Palm n’ Go - Ezio

Security Target

Common Criteria: EAL1

Version 1.3

16-MAY-11

Document management

Document identification

Document ID	MMU_EAL1_ASE
Document title	Multimedia University Palm n' Go - Ezio Security Target
Product version	Version 1.0

Document history

Version	Date	Description
0.1	19-JUL-10	Release for internal review.
0.2	23-JUL-10	Updated to address internal comments
0.3	26-OCT-10	Addressed EOR from Evaluation Facility
1.0	27-DEC-10	Release for final ETR.
1.1	17-MAR-11	Update TOE name to Palm n' Go - Ezio
1.2	28-MAR-11	Update version for Palm n' Go – Ezio
1.3	16-MAY-11	Minor update

Table of Contents

1 Security Target introduction (ASE_INT)

1.1 ST and TOE identification

ST Title	Multimedia University Palm n' Go - Ezio Security Target
ST Reference	MMU_EAL1_ASE
ST Version	1.3, 16-MAY-11
TOE Reference	Multimedia University Palm n' Go - Ezio (Version 1.0)
Assurance Level	EAL1
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1, July 2009, incorporating: • Part One – Introduction and General Model, Revision Three, July 2009. • Part Two – Security Functional Components, Revision Three, July 2009. • Part Three – Security Assurance Components, Revision Three, July 2009. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004

1.2 Document organization

This document is organized into the following sections:

- Section 1 provides the introductory material for the ST as well as the TOE description including the physical and logical scope of the TOE.
- Section 2 provides the conformance claims for the evaluation.
- Section 3 defines the security objectives for the environment.
- Section 4 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.

- Section 5 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE.

- Section 6 provides key terms and definitions.

1.3 TOE Overview

1.3.1 TOE type and usage

The TOE is **Palm n' Go** - **Ezio** and is referred to as **Palm n' Go** in this document. The TOE is a touch-less palm vein authentication application developed using MMU's SDK[1] called EzioSDK. EzioSDK is a software development kit (software) and it is meant to be used by application developers to build a fully working biometric system.

The TOE provides a the ability to verify a claimed identity of a human being using their *palm vein pattern* as a unique characteristic of their body thus controlling access to a portal[2]. The Portal and everything beyond the portal and the activation of the portal is out of the scope of the TOE.

The TOE works in verification mode. Biometric Identification is not addressed by the TOE. Furthermore the enrolment process is out of scope of this ST and it is assumed that all authorized users have been enrolled.

The TOE also has a non-biometric mechanism to identify and authenticate an administrator of the TOE to enforce an access control to the management functions of the TOE.

1.3.2 Description of biometric processes

The core functionality of biometric systems can be divided into three processes: ***enrolment***, ***biometric verification*** and ***biometric identification***.

The biometric enrolment and identification are not addressed by the TOE. They are introduced for the interested reader in the following subchapters. Because of the different use of the words identification and authentication this section clarifies the use of these words in context of this **Security Target**.

[1] A software development kit is typically a set of development tools that allows for the creation of applications for a certain software package

[2] Portal: The physical or logical point beyond which information or assets are protected by a biometric system. With failed verification, the portal is closed for the user. Via successful verification, the portal is open. Therefore, only two allowed states are possible after biometric verification: failed or successful. The converting from a biometric probabilistic message into a Boolean value is part of the TOE. Everything beyond the portal and the activation of the portal is out of the scope of the TOE.

Enrolment

Usually, the enrolment process is the first contact of a user with a biometric system. This process is necessary because a biometric verification system has to 'learn' to verify the identity of each user based on their biometric characteristic.

During the enrolment process the system captures the biometric characteristic of a user and extracts the features it is working with. This feature vector is then combined with the identity of the user to a biometric reference and stored in a database.

The quality of the biometric reference has to be assured and quality proofed. In the case of inadequate biometric characteristics or lower reference quality, the person to be enrolled has to repeat the process or is not possible to be enrolled. Additionally, it is useful to be able to update a user biometric reference considering possible physiology changes. Only an administrator should be allowed to start the enrolment process. He has to observe the whole process to ensure a correct enrolment. Furthermore, the administrator has to ensure that the user claims his correct identity to the system during the enrolment process.

