MorphoSmart Optic 301 Public Security Target

Reference: ***SSE-0000096154-01***

Date: ***2013-01-18***

TABLE OF CONTENTS

1. INTRODUCTION

1.1 SECURITY TARGET AND TOE REFERENCE

ST reference:

Title : MorphoSmart Optic 301 Public ST
Version : 1
Security target identifier : SSE-0000096154

TOE reference:

TOE Identifier MorphoSmart Optic 301
TOE version : 1.0

CC compliance:

Version : 3.1
Assurance level : Explicit Assurance Package, see Chapter 6.5
Protection Profile BSI-CC-PP-0062, Version 1.7 [R2]

1.2 GENERAL OVERVIEW OF THE TARGET OF EVALUATION (TOE)

1.2.1 Product presentation

The MorphoSmart™ Optic (MSO) 301 device is a high end fingerprint optical scanner, offering a large capture surface. It covers a wide range of applications: enrollment, authentication and identification (using an internal database capable to store up to 5000 users) in industrial/commercial and governmental environments. It integrates a patented technology from Morpho which enables the detection of fake fingers and helps to fight against fraud.

To authenticate a user, an administrator sends a command to the MSO. Once the command is received, the MSO is waiting for the user to put his finger on the capture device.

1.2.2 TOE type

The Target of Evaluation (TOE) is a system that provides fingerprint spoof detection as part of a biometric system for fingerprint recognition.

The TOE has a hardware part which is the capture device and a software part which is the spoof detection module.

Minimum requirements for the TOE are :

- a PC Intel Pentium® IV 1.4 GHz or greater,
- 256 or more megabytes of RAM,
- available USB port,
- CD-ROM drive,
- MorphoSDK, the version and details are given in the Installation Guide [R3].

Supported OS are :

- Windows XP Professional edition SP3 32 bits
- Windows Server 2003 Enterprise SP2 32 bits
- Windows Server 2003 Enterprise SP3 64 bits
- Windows Server 2008 Enterprise SP2 32/64 bits
- Windows Vista SP2 32/64 bits
- Windows Seven 32/64 bits
- Linux 32 bits

The TOE determines whether a fingerprint presented to the biometric system is genuine or spoofed.

For this purpose the spoof detection system acquires spoofing evidences for a presented fingerprint using sensors . These sensors are part of the capture device that is used to capture the biometric sample of the fingerprint.

1.3 TOE DESCRIPTION

1.3.1 TOE Boundary

A simplified model of a biometric spoof detection system and its boundaries is shown in Figure 1.

