Bundesamt
für Sicherheit in der
Informationstechnik

Common Criteria Protection Profile

Biometric Verification Mechanisms

Common Criteria

BSI-PP-0016

Approved by the
Federal Ministry of the Interior

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn ▪ Postfach 200363, 53133 Bonn
Tel.: +49 (0) 1888 9582-0 ▪ Fax: +49 (0) 1888 9582-400 ▪ Internet: www.bsi.bund.de

—— this page was intentionally left blank ——

Document Revision History

Version	Date	Description
0.1 to 1.02		Drafts
1.03	2004-12-13	Successfully evaluated version
1.04	2005-08-17	Same as V1.03 but cover sheet, header, footer and formatting modified by BSI according to requirements for BSI publications

TABLE OF CONTENTS

LIST OF TABLES

List of Figures

Document Introduction

The development of this Protection Profile for Biometric Verification Mechanisms was sponsored by the German Federal Office for Information Security (BSI).

Correspondence and comments to this Protection Profile should be referred to:

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
D-53175 Bonn, Germany

Tel +49 1888 9582-0
Fax +49 1888 9582-400

Email bsi@bsi.bund.de

The following subchapters will provide some information for the further understanding of this document and introduce the reader to some used conventions:

A Acknowledgement

The author would like to acknowledge the significant contributions of four draft Protection Profiles for biometric systems [PP_UK_BD], [PP_US_BV_BR], [PP_US_BV_MR], and [PP_US_BS] as well as of the Biometric Evaluation Methodology Supplement [BEM] of the Common Criteria Biometric Evaluation Methodology Working Group. Due to its overall relevance, much of their work has been incorporated into this document.

B Application notes

Application notes are provided where they may contribute to the understanding of the reader. These notes, while not part of the formal statement of the Protection Profile, are included as an acknowledgment of the diverse backgrounds of potential users of this Protection Profile. It should be understood, that these application notes cannot completely substitute an understanding of the biometric techniques or related [CC] documents.

Application notes are divided into:

- General **Application Note (GEN) -** explains basic principles of the approach and provides general information.
- [CC] explanatory **Application Note (CC) -** provides details of Common Criteria definitions and usage; regarding biometric practitioners.
- Biometric **Application Note (BIO)** - provides details of biometric definitions and usage; applicable to [CC] practitioners.
- ST Development **Application Note (ST)** - provides guidance on the requirements for a ST production.
- PP **Application Note (PP)** - provides a further understanding of this Protection Profile.

C Notations

The notation, formatting, and conventions used in this PP are consistent with those used in the Common Criteria, Version 2.1, annotated with interpretations as of 2003-12-31, August 1999 [CC].

The [CC] allows several operations to be performed on security requirements; refinement, selection, assignment, and iteration are defined in paragraph 2.1.4 of [CC] part 2.

- **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 ("#")

D Abbreviations

Assumptions, threats, organisational security policies and security objectives (for TOE and environment) are assigned with a unique label for easy reference as follows:

A.<xxx>	Assumptions about the TOE security environment
O.<xxx>	Security objectives for the TOE
OE.<xxx>	Security objectives for the operating environment
OSP.<xxx>	Organisational security policies
R.<xxx>	Requirements for the TOE environment
T.<xxx>	Threats

E References

References in this document are specified with the help of brackets (e.g.: [<Reference>, <chapter number>]. A list of all used references <Reference> can be found in Annex C - References. Sometimes an additional <chapter reference> is given.

F Terminology

A complete list of used terms and abbreviations can be found in Annex B - Abbreviations and glossary. Thereby Common Criteria as well as biometric and IT technology terms relevant for this Protection Profile are described. Most of the definitions were taken out of the Biometric Evaluation Methodology [BEM] and supplemental from four previous draft biometric Protection Profiles [PP_UK_BD], [PP_US_BV_BR], [PP_US_BV_MR], and [PP_US_BS] as well as from the Common Criteria [CC].

1 Protection Profile Introduction

This chapter contains the following sections:

Identification (1.1)
Overview (1.2)
Common Criteria conformance (1.3)
Related documents (1.4)
Organisation (1.5)

1.1 Identification

Title:	Protection Profile for Biometric Verification Mechanisms
PP Version:	V1.04
PP Date:	2005-08-17
Editor:	Marcus Krechel, Nils Tekampe, TÜV Informationstechnik GmbH, Essen
Registration:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security
Certification ID:	BSI-PP-0016
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (annotated with interpretations as of 2003-12-31) [CC]
Keywords:	authentication; biometric; iris-recognition; face-recognition; fingerprint-recognition; identification; Protection Profile; verification; voice-recognition

1.2 Overview

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

Therewith the major mean 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 should be applicable to any biometric verification system, independent from the used biometric characteristic. It is therefore written in a generic way. Where a certain biometric characteristic had to be considered, fingerprint recognition is used while other biometric technologies are considered using application notes.

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

1.3 Common Criteria conformance

This PP is conformant to part II of [CC] and conformant to part III of [CC] at the selected Evaluation Assurance Level.

The assurance level for this Protection Profile is EAL2, augmented with ADV_SPM.1 and the minimum strength of function level is SOF-basic. Additional information related to [CC] biometric system evaluations are referenced in the Biometric Evaluation Methodology supplement [BEM]. For

the pure biometric verification process, the strength of function is defined in terms of the FAR (see Annex A)[1].

