Federal Office
for Information Security

Fingerprint Spoof Detection Protection Profile

based on Organisational Security Policies

FSDPP_OSP

v1.7

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of content

1. PP introduction

1.1 PP Reference

Title:	Fingerprint Spoof Detection Protection Profile based on OSP (FSDPP_OSP)
Version	1.7
Date	November, 27th 2009
Author	Boris Leidner, Nils Tekampe, TÜV Informationstechnik GmbH
Registration	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Certification-ID	BSI-CC-PP-0062
CC-Version	3.1 Revision 3
Keywords	biometric; fingerprint-recognition; Protection Profile; spoof detection

1.2 PP Overview

Biometric systems that work based on fingerprints are often subject to a well known and easy kind of attack: Attackers can use faked fingerprints (e.g. built out of gummy or silicone) 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 a faked finger in order to disguise their identity. Countermeasures against those attacks may be implemented by a set of dedicated hardware and software, the so called biometric spoof detection system.

In order to facilitate new mechanisms for spoof detection in fingerprint recognition systems and thereby advancing innovative technologies in the area of security the project “LifeFinger I” has been initiated by the Federal Office for Information Security. This Protection Profile forms part of this project that has been conducted by the Bundesdruckerei GmbH.

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.

This Protection Profile thereby focuses 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. Therefore, this PP is solely based on organizational security policies and threats are completely omitted. The explicit assurance package for an evaluation without a vulnerability assessment is defined in chapter 3.4.

When planning an evaluation according to this PP the ST author should also consider the Fingerprint Spoof Detection Protection Profile [FSDPP] which is based on threats and not organizational security policies only. In general, the use of the [FSDPP] should be the preferred option.

2. TOE Description

The Target of Evaluation (TOE) described in this PP is a system that provides fingerprint spoof detection either as part of, or in front of a biometric system for fingerprint recognition.

The TOE determines whether a fingerprint presented to the biometric system is genuine or spoofed. The term *spoofed biometric characteristics* hereby refers to artificially created fake fingers which are currently known to circumvent fingerprint recognition systems.

For this purpose the spoof detection system acquires spoofing evidences for a presented fingerprint using a sensor device. This sensor can either be part of the capture device that is used to capture the biometric sample of the fingerprint (or even be identical to it) or be a separate sensor device (or more than one) that is completely dedicated to spoof detection.

Beside the fingerprint spoof detection functionality every TOE that claims conformance to this PP shall implement:

- Management functionality to modify security relevant parameters
- Quality control for management parameters
- Audit functionality for security relevant events
- Protection of residual and security relevant data.

2.1 Protection of biometric systems

Systems claiming compliance to this Protection Profile are developed to protect biometric systems for fingerprint recognition against one specific kind of attacks: The use of well known faked finger(prints). The following paragraphs introduce the core biometric processes of a biometric system in order to improve the understanding of the direct environment of the TOE and to explain the motivation of an attacker.

- **Enrollment:**

  Often, the enrollment process is the first contact of a user with a biometric system. This process is necessary because a biometric system has to be trained in order to verify the identity of each user based on their fingerprint.

  During the enrollment process the system captures the fingerprint image of a user and extracts the features it is working with. These features are then combined with the identity of the user to a biometric reference and stored as template in a database.

  During enrollment an attacker could try to present faked finger(prints) to the capture device in order to get enrolled with another biometric characteristic. When having success the attackers identity would be associated with the fake fingerprint. The important thing to notice in this context is that an attacker must not necessarily have to have any knowledge about the biometric characteristic of another user to perform this attack.

- **Biometric verification:**

  The objective of a verification process is to verify or refuse the claimed identity of a user based on their fingerprint. Therefore the user has to claim an identity to the system. The system retrieves the fingerprint reference record associated with this identity from the database and captures the live fingerprint. If the fingerprint features that are extracted from the live fingerprint image and the fingerprint reference from the database are similar enough, the claimed identity of the user is considered to be verified.

