Liveness Detection for Biometric Systems with Touch Sensor Protection Profile
LDBS_TS
V1.0

TURKISH STANDARDS INSTITUTION

Table of Content

1.PP INTRODUCTION

1.1 PP REFERENCE

Title	Liveness Detection for Biometric Systems with Touch Sensor Protection Profile
PP Version	6.0
Date	June 06, 2014
Author	Turkish Standards Institution
CC-Version	3.1(Release 4)
Keywords	Protection profile, biometric systems, liveness detection
Assurance Level	EAL 2+ (ALC_FLR.1)

1.2 PP OVERVIEW

Biometric systems use unique physical and/or behavioral characteristics of individuals. These characteristics are considered as private and secret. However, this assumption is not quite correct; one can steal any person’s fingerprints, face or iris images, voice recordings, even the DNA which are used as private features in the biometric systems. It is almost impossible to avoid our biometric features from capturing by unauthorized people. A biometric system has to be sensitive to spoofing attacks where a person tries to masquerade as another one by falsifying data and thereby gaining an illegitimate advantage. Therefore, a biometric system has to be capable of discriminating real human traits from fake traits i.e. silicon face masks, gummy fingers, organs taken from cadavers etc.

In order to develop security related testing criteria for biometric systems, a project has been initiated by the Turkish Standard Institute according to National Cyber Security Action Plan. This Protection Profile, which includes liveness detection for touch sensor based biometric systems, forms part of this project that has been conducted by the MEDALab in Yildiz Technical University.

The scope of this PP is to describe the functionality of a liveness detection systems in terms of CC and to define functional and assurance requirements for the evaluation of these systems. Chapter 2 gives the details of the TOE and its boundaries. Chapter 3 defines the conformance claims of the PP. In Chapter 4 security problems are identified. The security objectives of this PP are given in the Chapter 5. In Chapter 6 one extended is defined, and finally, the security requirements are discussed in Chapter 7.

2. TOE DESCRIPTION

The Target of Evaluation (TOE) described in this PP is a system which provides liveness detection either as part of or in front of a biometric system including fingerprint, palm print, vein, or any other touch sensor based recognition operation. The systems working with contactless sensors are omitted. The TOE determines whether the object evaluated by the system is alive or not. The term liveness means to be in a state of being alive; tissues cut off from a body are considered as not alive. Any TOE claiming conformance with this PP has to be include a liveness detection system.

2.1 TOE Functionality

The physical and logical structure of the TOE is dependent to vendors, but any biometric TOE should include following common processes:

Enrollment: The enrollment process introduces the users to the biometric system. During the enrollment, the system captures the biometrics of the users for the first time, then calculates and stores the features for future usage. If required, additional identification information of the user such as password, PIN code, ID number or similar data are provided to the system. The calculation and storage processes are out of scope of this PP. At this stage, an attacker could try to fake the system by using a fake biometric. The attacker does not need any information about the biometric characteristics of any other user.

Verification: Once a user has been enrolled to the system, he/she has to claim an identity to the system. The objective of the verification process is to verify the user’s claimed identity from the data stored during the enrollment. During verification, an attacker could try to use fake traits to mislead the biometric system to accept himself/herself as another person. For these kinds of attacks, the attacker needs to owe the biometric traits of the victim.

Identification: Identification is very similar to verification. However, during the identification process, the user does not claim any identity. Again, the attacker could use fake biometric traits to deceive the system. If the system finds a template in its database close enough to the proposed traits, the system accepts the attacker as a user.

To avoid attacks mentioned above, liveness detection on biometric data is very essential for security.
Liveness detection can be performed in a biometric device/system either at the acquisition stage or at the processing stage. It is generally performed into a system via three ways;

- By adding extra hardware. It is often expensive, cumbersome and not always as effective as we expect
- By using the information already captured by the device. It often needs extra hardware to extract life signs at the biometric data
- By using liveness information inherent to the biometric in question. It is very effective for biometric systems that perform iris recognition, facial thermogram measurements, gait recognition, body odor, etc. It is because that the outer layer of a finger (the epidermis) is

dead, there is no inherent liveness information. That’s why this technique can’t be applied to fingerprint recognition system.