Biometric Verification

The verification process is the major functionality of a biometric system in context of this ST. Its objective is to verify or refuse a claimed identity of a user.

Therefore the user has to claim an identity to the system. The system gets the biometric reference associated with this identity from the database and captures the biometric characteristic of the user. If the Biometric Live Record (BLR) that is extracted from the characteristic and the biometric reference from the database are similar enough, the claimed identity of the user is verified.

Otherwise or if no biometric reference was found for the user, the claimed identity is refused. The matching component of a biometric system that decides whether a biometric reference and BLR are similar enough usually uses a threshold value for this decision that can be configured by an administrator. If the matcher finds that the BLR and the biometric reference are more similar than demanded by the threshold, it returns successful verification, otherwise failed verification.

Biometric Identification

The objective of a biometric identification process is quite 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 biometric characteristic of a user and compares it to all biometric references in the database. If at least one biometric reference is found to be similar enough, the system returns this as the found (and verified) identity of the user. Biometric identification systems introduce many additional issues in the

context of security evaluations. The possibility to find more than one biometric reference that matches or the higher error rates of those systems are only two of them.

1.3.3 Common Criteria context

In context of Common Criteria, identification usually means the statement of a claimed identity while authentication means the confirmation of this identity. In context of biometric technology identification usually means a process as described in section 1.3.2. Because biometric identification is out scope of this ST there should not be a conflict in wording. To avoid any misunderstanding: the wording in this ST is as follows:

- Identification: As defined in Common Criteria
- Authentication: As defined in Common Criteria
- Verification: biometric verification as described in chapter 1.3.2

1.3.4 TOE security functions

The following table highlights the range of security functions and features implemented by the TOE.

Security function	Description
Auditing	The TOE captures the success/failures of user verification and the success/failure of the TOE administrator verification. Note that an application that uses the TOE can use this information for audit review.
Identification and Authentication	This is the main security functionality of the TOE. The TOE can verify the claimed identity of a user by using their *palm vein pattern as* a unique characteristic of their body. Administrator of the TOE needs to be identified and authenticated by the TOE. This is provided by a non-biometric mechanism provided by the TOE.
Security Management	The TOE provides security management functions such as management of user, sensitivity of the capture device, etc to the TOE administrator.

1.4 TOE Description

1.4.1 Physical scope of the TOE

The TOE comprises the Palm n' Go - Ezio application. The capture device shown in Figure 1 is Palm Vein Scanner, version 1.0 developed by MMU. Other infrared vein scanner/camera maybe used as long as it supported by Microsoft DirectX SDK and able to provide hand vein image.

The TOE is installed on a Windows-based operating system with Microsoft .NET framework and underlying suitable hardware. The underlying operating system provides reliable timestamps to the TOE.

The following software components are required to support the TOE:

- Microsoft Visual Studio 2010 (or Version 10)
- Microsoft .NET framework Version 4.0
- Operating system: Windows XP/Vista/7

The TOE requires the support of an SQL database. The TOE will output a result upon an authentication is performed as well as outputting the audit data to an external application. This application can be developed by the users of the TOE to control an access to a portal based on the authentication mechanism provided by the TOE. The scope of the TOE can be found in Figure 1 below and identifies the various components of the Palm n' Go - Ezio.