The assessment of the strength of any cryptographic algorithms used is outside the scope of the [CC], and therefore not part of this Protection Profile.

1.4 Related documents

All related Protection Profiles can be found in Annex C - References. They can be identified by [PP_<...>].

References to related documents regarding to the production of this Protection Profile are referenced in the Annex C as follows: [BEM], [CC], [ISO15446] and [CEM].

1.5 Organisation

The main chapters of this Protection Profile are **TOE description**, **TOE security environment**, **security objectives, IT security requirements**, **rationale**, and **annexes** as well as the Protection Profile **introduction** inside this chapter. This document is structured according to the Protection Profile requirements of [CC] part 1 and [ISO15446].

- **Chapter 2:** The TOE description provides general information about the TOE, its generic structure and boundaries.
- **Chapter 3:** The TOE security environment describes security aspects of the environment in which the TOE is intended to be used and the manner in which it is intended to be employed. The TOE security environment includes assumptions regarding the TOE's intended usage and environment of use (chapter 3.2), threats relevant to secure TOE operation (chapter 3.3) and organisational security policies (chapter 3.4), which must be complied by the TOE.
- **Chapter 4:** The statement of security objectives defines the security objectives for the TOE (chapter 4.1) and for its environment (chapter 4.2).
- **Chapter 5:** The IT security requirements are subdivided into TOE security requirements (chapter 5.1) and security requirements for the environment (chapter 5.2).
- **Chapter 6:** The rationale presents evidence that the security objectives satisfy the threats and policies. This chapter also explains how the set of requirements is complete relative to the security objectives and presents a set of arguments that address dependency analysis and Strength of Function.

The **annexes** offer a glossary and abbreviations as well as relevant references and biometric standards.

[1] **Application Note (BIO)**: The value of FRR is primarily not important, because it is not related to security. A system that rejects every user is not usable but it is secure. Nevertheless the FRR has to be within an acceptable range.

2 TOE Description

This chapter TOE Description contains the following sections:

Description of biometric processes (2.1)

Wording in context of Common Criteria (2.2)

TOE configuration and TOE environment (2.3)

Generic design of a biometric system (2.4)

TOE boundary (2.5)

Biometric products, which are conformant to this Protection Profile, provide a verification process to verify the claimed identity of a human being using a unique characteristic of his body.

This PP should cover 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 general level so that the manufacturing of conformant products is possible for various IT environments. Where a relation to a certain biometric characteristic was necessary, fingerprint recognition is used in this PP. In these cases other technologies are addressed via application notes.

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

This PP describes a biometric system that works in a verification mode. 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 with this PP has to verify the identity of a user for the purpose of controlling access to a portal[2].

Beside the biometric verification process every biometric system that is conformant to this PP includes a mechanism to identify and authenticate an administrator of the system with other means[3] than biometrics and to enforce an access control for the objects of the TOE. This is especially important to limit the ability to change the threshold settings for the biometric verification process to an authorized administrator.

2.1 Description of biometric processes

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

- Enrolment (2.1.1)
- Biometric Verification (2.1.2)
- Biometric Identification (2.1.3)

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

[3] **Application Note (GEN):** In general the identification and authentication of an administrator of a biometric system should never be realized thru the biometric verification process itself. There are two reasons for this: 1. A user could try to authenticate himself as an administrator thru the biometric process. Because of the FAR of this algorithm he could have success and would then compromise not only the security of the primary assets behind the portal but of the whole system. 2. An administrator could fail to authenticate himself thru the biometric verification process (because of the FRR) and would then not be able to configure the system.

Also if the biometric enrolment and identification are not addressed in this PP, they are introduced for the interested reader in the following subchapters. Because of the different use of the words identification and authentication chapter 2.2 clarifies the use of these words in context of this PP.

2.1.1 Enrolment

Usually, the enrolment process is the first contact of a user with the biometric system. This process is necessary because a biometric verification system has to 'learn' to verify the identity of a each user based on his 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 Identification Record (BIR) and stored in a database. The BIR is also called template.

The quality of the biometric template has to be assured and quality proofed. In the case of inadequate biometric characteristics or lower template 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 template regarding to possible physiology changes.

Only an administrator is 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.

An unauthorised user becomes an authorised user after a successful enrolment procedure.

As mentioned before: Within this PP it is assumed that the enrolment process has already been performed.

2.1.2 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 then gets the BIR 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 BIR from the database are similar enough, the claimed identity of the user is verified. Otherwise or if no BIR was found for the user, the claimed identity is refused.

The matching component of a biometric system that decides whether a BIR 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 BIR are more similar than demanded by the threshold, it returns successful verification, otherwise failed verification.

The process of biometric verification is pointed up in part b of the following figure.

