1 ST introduction

1.1 ST reference

Title	Security Target for E-Jari version 4.0
Version	V0.24
Date	2010-12-03
Author	Neural

1.2 TOE reference

The TOE (E-Jari version 4.0) is identified by the combination of its hardware and its software identifiers.

The software identifier of the TOE is **E-Jari version 4.0.**

The hardware identifier of the TOE is **NM4000**.

The TOE should be verified as follows: As shown in the picture, at power-up, the TOE displays the software identifier in the top line of the LCD display. The hardware identifier can be found in the top right. Both must match to the identifiers above or it is not the evaluated version.

Figure 1: TOE identifiers

1.3 ST Overview

The scope of this Security Target is to describe the functionality of a biometric verification (fingerprint) system in terms of [CC] and to define functional and assurance requirements for this system.

In this context the major scope of a biometric verification system is to verify or reject the claimed identity of a human being using unique characteristics of his body: his fingerprint.

Please note that inside this Security Target the enrolment and the identification process of a biometric system (see also the section “Description of biometric processes”) are not considered. Chapter “TOE boundary“ gives a more detailed overview about the design of the TOE and its boundaries.

2 TOE Overview

2.1 TOE Type and major functionality

Consistent with [BVMPP], this ST describes a biometric (fingerprint) system that operates in a verification mode only: the system verifies whether, for a specific user ID, the fingerprint offered matches the fingerprint stored for that and only that user (commonly referred to as 1:1 matching).

Biometric Identification (commonly referred to as 1:N matching) is not addressed by this Security Target. Although the product in general can perform biometric identification, this is not the evaluated functionality of the TOE.

Furthermore the enrolment process is out of scope of this Security target and it is assumed that all authorized users have been enrolled.

Last but not least this biometric (fingerprint) verification system aims to verify the identity of a user in a group of authorized users for the purpose of controlling access to a portal (typically: a door inside an environment protected with guards and CCTV). Such a portal can be a physical or logical point beyond which information or assets are protected by the biometric system. With failed verification, the portal stays closed for the user. Only after successful verification, the portal will be opened. Therefore, such a portal requires one of two states after biometric verification: failed or successful authentication of the user. The final decision on the claimed identity of the user (resulting from a biometric probabilistic message into a boolean value) is considered to be part of the TOE. Everything beyond the portal and the control of the portal itself (i.e. which users have access to the portal) is out of the scope of the TOE.

Beside the biometric verification process the system has a mechanism to identify and authenticate an administrator of the system with other means than the biometric mechanism and to limit the access to administrative functions. This is used to limit the ability to change security relevant settings of the biometric functionality to an authorized administrator.

2.2 Description of biometric processes

(taken verbatim from [BVMPP])

The core functionality of biometric systems can be divided into three processes:

- Enrolment[1]:
  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 PP. 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] As mentioned before: Within the PP used it is assumed that the enrolment process for all users has already been performed.

Please note that the biometric system as defined in this ST only offers a process for biometric verification.

2.3 TOE configuration and TOE environment

(Consistent to [BVMPP], see there for the generic description)

The TOE can be used in both stand-alone or network-integrated solutions, with the same configuration of the TOE. In both situations, the network interface is considered to be trusted by the device and any unauthorized access by physical or logical means should be protected against by the user, as described later in the objectives for the environment. The network interface allows centralized enrolment, but enrolment functionality is outside the scope of evaluation.

The TOE contains the fingerprint sensor needed to acquire the fingerprint. For the sensor to operate reliably, the TOE must be installed in a way that it is sheltered from the weather. Besides the environment conditions, the TOE requires power and a physical protection for it to operate according to the claimed functionality. For the exact requirements, the reader is referred to the [installation manual].

2.4 TOE boundary

2.4.1 Physical boundary and features

The TOE physically consists out of

- Hardware and firmware: NM4000 including the firmware (See TOE Reference for exact list and the unique reference)
- Software: None (server software for network-connected situation is out of scope for the evaluation)
- Guidance:
    - [Installation manual]
    - [User manual]

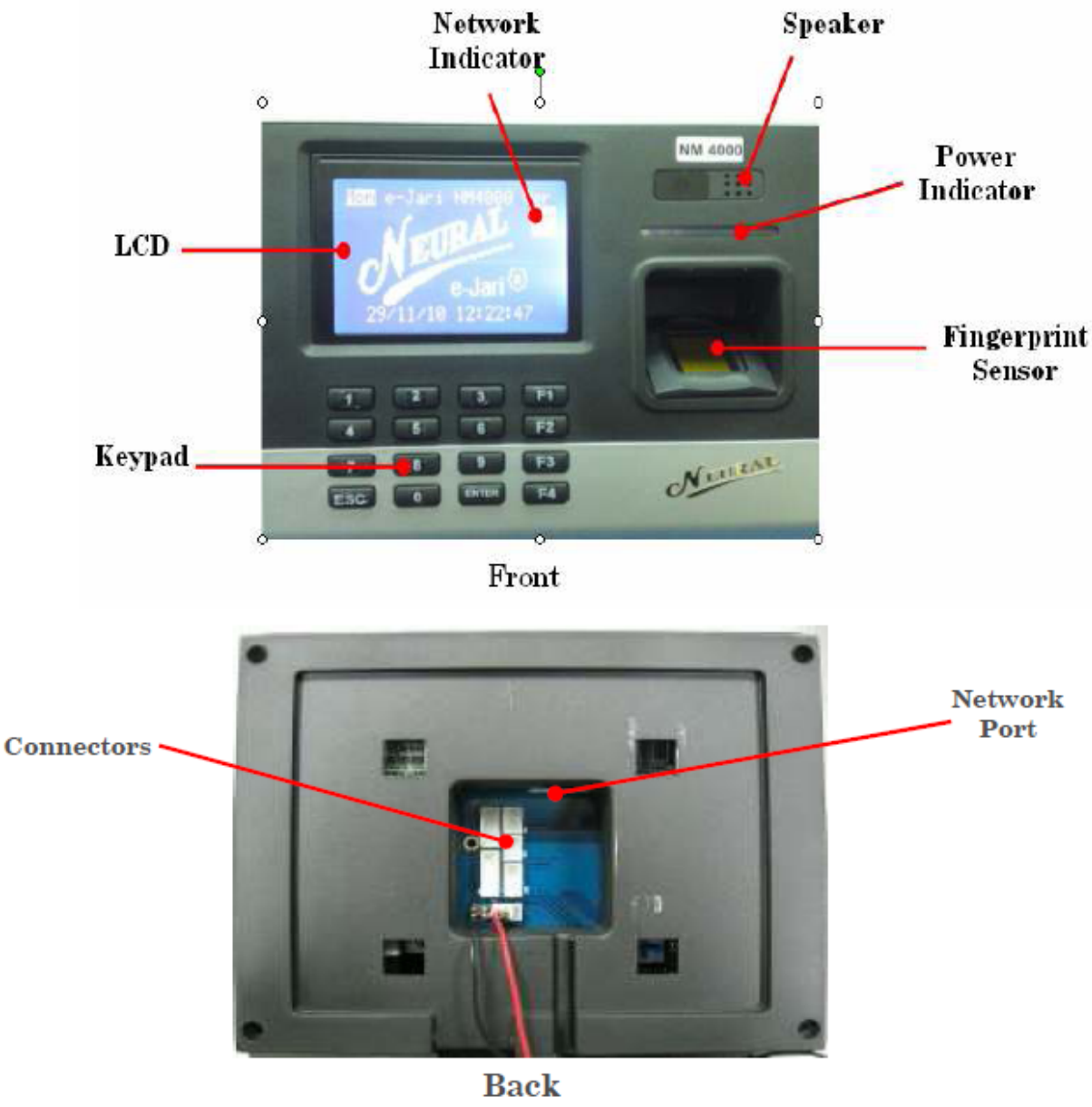

Figure 2: Physical scope and interfaces (from [User manual])

The TOE is able to run stand-alone, for which it needs to be connected physically to the environment for power and output of the result (typically: by opening an electronic lock). In the optional network-connected situation the TOE additionally needs to be connected to the network for the network-features to work. The following figure shows the typical physical deployment of the TOE and its connections.