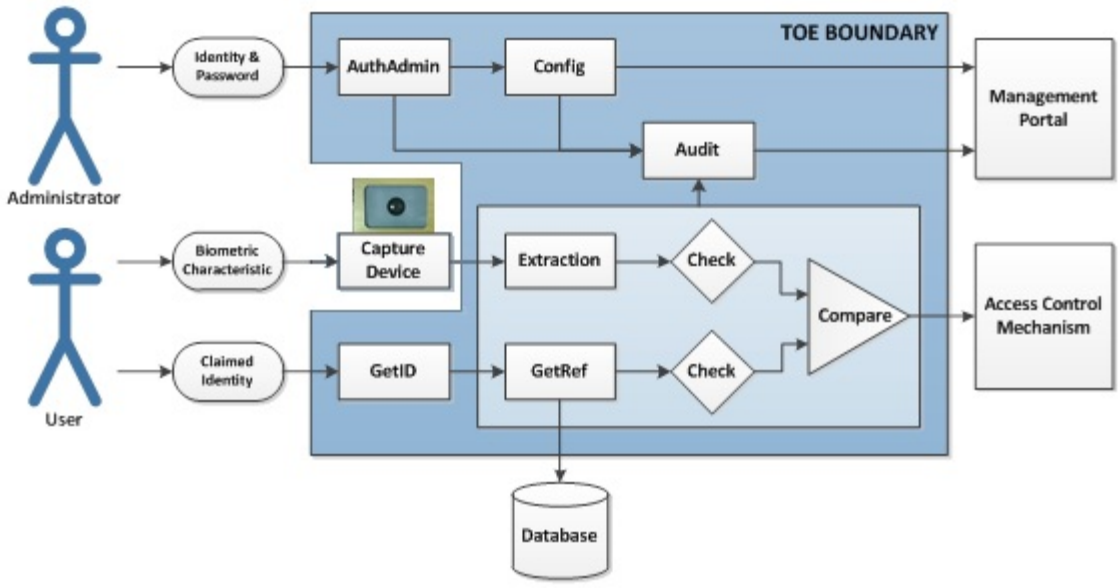

Figure 1 – Palm N' Go design

The following table describes each of the components of the TOE specified in Figure 1 above.

Components	Description
GetID	This component is responsible for getting the user's claimed identity. Its functionality is security relevant because the system uses the claimed ID to determine, which biometric reference has to be used for comparison. Furthermore, this component provides a mandatory user visible interface.
Capture Device	An infrared vein scanner/camera that supports Microsoft DirectX SDK and able to provide a digital representation of a hand vein image.
GetRef	This component is responsible for getting the stored (already enrolled) biometric reference related to a claimed user's identity.
Check	This component ensures the minimum quality requirements regarding the biometric references. It can be differentiated into integrity and authenticity check during the process of getting the biometric reference as well as the quality check of the biometric information during the processing of the live biometric characteristics.
AuthAdmin	This component is responsible for identification and authentication of the administrator with other means than the biometric verification mechanism itself. This mechanism is a classical identification and authentication component that is realized through a password based mechanism. Authentication of the TOE administrator needs to be successful before he is allowed to configure security relevant settings of the TOE.
Configure	This component provides an interface for the administrator to set security relevant TOE parameters. This component is especially used to configure the threshold setting for the comparator component and to determine audit events.

Components	Description
Compare	This is an important component regarding the scope of this ST. It compares the enrolled biometric reference with the Biometric Live Record (BLR) and includes the determination whether these records match or not. It produces a value that shows how well the biometric reference and BLR match. To get a successful/failed return value from the biometric system, the comparator considers a threshold during the matching process. If the biometric reference and the BLR are more similar than demanded by the threshold, the return value is success, otherwise it is fail. An “Exact match” comparison will result in a positive verification and is recorded in the audit log.
Audit	This component of the TOE records security relevant events to ensure that information exists to support effective security management.

The following table describes each of the components of the environment specified in Figure 1 above.

Components (Environment)	Description
Management Portal	The management portal provides the environment in which the Administrator can view audit records and also access configuration data for the TOE. The Management Portal provides a policy management environment for the TOE.
Database	The environment has to provide a database to be used by the TOE. This is used to store the biometric reference of a user but it can be used to store additional information too. The TOE supports the use of any SQL databases.
Access Control Mechanism	The physical or logical point beyond which information or assets are protected by a biometric system is controlled by the TOE environment policy management, which gets the verification results (verification "failed" or "successful") related to the user identity from the TOE. The access control mechanisms are not within the scope of the evaluation.

1.4.2 Logical scope of the TOE

The logical boundary consists of the security functionality of TOE and is summarized below.

1.4.2.1 Identification & Authentication

The users enter their user ID and have their palm vein patterns to be taken by the capture device. The TOE gets the user ID and references it to the database to get the enrolled biometric reference and compares it to the BLR (the TOE will use the pictures of the vein patterns taken by the capture device and converts them to a binary string. This is the BLR). If it matches, it is a positive verification of the user.