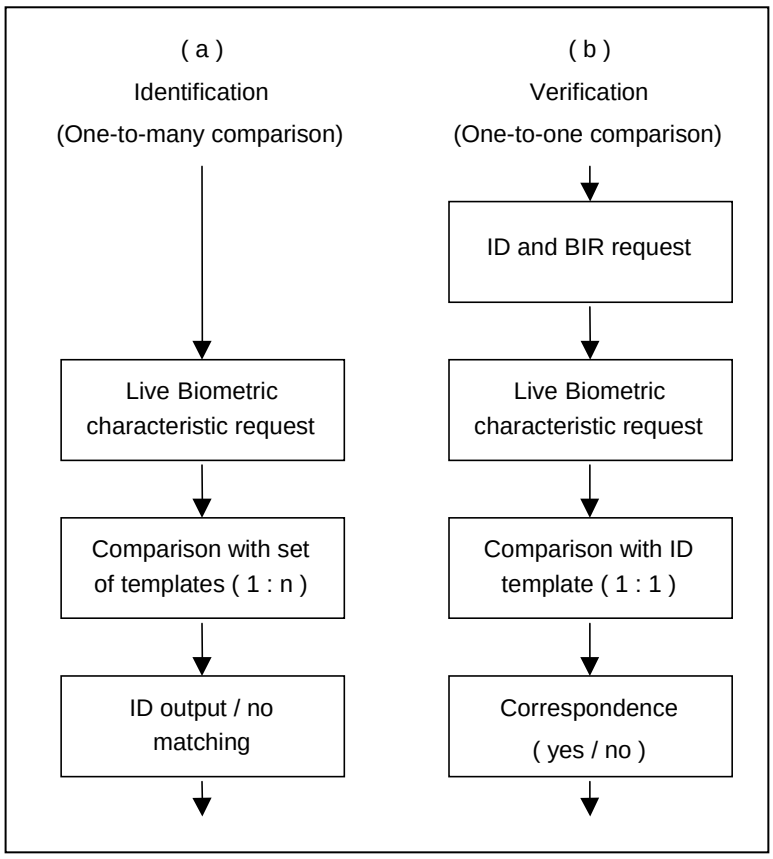

Figure 1: Identification / Verification flowchart

2.1.3 Identification

The objective of a biometric identification process is quite similar to a verification process. But in contrast to verification process there is no claimed identity necessary.

The system directly captures the biometric characteristic of a user and compares it to all BIR in the database. If at least one BIR is found to be similar enough, the system returns this as the found (and verified) identity of the user. The process of biometric identification in contrast to biometric verification is shown in the previous figure.

Biometric identification systems produce many additional problems. The possibility to find more than one BIR that matches or the higher error rates of those systems are only two of them.

The biometric identification process is out of scope of this PP. Please see [BEM] or [BPT] for further explanations.

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 2.1.3. Because biometric identification is out scope of this PP there should not be a 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. Verification: biometric verification as described in chapter 2.1.2

2.3 TOE configuration and TOE environment

Beside the fact that many biometric characteristics could be used to build a biometric verification system that is conformant 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 in an existing network.

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

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

The performance of biometric systems (especially the capture device) depends on physical environmental conditions in its environment. The environmental factors that could influence a biometric system are dependent on the used biometric characteristic and on the used capture device. Because the capture device is not part of the TOE and assumed to work within acceptable ranges, these factors do not have to be mentioned here[4].

2.4 Generic design of a biometric system

This chapter provides a general description of the main and necessary components of a biometric verification system.

The following figure shows a simplified biometric verification system which components are described in the following paragraphs[5]:

[4] **Application Note (ST):** The author of a ST of course has to describe the environment of the TOE more detailed. He has to specify, which capture devices are suitable to be used with the TOE and how the environment has to be for these devices. He should consider [BEM] for further details.

[5] **Application Note (ST):** The Security Target author is in charge of describing the components of the TOE more closely.