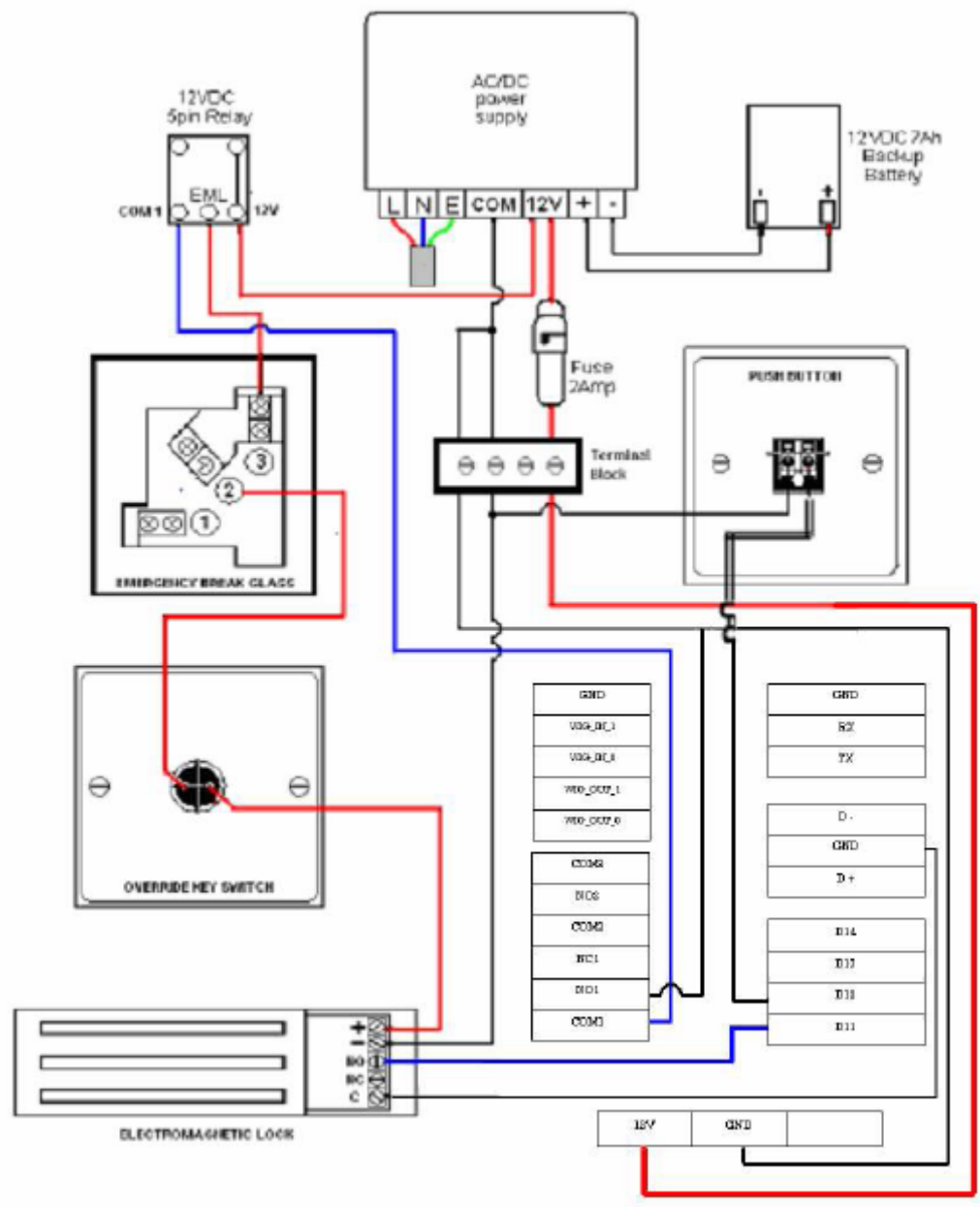

Figure 3: TOE and its connections to the environment (from [User manual])

2.4.2 Logical boundary and features

The simplified model of a biometric verification system and its boundaries has been taken from [BVMPP] Figure 1 and annotated with this TOEs boundaries and internal design structure.

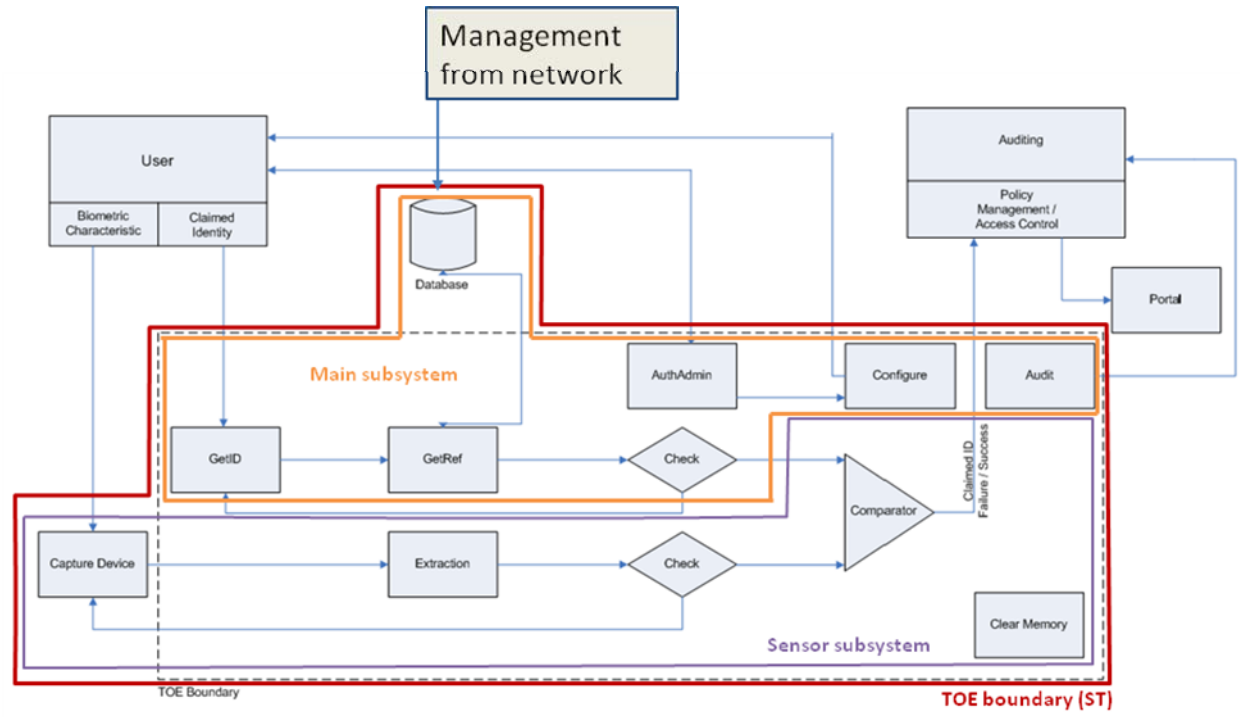

Figure 4: TOE logical boundary and subsystems

This TOE includes the capture device (the fingerprint sensor) into its boundary, as part of the sensor subsystem. Compared to the minimum TOE boundary of the PP, this TOE additionally includes the local database holding the user IDs and corresponding fingerprint templates. Having the database inside the TOE allows it to perform its functionality without the need of an external database. The TOE does allow management access via the network to this database, for centralized enrolment and other management tasks. This functionality is outside the scope of the evaluation as it is performed over the network, a trusted secure interface (see objectives for the environment) and because the enrolment functionality is also outside the scope of the evaluation.