  During biometric verification an attacker could try to use a faked finger to get recognized by the system as another user (this kind of attack is often referred to as impersonation). For such an attack however, the attacker will have to know about the biometric characteristic of the attacked user.

Another specific aspect for a spoof detection system that is used to protect a biometric verification process is that a claimed identity is available.

- **Biometric identification:**

  The objective of a biometric identification process is similar to a verification process. However, in contrast to a verification process there is no claimed identity for the user. The system directly captures the fingerprint of a user and compares it to all fingerprint references in the database. If at least one reference is found to be similar enough according to the relevant threshold settings, the system returns this as the found identity of the user.

  In the identification scenario an attacker can have multiple aims:

  - An attacker could try to get identified as a specific enrolled user (i.e. using a fake finger of that specific user). The reason for doing so may be that this attacked user has a specific credential that the attacker is after.
  - An attacker could try to get identified as any enrolled user (i.e. using a faked fingerprint of any enrolled user). This can be relevant for cases where all enrolled users for a system have similar permissions.
  - An attacker who is enrolled in the system could try avoid identification (i.e. disguise their identity) For such an attack the attacker may not need any knowledge about the biometric characteristic of another user.

More information on how the environment contributes to the security problem addressed by the TOE can be found in the Fingerprint Spoof Detection Evaluation Guidance [FSDEG].

2.2 TOE configuration and TOE environment

A biometric spoof detection system in general could be realized in two major configurations:

- **An integrated solution:** All relevant parts of the TOE are integrated into one physical unit.
- **A distributed solution:** Relevant parts of the TOE are implemented in physically separated parts.

This PP describes a biometric spoof detection system for fingerprints as an integrated solution but should be applicable to distributed solutions as well. However, if applied to a distributed TOE additional aspects of security shall be considered by the author of the Security Target in form of:

1. Assumptions for the TOE environment
2. Requirements for additional functionality: e. g. encrypted transmission

It is known that environmental factors may influence the performance and therewith the protection provided by a spoof detection system. Therefore the author of a Security Target claiming compliance to this PP shall clearly identify the relevant environmental factors and their acceptable range for the operation of the TOE. More information about influencing factors can be found in [FSDEG].

In general it should be noted that the TOE should not impact the functionality of the protected biometric system (e.g. by a deterioration of image quality) beyond what is necessary for the desired application. If a negative impact cannot be completely avoided this shall be clearly pointed out by the ST author.

2.3 TOE boundary

A simplified model of a biometric spoof detection system and its boundaries is shown in Figure 1.The following chapters provide more details about the physical and logical boundaries of the TOE.

