated by comparing the calculated score value to the threshold. If the score value is less or equal than the threshold, a TRUE is returned (meaning the presented image shows an artefact).

The TOE does not pose any reaction based on the decision; this is left to the calling application.

8 Appendix

8.1 References

ID	Title
[PP]	Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies, FSDPP_OSP, Version 1.7, BSI-CC-PP-0062
[CCPart1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; Version 3.1 Revision 5 April 2017, CCMB-2017-04-001
[CCPart2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements; Version 3.1 Revision 5, April 2017, CCMB-2017-04-002
[CCPart3]	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; Version 3.1 Revision 5, April 2017, CCMB-2017-04-003
[FSDEG]	Fingerprint Spoof Detection Evaluation Guidance, version 2.0 (or a more recent version)
[USB2.0]	USB 2.0 specification, usb.org

8.2 Acronyms and Glossary

ID	Title
CC	Common Criteria
DLL	Dynamic Linked Library
GHz	Gigahertz
IR	Infrared
LED	Light-emitting diode
OEM	Original Equipment Manufacturer
OSP	Organizational Security Policy
PAD	Presentation Attack Detection
PC	Personal Computer
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE security functionality
UV	Ultraviolet