The TOE includes auditing functionality which operates stand-alone. In the networked-solution can also be retrieved via the network interface for convenient audit review, but this is outside the scope of the evaluation.

Following describes the functionality and general design of the TOE with respect to the terms of [BVMPP]:

- Get ID: The user's claimed identity is retrieved by reading the smartcard offered in the field of the contactless smartcard reader (part of the main subsystem). (Note that product allows entry of the normal user ID via the PIN pad, but this is outside the scope of the evaluation). The main subsystem also provides the PIN pad, display and status LEDs as the user visible interface, as well as audio feedback.
- GetRef: The main subsystem is responsible for getting the stored (already enrolled) fingerprint reference related to a claimed user's identity.

- Extraction: The sensor subsystem extracts the feature vector from the fingerprint sensor image. This feature vector allows robust and efficient verification in the checking phase, and effectively compressed the large sensor image to a much smaller feature vector.
- Check: The integrity and authenticity of the fingerprint sensor image is ensured by including the sensor into the physical and logical boundary of the TOE. The integrity and authenticity of the stored fingerprint reference is also ensured by including the database into the physical and logical boundary of the TOE. The quality check on the live fingerprint offered is performed during the sensor module's processing of the fingerprint sensor image. Insufficient quality will lead to a rejection in the verification.
- AuthAdmin: Using the PIN pad of the main subsystem, the administrators can identify (by them using the PIN pad) and authenticate (by entering the correct PIN) themselves. Only after successful identification and authentication will the main subsystem allow access to the administration functionality (described directly below as "Configure"). This way it is ensured that only authenticated administrators are allowed to configure any of the security relevant settings of the TOE.
- Configure: Using the PIN pad and display of the main subsystem, the administrator can set the TOE parameters (both security relevant and non-security relevant). The threshold setting for the comparator component as well as the auditable events are fixed to a secure value to avoid potential mistakes in configuration.
- Comparator (also called Matcher): The sensor subsystem compares the enrolled fingerprint reference (retrieved via GetRef) with the offered fingerprint's feature vector (from Extraction). The sensor module internally verifies the two within a threshold that provides a False Acceptance Rate FAR of more than 1/100 and provides a fail/success value to the main subsystem. The main system optionally can perform time based access control but this is not in the scope of the evaluation. The result is provided to the environment and an audit event is generated. An "Exact match" comparison does not result in a positive verification as it may be a replay attempt and should be recorded in the audit log.
- Clear memory: In order to protect against attacks on the raw fingerprint image data of the offered fingerprint, the sensor subsystem alone handles this data (hence its inclusion in the scope of the sensor module). The main subsystem does not access this data on the sensor subsystem. After the acquisition of the image, extraction and comparator actions, the fingerprint image data is therefore not accessible after deallocation. Biometric reference data must be stored in the database for use in the system and is therefore exempt of this requirement.
- Audit: Audit events are generated by the main subsystem and stored in its memory. It can be read via the management interface and the network interface, but this audit reviewing functionality is not in the scope of the evaluation.
- Capture device: the fingerprint sensor is part of the sensor subsystem. It captures the fingerprint using a capacitive sensor array as described in the ADV evidence.
- Database: Included in the TOE is the database used by the TOE to store the fingerprint reference of a user together with the user ID.

Some security related components, functions and interfaces of the TOE environment should be considered here (outside the scope of the evaluation):

- Policy management/Access control: The result of the fingerprint verification process (i.e. the Comparator) is passed on to the policy manager of the environment. This component is responsible for checking the user's rights and opening the portal if the user has sufficient privileges and was successfully verified by the TOE and is therewith realizing an access control mechanism for the portal. A common deployment of the TOE is to have the simple policy that successfully verified users are granted entry by opening the portal (i.e. the door).
- Portal: 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. In the common deployment of the TOE the portal is the electronic lock of a door.
- Auditing: The environment may provide additional audit functionalities and has to provide a mechanism for audit review of the TOE audit logs. The developer of the TOE has complementary network software to provide this functionality, but this is outside the scope of this evaluation.
- Transmission / Storage: The environment cares for a secure communication and storing where security relevant data is transferred to or from the TOE. This especially applies to the network connection and the connection to the portal.

3 Conformance Claims

3.1 CC Conformance Claims

This ST and TOE claim conformance to Version 3.1 R3 of Common Criteria [CC].

This ST and TOE are conformant to part 2 and 3 of [CC]; no extended components have been defined.

3.2 PP Conformance Claims

This ST and TOE claim **no** conformance to a PP.

This ST is based on [BVMPP], refers to it and its application notes, is however **not conformant** to it (the [BVMPP] additionally has the SFR FPT_RPL.1 and the assurance level EAL2).

Note that this is not a composed TOE.

3.2.1 TOE Type conformance rationale

Not applicable.

3.2.2 Security Problem Definition rationale

Not applicable.

3.2.3 Security Objectives rationale

Not applicable.

3.3 Further Package Claims

This ST and TOE claim conformance to assurance package EAL1 as defined in Common Criteria Part 3. EAL1 consists of ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_TSS.1, ATE_IND.1 and AVA_VAN.1.

4 Security Problem Definition

4.1 External entities

The following external entities interact with the TOE:

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 portal.

4.2 Assets

The following assets are defined:

4.2.1 Primary assets:

The primary assets which are protected against unauthorised access do not belong to the TOE itself. The portal in the environment permits access only after successful authentication as a result of the biometric verification. The primary assets, either physical or logical systems, are behind that portal.

4.2.2 Secondary assets:

Assets (i.e. TSF data), which are generated by the TOE itself (e.g.: passwords to protect security relevant TOE settings and biometric references) are:

- Biometric Reference Record (BRR): This object includes the enrolled biometric data linked with the identity of a user. It is produced during the enrolment process and assumed to be given and quality checked.
- Biometric Live Record (BLR): This record includes the live (actual) biometric data (actual biometric characteristic and claimed user identity) to be verified against the biometric reference.
- The claimed identity of a user
- Security relevant system configuration data: This type of assets specifically includes the threshold level that is used by the TOE for the authentication of users.
- User related security attributes and authentication data for non biometric authentication

4.3 Assumptions

The reader is reminded that **all** the below assumptions **must hold or the TOE cannot be trusted to protect against the threats or implement the organisational security policies.**

4.3.1 A.ADMINISTRATION

The TOE administrator is well trained and non hostile. He reads the guidance documentation carefully, completely understands and applies it.

The TOE administrator is responsible to accompany the TOE installation and oversees the biometric system requirements regarding the TOE as well as the TOE settings and requirements.

4.3.2 A.ENROLMENT

The enrolment is assumed to be already performed and therefore, the biometric reference for each authorized user is assumed to be given. The generated reference is of sufficient quality and is linked to the correct user.