There are some methods to detect liveness of biometrics. One of them is measuring the temperature of the proposed biometric. The temperature of the epidermis is about 26-30^{o} C. Using a thin silicone artificial fingerprint results in a decrease by a maximum of 2^{o}C of the temperature, while it transfers to the sensor. Obviously, it will not be difficult to have the temperature of the artificial fingerprint within the working tolerances of the sensor. Sensors that are used outdoors often have a wider working tolerance, giving the intruder even better prerequisites.

The pulse in the tip of the finger can be detected via pulse oximetry and used as liveness detection method, too. The pulse oximetry is widely used in the medical field to measure the oxygen saturation of a patient’s arterial blood. It also measures pulse rate. This device works based on two basic principles. One of them is that hemoglobin absorbs light differently at two different wavelengths depending on the degree of oxygenation. And the other one is that the fluctuating volume of arterial blood for each pulse beat adds a pulsatile component to absorption. By similar way blood pressure is a sign for liveness.

There can be derived more methods according to biometrics data used the system. In a system requiring a high security level, liveness detection is very important to help preventing direct attacks those carried out with synthetic traits, and very difficult to detect

2.2 TOE Environment and Boundary

A generalized block diagram of the TOE is given in the Fig. 1. This chapter gives the details of the physical and logical boundaries of the TOE.

The liveness detection system should be a part of the capturing device, a separate sensor or device, or a software application behind the capturing device, or even a mixture of these. The TOE has to decide whether a given trait is alive or not. The liveness detection sensor should be a separate sensor (or sensors), or the capturing device used in the biometric system. If separate sensors are used, the system has to be ensured that the same trait is evaluated by both processes.

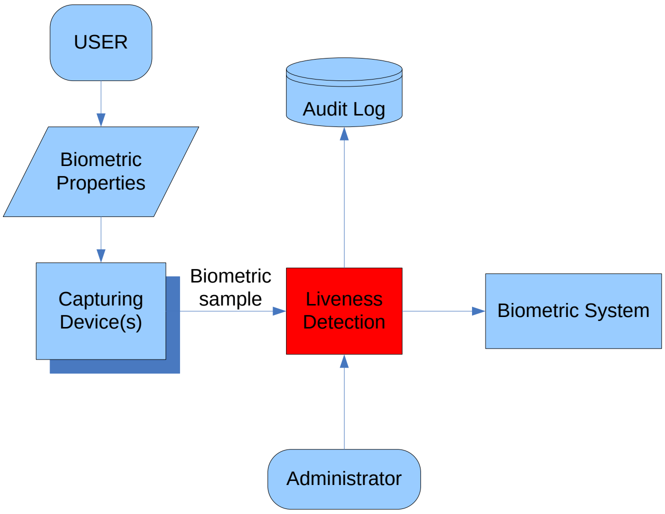

Figure 1. Block diagram of the TOE and its environment

If the TOE is physically separated from the biometric device, the communication between the TOE and the biometric device must be encrypted. The communication method must be able to detect whether the incoming data altered or not. Furthermore, the output of the TOE must be a yes/no decision. If the parts of TOE are physically separated, the sensor/capturing device may transfer the actual data through an untrusted media, but in this case, the data must be encrypted and cryptographically signed by the TOE. Once the yes/no decision is generated, it is out of scope of the TOE, hence the security of the decision information is left to the environment. The TOE must not be produce a confidence score which would need further processing by the environment.

The TOE shall be providing audit data. This data can be utilized to determine the quality assurance, statistics, or any related information. On the other hand, the TOE is not responsible for the storage, protection and processing the audit data. These functions are assumed to be realized by the environment.

This TOE does not require a second, non-biometric authentication mechanism.

3. CONFORMANCE CLAIMS

3.1 Conformance statement

Any PP claims conformance to this PP must be strictly conform this PP. Demonstrable conformances are not allowed.

3.2 CC Conformance Claims

- This PP has been developed by using Common Criteria Ver. 3.1.
- The conformance of this Protection Profile is Common Criteria Part II. 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 PP.

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

The external entities interacting with the TOE are the administrator and the user. The administrator has the right to use the administrative, maintenance and configuration functions of the TOE. The administrator is also responsible of the installation of the TOE. The user is a person who interacts with the biometric system protected by the TOE in the means of enrollment, identification, and verification.

4.1 External Entities

TOE Administrator: The TOE administrator is authorised to perform the 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 also more than one administrative role.