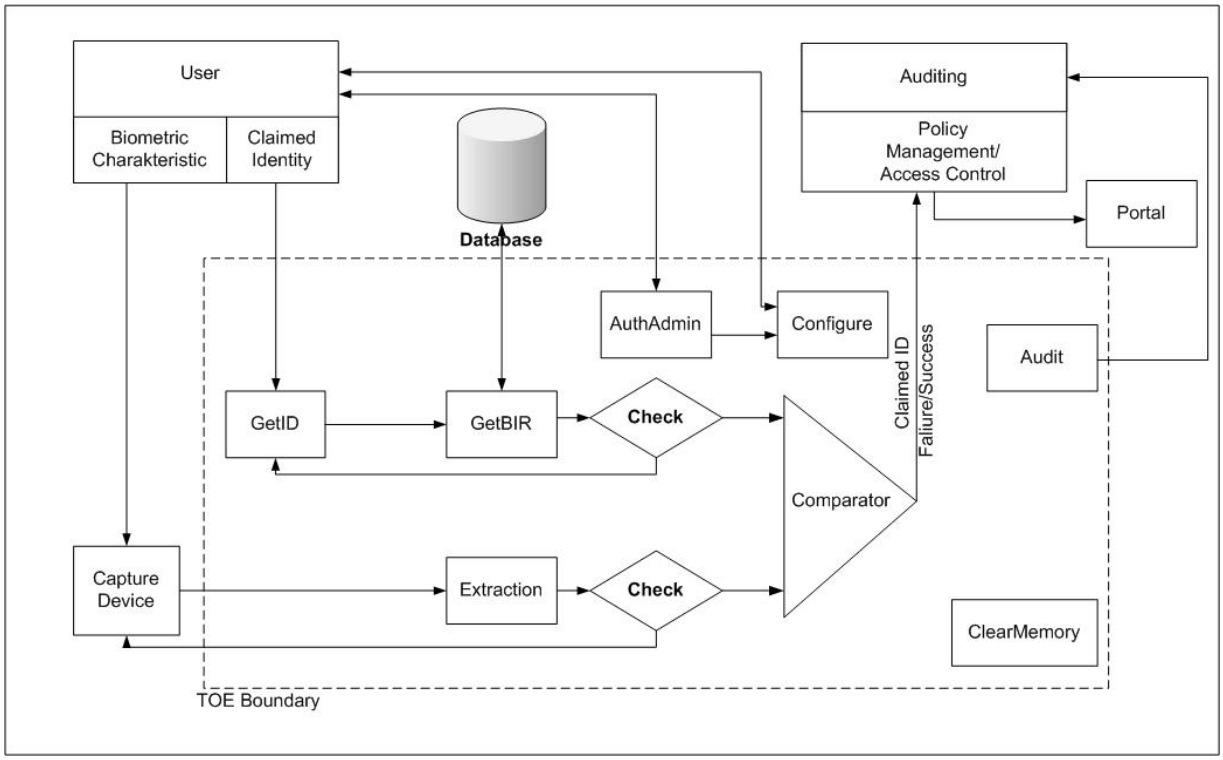

Figure 2: Simplified biometric verification system

- 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 BIR has to be used for comparison. Furthermore this component provides an obligatory user visible interface.
- **Get BIR:** This component is responsible for getting the stored (already enrolled) biometric identification record (BIR) related to one claimed user's identity.
- **Extraction:** In preparation of the verification a feature vector has to be extracted from the captured data. This is the objective of this component. Optionally, the biometric data can be compressed.
- **Check:** This component ensures the minimum quality requirements regarding the biometric templates (BIR; BLR). However, it can be differentiated between integrity and authenticity check during the process of getting the BIR as well as the quality check 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 especially necessary to authenticate an administrator before he is allowed to configure the thresholds of the system.
- **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[6].
- **Comparator** (also called Matcher): This is an important component regarding the scope of this Protection Profile. It compares the enrolled Biometric Identification Record (BIR) with the Biometric Live Record (BLR) and includes the determination whether these records match or not. Usually a comparator returns a value that shows how well the BIR and BLR match. To get a

[6] **Application Note (ST):** The ability to review audit information is arranged via the TOE environment.

successful/failed return value from the biometric system, the comparator considers a threshold during the matching process. If the BIR and the BLR are more similar than demanded by the threshold, the return value is success, otherwise it is fails.
"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 using.
  The information that has to be cleared is not limited to the verification result but especially includes the BIR, 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 signed in the picture before to or from 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 in 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 or an image enhancement could be performed by this device.[7]
- **Result passing on:** The verification result as Boolean value (verification successful or fail) is passed on via the policy management to the portal. Furthermore the claimed ID of the user is forwarded. The last decision, whether a user gets access to a portal is therefore done in the environment based on the biometric verification result.
- **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 door if the user has enough 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 the TOE. This is especially used to store the BIR 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.

[7] **Application Note (ST):** The capture device is outside the TOE because only in this way it is possible to keep this PP generic enough to cover all biometric technologies. The TOE relies on some functionalities provided by the environment. Nevertheless it is possible for a ST author to specify that the sensor is part of his TOE. In this case all the requirements regarding the capture device that are fulfilled by the environment in this PP would have to be fulfilled by the TOE. Because this scenario would exceed the functionality of the TOE as described in this PP it would still be possible to claim conformance to this PP.

2.5 TOE boundary

A simplified model of the biometric verification as and its boundaries is shown in Figure 2. Because the capture device is not part of the TOE the biometric verification system as described in this PP is a pure software system.

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 functionalities for auditing.

Furthermore the database where the BIR 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.

3 TOE Security Environment[8]

This chapter TOE Security Environment contains the following sections:

Assets and roles (3.1)
Assumptions (3.2)
Threats (3.3)
Organisational Security Policies (3.4)

3.1 Assets and roles

The following subchapters define assets and roles as follows:

3.1.1 Assets

Primary assets: Assets (i.e. user data), which are protected against unauthorised access and which do not belong to the TOE itself. The TOE permits access only after successful authentication as a result of the biometric verification. The primary assets, either physical or logical systems are behind a 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 templates). The following assets should be explicitly mentioned:

- **Biometric Identification Record (BIR):** This template 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 template includes the live (actual) biometric data (actual biometric characteristic and claimed user identity) to be verified against the BIR.
- The claimed identity of a user
- **User related security attributes** and authentication data for non biometric authentication

3.1.2 Roles

Roles are defined as follows:

TOE administrator: Is authorised to perform the administrative TOE operations and able to use the administrative functions of the TOE.

IT administrator: The IT administrator installs the TOE and maintains the IT system (e.g. access control), but not the TOE itself[9].

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 (BIR). He is allowed to get access to the protected portal.

Unauthorised user: A not enrolled user. He is not allowed to get access to the protected portal.

[8] **Application Note (ST)**: The Security Target must specify the intended environment of the biometric verification system and the certification will be valid only for that environment.