Additionally, it is assumed that all biometric references are stored in a way that ensures the authenticity and integrity of this data.

4.3.3 A.ENVIRONMENT

It is assumed, that necessary TOE operating equipment and adequate infrastructure is available (e.g.: operating system, database, LAN, public telephone, and guardian).

Specifically the following things are assumed:

- It is assumed that the direct environment of the TOE supports the functionality of the biometric system (e.g.: integration with the building's physical structure and door locks, audit functionality).
- It is assumed that all environmental factors are appropriate with respect to the used fingerprint sensor.
- The TOE environment provides a database for the biometric reference of enrolled users, whereby integrity and authenticity are ensured.
- The environment ensures a secure communication of security relevant data from and to the TOE.
- It is assumed that the environment provides a functionality to review the audit information of the TOE and to ensure that only authorized administrators have access to the audit logs.
- It is assumed that the TOE environment is free of viruses, trojans, and malicious software.

4.3.4 A.FALLBACK

It is assumed that a fall-back mechanism for the biometric verification system is available that reaches at least the same level of security as the biometric verification system does. This fall-back system is used in cases where an authorized user is rejected by the biometric verification system (False Rejection).

4.3.5 A.PHYSICAL

It is assumed that the environment physically protects the TOE and its components against unauthorized access or destruction. Only authorized users have access to the TOE and its public external interfaces (the display, the keyboard, the smartcard reader, and the fingerprint sensor). Only authorized administrators have access to the TOE's internals and restricted interfaces (as described in A.ENVIRONMENT).

4.3.6 A.TRUSTED_USERS

It is assumed that the environment protects the TOE sufficiently to prevent an attacker from presenting an imitated finger to the fingerprint sensor or to re-use the latent image on the fingerprint sensor surface, sufficient to withstand a real attacker up to moderate attack potential who uses a large amount of biometric characteristics and who really wants to get unauthorized access to the portal.

4.4 Threats

4.4.1 T.BRUTEFORCE

An attacker may perform a brute force attack in order to get verified by the TOE using the identity of another user.

In this way the attacker is trying to get access to the assets residing in the environment that should be protected with the support of the TOE.

This threat considers as threat agent a not really hostile user, who just tries to get verified with a wrong claimed identity a few times. The motivation of such a user is usually just curiosity. He does not need specific knowledge about the TOE to perform this attack.

4.4.2 T.MODIFY_ASSETS

An attacker may try to modify secondary assets like biometric references or other security-relevant system configuration data.

Such attacks could compromise the integrity of the user security attributes resulting in an incorrect result that might give unauthorized access to the portal.

This threat covers a number of distinct types of attacks:

- An attacker may attempt to modify the threshold level used by the biometric system to authenticate users. If the attacker is able to change the threshold (for one or more authorised users), the ability to verify the user(s) will be compromised and he may succeed in gaining access to the portal or an authorised user may be denied entry to the portal.
- An attacker may attempt to modify the biometric authentication data (the Biometric Reference Record) of an authorised user with the aim of enabling an attacker to masquerade as the authorised user and gain access to the portal. Alternatively, an authorised user may be denied access to the portal. The attacker may be able to insert a new biometric reference, containing biometric data belonging to an attacker, with the aim of enabling the impostor to gain access to the portal.

This kind of attack presupposes that the attacker has further knowledge about the TOE and maybe special equipment.

4.5 OSPs

4.5.1 OSP.ERROR

The TOE shall meet recognised national and/or international criteria[2] for its security relevant error rates (e.g. False Accept Rate (FAR) and False Rejection Rate (FRR)).

4.5.2 OSP.USERLIMIT

Impostors must be prevented from gaining access to the portal by making repeated verification attempts using one or more claimed user IDs.

Therefore the TOE shall be able to limit the maximum number of unsuccessful verification attempts.

[2] The ISO standard [19795] defines the FAR/FRR and the Common Criteria Biometric Evaluation Manual supplement [BEM] table 11 defines the acceptable limits. The [BEM] states that the acceptable worst-case FAR for SOF-Basic (i.e. Enhanced-Basic attack potential in CCv3.1) is 1/100. The TOE meets this requirement. Other rates are according to the [BEM] and the author's opinion not relevant for the security of the TOE at hand and not considered further. Proper strength of the complete mechanism against attacks is documented by the developer in the evaluation evidence of the security architecture, and assessed by the evaluators during the AVA evaluation activities.

5 Security Objectives

5.1 Security Objectives for the TOE

5.1.1 O.AUDIT_REACTION

The TOE shall ensure that all users can be held accountable for their security relevant actions.

In this context the TOE shall log all security relevant events and react in order to keep the TOE in a secure state.

The TOE shall specifically (but not exclusively) audit and react to:

- An unusual high amount of unsuccessful verification attempts against the same or different user identities (via the biometric authentication mechanism) could be caused by a brute force attack. In this case the system should block any further verification attempts for a specified time and should inform an administrator.
- Unsuccessful authentication attempts to one or more administrator account(s) may be caused by an attack. The TOE should lock the authentication mechanism if a configurable number of unsuccessful authentication attempts has been reached.

In the context of this functionality it is to mind, that no feedback information is provided, which may assist an impostor in gaining access.

5.1.2 O.ROLES

The TOE shall restrict its management functionality to authenticated and authorised TOE administrators. Other users are not allowed to manage the TOE.

5.1.3 O.BIO_VERIFICATION

The TOE shall provide a biometric verification mechanism to ensure access to a portal with an adequate reliability.

The TOE shall ensure that only suitable biometric references (i.e. records that have been created by the TOE itself or biometric references coming from a trustworthy source and following a standardised format) are processed.

The TOE shall meet national and/or international criteria for its security relevant error rates.

5.1.4 O.AUTH_ADMIN

The TOE shall provide a mechanism to authenticate an administrator with other means than the biometric verification process. This authentication process may be realized via a user name/password or a smartcard/pin based mechanism.

5.1.5 O.RESIDUAL

The TOE shall ensure that no residual or unprotected fingerprint image data remains after operations are completed.

5.2 Security objectives for the operational environment

The reader is reminded that **all** the below objectives for environments **must be implemented in the environment or the TOE cannot be trusted to protect against the threats or implement the organisational security policies.**

5.2.1 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 to accompany the TOE installation and oversees the biometric system requirements regarding the TOE as well as the TOE settings and requirements.

5.2.2 OE.ENROLMENT

The enrolment must already be already performed and therefore, the biometric reference for each authorized user is assumed to be given. The generated reference is of sufficient quality and is linked to the correct user.

Additionally, it is assumed that all biometric references are stored in a way that ensures the authenticity and integrity of this data.

5.2.3 OE.ENVIRONMENT

The environment must ensure that necessary TOE operating equipment and adequate infrastructure is available (e.g.: operating system, database, LAN, public telephone, and guardian).

Specifically the following things must be ensured:

- The direct environment of the TOE must support the functionality of the biometric system (e.g.: integration with the building's physical structure and door locks, audit functionality).
- All environmental factors must be appropriate with respect to the used fingerprint sensor.
- The TOE environment must provide a database for the biometric reference of enrolled users, whereby integrity and authenticity are ensured.
- The environment must ensure a secure communication of security relevant data from and to the TOE.
- The environment must provide a functionality to review the audit information of the TOE and to ensure that only authorized administrators have access to the audit logs.
- The TOE environment must be free of viruses, trojans, and malicious software.