2.3.1 Physical boundary

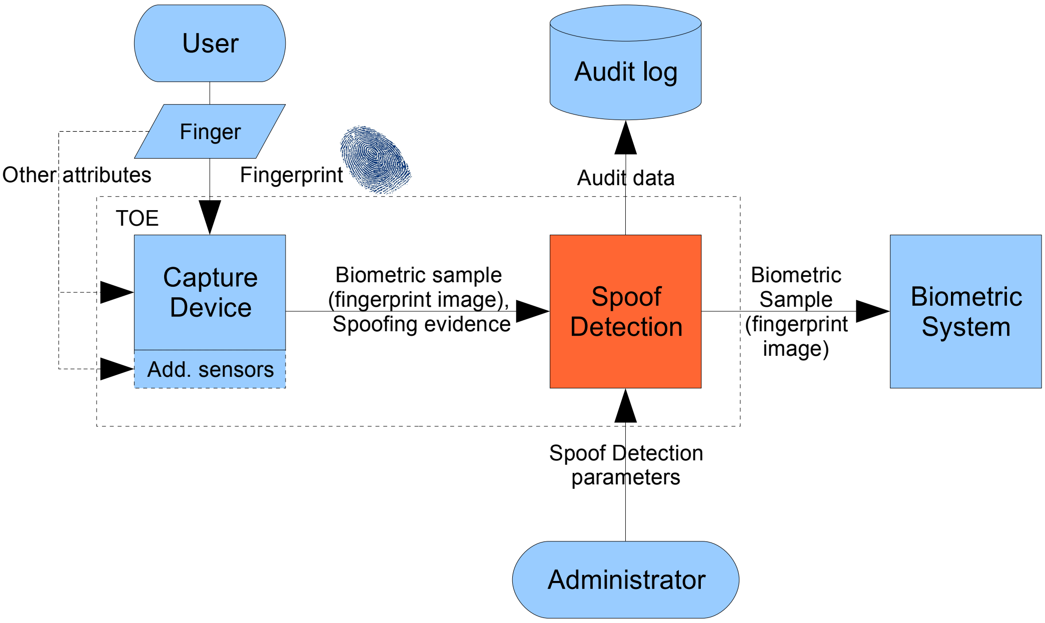

Figure 1: TOE demarcation

The TOE defined in this PP is limited to the biometric spoof detection system. This system shall decide whether a provided fingerprint is spoofed or genuine. The TOE shall comprise all parts of a product (hardware and software) that contribute to this functionality or any of the additional functionality outlined in chapter 2.3.2. In particular these are:

- the capture device for capturing of fingerprint images
- additional sensor devices for acquisition of spoofing evidences (if applicable)
- necessary software (if applicable)

The spoofing evidences for a fingerprint can either be captured by the same sensor device being also used for the biometric system (capture process) or using separate sensor devices. If separate sensor devices are used, it has to be ensured that the same fingerprint is used for both processes.

The biometric system that is protected by the TOE resides in the environment. It can be, e. g., a biometric identification system, a biometric verification system, or an enrollment system as described in chapter 2.1. This means that all aspects about the security of the biometric systems (e.g. questions about the error rates of this system) are out of scope for the evaluation of the TOE.

The TOE shall be able to generate audit data. This audit data can be used for quality assurance or statistics. However, functionality for storage, protection and review of audit records is assumed to be provided by the environment of the TOE.

Further the TOE may rely on access control mechanisms of the environment for its own protection and the restriction of access to management functions offered by the TOE (e.g. for adjustment of important parameters). Also for the implementation of management functions the TOE may partly rely on functions of the environment (i.e. in form of a file import that involves the Operating System).

2.3.2 Logical boundary

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

- **Spoof detection:** the TOE detects whether a presented fingerprint is spoofed or genuine. It shall perform appropriate actions in case of a spoofed and in case of a genuine biometric characteristic. It should be clearly mentioned that in the context of this PP a TOE is always required to decide about the presented fingerprint in form of a yes/no decision. It is not considered to be sufficient if a TOE would return a confidence value that would need further interpretation by the environment.

- **Management:** the TOE provides functionality to manage its relevant parameters. This specifically (but not only) refers to the parameters that are involved in the spoof detection process (e.g. a threshold). The TOE ensures that only secure values for spoof detection parameters are accepted to ensure the constant operation of the primary functionality.
- **Residual Information Protection:** in order to prevent the leakage of information the TOE deletes relevant information if not longer in use.
- **Audit:** the TOE produces audit events for security relevant events.

The following functionality on the other hand may be provided by the environment to support the operation of the TOE:

- **Access control:** the environment provides access control for the spoof detection parameters, the life record, audit data and any software parts of the TOE. To perform access control, the environment maintains roles for users 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 functionality. In any case it will provide reliable time stamps for auditing, storage for the audit records that are produced by the TOE and mechanisms for review of audit logs. The developer will probably have to consider privacy concerns (in case that personal information is part of the audit logs). Applicable data protection laws and protection mechanisms might have to be considered.
-

Application Note: To allow the application of this PP to a wide range of systems, several functions are stated to be implemented in the environment. However, if a TOE is able to provide those functions on its own the ST author should consider to define those functions as part of the TOE.

3. Conformance Claims

3.1 Conformance statement

The PP requires **strict conformance** of any PPs/STs to this PP. A **demonstrable conformance** is not allowed.