[9] **Application Note (PP):** IT and TOE administrator could be the same person, but it is not necessary or obligatory.

Attacker: An attacker is any individual who is attempting to subvert the operation of the biometric system. The intention may be either to gain unauthorized entry to the portal or to deny entry to legitimate users.

3.2 Assumptions

This chapter describes the assumptions about the operating environment including physical, personnel, and connectivity aspects[10].

A.ADMINISTRATION
The TOE- and IT-administrator are well trained and can be trusted (non hostile), read the guidance documentation carefully, completely understand and apply it.

Moreover, the TOE administrator is responsible to accompany the TOE installation and oversee the biometric system requirements regarding to 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 for the use with the TOE[11]. Therefore, environmental influences must be assured regarding the operating environment. Furthermore it is assumed that a bypassing of the capture device in a technical manner is not possible. This assumption does not exclude the possibility to present 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 is publicly available moderate physical robustness is presupposed[12].

A.ENROLMENT
The enrolment is assumed to be already performed and therefore, the BIR for each authorized user is assumed to be given. The generated BIR suffices minimum quality standards and is linked with the correct user[13].

Additionally it is assumed that all biometric templates are protected stored and measures regarding to authenticity and integrity are available.

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).[14]

- Operating System: It is assumed that the biometric system underlying operating system compatibly supports the functionality of the biometric system (e.g.: GINA replacement, audit functionality). Regarding the request of the claimed identity, which is necessary for the biometric authentication, the underlying operating system offers the possibility to integrate a claimed identity into the biometric verification process[15].

---

[10] **Application Note (ST):** If needed, further assumptions must be added in the Security Target.

[11] **Application Note (ST):** The author of a ST has to specify which capture devices are allowed to be used with the TOE and has to clearly define the range of operation.

[12] **Application Note (ST):** Otherwise, additional assumptions like a controlled or guarded capture device as well as restricted admittance should be considered.

[14] **Application Note (ST):** The ST author is in charge of describing the environment for the TOE more closely and adjusting this quite general assumption.

[15] **Application Note (ST):** Different scenarios are imaginable, e.g.:

- The operating system might support a replacement of the GINA and therefore the user has to perform a two-stage authentication (first GINA supported identification and second biometric verification).

Additional it is assumed that the operating system is able to protect itself and its own functionality (e.g.: policy management, access control, non-authenticated start-up).

- Storage: The TOE environment provides a database for the already enrolled biometric templates, whereby integrity and authenticity are guaranteed. The storage is a secure IT-product (e.g. SmartCard or hard disk in a secure area) and provides an access interface for the TOE.
  In case of user supplied templates (e.g. stored on SmartCard or token), measures exist to protect the authenticity and integrity of the template.
- Transmission: The environment takes care for a secure communication of security relevant data from and to the TOE.
- Audit: It is assumed that the environment provides a functionality to review the audit information of the TOE and to ensures that only authorized administrators are able to do this
- Beside this it is assumed that the surrounding TOE environment is Virus, Trojan, and malicious software free.

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 TOE or IT administrators. This does not cover the capture device that has to be accessible for each user.

A.FALLBACK

It is assumed that a fallback mechanism for the biometric verification system is available that reaches at least the same security level as the biometric verification system does. This fallback system is used especially if an authorized user is rejected by the biometric verification system (False Rejection).

3.3 Threats

General threats that need to be considered are described as follows[16]:

T.BRUTEFORCE

An attacker may use a brute force attack to find biometric data of a (e.g. randomly) chosen user's identity in order to get verified. During this attack a fraction of possible characteristics until one’s matching is presented to the TOE. This threat also covers two distinct scenarios:

- A not really hostile user who just tries to get verified with a wrong claimed identity a few times. The motivation if these people is usually just curiosity
- A real attacker who uses a large fraction of biometric characteristics and who really wants to get an illegal access to the portal.

This threat can be performed without a specific knowledge about the TOE. It is well known that biometric system have error rates that could lead to success for such an attack. But of course also in a non guarded environment the time to perform such an attack is limited thru the normal usage of the TOE by authorized users. The temptation to perform such an attack on the other hand is quite high especially for not really hostile users.

- The presupposed claimed identity could be reached through an assured identity via e.g. token or SmartCard (appanage based).

[16] **Application Note (BIO):** Through the presupposed enrolment it is not necessary to consider threats, which are related to the enrolment.

T.MODIFY_ASSETS

An attacker may modify secondary assets like biometric templates or security-relevant system configuration data or settings.

Such attacks could compromise the integrity of the user security attributes (e.g. BIR) resulting in an incorrect result that might give illegal 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 an impostor may succeed in gaining entry 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 template) of an authorised user with the aim of enabling an impostor 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 template, containing biometric data belonging to an impostor, with the aim of enabling the impostor to gain entry to the portal.

This kind of attack usually presupposes special knowledge about the TOE and often special equipment. Which kind of knowledge or equipment is needed is highly dependent on the identified vulnerability the threat tries to exploit.

T.REPRODUCE

An attacker may try to record and replay, imitate, or generate the biometric characteristic of an authorised user. Therefore, the attacker could use technical equipment for analysing and generation of the biometric characteristics[17].