A separated verification mechanism is provided by the TOE to TOE administrator. TOE administrator has to enter their user ID and a password to the TOE. The TOE will then identify and authenticate the TOE administrator and he/she will get access to security management functions of the TOE.

1.4.2.2 Auditing

The TOE records security relevant events such as the success/failure of biometric and non-biometric verification mechanisms, changing of administrator password and startup and shutdown of the audit function.

1.4.2.3 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE:

- User management;
- Sensitivity of the capture device;
- Threshold of the comparator in the TOE;
- Number of pictures taken by the capture device needed to generate the BLR.

The TOE maintains two roles within the TOE to ensure that the functions are restricted to only the TOE administrator. The roles maintained by the TOE are users and administrator. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

2 Conformance Claim (ASE_CCL)

The ST and TOE are conformant to version 3.1 (Revision 3) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- Part 2 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, Revision 3, July 2009.
- Part 3 conformant, EAL1 Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 3, July 2009.

3 Security objectives (ASE_OBJ)

3.1 Overview

The security objectives at an EAL1 level of assurance include concise statements of the objectives to be achieved by the supporting environment.

3.2 Security objectives for the operational environment

Identifier	Objective statements
OE.ADMINISTRATION	It has to be ensured that the TOE administrator is well trained and non-hostile. He has to read the guidance documentation carefully, completely understand and apply it. The TOE administrator shall be responsible for the installation and configuration of the TOE
OE.ENVIRONMENT	The TOE operating environment shall provide adequate infrastructure and hardware for the operation of the software components of the TOE, specifically, the operating environment shall provide: • a database for the biometric references of enrolled users; • reliable time stamps for the TOE to support generation of audit records
OE.ENROLMENT	The enrolment shall be already performed and therefore, the biometric reference for each authorized user is given. The generated references shall be of sufficient quality and linked to the correct user. Additionally, all biometric references shall be stored in a way that ensures the authenticity and integrity of this data.
OE.PHYSICAL	The TOE and its components shall be physically protected against unauthorized access or destruction. Physical access to the hardware that is used by the TOE may only be allowed for authorized administrators. This may not cover the capture device that has to be accessible for every user.

4 Security requirements (ASE_REQ)

4.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

4.2 SFR conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

4.3 Security functional requirements

4.3.1 Overview

The security functional requirements are expressed using the notation stated in Section 4.2 and summarized in the table below.

Identifier	Title
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behaviour
FMT.MTD.1	Management of TSF data
FMT.MTD.3	Secure TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles

4.3.2 FAU_GEN.1 Audit Data Generation

Hierarchical to:	No other components.
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [***not specified***] level of audit; and c) [**the following auditable events:** **i. User authentication** **ii. Changing the sensitivity settings of the capture device** **iii. Changing the threshold of the comparator** **iv. Changing the number of pictures of the palm vein the capture device take** **v. Enrolment of users** **vi. Creation and deletion of users** **vii. Turning and switching off audit mechanism, Clearing audit records; and** **viii. Administrator authentication**].
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, [**i. date,** **ii. time, and** **iii. user or TOE administrator identity**].
Dependencies:	FPT_STM.1
Notes:	There is only 1 administrator for the TOE. The ID and password of the administrator is set during the installation or 1st run of the application.

4.3.3 FAU_GEN.2 User identity association

Hierarchical to:	No other components.

FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
Notes:	None.

4.3.4 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**a) User ID,** **b) Authentication reference (either Biometric reference and/or Administrator password)**].
Dependencies:	No dependencies
Notes:	None.

4.3.5 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2a.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.3.6 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to:	No other components.
FIA_UAU.5.1	The TSF shall provide [**a) a biometric verification mechanism for users, and** **b) a non-biometric verification mechanism for administrators**] to support user authentication.

FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the [**following rules:** **a) users shall be authenticated using the biometric verification mechanism, and** **b) administrator shall be authenticated using the non-biometric verification mechanism**].
Dependencies:	No dependencies
Notes:	None.