3.2 CC Conformance Claims

- This PP has been developed using Version 3.1 R3 of Common Criteria [CC].
- The conformance of this Protection Profile is Common Criteria [CC] Part II extended (due to the use of FPT_SPOD.1)
- The conformance of this Protection Profile is Common Criteria [CC] Part III conformant.

3.3 PP Claim

- This PP does not claim conformance to any other Protection Profile.

3.4 Package Claim

This PP does not claim conformance to any assurance package (i.e. EAL) as defined in Common Criteria Part III. Instead, this PP defines an explicit assurance package that bases on EAL 2. However, in contrast to EAL 2 as defined in part III of [CC], the assurance package in this PP does not contain any AVA_VAN component. It further includes the assurance component ALC_FLR.1.

The reason for this explicit assurance level is to allow a purely functional evaluation of the performance of a system for spoof detection. Such an evaluation will allow to determine whether the functionality of a system for spoof detection is sufficient to recognize spoofed biometric characteristics that are know for a certain biometric modality.

An evaluation using this explicit assurance level is deliberately ignoring the fact that an attacker could try to circumvent the functionality of the TOE (e.g. by using different/innovative spoofed characteristics) and focuses on the basic functionality of the TOE. A system claiming compliance to this Protection Profile is therefore suitable for the use in application cases in which an assurance about the basic functionality of a system is sufficient. To emphasize that this PP only deals with the pure functionality of spoof detection, the definition of threats has been omitted and the PP is completely based on organizational security policies.

The complete list of the assurance components of the explicit assurance package can be found in chapter 7.2.

4. Security Problem Definition

4.1 External entities

The following external entities interact with the TOE:

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.

4.2 Assets

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

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.
- **Audit 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.

4.3 Assumptions

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.

4.4 Threats

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

4.5 Organizational Security Policies

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.

5. Security Objectives

5.1 Security Objectives for the TOE

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.

5.2 Security objectives for the operational environment

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.

5.3 Security Objectives rationale

5.3.1 Overview

The following table gives an overview of how the assumptions, threats, and organizational security policies are addressed by the security objectives of the TOE. The text of the following sections justifies this in more detail. Aspects of the TOE operational environment are marked grey.

	O.SPOOF_DETECTION	O.AUDIT	O.RESIDUAL	O.MANAGEMENT	OE.ADMINISTRATION	OE.PHYSICAL	OE.PLATFORM	OE.BIO
OSP.SPOOF_DETECTION	X			X	X	X	X	
OSP.MANAGEMENT				X	X	X	X	
OSP.RESIDUAL			X		X	X	X	
OSP.AUDIT		X					X	
A.BIO								X

Table 1: Security Objectives Rationale

5.3.2 Justification for coverage of assumptions

The only assumption **A.BIO** is covered by security objective **OE.BIO** as directly follows.

5.3.3 Justification for the coverage of organizational security policies

5.3.3.1 OSP.SPOOF_DETECTION

The organisational security policy **OSP.SPOOF_DETECTION** is covered by the security objective **O.SPOOF_DETECTION** which is supported by **O.MANAGEMENT**, **OE.ADMINISTRATION**, **OE.PHYSICAL**, and **OE.PLATFORM**..

O.SPOOF_DETECTION detects whether a presented fingerprint is spoofed or genuine, and performs appropriate actions in case of a spoofed and in case of a genuine fingerprint. Therefore, a spoofed fingerprint will not be used by the Biometric System being behind the TOE. This objective covers the main part of the OSP.

O.MANAGEMENT provides necessary management functionality for the modification of security relevant parameters to TOE administrators which are authenticated and authorized by the TOE platform as stated in **OE.PLATFORM**. TOE administrators are well-trained and non-hostile according to **OE.ADMINISTRATION** and will therefore unlikely misconfigure the spoof detection functionality. All three objectives ensure that the spoof detection is securely managed and therefore support that spoof detection performs as intended.