5.2.4 OE.FALLBACK

A fall-back mechanism for the biometric verification system must be available that reaches at least the same level of security as the biometric verification system does. This fall-back system can be used in cases where an authorized user is rejected by the biometric verification system (False Rejection).

5.2.5 OE.PHYSICAL

The environment must physically protect the TOE and its components against unauthorized access or destruction. Only authorized users should have access to the TOE and its public external interfaces

(the display, the keyboard, the smartcard reader, and the fingerprint sensor). Only authorized administrators should have access to the TOE's internals and restricted interfaces (as described in OE.ENVIRONMENT).

5.2.6 OE.TRUSTED_USERS

It is assumed that the environment protects the TOE sufficiently to prevent an attacker from presenting an imitated finger to the fingerprint sensor or to re-use the latent image on the fingerprint sensor surface, sufficient to withstand a real attacker up to moderate attack potential who uses a large amount of biometric characteristics and who really wants to get unauthorized access to the portal.

5.3 Security objectives rationale

The following shows that the complete security problem definition (SPD) with all threats, OSPs and assumptions is covered in the objectives.

SPD	Rationale
A.ADMINISTRATION	OE.ADMINISTRATION is a direct, one-to-one implementation of the assumption.
A.ENROLMENT	OE.ENROLMENT is a direct, one-to-one implementation of the assumption.
A.ENVIRONMENT	OE.ENVIRONMENT is a direct, one-to-one implementation of the assumption.
A.FALLBACK	OE.FALLBACK is a direct, one-to-one implementation of the assumption.
A.PHYSICAL	OE.PHYSICAL is a direct, one-to-one implementation of the assumption.
A.TRUSTED_USERS	OE.TRUSTED_USERS is a direct, one-to-one implementation of the assumption.
T.BRUTEFORCE	O.AUDIT_REACTION describes that the TOE detects and reacts to brute force attacks, for biometric authentications (for users) at thresholds offering sufficient protection considering the false acceptance rates (FAR) described in the O.BIO_VERIFICATION . Attacking via the residual finger print data temporarily stored in the fingerprint sensor would allow better than brute force attacks, so the TOE is must protect this information too. The environment keeps attackers from the TOE (OE.PHYSICAL) and the users are not attackers

	either (OE.TRUSTED_USERS). Still access to the residual finger print data could be possible and must be protected against (O.RESIDUAL). O.AUDIT_REACTION also describes that the TOE detects and reacts to brute force attacks for the non-biometric authentication (for administrators).
T.MODIFY_ASSETS	O.ROLES describes that the TOE distinguishes between users and administrators. O.AUTH_ADMIN describes that only the administrators can modify the assets. As the administrators are trusted (OE.ADMINISTRATION), they are not the attackers. Therefore attackers cannot change these parameters.
OSP.ERROR	O.BIO_VERIFICATION describes that the TOE follows the FAR required.
OSP.USERLIMIT	O.AUDIT_REACTION describes that there are brute force limitations on the biometric and non-biometric authentications (as further described above in the rationale for T.BRUTEFORCE).

6 Extended Component definition

This ST does not use any extended functional or assurance components.

7 Security Requirements

This chapter describes the security functional and the assurance requirements which have to be fulfilled by the TOE. All are drawn from [BVMPP] and the operations are indicated relative to that PP, using the standard notation method.

7.1 Security Functional Requirements for the TOE

The following are the Security Functional Requirements for this TOE. The notation method of [BVMPP] is followed:

The following notations are used:

- Refinement operation (denoted by **bold text**): is used to add details to a requirement, and thus further restricts a requirement.
- Selection operation (denoted by underlined text): is used to select one or more options provided by the [CC] in stating a requirement.
- Assignment operation (denoted by *italicised text*): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- Iteration operation: are identified with a number inside parentheses (e.g. "(1)")

7.1.1 FAU_GEN.1 Audit data generation

7.1.1.1 FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) **None**[3];
b) All auditable events for the basic [4]level of audit; and
c) None[5]

7.1.1.2 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 **ST**[6].

Remark to application note on page 27 of [BVMPP]: No additional reactive capabilities are provided by the TOE and accordingly the SFRs are not extended.

7.2 FAU_GEN.2 User identity association

7.2.1.1 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.

[3] Refinement of "Start-up and shutdown of the audit functions" to make clear that the audit functions cannot actually start or shutdown (they are always available), hence the audit event never occur. This is a stronger requirement then allowing the start-up and shutdown of the audit functions, therefore it is a valid refinement.
[4] [selection, choose one of: minimum, basic, detailed, not specified]
[5] [assignment: other specifically defined auditable events or none].

[6] Assignment to "None" of [assignment: other audit relevant information], then refined away completely. Also refined "PP/ST" to "ST".

7.2.2 FDP_RIP.2 Full residual information protection

7.2.2.1 FDP_RIP.2.1

The TSF shall ensure that any previous information content of a resource **containing the fingerprint image**[7] is made unavailable upon the deallocation of the resource[8] from all objects.

7.2.3 FIA_AFL.1(1) Authentication failure handling for users accounts

7.2.3.1 FIA_AFL.1.1(1)

The TSF shall detect when ***3*** [9]unsuccessful authentication attempts occur related to the biometric verification of one or more users.

7.2.3.2 FIA_AFL.1.2(1)

When the defined number of unsuccessful authentication attempts has been met[10], the TSF shall *disable the biometric verification for the corresponding user account* **for at least 10 minutes**[11] *and generate an audit event*[12][13]

7.2.4 FIA_AFL.1(2) Authentication failure handling for administrators accounts

7.2.4.1 FIA_AFL.1.1(2)

The TSF shall detect when ***3*** [14]unsuccessful authentication attempts occur related to the authentication of one or more administrators accounts.

7.2.4.2 FIA_AFL.1.2(2)

When the defined number of unsuccessful authentication attempts has been met[15], the TSF shall *disable the verification for the corresponding administrator account* **for at least 10 minutes**[16] *and generate an audit event*[17][18].

---

[7] Refinement to explicitly state the sensitive information to be protected: the fingerprint image

[8] [selection: allocation of the resource to, deallocation of the resource from]

[9] Assignment of "3-3" to the acceptable range in "an administrator configurable positive within [assignment: range of acceptable values]" is refined away to a clear statement that at every 3 unsuccessful authentication attempt this requirement applies.

[10] [selection: met, surpassed]

[11] Refinement to clearly integrate the unlocking mechanism. For sufficient protection against brute force attacks up to AVA_VAN.2 level, administrator account authentication attempts must be rate limited to 1 per 10 seconds. Compensating for potential parallel attacks and balancing this against practical availability, 1 per 10 minuts per device is a good balance.

[12] [assignment: list of other actions].

[13] [assignment: list of actions]

[14] Assignment of "3-3" to the acceptable range in "an administrator configurable positive within [assignment: range of acceptable values]" is refined away to a clear statement that at every 3 unsuccessful authentication attempt this requirement applies.

[15] [selection: met, surpassed]

[16] Refinement to clearly integrate the unlocking mechanism. For sufficient protection against brute force attacks up to AVA_VAN.2 level, administrator account authentication attempts must be rate limited to 1 per 10 seconds. Compensating for potential parallel attacks and balancing this against practical availability, 1 per 10 minuts per device is a good balance.

Remark on the application note on page 29 of [BMVPP]: The TOE can be used in a stand-alone situation and a network-connected situation. In both cases, parallel attacks on the either authentication mechanism are possible. The minimum of 10 minutes provides sufficient protection. Note that the TOE will disable verification for all user accounts when 10 user accounts have been locked, requiring the administrator to unlock user verification. This is a specific case of the "at least 10 minutes" lockout and therefore not explicitly defined in the SFR. The AVA evaluation activities by the evaluator will verify this is within the attack potential. Therefore this application note has been taken into account.

