Federal Office
for Information Security

Biometric Verification Mechanisms Protection Profile

BVMPP

v1.3

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

Table of content

1. PP introduction

1.1 PP Reference

Title:	Protection Profile for Biometric Verification Mechanisms (BVMPP)
Version	1.3
Date	2008-08-07
Author	Nils Tekampe, Boris Leidner, TÜV Informationstechnik GmbH
Registration	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Certfication-ID	BSI-CC-PP-0043
CC-Version	3.1 Revision 2
Keywords	authentication; biometric; iris-recognition; face-recognition; fingerprint-recognition; identification; Protection Profile; verification; voice-recognition

1.2 PP Overview

The scope of this Protection Profile is to describe the functionality of a biometric verification system in terms of [CC] and to define functional and assurance requirements for such a 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.

This Protection Profile aims to be applicable to any biometric verification system, independent of the used biometric modality. It is therefore written in a generic way. However, where a certain biometric modality had to be considered, this PP focusses on fingerprint recognition.

Please note that inside this Protection Profile the enrolment and the identification process of a biometric system (see also chapter 2.1) are not considered. Chapter 2 gives a more details overview about the design of the TOE and its boundaries.

2. TOE Description

Biometric products, which claim to be conformant to this Protection Profile, provide a verification process for the claimed identity of a human being using a unique characteristic of their body.

This PP covers the biometric verification process on a generic level and should be applicable to any biometric verification system. Therefore the descriptions of the requirements for the TOE are kept on a very generic level so that the development of conformant products is possible for various IT environments. Where a relation to a certain biometric characteristic has been necessary, fingerprint recognition has been used in this PP.

The basic processes of a biometric system are described in chapter 2.1.

This PP describes a biometric system that operates in a verification mode only. Biometric Identification is not addressed within this PP. Furthermore the enrolment process is out of scope of this PP and it is assumed that all authorized users have been enrolled. Last but not least a biometric verification system that is conformant to this PP aims to verify the identity of a user for the purpose of controlling access to a portal.

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 every biometric system that is conformant to this PP includes mechanisms 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 specifically important to limit the ability to change security relevant settings of the biometric functionality to an authorized administrator.

2.1 Description of biometric processes

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 a 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.

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

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.

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

2.2 Wording in context of Common Criteria

In context of [CC] 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 chapter 2.1 Because biometric identification is out scope of this PP there should not be any conflict in wording. To avoid any misunderstanding: the wording in this PP is as follows:

1. Identification: As defined in [CC]
2. Authentication: As defined in [CC]
3. (Biometric) Verification: biometric verification as described in chapter 2.1

2.3 TOE configuration and TOE environment

Beside the fact that many biometric characteristics could be used to build a biometric verification system that conforms to this PP, a biometric system in general could be realized in two major configurations:

- **A Stand-alone solution:** The stand-alone solution is not integrated into another network and works with one database
- **A Network-integrated solution:** The network-integrated solution is embedded into an existing network.

This PP describes a biometric verification system as a stand alone solution but should be applicable to network integrated solutions as well.

The security related problems of those distributed systems should then be considered via:

1. Assumptions for the TOE environment: e.g. firewall, Virus and Trojan protection, trustworthy internal network environment, physical protection

2. Requirements for additional functionality: e.g. encrypted transmission, encrypted storage, clear memory, etc.

The performance of biometric systems depends on physical environmental conditions in its environment. Those environmental factors that could influence a biometric system are dependent on the used biometric modality and on the used capture device. Because the capture device is not necessarily part of the TOE and assumed to work within acceptable ranges, those factors are not mentioned here in more detail. However, the author of a ST of has to describe the environment of the TOE in more detail. It has to be specified, which capture devices are suitable to be used with the TOE and how the environment has to be for these devices.

It is likely that the TOE is not able to run stand-alone. In this case the ST author shall specify the IT components which are necessary to run the TOE (e.g. a PC with a specific operating system).

2.4 TOE boundary

A simplified model of the biometric verification system and its boundaries is shown in Figure 1. Because the capture device is not necessarily part of the TOE the biometric verification system as described in this PP may be a pure software system. However, it should be noted that the ST author has the option to decide that the capture device is part of the TOE. This may be necessary in cases where the capture device contributes to the Security Functionality of the TOE.

The functionality to perform an audit review is not part of the TOE but of the environment. Nevertheless, the TOE of course has to include functionality for auditing.

Furthermore, the database where the biometric references and other information is stored in, is not part of the TOE. The TOE has to provide an interface to this database that ensures a correct and secure communication.