OE.PHYSICAL ensures that the TOE is physically protected against manipulation so that the spoof detection functionality can not be compromised using physically means.

OE.PLATFORM further ensures that the platform for the TOE provides secure communication and storage of data and ensures that the TOE is free of malware which could otherwise compromise the spoof detection.

OE.ADMINISTRATION further ensures that environmental factors which influence the capture and sensor devices are within acceptable ranges. It therefore supports that the spoof detection functionality is not compromised by environmental conditions.

5.3.3.2 OSP.MANAGEMENT

OSP.MANAGEMENT is covered by the security objectives **O.MANAGEMENT** which is supported by **OE.ADMINISTRATION**, **OE.PHYSICAL**, and **OE.PLATFORM**..

O.MANAGEMENT provides the necessary management functionality to securely modify security parameters. It comprises the main part to cover the OSP. It is supported by **OE.PLATFORM** which ensures that only authenticated TOE administrators are authorized to manage the TOE. **OE.ADMINISTRATION** thereby ensures that these TOE administrators are well-trained and non-hostile so that misconfiguration is unlikely.

OE.PHYSICAL ensures that the TOE is physically protected against manipulation so that management functionality can not be altered by physically means.

OE.PLATFORM further ensures that the platform for the TOE provides secure communication and storage of data and ensures that the TOE is free of malware which could otherwise compromise the management functionality.

5.3.3.3 OSP.RESIDUAL

OSP.RESIDUAL is covered by security objective **O.RESIDUAL** which is supported by **OE.ADMINISTRATION**, **OE.PHYSICAL**, and **OE.PLATFORM**..

O.RESIDUAL ensures that no residual or unprotected security relevant data remains after operations are completed and therefore residual security relevant data from a previous usage of the TOE can not be used by an attacker. It comprises the main part to cover the OSP. It is supported by **OE.PHYSICAL** which ensures that the TOE is physically protected against manipulation and therefore residual information can not be obtained via physical attacks.

OE.PLATFORM ensures that the TOE platform is free of malware and therefore does not compromise functionality for residual information protection. **OE.ADMINISTRATION** supports that as it ensures that the platform is securely installed by the TOE administrator.

5.3.3.4 OSP.AUDIT

The organizational security policy **OSP.AUDIT** is covered by **O.AUDIT** which is supported by **OE.PLATFORM**..

O.AUDIT ensures that the TOE generates audit records for security relevant events and therefore comprises the main part to cover the OSP.

OE.PLATFROM ensures that the environment provides the time stamps necessary for audit, the secure storage for audit data, and mechanisms for review of audit data. It therefore supports the task of **O.AUDIT**.

6. Extended Component definition

The extended functional family FPT_SPOD (Biometric Spoof Detection) of the Class FPT (Protection of the TSF) has been defined here to describe the core security function as provided by the TOE described in this PP: The TOE shall prevent that a spoofed biometric characteristics can be used with a biometric system that is protected by the TOE. The class FPT (Protection of the TSF) as defined in part II of Common Criteria has been selected even if the functionality to be protected is not part of the TOE. The following chapter contains the detailed definition.

6.1 FPT_SPOD Biometric Spoof Detection

Family behavior

This family defines functional requirements to detect spoofed biometric characteristics.

Component leveling:

FPT_SPOD.1 Biometric Spoof Detection has four elements:

FPT_SPOD.1.1 FPT_SPOD.1.1 requires to provide spoof detection functionality for a specific biometric characteristic.

FPT_SPOD.1.2 FPT_SPOD.1.2 defines actions to be performed if a spoofed biometric characteristic is detected.

FPT_SPOD.1.3 FPT_SPOD.1.3 defines actions to be performed if a genuine biometric characteristic is detected.

FPT_SPOD.1.4 FPT_SPOD.1.4 defines additional information returned with the feedback about spoof status.

Management: FPT_SPOD.1

The following actions could be considered for the management functions in FMT:

a) Management of the parameters used for spoofed detection.