Therefore, an attacker may use an artificial replica to gain access. If an impostor can access a biometric sample or template, the impostor may be able to produce an artefact with an equivalent biometric template.

This vulnerability is not very difficult to identify. Furthermore the time that is needed to exploit this vulnerability is quite moderate. But depending on the used biometric characteristic the efforts of time and money to create an artefact can be quite high.

T.RESIDUAL

An attacker tries to take advantage of unprotected residual security relevant data (biometric data, templates, and settings) during a user's session or from a previous, already authenticated user. Several different scenarios are possible:

- An attacker takes advantage of the verification memory content (e.g. by reading the memory content, cache or relevant temporary data).
- 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 involved, the obvious case are fingerprints[18].

[17] **Application Note (BIO):** 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.

[18] **Application Note (ST):** The author of this PP is aware of the fact that the capture device is part of the environment. But in an unguarded environment it is impossible to prevent an attacker from exploiting a residual characteristic. In the scope of this PP, this threat is therefore possible. If the capture device of a TOE is not vulnerable in this kind, this part of this threat has not to be part of the ST.

A physical access to the components of the TOE is not possible for an attacker because of the Assumption A.PHYSICAL. For the first kind of this attack (taking advantage of memory content) the attacker would therefore have to use a flaw in the user visible interfaces of the TOE.

At some biometric systems this vulnerability can be obviously. This is highly dependent on the used capture device. In these cases the effort of time and money to identify this vulnerability is quite moderate.

On the other hand, an attacker needs special knowledge about the TOE to find and exploit a vulnerability regarding residual data in memory. The effort of time and money that is needed to attack a biometric system via taking advantage of residual data in memory could also be quite high.

T.ROLES

An already enrolled and authenticated user tries to exceed its authority.

Two types of this threat are possible within the scope of this PP:

- If more than one portal is secured by the TOE, an authorized user may try to get access to a portal where he has no rights for.
- An authorized user may try to get administrator privileges to modify the threshold settings of the system or other secondary assets.

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

The efforts in time and money to exploit such vulnerability could be quite high, depending on the detailed approach of this attack.

3.4 Organisational security policies

The TOE must comply with the following organisational security policies:

OSP.FAR[19]

As minimum requirement the TOE must meet recognised national and/or international criteria (see Annex A - BSI biometric performance standard) for false acceptance rate (FAR) as appropriate for the specified assurance level and strength of function claim.

OSP.USERLIMIT[20]

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

This organisational security policy shall establish the maximum number of unsuccessful verification attempts permitted by the biometric verification system.

[19] **Application Note (BIO):** To establish a claimed FAR, cross comparison is the most efficient test technique, because cross comparisons are statistically dependent, no claims to statistical confidence can be made. Determination of test size will depend on both the unknown correlations and the anticipated error rates.

[20] **Application Note (BIO):** One way to realise the userlimit OSP is to set a limit of unsuccessful authentication attempts. Once these limits are reached, further attempts will not be accepted.

4 Security Objectives

This chapter Security Objectives contains the following sections:

Security objectives for the TOE (4.1)

Security objectives for the TOE or the environment (4.2)

Security objectives for the environment (4.3)

4.1 Security objectives for the TOE

O.AUDIT_REACTION

The TOE shall ensure to support security management by recording security relevant events and that all TOE users can subsequently be held accountable for their security relevant actions.

The TOE shall perform logging about all security critical processes and inform about insecure states. This includes countered, unsuccessful attacks to the TOE.

These messages can be send to authorised users (monitoring and reaction in case of unwanted authorisation) as well as to the TOE or IT administrator (supervision). However, thereby it is to mind, that no feedback information is provided, which may assist an impostor in gaining access[21].

The TOE should for example (but not exclusively): react to,

- Administrator's authentication: This objective should audit the number of unsuccessful authentication attempts to one administrator account and should lock the authentication mechanism if a configurable number of unsuccessful authentication attempts has been reached
- Replay or brute force attacks against the same identity. This means that the reaction part of this objective should realize a mechanism thru which more than an administrator defined number of unsuccessful verification attempts with the same claimed identity is blocked.
- The detection of attacks based on the use of residual information (as specified T.RESIDUAL)
- Less quality: This means that the verification process should be stopped if either the BIR or the BLR do not have sufficient quality
- An unusual high amount of unsuccessful verification attempts against different identities could be caused by a brute force attack. In this case the system should shut down for a specified time of should inform an administrator. The limit of unsuccessful attempts and the action taking place has to be specified by the administrator.

O.ROLES_AND_ACCESS

The TOE shall limit restricted functionality to those authorised and authenticated. Therefore, the TOE must especially enforce access control such that only authorised administrators may create, modify and delete security relevant data.

The TOE administrator shall be the only one to authenticate to the TOE administration functionality (e.g.: Administration tool).

[21] **Application Note (ST):** It is often useful for a biometric system to provide feedback to legitimate users in order to help them to be identified reliably by the system. For example, a fingerprint biometric may provide an image of the captured fingerprint to the user, to facilitate the correct positioning of the finger and the generation of a good image. This feedback should not be such, however, 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.

O.BIO_VERIFICATION

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

- The TOE shall process only its own templates (respectively standardised) from the enrolment process (consideration of integrity and authenticity).
- The BIR as well as the BLR shall suffice minimum quality standards and compatible among each other.