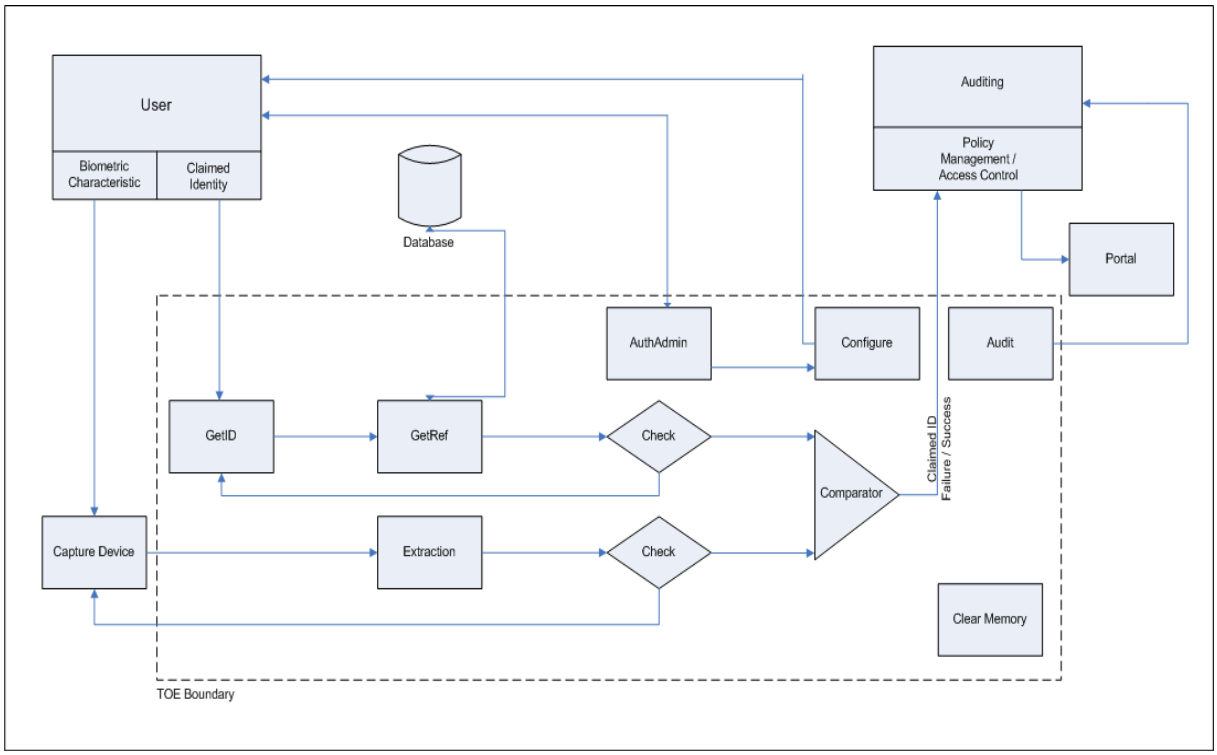

Figure 1: Generic TOE design

- **Get ID:** 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.
- **GetRef:** This component is responsible for getting the stored (already enrolled) biometric reference related to a claimed user's identity.
- **Extraction:** In preparation of the verification process a feature vector has to be extracted from the captured data. This is the objective of this component. Optionally, the biometric data may be compressed.
- **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 could for example be realized via a SmartCard/PIN based mechanism. It is necessary to authenticate an administrator 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.
- **Comparator** (also called Matcher): This is an important component regarding the scope of this Protection Profile. It compares the enrolled biometric reference with the Biometric Live Record (BLR) and includes the determination whether these records match or not. A comparator 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 should 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, this component clears the content of memory after use. The information that has to be cleared is not limited to the verification result but especially includes the biometric reference, BLR or any biometric raw data as well as authentication data for the administrator authentication. Because the memory that has to be cleared could belong to every other component no lines are drawn into the figure for this component.
- **Audit:** This component of the TOE records security relevant events to ensure that information exists to support effective security management (e.g. verification protocol, retry counter, etc.).

Some security related components, functions and interfaces of the TOE environment should be considered here:

- **Capture Device:** This component that is also called sensor is responsible for capturing the biometric characteristic from the user and forwards it into the biometric system. Depending on the used sensor technology also additional processes as a liveness detection or an image enhancement could be performed by this device.
- **Policy manager**: The result of the biometric verification process 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.
- **Storage:** 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.

- **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.
- **Auditing**: The environment may provide additional audit functionalities and has to provide a mechanism for audit review of the TOE audit logs.
- **Transmission / Storage:** The environment cares for a secure communication and storing where security relevant data is transferred to or from the TOE.

3. Conformance Claims

3.1 Conformance statement

The PP requires strict conformance of any PPs/STs to this PP.

3.2 CC Conformance Claims

- This PP has been developed using Version 3.1 R2 of Common Criteria [CC]
- This PP is conform to part II and III of [CC]; no extended components have been defined

3.3 PP Claim

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

3.4 Package Claim

- This Protection Profile conforms to assurance package EAL2 as defined in Common Criteria Part 3.

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 in the context of this Protection Profile.

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.

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). The following assets should be explicitly mentioned:

- **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

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.

A.CAPTURE The capture device as user visible interface operates inside its regular range and is suitable to be used with the TOE[2]. It is assumed that all environmental factors (e.g. lightning) are appropriate with respect to the used capture device and biometric modality.

Furthermore, it is assumed that bypassing the capture device in a technical manner is not possible. This assumption does not prevent an attacker from presenting an imitated or recorded biometric characteristic to the capture device because even in a guarded environment (and the TOE is primarily unguarded) such a misuse of the system would be possible. Because the capture device has to be accessible for each user a moderate physical robustness is presupposed.

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.

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 of a GINA replacement, audit functionality). Regarding the request of the claimed identity, which is necessary for the biometric authentication, the environment offers the possibility to integrate a claimed identity into the biometric verification process.
- The TOE environment provides a database for the biometric reference of enrolled users, whereby integrity and authenticity are ensured. Also in case of user controlled references (e.g. stored on SmartCard or token), measures exist to protect the authenticity and integrity of the biometric reference.
- 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

[2] **Application Note (ST):** The author of a ST has to specify one or more capture devices which are allowed to be used with the TOE and has to clearly define the range of operation. Furthermore, he has to provide evidences that the captures devices will work with the TOE. The TOE will have to be used with one of the specified capture devices in order to be in its certified configuration.

review the audit information of the TOE and to ensures 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.