4.3.7 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2a.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies
Notes:	None.

4.3.8 FMT_MOF.1 Management of security function behaviour

Hierarchical to:	No other components.
FMT_MOF.1.1	The TSF shall restrict the ability to [***determine the behaviour of, disable, enable, modify the behaviour of***] the functions [**Audit Mechanism**] to [**TOE administrator**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

4.3.9 FMT_MTD.1 Management of TSF data

Hierarchical to:	No other components.
FMT_MTD.1.1	The TSF shall restrict the ability to [***change_default, query, modify, delete, clear***] the [**a) sensitivity of the capture device,** **b) number of pictures of palm veins taken by the capture device,** **c) threshold of the comparator** **d) user ID,** **e) role,** **f) user binary string, and** **g) administrator password**] to [**TOE administrator**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

4.3.10 FMT_MTD.3 Secure TSF data

Hierarchical to:	No other components.
FMT_MTD.3.1	The TSF shall ensure that only secure values are accepted for [**a) biometric reference records,** **b) sensitivity of the capture device,** **c) number of pictures of palm veins taken by the capture device, and** **d) threshold of the comparator**].
Dependencies:	FMT_MTD.1 Management of TSF data
Notes:	None.

4.3.11 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**users, TOE administrator**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.3.12 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**a) changing the sensitivity settings of the capture device,** **b) changing the threshold of the comparator,** **c) changing the number of pictures of the palm vein the capture device take,** **d) enrolment of users,** **e) creation and deletion of users, and** **f) turning on and switching off the audit mechanism**]
Dependencies:	No dependencies.
Notes:	None.

4.4 Dependency analysis

SFR	Dependency	Inclusion
FAU_GEN.1	FPT_STM.1 Reliable time stamps	See section 4.4.1
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	FIA_UID.2 FIA_UID.2 FIA_GEN.1
FIA_ATD.1	No dependencies.	None.
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UAU.5	No dependencies.	None.
FIA_UID.2	No dependencies.	None.
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT.MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT.MTD.3	FMT_MTD.1 Management of TSF data	FMT_MTD.1
FMT_SMF.1	No dependencies.	None.
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2, FIA_UID.2

4.5 Rationale for not addressing all 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.ENVIRONMENT).

4.6 TOE security assurance requirements

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 1 (EAL1).

Assurance class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.1 TOE CM coverage
	ALC_CMC.1 Labelling of the TOE
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing – conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

5 TOE summary specification (ASE_TSS)

5.1 Overview

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

The TOE security functions include the following:

- **Identification and Authentication:** The TOE provides biometric verification mechanism for users as well as provides non-biometric verification mechanism for administrator only.
- **Auditing:** The TOE generates audit events like the success or failures of user and administrator authentications as well as the startup and shutdown of audit mechanism.
- **Security Management**: The TOE provides TOE administrators with the capabilities to perform management functions.

5.2 Identification and Authentication

User will first identify himself by entering a user ID. This can be done by a keypad system or touch screen user interface that will be handled by the application developer using the TOE. The TOE will use the user ID and check the database to get the biometric reference of that user (FIA_UID.2).

The biometric raw data (palm vein patterns) of the user is read by the capture device and then sent it will be sent to the TOE. The TOE processes the raw data and converts it into a binary string format and compares the result with the biometric reference as retrieved from the database using the user ID as reference previously. This can be used by the application developer to display the information to the users. The result of the comparison (authentication successful or not) is returned to the application, which can then decide to allow further actions to the user (FIA_UAU.2).

The TOE also provides another verification mechanism to the TOE administrator. Administrator will first identify himself by entering a user ID. This can be done by a keypad system or touch screen user interface that will be handled by the application developer using the TOE. The TOE will use the user ID and check the database to get the password reference of the administrator (FIA_UID.2).

The administrator will enter his password and the TOE compares the password with the password reference as retrieved from the database using the user ID as reference previously. Only after a

successful verification of the TOE administrator will the TOE allows the access to the management functions of the TOE (FIA_UAU.2).

Other functional requirements satisfied: FIA_ATD.1, FIA_UAU.5.