Audit: FPT_SPOD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: spoof detected

b) Basic: no spoof detected

6.1.1 Biometric Spoof Detection (FPT_SPOD.1)

FPT_SPOD.1 Biometric Spoof Detection

FPT_SPOD.1.1 The TSF shall be able to detect whether a presented [*assignment: biometric characteristic*] is spoofed or genuine.

FPT_SPOD.1.2 If a spoofed biometric characteristic is detected, the following action(s) shall be performed:

- [*assignment: list of actions*]

FPT_SPOD.1.3 If a genuine biometric characteristic is detected, the following action(s) shall be performed:

- [*assignment: list of actions*]

FPT_SPOD.1.4 Along with the feedback about the spoof status of the presented biometric characteristic the TOE shall deliver the following information:

- [*assignment: list of information*]

Hierarchical to: No other components

Dependencies: FMT_MTD.3 Secure TSF data
FMT_SMF.1 Specification of Management Functions

6.1.2 Justification for the definition of functional family FPT_SPOD

Spoof detection functionality describes mechanisms that protect biometric systems like fingerprint verification systems against threats of non-genuine biometric characteristics like fake fingers. It therefore provides protection of the TSF which is subject of the functional class FPT.

There is no family in FPT that deals with detection of spoofing attacks or biometric functionality at all, therefore a new family has been defined.

7. Security Requirements

This chapter describes the security functional and the assurance requirements which have to be fulfilled by the TOE.

Those requirements comprise functional components from part II of [CC] and assurance components from part III of [CC]. Further the extended requirement FPT_SPOD.1 as defined in chapter 6 is used.

The following notations are used to mark operations that have been performed:

- **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.

7.1 Security Functional Requirements for the TOE

The following table summarizes all security functional requirements of this PP:

Class FAU: Security Audit	
FAU_GEN.1	Audit Data Generation
Class FDP: User Data Protection	
FDP_RIP.2	Full residual information protection
Class FMT: Security Management	
FMT_MTD.3	Secure TSF data
FMT_SMF.1	Specification of Management Functions
Class FPT: Protection of the TSF	
FPT_SPOD.1	Spoof Detection

Table 2: Security Functional Requirements

7.1.1 Security audit (FAU)

7.1.1.1 Security audit data generation (FAU_GEN)

FAU_GEN.1 Audit data generation

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) [assignment: other specifically defined auditable events]].

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, [assignment*: other audit relevant information*].

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_SMF.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.

7.1.2 User data protection (FDP)

7.1.2.1 Residual information protection (FDP_RIP)

FDP_RIP.2 Full residual information protection

FDP_RIP.2.1 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

7.1.3 Security management (FMT)

7.1.3.1 Management of TSF data (FMT_MTD)

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for [

- *[assignment: list of all spoof detection parameters]*
- *[assignment: list of other TSF data or none]*

]

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.

7.1.3.2 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

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.

7.1.4 Protection of the TSF (FPT)

7.1.4.1 Biometric Spoof Detection (FPT_SPOD.1)

FPT_SPOD.1 Biometric Spoof Detection

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:

- [*assignment: list of actions*]

FPT_SPOD.1.3 If a genuine biometric characteristic is detected, the following action(s) shall be performed:

- [*assignment: list of actions*]

FPT_SPOD.1.4 Along with the feedback about spoof status of the presented biometric characteristic the TOE shall deliver the following information:

- [*assignment: list of information*]

Hierarchical to: No other components

Dependencies: FMT_MTD.3 Secure TSF data
FMT_SMF.1 Specification of Management Functions

Application Note: FPT_SPOD.1 represents the core functionality to be provided by the TOE. Due to the special character of this technology additional guidance for evaluation is provided in form of [FSDEG]. This guidance shall be applied during evaluation.

Application Note: 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.

Application Note: 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.

7.2 Security Assurance Requirements for the TOE

Due to the special character of the technology described in this PP, the following explicit assurance package has been defined for the TOE based on EAL 2. In contrast to EAL 2, it does not contain AVA_VAN.2 but is augmented by ALC_FLR.1.