A.PHYSICAL It is assumed that the TOE and its components are physically protected against unauthorized access or destruction. Physical access to the hardware that is used by the TOE is only allowed for authorized administrators. This does not cover the capture device that has to be accessible for every user.

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).

4.4 Threats

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 two different threat agents and corresponding adverse actions:

- 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.
- A real attacker who uses a large amount of biometric characteristics and who really wants to get unauthorized access to the portal. This type of threat agent is supposed to have further public knowledge on biometric verification systems.

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.

T.REPRODUCE An attacker may try to record and replay, imitate, or generate the biometric characteristic of an authorised 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.

The attacker will need further knowledge on biometric verification systems and the used biometric modality. He may use technical equipment for analysing and generation of the biometric characteristics.[3]

The attacker may also be supported by an authorized user of the TOE (e.g. to imitate his biometric characteristic).

T.RESIDUAL An attacker may try to take advantage of unprotected residual security relevant data (e.g. biometric data and settings) during a user's session or from a previous, already authenticated user.

In this way the attacker tries to get access to the security relevant settings of the TOE.

This threat covers several scenarios including:

- An attacker takes advantage of the verification memory content (e.g. by reading the memory content, cache or relevant temporary data) using a flaw in a user visible interface of the TOE.[4]
- An attacker may take advantage of residual images at the capture device. These are likely to be limited to cases where physical contact with the biometric capture device is necessary for the biometric modality (e.g. fingerprints [5])

The attacker needs further knowledge about the TOE to find and exploit a vulnerability regarding residual data in memory.

T.ROLES An already enrolled and authenticated user may try to exceed their privileges. Two types of this threat are possible within the scope of this PP:

1. If more than one portal is secured by the TOE, an authorized user

[3]Fingerprint and hand geometry systems are known to be vulnerable to artefacts. The setup costs are often low making the production of artefacts worthwhile for impostors for common use biometric technologies.

[4]A physical access to the components of the TOE is not possible for an attacker due to the Assumption A.PHYSICAL.

[5]The author of this PP is aware of the fact that the capture device is primarily part of the environment. But in an unguarded environment it is impossible to prevent an attacker from exploiting a residual characteristic that remains on the sensor. In the scope of this PP, this threat is therefore included. If the capture device of a TOE is not vulnerable to this kind of attack, this part of the threat may be countered implicitly be the use of a certain sensor technology.

may try to get access to a portal where he has no rights for.

2. An authorized user may try to get administrator privileges in order to modify the threshold settings of the system or other secondary assets.

No special knowledge is needed by the attacker to identify the general possibility because each authorized user of the system knows (after his own enrolment process) that an administrator account with higher privileges exists.

4.5 OSPs

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

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.

Application Note: Reasonable requirements on error rates are highly dependent on other characteristics of the biometric authentication mechanism. Characteristics that shall be considered to decide on the acceptable values include (but are not limited to):

- The number of allowed unsuccessful authentication attempts,
- The time that is needed to process one authentication attempt,
- The concrete environment of the TOE

The ST author should consider [19795] in order to identify the security relevant error rates and provide a justification for the choice of security relevant error rates.

5. Security Objectives

5.1 Security Objectives for the TOE

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.

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

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.

An “Exact match”[6] comparison should not be counted as a positive verification as it may be a replay attempt and should be recorded in the audit log.

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

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.

O.RESIDUAL The TOE shall ensure that no residual or unprotected security relevant data remains after operations are completed.

[6]The term “Exact match” in this context refers to a result of the comparison that is so “good” that it is likely that it is the result of a replay attack.

Application Note: It is often useful for a biometric system to provide feedback to legitimate users in order to help them to be verified by the system. For example, a fingerprint system may provide an image of the captured fingerprint to the user in order to facilitate the correct positioning of the finger and the generation of a good sample.

However, this feedback shall not be such, as to help impostors to gain unauthorised access; for example by providing "scores" which might allow impostors to train themselves on the system and observe how close they are to being identified or verified by the system.

5.2 Security objectives for the TOE or its operational environment

Due to the broad spectrum of biometric technology it is not possible to specify on the level of this PP whether some aspects of threats are countered by the TOE itself or the environment or a combination of both. Parts of the threat T.RESIDUAL (exploiting residual data at the capture device) and the threat T.REPRODUCE can optionally be countered in the environment of the TOE.

Therefore, the following objectives (that serve to counter those threats) have neither been assigned to the TOE nor its environment. The ST author is in charge of describing whether the TOE or the environment is responsible for these objectives. For cases where the TOE is able to fulfil theses objectives it is of course preferable to fulfil theses objectives with requirements for the TOE. In this case the ST author is in charge of defining those objectives in form of appropriate SFRs. The PP author provides a recommendation for SFRs used to model those objectives in chapter 8.1.

Please note that it should be specifically considered to assign those objectives to the TOE in cases where the capture device is part of the TOE.

OE.NO_REPRODUCE Recorded and replayed, imitated or generated biometric data must not be accepted as legitimate by the biometric system. This includes forgery of complete biometric samples.

OE.RESIDUAL_CAPTURE It has to be assured that residual data that may remain at a capture device after use cannot be used to gain access.