7.2.5 FIA_ATD.1 User attribute definition

7.2.5.1 FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:

- **user ID**[19]
- *biometric reference*
- *role*[20]
- *none*[21].

7.2.6 FIA_UAU.2(1) User authentication before any action

7.2.6.1 FIA_UAU.2.1(1)

For biometric verification, t[22]he TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user**, with a False Acceptance Rate (FAR) of 1/100 or better**[23].

Remark about application note on page 29 of [BVMPP]: The FAR has been addressed on the above SFR. See also earlier remarks on OSP.ERROR and the TOE overview.

7.2.7 FIA_UAU.2(2) User authentication before any action

7.2.7.1 FIA_UAU.2.1(2)

For non biometric verification, t[24]he TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Remark about application note on page 30 of [BVMPP]: This ST follows the same guidelines.

---

[17] [assignment: list of other actions]
[18] [assignment: list of actions]
[19] Refinement of "user ID or name": the TOE only uses user IDs, not user names.
[20] Although the TOE does associate roles to users, it does so based on the method used for identification/authentication: the "user" role is assigned to users successfully authenticated using the biometrical mechanism, and the "administrator" role is assigned to users successfully authenticated using the password mechanism.
[21] [assignment: other attributes or none]
[22] Refinement
[23] Refinement: added the FAR explicitly to address the application note. The FAR of 1/100,000 is much lower then the rate demanded by OSP.ERROR which is 1/100.
[24] Refinement

7.2.8 *FIA_UAU.5 Multiple authentication mechanisms*

7.2.8.1 FIA_UAU.5.1

The TSF shall provide

- *a biometric verification mechanism and*
- *a non biometric verification mechanism*[25]

to support user authentication.

7.2.8.2 FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the following rules:

- *users shall be authenticated using the biometric verification mechanism (FIA_UAU.2(1))*
- *administrators shall be authenticated using the non biometric verification mechanism (FIA_UAU.2(2))*[26]
- *None*[27]

7.2.9 FIA_UAU.7 Protected authentication feedback

7.2.9.1 FIA_UAU.7.1

The TSF shall provide no *messages*[28] to the user while the biometric authentication is in progress.

7.2.10 FIA_UID.2(1) User identification before any action

7.2.10.1 FIA_UID.2.1(1)

For biometric verification,[29] the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.2.11 FIA_UID.2(2) User identification before any action

7.2.11.1 FIA_UID.2.1(2)

For non biometric verification,[30] the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.2.12 FMT_MOF.1 Management of security function behaviour

7.2.12.1 FMT_MOF.1.1

The TSF shall restrict the ability to determine the behaviour of, disable, enable, modify the behaviour of[31] the functions

---

[25] [assignment: list of multiple authentication mechanisms]
[26] [assignment: rules describing how the multiple authentication mechanisms provide authentication].
[27] [assignment: other rules describing how the multiple authentication mechanisms provide authentication or none].
[28] [assignment: list of feedback]
[29] Refinement to make the differences between the two identification mechanisms (biometric and non-biometric) explicit.
[30] Refinement to make the differences between the two identification mechanisms (biometric and non-biometric) explicit.

- *Audit mechanism,*
- *None*[32]

To **no one**[33].

7.2.13 FMT_MTD.1 Management of TSF data

7.2.13.1 FMT_MTD.1.1

The TSF shall restrict the ability to change_default, query, modify, delete, clear[34][35] the

- *The FAR*,[36]
- *The user security attributes governing the role*[37]
- *none*[38]

To **no one**[39].

7.2.14 FMT_MTD.3 Secure TSF data

7.2.14.1 FMT_MTD.3.1

The TSF shall ensure that only secure values are accepted for

- *biometric reference records*[40]
- *none*[41]

7.2.15 FMT_SMF.1 Specification of Management Functions

7.2.15.1 FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:

- *unlock a blocked user or administrator account*[42]
- *none*[43]

---

[31] [selection: determine the behaviour of, disable, enable, modify the behaviour of]
[32] [assignment: other functions or none]
[33] Refinement of "TOE administrators": the TOE allows no changes to the audit mechanism, not even by the TOE administrators. As this is a more secure situation, this is a valid refinement.
[34] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[35] ", [assignment: other operations or none]" was assigned "none" and then refined away for better readability.
[36] [assignment: list of security parameters which control the performance of the biometric system]
[37] [assignment: user security attributes]: as described in FIA_ATD.1, the role is not configurable. This is repeated here for clarity.
[38] [assignment: other attributes or none]
[39] Refinement of "TOE administrators": the TOE does not allow changes of such parameters or attributes at all, only enrollment and deletion of users which is out the scope of the evaluation. As the new requirement is more restrictive then the old, it is a valid refinement.
[40] [assignment: list of TSF data]
[41] [assignment: list of other TSF data or none]
[42] [assignment: list of management functions to be provided by the TSF]
[43] [assignment: list of other management functions to be provided by the TSF or none]

With respect to the application note on page 32 of [BVMPP], the reader is referred to the chapter "TOE Summary Specification" where for all the suggestions of the application note are also considered under the SFR FMT_FMF.1.

7.2.16 FMT_SMR.1 Security roles

7.2.16.1 FMT_SMR.1.1

The TSF shall maintain the roles

- *user*
- *TOE administrator*[44]
- *none*[45].

7.2.16.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

With respect to the application note on page 33 of [BVMPP], the concepts of users and administrators matches that of the TOE. No further restructuring of the roles is useful.

7.3 Assurance requirements

The TOE conforms to EAL1, which consists of ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_TSS.1, ATE_IND.1 and AVA_VAN.1..

7.4 Security Requirements rationale

All open operations in the security requirements have been performed as indicated in the chapter "Security Requirements ". All dependencies had already been satisfied or justified as shown below.

SFR	Dependencies	Fulfilled by
FAU_GEN.1	FPT_STM.1	See 7.4.1.1 "Justification for missing dependencies"
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.1
FDP_RIP.2	-	-
FIA_AFL.1(1)	FIA_UAU.1	FIA_UAU.2(1)
FIA_AFL.1(2)	FIA_UAU.1	FIA_UAU.2(2)
FIA_ATD.1	-	-
FIA_UAU.2(1)	FIA_UID.1	FIA_UID.2(1)

[44] [assignment: the authorised identified roles]
[45] [assignment: additional roles or none]

FIA_UAU.2(2)	FIA_UID.1	FIA_UID.2(2)
FIA_UAU.5	-	-
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2
FIA_UID.2(1)	-	-
FIA_UID.2(2)	-	-
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.3	FMT_MTD.1	FMT_MTD.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	FIA_UID.2(1) and FIA_UID.2(2)

7.4.1.1 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.ENVIRONMENT).

7.4.2 Security Functional Requirements rationale

See below for a mapping of the objectives for the TOE to the SFRs.

7.4.2.1 O.AUDIT_REACTION

- FAU_GEN.1 defines that the TOE has to capture all the events as required by O.AUDIT_REACTION and
- FAU_GEN.2 ensures that events can be traced back to the identity of a user if the event was caused by a user.
- FIA_AFL.1(1) ensures that reaching a threshold of unsuccessful authentication attempts for the biometric authentication mechanism is recognized to be a security relevant state.
- FIA_AFL.1(2) ensures that reaching a threshold of unsuccessful authentication attempts for the authentication mechanism for the administrator is recognized to be a security relevant state.