The following table lists the assurance components which are chosen for this PP.

Assurance Class	Assurance Component	Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic Design
Guidance documents	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 3: Assurance Requirements

Due to the special character of the technology described in this PP, the Spoof Detection Evaluation Methodology [FSDEG] shall be applied during evaluation. This methodology will provide the evaluator with additional information and guidance for some assurance requirements.

7.3 Security Requirements rationale

7.3.1 Security Functional Requirements rationale

7.3.1.1 Fulfillment of the Security Objectives

This chapter proves that the set of security requirements (TOE) is suited to fulfill the security objectives described in chapter 4 and that each SFR can be traced back to the security objectives. At least one security objective exists for each security requirement.

	O.AUDIT	**O. RESIDUAL**	**O.MANAGEMENT**	**O.SPOOF_DETECTION**
FAU_GEN.1	X			
FDP_RIP.2		X		
FMT_MTD.3			X	
FMT_SMF.1			X	
FPT_SPOD.1				X

Table 4:Fulfillment of Security Objectives

The following paragraphs contain more details on this mapping.

O.AUDIT

- **FAU_GEN.1** defines that the TOE has to capture all the events as required by **O.AUDIT**.

O.RESIDUAL

- This objective is completely covered by **FDP_RIP.2** as directly follows.

O.MANAGEMENT

- **FMT_MTD.1** defines that the TOE only accepts secure values for spoof detection parameters so that the spoof detection works correctly.
- **FMT_SMF.1** ensures that the TOE provides the necessary management functionality

O.SPOOF_DETECTION

- **FPT_SPOD.1** defines that the TOE is able to detect whether a presented fingerprint is spoofed or genuine and therewith directly addresses this objective.

7.3.1.2 Fulfillment of the dependencies

The following table summarizes all TOE functional requirements dependencies of this PP and demonstrates that they are fulfilled.

SFR	Dependencies	Fulfilled by
FAU_GEN.1	FPT_STM.1	See chapter 7.3.1.3
FDP_RIP.2	-	-
FMT_MTD.3	FMT_MTD.1	See chapter 7.3.1.3
FMT_SMF.1	-	-
FPT_SPOD.1	FMT_MTD.3 FMT_SMF.1	FMT_MTD.3 FMT_SMF.1

Table 5: Security Functional Requirements

7.3.1.3 Justification for missing dependencies

The functional component FAU_GEN.1 has an identified dependency on FPT_STM.1. This dependency is not satisfied by any TOE functional requirement as the functionality of reliable time stamps is provided by the TOE environment (OE.PLATFORM).

The functional component FMT_MTD.3 has an identified dependency on FMT_MTD.1. This dependency is not satisfied by any TOE functional requirement as the functionality of restricting the ability to query, modify, delete, and clear security parameters to TOE administrators is provided by the TOE environment (see OE.PLATFORM).

7.3.2 Security Assurance Requirements rationale

Due to the special character of the technology described in this PP, an explicit assurance package has been defined for the TOE. It has been chosen for this Protection Profile as it should 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 defined assurance package has been developed based on EAL 2. In contrast to EAL 2, it does not contain AVA_VAN.2 but has been augmented by the assurance component ALC_FLR.1. ALC_FLR.1 has been included as spoof detection systems are supposed to have flaws that will be found in future and that will then have to be addressed.

Additional guidance has been provided for some of the assurance components due to the special nature of the biometric technology in form of [FSDEG].