Exact match comparison: An “Exact match” comparison should not activate the portal 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 false acceptance rate (FAR) (see Annex A - BSI biometric performance standard or [BEM]) in accordance with OSP.FAR[22].

O.AUTHADMIN

The TOE should provide a mechanism to authenticate an administrator with other means than the biometric verification process. This authentication process could for example be realized thru a username/password or a smartcard/pin based mechanism.

A basic security level is sufficient for this mechanism because the administrative access to the TOE is additionally protected by the environment. Therefore the strength of this mechanism has to reach SOF basic.

O.RESIDUAL

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

4.2 Security objectives for the TOE or environment

Due to the broad spectrum of biometric technology for some threats it is not possible to specify on the level of a PP whether they are countered by the TOE itself or the environment or a combination. The threats T.RESIDUAL and T.REPRODUCE could optionally be countered in the environment of the TOE. Therefore the parts of these threats where it is not possible to fix whether they are countered by the TOE or the environment are countered by requirements for the environment in this PP.[23]

OE.NO_REPRODUCE[24]

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

---

[22] **Application Note (BIO):** To meet the national and/or international criteria for FAR, the adjustment of the related thresholds has to be proofed and adjusted by the TOE administrator.

[23] **Application Note (ST):** The ST author is in charge of describing whether the TOE or the environment is responsible for these objectives. It 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 it should be considered to change the notation of these objectives from OE.X to O.X.

[24] **Application Note (BIO):** 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 a an objective for the TOE (See also Application Note before).

OE.RESIDUAL_CAPTURE[25]
It has to be assured that residual data that may be at a capture device after use could not be used to gain access.

4.3 Security objectives for the environment

OE.ADMINISTRATION

The TOE- and IT-administrator are well trained and can be trusted (non hostile), read the guidance documentation carefully, completely understand and apply it.

Moreover, the TOE administrator is responsible to accompany the TOE installation and oversee the biometric system requirements regarding to the TOE as well as the TOE settings and requirements.

OE.CAPTURE

The capture device as user visible interface operates inside its regular range and is suitable for the use with the TOE. Therefore, environmental influences must be assured regarding the operating environment. Furthermore a bypassing of the capture device in a technical manner is not possible. This does not exclude the possibility to present 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 is publicly available moderate physical robustness is presupposed

OE.ENROLMENT

The enrolment has already been performed and therefore, the BIR for each authorized user is given. The generated BIR suffices minimum quality standards and is linked with the correct user.

Additionally all biometric templates are protected stored and measures regarding to authenticity and integrity are available.

OE.ENVIRONMENT

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

- Operating System: It is assumed that the biometric system underlying operating system compatibly supports the functionality of the biometric system (e.g.: GINA replacement, audit functionality). Regarding the request of the claimed identity, which is necessary for the biometric authentication, the underlying operating system offers the possibility to integrate a claimed identity into the biometric verification process.
  The OS has to provide a reliable time stamp mechanism to be used by the TOE.
  Additional it is assumed that the operating system is able to protect itself and its own functionality (e.g.: policy management, access control, non-authenticated start-up).
- Storage: The TOE environment provides a database for the already enrolled biometric templates, whereby integrity and authenticity are guaranteed. The storage is a secure IT-product (e.g. SmartCard or hard disk in a secure area) and provides an access interface for the TOE.
  In case of user supplied templates (e.g. stored on SmartCard or token), measures exist to protect the authenticity and integrity of the template.
- Transmission: The environment takes care for a secure communication of security relevant data from and to the TOE.

[25] **Application Note (BIO):** 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 then is able to detect the use of this data. For these technologies the ST author is in charge of defining this objective as an objective for the TOE (See also Application Note before).

- Audit: The environment provides a functionality to review the audit information of the TOE and ensures that only authorized administrators are allowed to do this
- The surrounding TOE environment is Virus, Trojan, and malicious software free.
- The environment cares for access control to the controlled portal(s) based on the verified id of a user.

OE.PHYSICAL

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 TOE or IT administrators. This does not cover the capture device that has to be accessible for each user.

OE.FALLBACK

A fallback mechanism for the biometric verification system is available that reaches at least the same security level as the biometric verification system does. This fallback system is used especially if an authorized user is rejected by the biometric verification system (False Rejection).

5 IT Security Requirements

5.1 TOE Security Requirements

This chapter describes the security functional and the assurance requirements which have to be fulfilled by the TOE. The requirements consist of functional components from part 2 of [CC] and an Evaluation Assurance Level (EAL2, augmented with ADV_SPM.1), which includes components from part 3 of the [CC]. Moreover a few requirements (functional and assurance) are adapted to biometrics via Application notes.