Application Note: In some biometric technologies the capture device is responsible to perform a check against recorded and replayed, imitated or generated biometric data. Because the capture device is not part of the TOE as specified in this PP it is here not possible to determine whether the TOE or its environment have to counter these kinds of attacks. If possible with the specific technology, the ST author is in charge of defining this objective as an objective for the TOE.

Application Note: In general the capture device that is outside the TOE is responsible to ensure that no residual data remains after it has been used. But in some biometric technologies it is also possible that residual data remains at the capture device but the TOE is able to detect and prohibit the use of this data.

5.3 Security objectives for the operational environment

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.
OE.CAPTURE	It shall be ensured that the capture device as user visible interface operates inside its regular range and is suitable for to be used with the TOE[7]. This includes that all environmental factors (e.g. lightning) are appropriate with respect to the used capture device and biometric modality. Furthermore, it has to be ensured that bypassing the capture device in a technical manner is not possible. Because the capture device has to be accessible for each user a moderate physical robustness has to be ensured.
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 ensure the authenticity and integrity of this data.
OE.ENVIRONMENT	The TOE operating equipment and adequate infrastructure shall be available (e.g.: operating system, database, LAN, public telephone, and guardian). Specifically the following things have to be ensured: ● The direct environment of the TOE has to support the functionality of the biometric system (e.g.: integration of a GINA replacement, audit functionality). Regarding the request of the claimed identity, which is necessary for the biometric authentication, the environment shall offer the possibility to integrate a claimed identity into the biometric verification process. ● The TOE environment shall provide a database for the biometric references of enrolled users, whereby integrity and authenticity have to be ensured. Also, in case of user controlled biometric references (e.g. stored on SmartCard or token), measures shall exist to protect the authenticity and integrity of the biometric reference. ● The environment has to implement the access control functionality for the protected portal. Specifically, if the environment has more than one portal that is secured using the services of the TOE the environment has to ensure that after authentication of a user (by the TOE) a portal is only opened if the user has the necessary permission. ● The environment shall ensure a secure communication of security relevant data from and to the TOE.

[7]**Application Note (ST):** The author of a ST has to specify one or more capture devices which are allowed to be used with the TOE and has to clearly define the range of operation. Furthermore, he has to provide evidences that the captures devices will adequately work with the TOE. The TOE will only be in its certified configuration when one of the specified capture devices is used.

	• The environment shall 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 has to be free of viruses, trojan horses, and other malicious software. • The TOE environment shall provide reliable time stamps.
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.
OE.FALLBACK	A fall-back mechanism for the biometric verification system shall 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).

5.4 Security Objectives rationale

5.4.1 Overview

The following table gives an overview, how the assumptions, threats, and organisational security policies are addressed by the security objectives. The text of the following subchapters justifies this more detailed.

	O.AUDIT_REACTION	O.ROLES	O.BIO_VERIFICATION	O.AUTH_ADMIN	O.RESIDUAL	OE.NO_REPRODUCE	OE.RESIDUAL_CAPTURE	OE.ADMINISTRATION	OE.CAPTURE	OE.ENROLMENT	OE.ENVIRONMENT	OE.PHYSICAL	OE.FALLBACK
T.ROLES	X	X		X							X		
T.RESIDUAL	X				X		X						
T.REPRODUCE	X					X							
T.MODIFY_ASSETS	X	X		X							X		
T.BRUTEFORCE	X		X										
OSP.ERROR			X										
OSP.USERLIMIT	X												
A.ADMINISTRATION								X					
A.CAPTURE									X				
A.ENROLMENT										X			
A.ENVIRONMENT											X		
A.PHYSICAL												X	
A.FALLBACK													X

5.4.2 Coverage of the security objectives

The TOE security objective **O.AUDIT_REACTION** can be traced back to the threats T.BRUTEFORCE (to log the amount/values of the attack and the attacked user identity and to keep the system in a secure state in such a situation), T.REPRODUCE, T.RESIDUAL, T.MODIFY_ASSETS (each to log that an unsuccessful impostor attempt happened), T.ROLES (because it audits every unsuccessful authentication attempt to an administrators account and locks the system in insecure states), and OSP.USERLIMIT because the demanded user limit from OSP.USERLIMIT is realized via O.AUDIT_REACTION.

The TOE security objective **O.ROLES** (the TOE shall limit access to administrative functions) can be traced back to the threat T.ROLES as directly follows and to T.MODIFY_ASSETS as the role concept supports the limitation of management function to administrators.

The TOE security objective **O.BIO_VERIFICATION** as the core objective for the biometric system can be traced back to the threats T.BRUTEFORCE (to be resistant against brute force attacks) and OSP.ERROR because O.BIO_VERIFCATION requires that the biometric verification mechanism meets the limits for the security relevant error rates as required by OSP.ERROR.

The TOE security objective **O.AUTH_ADMIN** (the TOE shall be able to authenticate an administrator by a non biometric mechanism) can be traced to the threats T.ROLES because it describes the role concept of the TOE and T.MODIFY_ASSETS because this objective is responsible for authentication of the administrator which is important to enforce the limitation of administrative operations to administrators.

The TOE security objective **O.RESIDUAL** can be traced back to the threat T.RESIDUAL as directly follows.

The TOE security objective **OE.NO_REPRODUCE** (the TOE shall be resistant against fake and similar attacks) can be traced back to the threat T.REPRODUCE as directly follows.