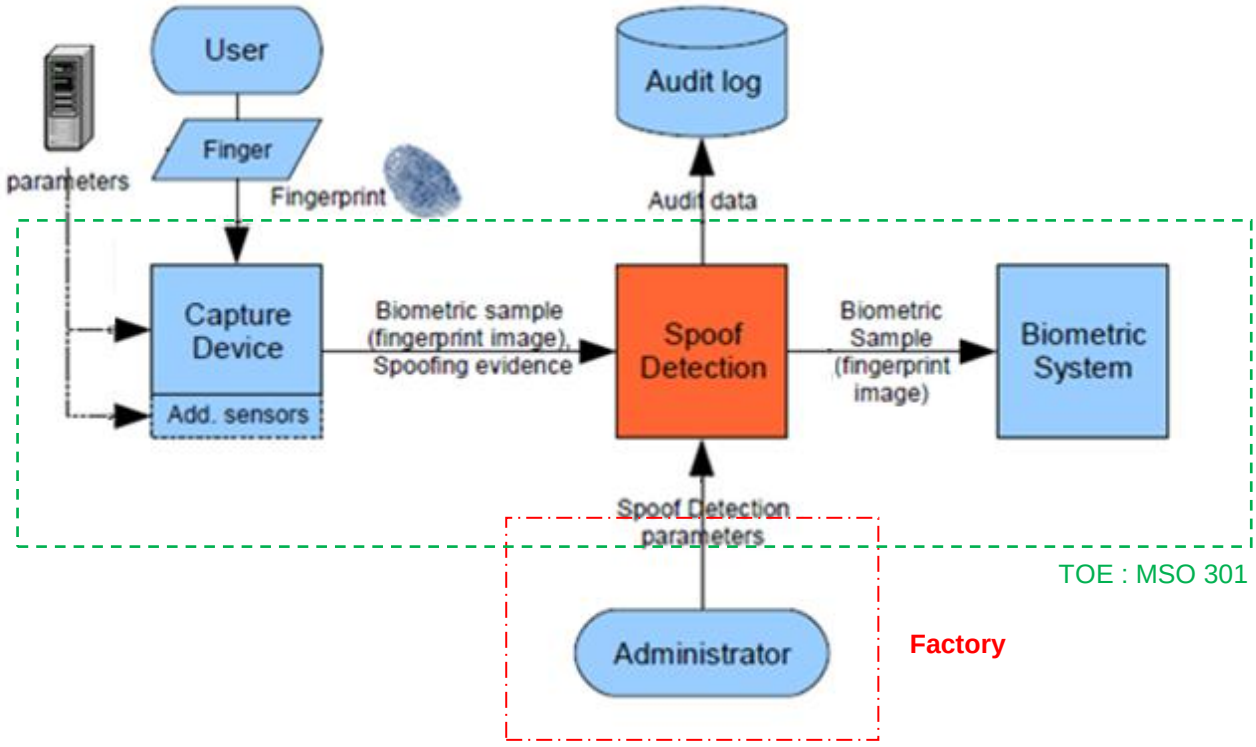

Figure 1: TOE Boundary

The TOE is the MSO 301.

The capture device is responsible for acquiring the fingerprint image. It processes the image to obtain an image compliant with the expected quality.

The Spoof Detection module represents the main software part of the TOE. It receives the fingerprint image from the capture device and the spoofing evidence from the sensors.
Depending on the security level, the interpretation is different.

Depending on the spoof detection parameters (security level), the spoof detection module will check if the fingerprint image corresponds to a fake finger or a real finger. The parameters received from the Administrator are checked to be sure that they are in the defined range. Every decision and actions done by this module are logged in the Audit log.

The spoof parameters are configured in the factory: a range of values for the security level (3 values) is defined in the factory. Afterwards, in the user phase, the administrator can select his preferred values for security level among the pre-defined values only.

Once this module identifies a real fingerprint, it sends the sample to the Biometric System to check if it matches or not with the expected user's fingerprint. The Biometric System contains the matching and the decision module, which are part of the TOE but do not realize any part of the fake finger detection functionality and are therefore out of scope of the certified security functionality.

The storage of the generated log, i.e., the Audit log, is not part of the TOE.

Beside the fingerprint spoof detection functionality, the TOE implements:

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

1.3.2 TOE architecture

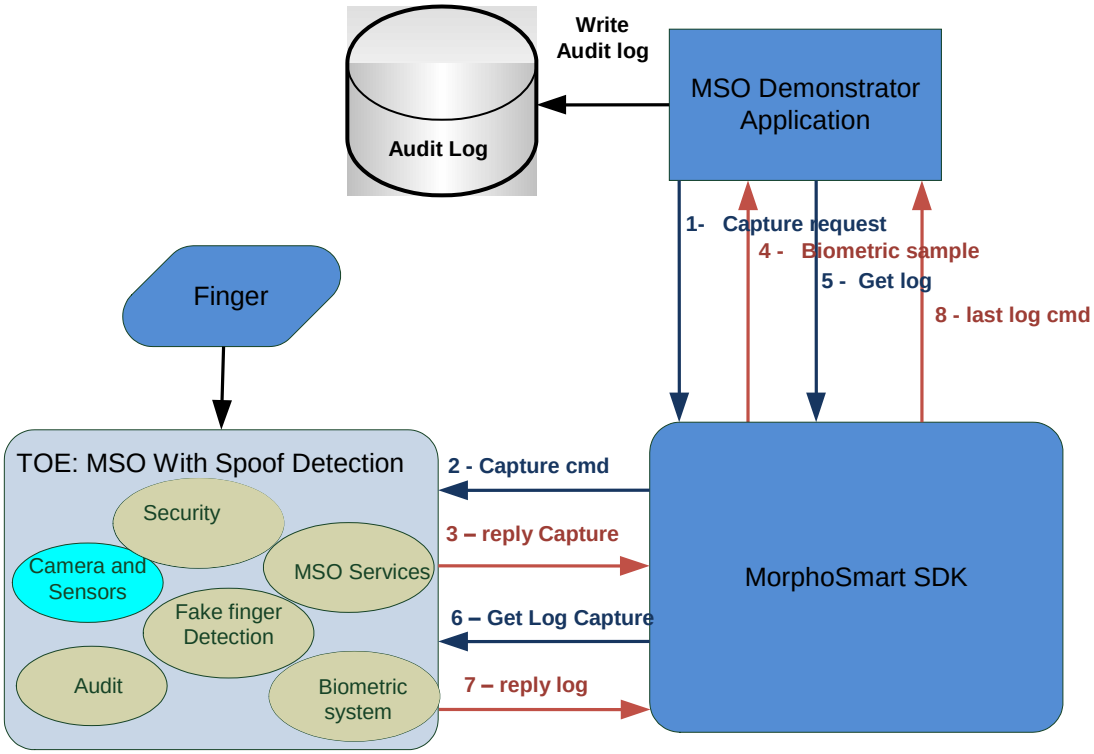

Figure 2: Architecture of the MSO

The TOE consists of:

- Camera and Sensors hardware/software part
- Fake Finger Detection software part
- Audit generation software part
- Security software part
- MSO Services software part
- Biometric system software part
- MSO 301 Guide [AGD]
- MorphoSmart Host System Interface [HSI]
- MorphoSmart Programmer's Guide [MPG]
- Morpho Biometric terminals Finger Positioning Recommendations [FPR]

The Camera and Sensors and Fake Finger Detection parts can be considered the core of the MSO 301.

The Fake Finger Detection software part deals with image acquisition from the Camera and Sensors using the corresponding internal interface, and selects the most adapted image to the biometric coding (software presence detection). Then, it checks whether the proposed finger is fake or not, according to the security level. Then, it sends a message to the SDK for thumbnail display during the capture and finger positioning. It also reports on the status of the acquisition (fake finger, moist finger, genuine finger) and the fingerprint if genuine. Please be aware that the mechanism for biometric matching is out of scope of the certification.

The MSO Demonstrator Application is a software which enables using the MSO. It sends commands to the SDK in accordance with the SDK User Guide.

The MorphoSmart SDK allows applications to use the MSO.

The SDK User Guide describes the way to use the MSO. The System Interface Specification describes interactions between the MSO and the SDK.

Authorized administrators only can send requests to the MSO. Administrators have to be connected to launch the MSO Demonstrator application. More details are provided in the MSO Administrator Application user guide.

2. CONFORMANCE CLAIMS

2.1 CC CONFORMANCE CLAIMS

This ST has been developed using Version 3.1 R3 of Common Criteria [R1].

The conformance of this Security Target is Common Criteria [R1] Part II extended (due to the use of FPT_SPOD.1)

The conformance of this Security Target is Common Criteria [R1] Part III conformant.

This Security Target claims strict conformance to the Fingerprint Spoof Detection Protection Profile [R2].

This Security Target claims to be conformant to the Explicit Assurance Package, see Chapter 6.5.

3. SECURITY PROBLEM DEFINITION

3.1 EXTERNAL ENTITIES

The following external entities interact with the TOE:

TOE administrator The TOE administrator is authorized to perform administrative TOE operations and is able to use the administrative functions of the TOE.