7.3.2.1 Dependencies of assurance components

The dependencies of the assurance requirements are fulfilled as shown in Table 6:

Assurance Class	Assurance Component	Dependencies	Fulfillment
Development	ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	ADV_FSP.2, ADV_TDS.1
	ADV_FSP.2	ADV_TDS.1	ADV_TDS.1
	ADV_TDS.1	ADV_FSP.2	ADV_FSP.2
Guidance documents	AGD_OPE.1	ADV_FSP.1	ADV_FSP.2
	AGD_PRE.1	No dependencies	-
Life-cycle support	ALC_CMC.2	ALC_CMS.1	ALC_CMS.2

Assurance Class	Assurance Component	Dependencies	Fulfillment
	ALC_CMS.2	No dependencies	-
	ALC_DEL.1	No dependencies	-
	ALC_FLR.1	No dependencies	-
Security Target Evaluation	ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.2
	ASE_ECD.1	No dependencies	-
	ASE_INT.1	No dependencies	-
	ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1
	ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_OBJ.2, ASE_ECD.1
	ASE_SPD.1	No dependencies	-
	ASE_TSS.1	ASE_INT.1, ASE_REQ.1 ADV_FSP.1	ASE_INT.1, ASE_REQ.2 ADV_FSP.2
Tests	ATE_COV.1	ADV_FSP.2, ATE_FUN.1	ADV_FSP.2, ATE_FUN.1
	ATE_FUN.1	ATE_COV.1	ATE_COV.1
	ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1

Table 6: Dependencies of assurance components

8. Appendix

8.1 Glossary

Term	Description
AD	Audit data
Audit data	Content of the audit trace generated by the TOE.
Attacker	An attacker in the context of this PP is any individual who is attempting to subvert the operation of the biometric system protected by the TOE using a faked fingerprint. This does explicitly included cases in which users try to subvert the operation of the TOE directly but in any case it is the final focus of an attacker to subvert the operation of the protected biometric system using a faked fingerprint.
Biometric	A measurable physical characteristic or personal behavioral trait used to recognize the identity of a user or verify a claimed identity.
Biometric identification	Application in which a search of the enrolled database is performed, and a candidate list of 0, 1 or more identifiers is returned.
Biometric system	An automated system capable of capturing a biometric sample from a user, extracting biometric data from the sample, comparing the data with one or more biometric references, deciding on how well they match, and indicating whether or not an identification or verification of identity has been achieved. Note that in [CC] evaluation terms, a biometric system may be a product or part of a system.
Biometric verification	The objective of a verification process is to verify or refuse the claimed identity of a user based on their biometric characteristic.
CC	Common Criteria - Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
FAU	Class of functional requirements for audit
FDP	Class of functional requirements for data protection
FMT	Class of functional requirements for management
FPT	Class of functional requirements for TSF protection
Identification system	Biometric system that provides an identification function (see also biometric identification)
I&A	Identification and authentication
LAN	Local Area Network
OS	Operating system

Term	Description
PP	Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
SDP	Spoof detection parameters
Sensor	The physical hardware device used for biometric capture. Also called capture device
SFR	Security Functional Requirement
ST	Security Target – A set of implementation-dependent security requirements for a specific TOE.
Spoof detection parameters	Settings (configuration data) necessary to detect a spoofed biometric characteristic, e. g., temperature limits, thresholds, typical movement patterns.
Spoofing evidence	Information that is acquired from a biometric characteristic to decide whether it is spoofed or genuine.
Threshold	A parametric value used to convert a matching score to a decision.
TOE	Target of Evaluation
TSF	TOE Security Functionality.
Verification system	A biometric system that provides verification functionality.
WAN	Wide Area Network
WLAN	Wireless Local Area Network

8.2 References

[FSDPP]	Fingerprint Spoof Detection Protection Profile, version 1.8, November 2009
[Toolbox]	Standard Fake Finger Toolbox for Common Criteria evaluations of Spoof Detection systems, as referenced in [FSDEG]
[FSDEG]	Fingerprint Spoof Detection Evaluation Guidance, version 2.0 (or a more recent version)
[CC]	Common Criteria for Information Technology Security Evaluation – ● Part 1: Introduction and general model, dated July 2009, version 3.1 R3 ● Part 2: Security functional requirements, dated July 2009, version 3.1, R3 ● Part 3: Security assurance requirements, dated July 2009, version 3.1, R3
[CEM]	Common Evaluation Methodology for Information Technology Security – Evaluation Methodology, dated July 2009, version 3.1 R3