The TOE security objective **OE.RESIDUAL_CAPTURE** can be traced back to the threat T.RESIDUAL as T.RESIDUAL has the aspect that an attacker may use residual data that remains on the capture device.

5.4.3 Coverage of the assumptions, coverage of security objectives for the environment

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

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

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

The assumption **A.ENVIRONMENT** is covered by security objectives **OE.ENVIRONMENT** as directly follows.

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

The assumption **A.FALLBACK** is covered by objective **OE.FALLBACK** as directly follows

For all assumptions, the corresponding objectives are stated in a way, which directly correspond to the description of the assumption. It is clear from the description of each objective that the corresponding assumption is covered, if the objective is valid. Nevertheless some objectives exceed the statements of the assumptions they cover.

5.4.4 Countering the threats

The threat **T.ROLES** is fully countered by a security objective combination of O.AUDIT_REACTION, O.ROLES, O.AUTH_ADMIN and OE.ENVIRONMENT. O.AUTH_ADMIN ensures a secure authentication of administrators. O.ROLES ensures that only authorized administrators are allowed to perform the administration of the TOE via limiting access to security relevant data of the TOE to administrators. O.AUDIT_REACTION logs every impostor attempt. Regarding the part of the threat that a user may try to gain access to another portal as he has rights for, this threat is covered by the environment via OE.ENVIRONMENT because the decision whether a user gets access to a portal is done by the policy management of the environment.

The threat **T.BRUTEFORCE** (using a large amount of possible biometric data to verify against a wrong claimed id) is fully countered by a security objective combination of O.AUDIT_REACTION and O.BIO_VERIFICATION. O.BIO_VERIFICATION ensures that the verification process itself is done with an appropriate reliability and that the chance of impostor brute force attempts is less then the specified limit for the assurance claim of the TOE. O.AUDIT_REACTION records an unusual high amount of verification attempts to one claimed ID or an unusual high amount of unsuccessful verification attempts against different IDs and reacts via blocking the verification function system for a specific time or informing an administrator.

The threat **T.RESIDUAL** is fully countered by a security objective combination of O.RESIDUAL, OE.RESIDUAL_CAPTURE and O.AUDIT_REACTION. O.RESIDUAL directly protects against memory attacks as described in T.RESIDUAL, OE.RESIDUAL_CAPTURE counters the possibility to use residual data from the capture device and O.AUDIT_REACTION audits a potential impostor attempt.

The threat **T.REPRODUCE** is fully countered by a security objective combination of OE.NO_REPRODUCE (as directly follows from the security objective definition) and O.AUDIT_REACTION because the impostor attempt is logged.

The threat **T.MODIFY_ASSETS** is countered by a combination of the objectives O.ROLES, O.AUTH_ADMIN, O.AUDIT_REACTION and OE.ENVIRONMENT. O.ROLES is responsible to limit the access to security relevant objects of the TOE to authorized administrators. O.AUTH_ADMIN is responsible to authenticate the administrator. O.AUDIT_REACTION is logging an impostor attempt. OE.ENVIRONMENT prevents tampering with the database containing the BRRs.

5.4.5 Coverage of organisational security policies

The organisational security policy **OSP.ERROR** (the TOE must meet criteria for security relevant error rates) is directly met by O.BIO_VERIFICATION as this objective describes that the biometric verification mechanism has to reach the security relevant error rates as required by OSP.ERROR.

The organisational security policy **OSP.USERLIMIT** is met by O.AUDIT_REACTION because this objective ensures that unsuccessful verification attempts to one or more claimed IDs are logged and that the TOE reacts to keep itself in a secure state after a configurable number of those attempts occurred.

6. Extended Component definition

This PP 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. Those requirements comprise functional components from part 2 of [CC] and the assurance components as defined for the Evaluation Assurance Level 2 part 3 of [CC].

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 Security Functional Requirements for the TOE

The following table summarises all TOE functional requirements of this PP:

Class FAU: Security Audit	
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
Class FDP: User Data Protection	
FDP_RIP.2	Full residual information protection
Class FIA: Identification and Authentication	
FIA_AFL.1(1)	Authentication failure handling for users accounts
FIA_AFL.1(2)	Authentication failure handling for administrators accounts
FIA_ATD.1	User attribute definition
FIA_UAU.2(1)	User authentication before any action
FIA_UAU.2(2)	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.7	Protected authentication feedback
FIA_UID.2(1)	User identification before any action
FIA_UID.2(2)	User identification before any action
Class FMT: Security Management	
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
Class FPT: Protection of the TSF	
FPT_RPL.1(1)	Replay Detection

Table 1:Security Functional Requirements

7.1.1.1 Security audit (FAU)

Security audit data generation (FAU_GEN)

FAU_GEN.1	Audit data generation
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [*basic*] level of audit; and c) [assignment: *other specifically defined auditable events* ***or none***].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*assignment: other audit relevant information*].
Hierarchical to:	No other components
Dependencies:	FPT_STM.1

FAU_GEN.2	User identity association
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.
Hierarchical to:	No other components
Dependencies:	FAU_GEN.1 FIA_UID.1

Application Note: It should be noted that O.AUDIT_REACTION defines that the TOE has to be able to react to detected attacks in order to keep the system in a secure state. This reactive aspect of O.AUDIT_REACTION has been modelled in form of FIA_AFL.1(1) and FIA_AFL.1(2) as the examples in O.AUDIT_REACTION focus on brute force attacks against users or administrators accounts.