The administrator is also responsible for the installation and maintenance of the TOE.

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.

3.2 ASSETS

The following assets are defined in the context of this Security Target.

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 connected to 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: security level. The integrity of this parameter 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 have to be protected.

3.3 ASSUMPTIONS

A.BIO The spoof detection system addressed in this Security Target 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 protect 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.

3.4 THREATS

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

3.5 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.

4. SECURITY OBJECTIVES

4.1 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), 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.

4.2 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[1]) 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

[1] The environmental factors listed as examples do not apply tot he TOE covered in this ST document.

attacks.

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 Overview

The following table gives an overview of how the assumptions 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

4.3.2 Justification for the coverage of assumptions

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

4.3.3 Justification for the coverage of organizational security policies

4.3.3.1 OSP.SPOOF_DETECTION

The organizational 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 connected to 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.

4.3.3.2 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.

4.3.3.3 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.

4.3.3.4 OSP.AUDIT

OSP.AUDIT is covered by the security objective **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.PLATFORM 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**.

5. 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 ST: 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 two chapters contain the detailed definitions.

5.1 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
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 spoofed a biometric characteristic is detected.
FPT_SPOD.1.3	FPT_SPOD.1.3 defines actions to be performed if 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

5.1.1 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

5.1.2 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.

6. 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 Common Criteria [R1] and assurance components from part III of Common Criteria [R1]. Further the extended requirement FPT_SPOD.1 as defined in chapter 5 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 Common Criteria [R1] 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.

6.1 SECURITY AUDIT (FAU)

6.1.1 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) [A use of the TOE where a faked fingerprint has been detected with the used security parameters, and* *A use of the TOE where a genuine fingerprint has been detected with the used security parameters, and* *All Spoof Detection parameters rejected by the TOE]*].
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, [*MSO serial number*].

6.2 USER DATA PROTECTION (FDP)

6.2.1 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.

6.3 SECURITY MANAGEMENT (FMT)

6.3.1 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 [●*[security level]* ●*[none]*]

6.3.2 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: [*setting of security level*].

NOTE: When administrator sends a request to the TOE, he sends the security level to be used for this verification. That is, when using the Fake Finger Detection Function, a value is passed to the functionality and this value is used for the current verification. The values to be used for a secure use of the product are described in the User Guidance [R3].

6.4 PROTECTION OF THE TSF (FPT)

6.4.1 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: ●[*creating a log event, send a negative command to the biometric system to stop the biometric matching*]
FPT_SPOD.1.3	If a genuine biometric characteristic is detected, the following action(s) shall be performed: ●[*creating a log event, send a positive command to the biometric system to initiate the authentication process*]
FPT_SPOD.1.4	Along with the feedback about spoof status of the presented biometric characteristic the TOE shall deliver the following information: ●[*log events*]

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.

6.5 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE

Due to the special character of the technology described in this ST, an explicit assurance package has been defined for the TOE. It has been chosen for this Security Target 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.

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

Assurance Class	Assurance Component	Title
	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 2: Explicit Assurance Package

6.6 SECURITY REQUIREMENTS RATIONALE

6.6.1 Security Functional Requirements rationale

6.6.1.1 Fulfillment of the Security Objectives

	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 3:Fulfillment of Security Objectives

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.3** 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.

6.6.1.2 Fulfillment of the dependencies

SFR	Dependencies	Support of the dependencies
FAU_GEN.1	FPT_STM.1	See chapter 6.6.1.3
FDP_RIP.2	-	-
FMT_MTD.3	FMT_MTD.1	See chapter 6.6.1.3
FMT_SMF.1	-	-
FPT_SPOD.1	FMT_MTD.3 FMT_SMF.1	FMT_MTD.3 FMT_SMF.1

6.6.1.3 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 (see 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).