User: A person who wants access to the portal, which is protected by a biometric system
Authorised user: An enrolled user with an assigned identity.
Unauthorised user: A not enrolled user.
Attacker: An attacker is any individual who is attempting to subvert the operation of the biometric system. The intention may be to gain unauthorized access to the assets protected by the

system.
Biometric Sample: A biometric data to enroll and store

Capturing Devices: The capturing device enables to capture

4.2. Assests

The following assets are clasified in the context of this Protection Profile

Major Assests: The major scope of the

biometric liveness 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 major asset for the TOE.
For example;The decision taken by TOE(spoofed /genuine) can be considered being major assest.
Secondary Assests: Secondary assets are functionalities which are used by the TOE to

provide its basic services and which will need to be protected. The

following assets should be explicitly mentioned for the TOE:

- **Liveness Detection Parameters:** the parameters may be specific for claimed identity including temparature limits,general threshold,typical movements patterns..etc.The integrity and confidentiality of these parameters will have to be protected.
- **Liveness Evidence :** This data is acquired by the capture device and/or additional sensor devices for the purpose of liveness detection. The TOE decides about a biometric sample being a fake or not based on this data. The integrity and confidentiality of this data have to be protected.
- **Audit Data:** This data includes the audit information(fake or not) that is generated by the TOE. The integrity, confidentiality and authenticity of the information has to be protected.

4.3. Assumptions

A.BIO : The TOE described in this PP is a protecting mechanism for a biometric system. The TOE's responsibility is to perform liveness detection. Hence, all other threats are assumed to be handled by the biometric system protected by the TOE.

A.OPERATING_RANGE: The TOE is assumed to be placed in an environment that does not exceed its normal operating range (e.g. supply voltage, temperature, humidity etc.) as defined by the vendor.

4.4. Threats

T.ADMIN_ERROR: An administrator may configure the TOE resulting in ineffective security mechanism (e.g. giving a wrong threshold level) incidentally.

T.BYPASS: An attacker may bypass the TOE, and cheats the protected biometric system with artificially created samples.

4.5. Security Policies

P.LIVENESS_DETECTION: The TOE shall be able to detect whether a presented trait is live or not.

P.AUDIT: The TOE shall produce audit data for

a. Generating statistics to adjust the parameters for better quality.

b. Chasing the attacks.

c. Tracking the modifications made by the administrators.

P.MANAGEMENT: The TOE shall provide the management functionalities for the modification of security relevant parameters. These functionalities shall reject non-valid or insecure values for these parameters.

5. SECURITY OBJECTIVES

This chapter is dedicated to security objectives both for the TOE and its environment.

5.1. Security Objectives of the TOE

O.LIVENESS-DETECTION: The TOE must detect whether a presented entity is alive or not. The liveness decision may be given by using the data taken from the biometric sensor, or by using separate sensors dedicated to liveness detection only.

O.AUDIT: The TOE will be able to generate audit data. An audit data must be produced when;

i. A non-alive entity has been presented to the TOE

ii. An alive entity has been presented to the TOE

iii. Any management function has been used.

O.MANAGEMENT: The TOE must provide the necessary management functions for the security related parameters of the TOE. Usage of these functions must be restricted by the administrator. The management functions must accept only valid values for the security related parameters to prevent the TOE from malfunctioning.

O.SELF_PROTECTION: The TOE must provide necessary functionalities to protect itself from external intervention and bypassing.

5.2. Security Objectives for the Operational Environment

OE.ADMINISTRATION: The administrators who have the access rights of the TOE are well trained and trusted. They have all the necessary documents related to the TOE, read them carefully and have the ability to apply the required operations. The administrator is responsible for the maintenance and installation of the TOE and its platform. The administrator must check and ensure the environmental requirements of the TOE (lighting, supply voltage, temperature etc.) are met. The administrator is responsible for the periodically checking of audit recordings in order to detect and prevent attacks.

OE.PHYSICAL: The physical access of the TOE and the platform must be under control and only the administrator must have the full access to the TOE and its components. The TOE and its components must be protected physical intervention.

OE.BIO: The biometric device protected by the TOE must handle any security threat except the liveness detection. The biometric device must use the functionality of the TOE for the liveness detection only.

OE.PLATFORM: The platform which the TOE runs on must provide the necessary services for the TOE. These functions will be provided by the platform:

i. Identification and authentication of the administrator.

ii. Protection of the management functions of the TOE from the unauthorized users.

iii. Providing the access control of the assets and the software part (if available) of the TOE.

iv. Providing a secure communication channel and storage for the security related data transferred to or from the TOE.

v. Providing storage and review functionalities of audit data and providing the security of audit data.

vi. Providing the time stamp for the TOE and audit data.

vii. Providing a secure environment free from any kind of malicious software.