If additional reactive capabilities should be needed by a TOE the ST author should consider to model those capabilities and extend the set of SFRs by FAU_ARP.1 and FAU_SAA.1

7.1.1.2 User data protection (FDP)

Residual information protection (FDP_RIP)

FDP_RIP.2	Full residual information protection
FDP_RIP.2.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*deallocation of the resource from*] all objects.
Hierarchical to:	FDP_RIP.1
Dependencies:	No dependencies

7.1.1.3 Identification and authentication (FIA)

Authentication failures (FIA_AFL)

FIA_AFL.1(1)	Authentication failure handling for users accounts
FIA_AFL.1.1(1)	The TSF shall detect when [an administrator configurable positive integer within *[assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [*the biometric verification of one or more users*].
FIA_AFL.1.2(1)	When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [*disable the biometric verification for the corresponding user and [assignment: list of other actions]*]**.**
Hierarchical to:	No other components
Dependencies:	FIA_UAU.1

FIA_AFL.1(2)	Authentication failure handling for administrators accounts
FIA_AFL.1.1(2)	The TSF shall detect when [an administrator configurable positive integer within *[assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [*the authentication of one or more administrators accounts*].
FIA_AFL.1.2(2)	When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [*disable the verification for the corresponding administrator account and [assignment: list of other actions]*].
Hierarchical to:	No other components
Dependencies:	FIA_UAU.1

Application Note: The range of acceptable values for unsuccessful authentication attempts and the action to be taken in case this valued is met or surpassed is highly depending on the used biometric technology and the concrete application of the biometric system. Specifically, parallel attacks on multiple accounts have to be considered here and those are dependent on the workload of the respective TOE. As such the open operations in FIA_AFL.1(1) and FIA_AFL.1(2) are left to the ST author.

User attribute definition (FIA_ATD)

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

- user ID or name
- biometric reference
- role
- *[assignment: other attributes or none]*].

Hierarchical to: No other components

Dependencies: No dependencies

User authentication (FIA_UAU)

FIA_UAU.2(1) User authentication before any action

FIA_UAU.2.1(1) **For biometric verification, T**the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1

Application Note: The security relevant error rates of the biometric verification function that is used to realize this authentication has to be lower than or equal to the value for those rates demanded by OSP.ERROR.

FIA_UAU.2(2) User authentication before any action

FIA_UAU.2.1(2) **For non biometric verification, T**the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1

Application Note: Typically, authentication is a function provided by a TOE whose main purpose is entirely different (e.g. office automation network, a numerical analysis system, etc.). In this case, however, authentication is assumed to be the prime purpose of the TOE. This security functional requirements (FIA_UAU.2(1)), therefore, expresses the primary objective of the TOE.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [

- a biometric verification mechanism and
- a non biometric verification mechanism

] to support user authentication.

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))
- *[assignment: other rules describing how the multiple authentication mechanisms provide authentication or none]*.

]

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only [*a message indicating that verification efforts are in progress*] to the user while the **biometric** authentication is in progress.

Hierarchical to: No other components

Dependencies: FIA_UAU.1

User identification (FIA_UID)

FIA_UID.2(1)	User identification before any action
FIA_UID.2.1(1)	**For biometric verification, T**~~**t**~~he TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Hierarchical to:	FIA_UID.1
Dependencies:	No dependencies

FIA_UID.2(2)	User identification before any action
FIA_UID.2.1(2)	**For non biometric verification, T**~~**t**~~he TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Hierarchical to:	FIA_UID.1
Dependencies:	No dependencies

7.1.1.4 Security management (FMT)

Management of functions in TSF (FMT_MOF)

FMT_MOF.1	Management of security function behaviour
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, • [*assignment: other functions or none*] to [*TOE administrators*].
Hierarchical to:	No other components
Dependencies:	FMT_FMR.1 FMT_SMF.1

Management of TSF data (FMT_MTD)

FMT_MTD.1	Management of TSF data
FMT_MTD.1.1	The TSF shall restrict the ability to [change_default, query, modify, delete, clear, *[assignment: other operations or none]*] the [• *[assignment: list of security parameters which control the performance of the biometric system]* • [assignment: user security attributes] • *[assignment: other attributes or none]*] to [*TOE administrators*].
Hierarchical to:	No other components
Dependencies:	FMT_SMR.1 FMT_SMF.1

FMT_MTD.3	Secure TSF data
FMT_MTD.3.1	The TSF shall ensure that only secure values are accepted for [• biometric reference records • *[*assignment: *list of other TSF data or none]*]
Hierarchical to:	No other components
Dependencies:	FMT_MTD.1

Specification of Management Functions (FMT_SMF)

FMT_SMF.1	Specification of Management Functions
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [• unlock a blocked user or administrator account • *[assignment: list of other management functions to be provided by the TSF or none]*].
Hierarchical to:	No other components
Dependencies:	No dependencies

Application Note: To allow this PP being applied to a wide variety of biometric technology and application cases many SFRs do have open assignments and selections that have to be completed by the ST author. As such it is not possible to finally decide, which of the SFRs do require dedicated management functionality to be defined in FMT_SMF.1.