7.4.2.2 O.ROLES

- FIA_ATD.1 defines that the role of a user is a user attribute.
- FMT_MOF.1 limits the ability to modify the behaviour of audit functions and other relevant functions to administrators,
- FMT_MTD.1 restricts the ability to control the relevant settings of the TOE to administrators.

- FMT_SMF.1 defines that the TOE has to provide some specific management functions to control the security relevant attributes and
- FMT_SMR.1 ensures that the TOE maintains roles and that each user can be associated with a role.

7.4.2.3 O.BIO_VERIFICATION

- FIA_ATD.1 defines the user attributes that are also used for the biometric verification.
- FIA_UAU.2(1) states that each user has to be successfully authenticated by the biometric mechanism before performing any action.
- FIA_UAU.5 defines that the TOE has a different authentication mechanism for administrators beside the biometric verification process.
- FIA_UAU.7 ensures that no harmful authentication feedback is given to a potential attacker.
- FIA_UID.2(1) states that the each user has to be identified before performing any action.
- FMT_MTD.3 assures that only secure values are accepted for TSF data that is used by the biometric verification process.

7.4.2.4 O.AUTH_ADMIN

- FIA_ATD.1 defines the user attributes that are also used for the authentication of an administrator.
- FIA_UAU.2(2) states that administrators have to be successfully authenticated before performing any action.
- FIA_UAU.5 defines that the TOE has a different authentication mechanism for administrators beside the biometric verification process.
- FIA_UID.2(2) states that administrators have to be identified before performing any action.

7.4.2.5 O.RESIDUAL

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

7.4.3 Security Assurance Requirements rationale

The assurance level EAL1 has been chosen as it offers the appropriate assurance for the TOE in its market. Note that it is **not** in conformance to [BVMPP], which requires EAL2.

7.5 Dependencies of assurance components

The dependencies of the assurance requirements taken from EAL1 are fulfilled automatically.

8 TOE Summary Specification

8.1 Implementation of the SFRs

The below table is an excerpt of the SFR-tracing provided in the ADV evaluation evidence and shows per-SFR for all the relevant details in the SFR, how the TOE meets each of these details. This form allows for better performance of the ASE_TSS.1 and ADV tasks, at the cost of slightly reduced readability.

SFR	SFR detail		Rationale
FAU_GEN.1	Start-up and shutdown of audit functions		The audit functions are always on and cannot be shutdown. For auditable events to occur the TOE must be powered on and initialized (see also the security architecture description, section secure initialization), at which point the audit functions are also on as they are performed as part of the operation.
	All auditable events for basic level of audit.		See per auditable event below.
	FAU_GEN.1	No auditable events foreseen	N/A
	FAU_GEN.2	No auditable events foreseen	N/A
	FIA_AFL.1(1)	reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken	The main subsystem detects the reaching of the threshold, disables the access according to the SFR and creates the audit event. The audit event is available for review via the administrator interfaces via the display and via the network.
		subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a	The administrator can re-enable the access using the main subsystem via the administrator interfaces. At this point, the TOE generates an audit event, which again is available via these administrator interfaces.

		terminal).	
	FIA_AFL.1(2)	reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken	The main subsystem detects the reaching of the threshold, disables the access according to the SFR and creates the audit event. The audit event is available for review via the administrator interfaces via the display and via the network.
		subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	The administrator can re-enable the access using the main subsystem via the administrator interfaces. At this point, the TOE generates an audit event, which again is available via these administrator interfaces.
	FIA_ATD.1	No auditable events foreseen	N/A
	FIA_UAU.2(1)	All use of the authentication mechanism	At authentication, successful or unsuccessful, an audit event is generated. The audit event is available for review via the administrator interfaces via the display and via the network.
	FIA_UAU.2(2)	All use of the authentication mechanism	At authentication, successful or unsuccessful, an audit event is generated. The audit event is available for review via the administrator interfaces via the display and via the network.
	FIA_UAU.5	The result of each activated mechanism together with the final decision.	The biometric authentication is audited as described in FIA_UAU.2(1), the non-biometric as FIA_UAU.2(2). The decision between the two mechanisms is represented in the audit event type. In both cases, the result of the authentication is audited also.

	FIA_UAU.7	No auditable events foreseen	N/A
	FIA_UID.2(1)	All use of the user identification mechanism, including the user identity provided.	The smartcard identity value is audited as part of the audit event for FIA_UAU.2(1).
	FIA_UID.2(2)	All use of the user identification mechanism, including the user identity provided.	The PIN pad entered identity value is audited as part of the audit event for FIA_UAU.2(2).
	FMT_MOF.1	All modifications in the behaviour of the functions in the TSF.	As stated in the FMT_MOF.1, no changes to the audit mechanism or other behaviours of the functions of the TSF are possible, hence this audit functionality is implemented by not having the cause of the auditable event.
	FMT_MTD.1	All modifications to the values of TSF data.	As stated in the FMT_MTD.1, no changes to the TSF data are possible, hence this audit functionality is implemented by not having the cause of the auditable event.
	FMT_MTD.3	All rejected values of TSF data.	An insufficient quality fingerprint scan does not have any data that can be stored as part of the audit event, after all the sensor subsystem was not able to get the image in the first time. Hence this audit functionality is implemented by not having the cause of the auditable event.
	FMT_SMF.1	Use of the management functions	See FIA_AFL.1(1)
	FMT_SMR.1	modifications to the group of	Adding the normal users is done with the enrolment mechanism (out of the evaluated scope by the

		users that are part of a role	[BVMPP]). Removal of users (biometric access control) is implemented by the main subsystems using the administrative interfaces, this results in an audit event. There is no management of the administrators, only the change of the administrator password. This is an auditable event.
	None		N/A
	Date and time of the event		The main subsystem contains a real time clock that allows tagging of all audit events with the date and time. Audit data can be read using the display (in administrator mode) of via the network interface.
	type of event		The type of event is logged also.
	subject identity (if applicable)		The user ID is logged as part of the audit events.
	Outcome (success or failure) of the event		The outcome is logged as part of the audit events.
	None		N/A
FAU_GEN.2	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.		Users are identified by their user ID.
FDP_RIP.2	Any previous information content of a resource is made unavailable upon the deallocation of the resource from all objects		The sensor subsystem holds the relevant resources (the biometric parameters of the offered fingerprint). The sensor subsystems has functions that indirectly could lead to access this offered fingerprint but only the main subsystem can access this interface (see security architecture and design documentation). The main subsystem does not call these functions. Hence the main subsystem does not access to the relevant resources at all, including at deallocation. As the main subsystem is the only access to this interface, the main subsystem does not perform the functions, and the bypass/tampering is not possible (see security architecture), the access to the resources is available