6.6.2 Security Assurance Requirements rationale

Due to the special character of the technology described in this ST, an explicit assurance package has been defined for the TOE. It has been chosen for this Security Target 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.

6.6.2.1 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
	ALC_CMS.2	No dependencies	-
	ALC_DEL.1	No dependencies	-
	ALC_FLR.1	No dependencies	-

Assurance Class	Assurance Component	Dependencies	Fulfillment
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

7. TOE SUMMARY SPECIFICATION

7.1 FAKE FINGER DETECTION FUNCTION TSF_FFD

This security feature detects if a finger presented on the sensor is a fake or not. It prevents attacks using fingerprint replicas and helps to fight against fraud.

This function covers FPT_SPOD.1. This function returns a status about the tested finger: spoof or no spoof.

If a fake finger is detected, the MSO does not perform the matching: this function sends information that a fake finger is detected to the biometric system and creates a log event by calling TSF_AUDIT.

If a real finger is detected, this function sends the result of the fake finger detection (real finger detected) and the acquired fingerprint image from the sensor to the biometric system and creates a log event by calling TSF_AUDIT.

This function covers FDP_RIP.2: after any fake finger verification (fake finger detected or not), this function ensures that all its sensitive information (fingerprint image, log event, security level and FAR level) are securely deleted.

7.2 SECURITY MANAGEMENT FUNCTION TSF_MANAGEMENT

This security feature permits to change the security parameters used by the Fake Finger Detection Function.

This function covers FMT_SMF.1: for each use of the TSF_FFD an individual security level value can be passed to the TSF_FFD, and this value will then be used for the fake finger verification.

Before the TSF_FFD function tested a presented finger, this function is called to check if the used parameters are in the acceptable range (as defined in user guide [R3]).

This function covers FMT_MTD.3: only spoof detection parameters described in [R3] are accepted.

If any received value is out of the defined range, this function returns an error to TSF_FFD function.

7.3 SECURITY AUDIT GENERATION FUNCTION TSF_AUDIT

This security feature produces an audit record for every use of the security functions of the TOE. The record is sent to the MSO Administration application, which is in charge to store it.

During operation of the TOE the TSF_AUDIT is always enabled, and log events are created.

When the TSF_FFD function tested a presented finger, this function is called to create the log event.

TSF_AUDIT receives from TSF_FFD:

- Used values for security parameters,
- Date and time,
- Test result (spoof/no spoof),
- Start and end of functions involving FFD.

This function is also called by TSF_MANAGEMENT when the used security parameters are out of the accepted range.

This function returns the created audit event when MSO SDK forwards the request.

This function covers FAU_GEN.1: it creates a log event at every use of the TOE (spoof or real finger detected) or when security parameters are refused by TSF_MANAGEMENT. To authenticate the MSO corresponding to the log, the log event contains the MSO serial number.

8. APPENDIX

8.1 GLOSSARY

Term	Description
CC	Common Criteria - Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
FAR	False Acceptance Rate
FAR level	This parameter specifies how tight the matching threshold is. Depending on the application requirements, this threshold can be adjusted by the developer or administrator in order to have a more secure control (higher threshold, less false acceptances) or a more comfortable control (lower threshold, less false rejections).
PP	Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
ST	Security Target – A set of implementation-dependent security requirements for a specific TOE.
TOE	Target of Evaluation

8.2 REFERENCE DOCUMENTS

Designation	Reference	Title	Revision	Date
[R1]	CCMB-2006-09-001	Common Criteria for Information Technology Security Evaluation – ➢ Part 1: Introduction and general model ➢ Part 2: Security functional requirements ➢ Part 3: Security assurance requirements	Version 3.1, Revision 3	July 2009
[R2]	FSDPP_OSP	FingerPrint Spoof Detection Protection Profile based on Organisational Security Policies	Version 1.7	27 November 2009
[R3]	MorphoSmartProgrammers Guide	MorphoSmart Programmer's Guide	Version 3.3	Septembre 2011