The following table summarizes the recommendations from part II of [CC] with respect to the management functionality that may be required by the SFRs as used in this PP. This table should be used as a guideline for completion of the assignment in FMT_SMF.1

SFR	Management aspect to be considered
FIA_AFL.1	● management of the threshold for unsuccessful authentication attempts; ● management of actions to be taken in the event of an authentication failure.
FIA_UAU.2	● management of the authentication data by an administrator; ● management of the authentication data by the user associated with this data
FIA_UID.2	● the management of the user identities.
FMT_MOF.1	● managing the group of roles that can interact with the functions in the TSF;
FMT_MTD.1	● managing the group of roles that can interact with the TSF data.
FMT_SMR.1	● managing the group of users that are part of a role.
FPT_RPL.1(1)	● management of the list of identified entities for which replay shall be detected; ● management of the list of actions that need to be taken in case of replay.

Security management roles (FMT_SMR)

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [
- user
- TOE administrator
- *[assignment: additional roles or none]*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Hierarchical to: No other components

Dependencies: FIA_UID.1

Application Note: The roles as defined in FMT_SMR.1 do only represent a very simple concept of users and administrators. Depending on the concrete focus and application case of a TOE it may be necessary for the ST author to add additional roles or even to restructure the existing concept of roles. In any case the ST author will have to ensure an appropriate separation of administrative roles from standard users.

7.1.1.5 Protection of the TSF (FPT)

Replay detection (FPT_RPL)

FPT_RPL.1(1)	**Exact match** Replay detection
FPT_RPL.1.1(1)	The TSF shall detect **exact match** replay**s** for the following entities: [*biometric authentication data*].
FPT_RPL.1.2(1)	The TSF shall ~~**perform**~~ [*ignore the replayed data*] when replay is detected.
Hierarchical to:	No other components
Dependencies:	No dependencies

7.2 Security Assurance Requirements for the TOE

The minimum Evaluation Assurance Level for this Protection Profile is **EAL 2**.

The following table lists the assurance components which are therefore applicable to this PP.

Assurance Class	Assurance Component	Additional guidance available
Development	ADV_ARC.1	-
	ADV_FSP.2	-
	ADV_TDS.1	-
Guidance documents	AGD_OPE.1	See chapter 7.2.1
	AGD_PRE.1	See chapter 7.2.1
Life-cycle support	ALC_CMC.2	-
	ALC_CMS.2	-
	ALC_DEL.1	-
Security Target Evaluation	ASE_CCL.1	-
	ASE_ECD.1	-
	ASE_INT.1	-
	ASE_OBJ.2	-
	ASE_REQ.2	-
	ASE_SPD.1	-
	ASE_TSS.1	-
Tests	ATE_COV.1	See chapter 7.2.2
	ATE_FUN.1	See chapter 7.2.2
	ATE_IND.2	See chapter 7.2.2
Vulnerability Assessment	AVA_VAN.2	See chapter 7.2.3

Table 2: Assurance Requirements

Due to the special character of biometric technology, the following chapters provide the evaluators with some additional guidance for specific aspects of assurance classes. By the time this Protection Profile has been developed, no comprehensive methodology for evaluations of biometric technology has been available in the scheme of Common Criteria. Once such a methodology is available it may supersede the recommendations of the following chapters.

7.2.1 Additional guidance for Guidance documents

The following aspects of biometric technology may require special consideration during the development and the evaluation of the guidance documentation:

- Biometric system operation is greatly affected by physical environmental influences (e.g. light and sound levels, dust, humidity, and cleanliness of the biometric capture device) and those can affect the accuracy of the verification processes. Hence, guidance documentation should include information on environmental influences and ways of minimising those influences. Specific attention shall be paid to the descriptions of the limits of the environmental conditions under which the TOE is able to operate.
- Where it is possible to modify security relevant settings of the biometric functionality (e.g. the matching thresholds used in the comparison process), the documentation shall include a description of the effects when changing these values and the importance of those values in the context of security. If the certified version of a product only includes a subset of all possible settings of an important parameter this shall be clearly identified and the administrator shall be advised to ensure that the TOE is only operated using those values.
- Biometric information shall in principle be treated as personal information and aspects of privacy in the context of collecting, storing and handling biometric data shall be addressed in the guidance documentation.

7.2.2 Additional guidance for tests

The tests of the developer and the evaluators shall include statistic performance testing of the security relevant error rates. Such a test comprises three important steps:

1) The security relevant error rates will have to be identified and their maximum values have to be claimed by the developer
2) The security relevant error rates will have to be tested by the developer
3) The test of the developer shall be reviewed and (partly) repeated by the evaluator.

The evaluator shall seek guidance on those tests in relevant documentation. Specifically the evaluator shall consider the information given in [19792] and [19795].

Those error rates that have been identified to be relevant for the TOE and their maximum values (the tests have to show that the TOE does not exceed those values) shall be reported in the ST.

7.2.3 Additional guidance for Vulnerability Assessment

While biometric verification systems solve some of the problems that classical authentication mechanisms that are based on knowledge (e.g. a PIN) are facing, the nature of biometric technology leads to some specific vulnerabilities that are inherent for this kind of technology.

As such each evaluation of a biometric system will have to consider those vulnerabilities like the use of fakes or the imitation of biometric characteristics. Some of those vulnerabilities are addressed by the description of the threats in this PP.

In the context of this PP the evaluator should seek their primary guidance for vulnerability assessment in public sources listing typical vulnerabilities of biometric technology. Those sources should include (but not be limited to) [19792] and [BEM] or their successor versions.