5.3. Rationales

5.3.1. Rationale for the Assumptions

i. A.BIO is covered by security objective OE.BIO.

ii. A.OPERATING_RANGE is covered by security objective OE.ADMINISTRATION. The administrator must check and ensure the environmental requirements of the TOE (lighting, supply voltage, temperature etc.) are met.

5.3.2 Rationale for the Threats

i. T.ADMIN_ERROR is covered by security objective O.MANAGEMENT. O.MANAGEMENT is supported by OE.ADMINISTRATION. O.MANAGEMENT provides the necessary management functions for the security related parameters of the TOE. The management functions accept only valid values for the security related parameters to prevent the TOE from malfunctioning. OE.ADMINISTRATION ensures that the administrator has the necessary documents related to the TOE, read them carefully and has the ability to apply the required operations.

ii. T.BYPASS is covered by the security objective O.SELF_PROTECTION. O.SELF_PROTECTION provides the necessary functionalities for self-testing against intervention and bypassing. OE.PLATFORM supports the O.SELF_PROTECTION by providing the access control of the assets of the TOE.

THREATS		ASSUMPTIONS	
T.ADMIN_ERROR	T.BYPASS	A.BIO	A.OPERATING_RANGE

Security Objectives of TOE	O.LIVENESS-DETECTION				
	O.AUDIT				
	O.MANAGEMENT	X			
	O.SELF_PROTECTION		X		
Security Objectives for Operational Environment	OE.ADMINISTRATION	X			X
	OE.PHYSICAL				
	OE.BIO			X	
	OE.PLATFORM		X		

5.3.3. Rationale for the Security Policies

P.LIVENESS_DETECTION : It is covered by security objective O.LIVENESS_DETECTION, supported by O.MANAGEMENT, OE.ADMINISTRATION, OE.PHYSICAL and OE.PLATFORM. O.LIVENESS_DETECTION detects whether a presented entity is alive or not. Hence, any artificial biometric trait presented to the system will be detected by the TOE. O.MANAGEMENT provides the necessary management functions for the security related parameters of the TOE. Usage of these functions is restricted by the administrator. The management functions accept only valid values for the security related parameters to prevent the TOE from malfunctioning. OE.ADMINISTRATION ensures that the administrator is well trained, has the ability to apply the required operations and ensures the environmental requirements of the TOE. OE.PHYSICAL protects the TOE from physical interventions. OE.PLATFORM ensures that the TOE management functions are protected, the communication channel is secured and audit data are stored securely. OE.PLATFORM also ensures the protection from any kind of malware.

P.AUDIT : It is covered by security objective O.AUDIT which supported by OE.ADMINISTRATION and OE.PLATFORM. O.AUDIT ensures that the TOE has the ability of generating audit data. OE.ADMINISTRATION ensures the periodically checking of audit recordings. OE.PLATFORM provides storage, security and review functionalities of audit data. OE.PLATFORM provides the time stamp for the audit data.

P.MANAGEMENT : It is covered by the security objective O.MANAGEMENT, which is supported by OE.ADMINISTRATION, OE.PHYSICAL and OE.PLATFORM. O.MANAGEMENT ensures that the TOE provides the necessary management functions for the security related parameters of the TOE. OE.ADMINISTRATOR guaranties that the administrator is well trained and non-hostile so that misconfiguration is prevented. OE.PHYSICAL ensures that the physical access to the TOE is under control, so that management functions cannot altered by physical attacks. OE.PLATFORM ensures that the management functions of the TOE are protected from the unauthorized users.

	O.LIVENESS-DETECTION	O.AUDIT	O.MANAGEMENT	O.SELF_PROTECTION	OE.ADMINISTRATION	OE.PHYSICAL	OE.BIO	OE.PLATFORM
P.LIVENESS_DETECTION	X		X		X	X		X
P.AUDIT		X			X			X
P.MANAGEMENT			X		X	X		X

6. EXTENDED COMPONENT DEFINITION

The extended functional family FPT_LIVD (Liveness 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 the biometric device, which is protected by the TOE, from attempt to fake it with artificial or dead biometric samples. 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_LIVD Liveness Detection

Family behavior

This family defines functional requirements to detect whether a biometric sample is alive or not.