		after deallocation.
FIA_AFL.1(1)	The TSF shall detect when 3 unsuccessful authentication attempts occur related to the biometric verification of one or more users	The main subsystem enforces the access control including the trial limit, by storing the current amount of unsuccessful authentication attempts with the identity, and increasing this after an unsuccessful attempt.
	Met the TSF shall disable the biometric verification for the corresponding user	If the unsuccessful authentication attempts are met or surpassed, the main subsystem will not allow further access unless the administrator has allowed access.
FIA_AFL.1(2)	An unsuccessful authentication attempts occur related to the authentication of one or more administrator accounts	The administrative accounts are accessed via a password as described in the guidance and FSP [User Manual]
	Met the TSF shall disable the verification for the corresponding administrator account for at least 10 minutes	The administrative access is not available for 10 minutes when the lockout occurs. The time is enforced by the main subsystem going in a loop for 10 minutes, locking out all access (administrative and user)..
	Application note: parallel attacks	The password lockout mechanism is enforced in the individual TOEs, not in a centralized location. The analysis in the security architecture takes this into account and shows the strength against parallel brute force attacks also.
FIA_ATD.1	User ID	A user is identified by his user id
	Biometric reference	Associated to the user id is the fingerprint reference data.
	Role	The TSF assigns the role based on the identification method. The “user” role is assigned to users who identified with the biometric verification mechanism. (The “administrator” role is assigned to users identifying using the password mechanism.). Note that the product also allows time-based access control which could be used to make a distinction between users (for example allowing access only during office hours to normal employees and 24h access to system administrators) but this is not considered to be a role distinction of the TSF, rather a potential usage

		pattern outside the scope of the evaluation.
FIA_UAU.2(1)	Biometric verification	User verification is done by fingerprint verification, which is obviously a biometrical verification mechanism.
	Before allowing any other TSF-mediated actions	Only after successful authentication will the TSF perform the requested action.
	Application note	The security relevant error rate for the biometric verification functions is the FAR (False Acceptance Rate, i.e. allowing an imposter to enter when he should be rejected). The verification is performed in the sensor subsystem. The sensor subsystem is configured by the developer to "secure(0x51)" mode as part of the production. In "secure(0x51)" mode the fingerprint matching has a FAR of at least 1/100,000 ([UniFinger SFM Series Packet Protocol Manual], section "Security"). This by several orders exceeds the FAR of at least 1/100 considered acceptable by the biometrical evaluation methodology ([BEM] table 11, SOF-basic is appropriate for enhanced-basic attack potential for EAL2).
FIA_UAU.2(2)	Non-biometric verification	The password entry is a clear non biometric verification mechanism.
	Before allowing any other TSF-mediated actions	Only after successful authentication will the TSF perform the requested action (as described in [User manual]).
	Application note	The functionality is considered here as a primary objective of the TOE, and fully implemented by the TOE
FIA_UAU.5	Biometric verification mechanism	The fingerprint verification mechanism delivered by the sensor subsystem is a clear biometrical mechanism.
	Non biometrical mechanism	The password mechanism is a clear non biometrical mechanism.
	Users ... authenticated using biometric verification	As described in FIA_ATD.1, verification by fingerprint is the authentication method for the "user" role.
	Administrators ... authenticated using the non biometric verification	As described in FIA_ATD.1, verification by password is the authentication method for the "administrator" role.
	None	N/A

FIA_UAU.7	no message to the to the user while a biometric authentication is in progress	No feedback is given to the user until the biometric authentication is successful or failed ([User manual]).
FIA_UID.2(1)	For biometric verification, ... user identified	In the evaluated configuration the TOE identifies the user by the ID number from the smartcard offered. Based on the ID number, the user's fingerprint template is retrieved for comparison. Successful comparison means successful identification and authorization, required for further actions (see also FIA_UAU.2(1)).
FIA_UID.2(2)	For non biometric verification, ... user identified	The password mechanism used for non biometrical verification of the administrators is both the identification and the authentication mechanism. Only after successful identification and authorization, required for further actions (see also FIA_UAU.2(2)).
FMT_MOF.1	Restrict ... audit mechanism	The audit mechanism cannot be disabled or enabled, nor can its behaviour be modified (the TOE simply does not offer these functions, not even to the administrators). The audit data can be observed and deleted (function "6" under the administrator menu, see [User guidance]), but only to the administrators. Note that the administrator can also change the network settings and could potentially set it to non-functional parameters. However the administrators are trusted (OE.ADMINISTRATION) and the logging facility to the central network is not a claimed security functionality.
FMT_MTD.1	Restrict ability to... security parameters which control the biometric system	Configuration of the biometrical parameters such as FAR and FRR is not possible at all (there simply is no interface), so this is also not possible to the administrators.
	Restrict ability to... User security attributes	There are no ways to change the user security attributes except for the enrolment and deletion of users, which is functionality that is out of scope. Note that all the management functions accessed on the TOE are restricted to the administrator, see FIA_UAU.2(2)/FIA_UID.2(2). Management via the network interface is considered out of scope for this

		evaluation as the environment must provide physical protection of that interface (OE.PHYSICAL), logical protection (OE.ENVIRONMENT) and safe usage from the administrators (OE.ADMINISTRATION). Therefore any access from the network side is trusted to be authorized management by the administrators outside the scope of this requirement.
	None	All other management functionality, both functional and potentially security impacting, is under the administrator menu as described directly above.
FMT_MTD.3	Only secure values ... for biometric reference records	During enrolment the sensor subsystem generates the fingerprint reference used to verify against. The sensor subsystem will return a failure to enrol if the value is insecure (i.e. if no fingerprint template can be made that will allow the set FAR to be met).
FMT_SMF.1	Unlock blocked user or administrator account	When user is being blocked after 3 unsuccessful authentication attempts, the TOE system access will be blocked. Admin can unblock user by re-enabling access to system in menu 4 Password Setting where Access Blocked is set to OFF (see [User guidance]). If administrator account is being blocked after 3 unsuccessful authentication, no possbility to unblocked the access to TOE system manually. The main subsytem will unblock the access to TOE system automatically after 10 minutes.
	FIA_AFL.1: Threshold for unsuccessful authentication attempts	Not relevant: No management possible.
	FIA_AFL.1: actions to be taken in event of an authentication failure	Not relevant: No management possible.
	FIA_UAU.2: management of authentication data by an administrator	Not applicable. Note that there are enrolment and user management functions available under the administrator menu and via the network interface, but this management is not claimed and outside the scope of this evaluation (consistent with the objective for the environment OE.ENROLL, OE.ENVIRONMENT and OE.ADMINISTRATION).

	FIA_UAU.2: management of user identities	Enrolling creates user identities, and deletion of profiles deletes them. However this functionality is outside the scope of this evaluation (see directly above).
	FIA_UID.2: managing groups of users	There are no groups of users (except the hardcoded notions of "users" and "administrators" described in the FIA_UAU and FIA_UID requirements). No management is possible.
	FMT_MOF.1: group of roles	There are no groups of roles.
	FMT_MTD.1: managing the group of users that are part of a role	There is no group management of this kind in the evaluated functionality. Users are assigned implicitly to the "user" role by enrolling them for biometric verification, and for "administrator role" by setting the password. However this functionality is outside the scope of this evaluation (see also above).
FMT_SMR.1	User/TOE administrator	The TSF associates the roles with the users by their identification/authentication mechanism, see FIA_UAU and FIA_UID.
	None	N/A
	Application note: more complex roles?	N/A, there are no more complex roles.

9 References

[19795]	ISO/IEC 19795, Biometric performance testing and reporting- Part 1:Principles and framework
[19792]	ISO/IEC 19792, Security Evaluation of Biometrics, 3rd Committee Draft
[BEM]	Biometrics Evaluation Methodology Supplement, Version 1.0, August 2002
[BVMPP]	Protection Profile for Biometric Verification Mechanisms (BVMPP), version 1.3, 2008-08-07
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and general model, dated July 2009, version 3.1 R3 • Part 2: Security functional requirements, dated July 2009, version 3.1, R3 • Part 3: Security assurance requirements,

	dated July 2009, version 3.1, R3
[CEM]	Common Evaluation Methodology for Information Technology Security – Evaluation Methodology, dated July 2009, version 3.1 R3