Each of the identified vulnerabilities will have to be considered during the analysis. While it may be easy for some of the potential vulnerabilities to argue that they are not relevant on a theoretical level the assessment of other vulnerabilities may require penetration testing or deeper information about the system architecture.

7.3 Security Requirements rationale

7.3.1 Security Functional Requirements rationale

7.3.1.1 Fulfilment of the Security Objectives

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

	O.AUDIT_REACTION	O.ROLES	O.BIO_VERIFICATION	O.AUTH_ADMIN	O.RESIDUAL
FAU_GEN.1	X				
FAU_GEN.2	X				
FDP_RIP.2					X
FIA_AFL.1(1)	X				
FIA_AFL.1(2)	X				
FIA_ATD.1		X	X	X	
FIA_UAU.2(1)			X		
FIA_UAU.2(2)				X	
FIA_UAU.5			X	X	
FIA_UAU.7			X		
FIA_UID.2(1)			X		
FIA_UID.2(2)				X	
FMT_MOF.1		X			
FMT_MTD.1		X			
FMT_MTD.3			X		
FMT_SMF.1		X			
FMT_SMR.1		X			
FPT_RPL.1(1)			X		

Table 3:Fulfilment of Security Objectives

The following paragraphs contain more details on this mapping.

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.

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.

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.
- **FPT_RPL.1(1)** ensures that the TOE ignores biometric authentication data that matches to a biometric reference too well as such an “exact match” is likely to be the result of a replay attack.
- **FMT_MTD.3** assures that only secure values are accepted for TSF data that is used by the biometric verification process.

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.

O.RESIDUAL

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

7.3.1.2 Fulfilment of the dependencies

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

SFR	Dependencies	Fulfilled by
FAU_GEN.1	FPT_STM.1	See chapter 7.3.1.3
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.2
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)
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(1)
FPT_RPL.1(1)	-	-

Table 4:Security Functional Requirements

7.3.1.3 Justification for missing dependencies

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

7.3.2 Security Assurance Requirements rationale

The assurance level EAL2 has been chosen for this Protection Profile and additional guidance has been provided for some of the assurance components due to the special nature of the biometric technology.

EAL2 has been chosen because it provides a basic assurance that the TOE operates as specified in the ST. Further it is expected that the special characteristics of the biometric technology may cause problems and lead to a complex evaluation and certification process when evaluated on higher EALs.

7.3.2.1 Dependencies of assurance components

The dependencies of the assurance requirements taken from EAL2 are fulfilled automatically.

8. Appendix

8.1 SFRs for OE.NO_REPRODUCE and OE.RESIDUAL_CAPTURE

If the ST author decides to include OE.NO_REPRODUCE and OE.RESIDUAL_CAPTURE into the scope of the TOE, then the following SFRs should be used to model the security functionality. Both SFRs do not have any dependencies. As such they can be added to the scope of the TOE without considering any additional SFRs.

Unforgeable authentication (FIA_UAU.3)

FIA_UAU.3	Unforgeable authentication
FIA_UAU.3.1	The TSF shall [selection: *detect **and prevent, or just** prevent*] use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2	The TSF shall [selection: *detect **and prevent, or just** prevent*] use of authentication data that has been copied from any other user of the TSF.
Hierarchical to:	No other components
Dependencies:	No dependencies

Replay detection (FPT_RPL)

FPT_RPL.1(2)	**Extended** replay detection
FPT_RPL.1.1(2)	The TSF shall detect replay for the following entities: [*biometric authentication data residing on the capture device*].
FPT_RPL.1.2(2)	The TSF shall ~~**perform**~~ [*ignore the replayed data*] when replay is detected.
Hierarchical to:	No other components
Dependencies:	No dependencies

Application Note: FPT_RPL.1(2) refers to replay attacks which are not exact matches of the biometric references but can be discovered by other means (e.g. biometric fake detection).

Application Note: FIA_UAU.3 can be traced back to OE.NO_REPRODUCE and OE.RESIDUAL_CAPTURE. FPT_RPL.1(2) can be traced back to OE.RESIDUAL_CAPTURE.

8.2 Glossary

Term	Desription
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
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.
CC	Common Criteria - Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology
Comparison	The process of comparing biometric data with a previously stored biometric reference

Term	Desription
EAL	Evaluation Assurance Level
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
GINA	Graphical Identification and Authentication as part of an operating system
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.
Matching Score	A measure of similarity or dissimilarity between the biometric data and a stored template, used in the comparison process.
Multimodal biometris	A biometric system, which uses information from different biometrics - e.g. fingerprint and hand shape; or fingerprints from two separate fingers.
OS	Operating system
Portal	The physical or logical point beyond which information or assets are protected by a biometric system.
PP	Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
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.
ST	Security Target – A set of implementation-dependent security requirements for a specific TOE.
Threshold	A parametric value used to convert a matching score to a decision.
TOE	Target of Evaluation
TSF	TOE Security Functionality.
Verification	See chapter 2.1.
Verification system	A biometric system that provides a verification functionality.
WAN	Wide Area Network
WLAN	Wireless Local Area Network

8.3 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
[CC]	Common Criteria for Information Technology Security Evaluation – ● Part 1: Introduction and general model, dated September 2006, version 3.1 R1 ● Part 2: Security functional requirements, dated September 2007, version 3.1, R2 ● Part 3: Security assurance requirements, dated September 2007, version 3.1, R2
[CEM]	Common Evaluation Methodology for Information Technology Security – Evaluation Methodology, dated September 2007, version 3.1 R2