5.3 Auditing

The TOE records the following events: (FAU_GEN.1)

- Start-up and shutdown of the audit functions
- User authentication
- Changing the sensitivity settings of the capture device
- Changing the threshold of the comparator
- Changing the number of pictures of the palm vein the capture device take
- Enrolment of users
- Creation and deletion of users
- Turning and switching off audit mechanism , clearing audit records; and
- Administrator authentication

All the events are recorded with the time, identify of the users, type of event, success and failure of the events (FAU_GEN.1, FAU_GEN.2). Upon receiving any of the above events, the TOE will generate an audit record. Timestamps are provided by the underlying operating system. Audit records will be stored in the database.

The TOE generates audit records in the database can then be used by an application developer to build an application for audit review.

5.4 Security Management

The TOE only allows only the TOE administrator to have access to the following security management functions (FMT_SMR.1, SMT_SMF.1, FMT_MOF.1, FMT_MTD.1, FMT_MTD.3):

- **Changing the sensitivity settings of the capture device:** this setting deals with the quality of the picture taken by the infra-red camera of the vein patterns. The default value for this is 5.

- **Changing the threshold of the comparator:** this setting deals with the threshold of the comparator. A high threshold level will result in a lower False Acceptance Rate and higher False Rejection Rate and vice versa. Administrator will need to configure this according to the requirements of the organization that uses the TOE and the application. The default value for this is5.

- **Changing the number of pictures of the palm vein the capture device takes:** this setting deal with the number of pictures the extraction engine of the TOE takes to form the binary string for the biometric reference. More pictures will result in a better quality biometric reference and vice versa. The default value for this is 3.

- **Enrolment of users:** enrolment of user can only be carried out in front of the administrator. The user will enter his biometric reference to the system and it will be stored into the database.

- **Creation and deletion of users:** administrator can create new user Ids as well as deletion of users from the system.

- **Turning and switching off audit mechanism:** The audit mechanism can be turned off and on by the administrator.

Access to these functions will only be available after the user has successfully identified and authenticate himself/herself through the password authentication mechanism.

6 Glossary

Term	Description
Attacker	An attacker is any individual who is attempting to subvert the operation of the biometric system. The intention may be either to subsequently gain illegal entry to the portal or to deny entry to legitimate users
Attempt	The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.
Authentication	Determination of authenticity; confirmation of the identity of a user. Generic term for the processes of the identification and verification
Biometric	A measurable physical characteristic or personal behavioural trait used to recognise the identity of a user or verify a claimed identity.
Biometrics biometric recognition	automated recognition of individuals based on their behavioural and biological characteristics
Biometric data	Extracted information taken from a biometric sample and used either to build a biometric reference on enrolment, or to compare against a previously created reference.
Biometric feature	A representation from a biometric sample extracted by the extraction system.
Biometric reference	one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison
Biometric Reference Record (BRR)	An object containing a Biometric Reference

Term	Description
Biometric sample	analog or digital representation of biometric characteristics prior to biometric feature extraction and obtained from a biometric capture device or biometric capture subsystem
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.
BLR	Biometric Live Record - includes the actual biometric data (actual biometric characteristic and user identity) to be verified against the biometric reference record.
Brute Force Attack	A brute force attack is an attack that requires trying all or a large fraction of all possible values until the right value is found.
Comparison	The process of comparing biometric data with a previously stored biometric reference
FAR	False Accept Rate (FAR) - proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed
FRR	False Rejection Rate (FRR) - proportion of verification transactions with truthful claims of identity that are incorrectly denied
Identification system	Biometric system that provides an identification function (see also identification)
LAN	Local Area Network
Live processing	Direct enrolment/identification of potential users via the normal biometric capture process

Term	Description
Matching Score	A measure of similarity or dissimilarity between the biometric data and a stored template, used in the comparison process
Portal	The physical or logical point beyond which information or assets are protected by a biometric system.
Replay attack	An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of an impostor attack.
Sensor	The physical hardware device used for biometric capture. Also called capture device
SmartCard	A credit card sized chip card with embedded integrated circuits. Often used to store keys for authentication.
Threshold	A parametric value used to convert a matching score to a decision.