Component leveling:

FPT_LIVD Liveness Detection

1

FPT_LIVD Liveness Detection 1

FPT_LIVD.1 Liveness Detection has four elements:

FPT_LIVD.1.1 FPT_LIVD.1.1 requires to provide liveness detection functionality for a specific biometric sample.

FPT_LIVD.1.2 FPT_LIVD.1.2 defines actions to be performed if a non-alive biometric sample is detected.

FPT_LIVD.1.3 FPT_LIVD.1.3 defines actions to be performed if a genuine biometric sample is detected.

FPT_LIVD.1.4 FPT_LIVD.1.4 defines additional information returned with the feedback about liveness status.

Management: FPT_LIVD.1

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

a) Management of the parameters used for liveness detection.

Audit: FPT_LIVD.1

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

a) Basic: non-alive sample detected

b) Basic: alive sample detected

6.1.1 Liveness Detection (FPT_LIVD.1)

FPT_LIVD.1 Liveness Detection

FPT_LIVD.1.1 The TSF shall be able to detect whether a presented [assignment: biometric sample] is alive or not.

FPT_LIVD.1.2 If a non-alive biometric sample is detected, the following action(s) shall be performed:

- [assignment: list of actions]

FPT_LIVD.1.3 If an alive biometric sample is detected, the following action(s) shall be performed:

- [assignment: list of actions]

FPT_LIVD.1.4 Along with the feedback about the liveness status of the presented biometric sample 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_LIVD

Liveness detection functionality describes mechanisms that protect biometric systems against threats of non-genuine biometric characteristics like fake fingers, fake faces etc. Hence, it provides protection of the TSF which is subject of the functional class FPT. There is no family in FPT that deals with detection of liveness detection functionality, therefore a new family has been defined.

7. SECURITY REQUIREMENTS

This section describes the security functional and the assurance requirements of this PP.

7.1. Security Functional Requirements

Table 6.1. summarizes the SFRs of this PP.

FAU_GEN.1	Audit Data Generation
FDP_RIP.2	Full residual information protection
FMT_MTD.3	Secure TSF data
FMT_SMF.1	Specification of management functions

7.1.1. Security Audit (FAU)

i. 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 to audit the following events:

- Start-up and shutdown of the audit functions
- All auditable events for the [basic] level of the audit
- [assignment: other specifically defined audible events]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success of failure) of the event (if applicable)
- 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 fake biometric has been detected (FPT_LIVD.1)

● A use of the TOE where a genuine biometric has been detected (FPT_LIVD.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)

i. 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)

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 liveness 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 liveness detection parameters) represents the minimum set of parameters which ensures the security of the TOE. On the other hand, the security objective O.MANAGEMENT requires that the TOE has to ensure secure values for all security relevant parameters. The list of these parameters depends on the structure and the technology of the TOE, hence the ST author shall add all security relevant parameters to this assignment.

Specificaton 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 other components

7.2. Security Assurance Requirements

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 spesification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user's 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_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements

	ASE_TSS.1	TOE summary specification
Testss	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample

ASE_OBJ.1 eklenebilir mi???? Gerekli mi??

7.3. Security Requiremets 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

- 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 liveness detection parameters so that the detection process works correctly.

- FMT_SMF.1 ensures that the TOE provides the necessary management functionality

O.LIVENESS_DETECTION

- FPT_LIVD.1 defines that the TOE is able to detect whether a presented biometric is alive or not 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	None	None
FMT_MTD.3	FMT_MTD.1	See chapter 7.3.1.3
FMT_SMF.1	None	None
FPT_LIVD.1	FMT_MTD.3, FMT_SMF.1	FMT_MTD.3, FMT_SMF.1

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.

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	None
Life-cycle support	ALC_CMC.2	ALC_CMS.1	ALC_CMS.2
	ALC_CMS.2	No dependencies	None
	ALC_DEL.1	No dependencies	None
	ALC_FLR.1	No dependencies	None
Security Target Evaluation	ASE_CCL.1	ASE_INT.1, ASE_ECD.1,	ASE_INT.1, ASE_ECD.1,

		ASE_REQ.1	ASE_REQ.2
	ASE_ECD.1	No dependencies	None
	ASE_INT.1	No dependencies	None
	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	None
	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

8.ACRONYMS

9.BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012