5.1.1 TOE security functional requirements

The following Table 1: TOE security functional requirements summarises all TOE functional requirements to meet the security objectives:

No.	SFR	Dependency
	FAU	
1.	FAU_ARP.1	FAU_SAA.1
2.	FAU_GEN.1	FPT_STM.1
3.	FAU_GEN.2	FAU_GEN.1, FIA_UID.1
4.	FAU_SAA.1	FAU_GEN.1
	FDP	
5.	FDP_ACC.1	FDP_ACF.1
6.	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
7.	FDP_RIP.2	No Dependency
	FIA	
8.	FIA_AFL.1	FIA_UAU.1
9.	FIA_ATD.1	No Dependency
10.	FIA_UAU.2	FIA_UID.1
11.	FIA_UAU.3	No Dependency
12.	FIA_UAU.5	No Dependency
13.	FIA_UAU.7	FIA_UAU.1
14.	FIA_UID.2	No Dependency
	FMT	
15.	FMT_MOF.1	FMT_SMR.1, FMT_SMF.1
16.	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1
17.	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
18.	FMT_MTD.1	FMT_SMR.1, FMT_SMF.1
19.	FMT_MTD.3	ADV_SPM.1, FMT_MTD.1

No.	SFR	Dependency
20.	FMT_SMF.1	No Dependency
21.	FMT_SMR.1	FIA_UID.1
	FPT	
22.	FPT_RPL.1	No Dependency

Table 1: TOE security functional requirements[26]

The following subchapters describe the functional requirements with respect to biometric systems and drawn from the standard set of functional components listed in [CC] part 2. In certain cases interpretations to deal with particular characteristics of biometric systems are needed and provided in form of application notes. The application notes are primarily written for ST writers and TOE developers. In cases where there are no application notes, the normal interpretation appropriate to IT system security functionality may be assumed.

To look up the different types of operations are used in this Protection Profile (see Document Introduction - C Notations).

5.1.1.1 Security audit (FAU)

The definition of the FAU class of requirements can be interpreted to accommodate the definitions of security audit requirements as they relate to biometrics. This class defines requirements for monitoring user activities and detecting violations of security policies. These functions are defined to help monitor security relevant events and act as a deterrent against security violations.

- **Security audit automatic response (FAU_ARP)**

FAU_ARP.1: Security alarms[27]

Hierarchical to: No other components.

[26] **Application Note (ST):** Additional functional requirements according to privacy (class FPR) are not considered within the scope of security. Moreover the cryptographic support is not definitely described in order to obtain maximum flexibility of this Protection Profile. Thereby the biometric vendors are free to realise a secure data transfer via TOE and e.g. storage / capture device.

[27] **Application Note (ST):** The TOE generates a signal indicating or an alarm condition by a method determined by the ST Author. Acceptable methods may include sending an interrupt or message to the TOE environment. The TOE could satisfy this requirement by indicating an alarm without interaction with the environment (e.g., a LED or audible indication that indicates an alarm condition). The intent of this requirement is to alert an administrator that the TOE has encountered a potential security violation.

The PP does not want to exclude devices that may not be able to “immediately alert” an administrator (e.g., stand alone TOEs with no connectivity). The intent is to provide an administrator the choice of preventing the TOE from authenticating users until an administrator takes some action (e.g., enable the TOE to perform authentication, clear the alarm and the TOE implicitly can resume performing authentication), or define a time period in which the TOE can begin performing authentication again. The time period should allow the flexibility of allowing the administrator to “throttle” throughput (e.g., a few minutes) or to assess the alarm and take the appropriate action (e.g., a few hours). The TOE may additionally send an alarm to the host TOE environment to signify a potential security violation, but simply signalling the TOE environment does not satisfy the intent of this requirement.

FAU_ARP.1.1: The TSF shall[28] [*one or more of the following actions:*

a) Generate an alarm condition to the environment by [assignment: method determined by the ST Author to generate the alarm],

b) Block any further authentication attempts until an administrator defined time period has elapsed, or an action is taken by the administrator,

c) Stop ongoing if the BIR and/or the BLR quality do not suffice a minimum quality standard.]

upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

- **Security audit data generation (FAU_GEN)**

FAU_GEN.1: Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1: The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the basic level of audit **plus events as defined in Table 2: Auditable events**; and

c) [assignment: *other specifically defined auditable events*].

Component	Auditable Event	Additional Information
Class FAU: Security Audit		
FAU_ARP.1	Detection of potential security violation.	Identification of the events caused the generation of the alarm.
FAU_SAA.1	The number of authentication failures/attempts according to administrative and non-administrative user identifier.	Specified number of authentication failures; specified number of consecutive authentication attempts
Class FIA: Identification and Authentication		
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	no
FIA_UAU.2	All use of the authentication mechanism.	no
FIA_UAU.3	All immediate measures taken.	Results on the fraudulent data.
FIA_UID.2	All use of the user identification system.	User identity provided.
Class FMT: Security management		
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF.	no

[28] **Application Note (PP):** The word “take” has been deleted from FAU_ARP1.1 to achieve a better readability.

Component	Auditable Event	Additional Information
FMT_MTD.1	All modifications to the values of TSF data.	no
FMT_MTD.3	All rejected values of the BIR and BLR.	no
Class FPT: Protection of the TSF		
FPT_RPL.1	Detected replay attacks.	no

Table 2: Auditable events

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[29] 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, *additional information as defined in Table 2 and* [assignment: *other audit relevant information specific to the particular biometric system*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1: The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

- **Security audit analysis (FAU_SAA)**

FAU_SAA.1: Potential violation analysis[30]

Hierarchical to: No other components.

FAU_SAA.1.1: The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2: The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of

- An administrator specified a number of authentication failures against a single non-administrative user identifier,

- An administrator specified a number of consecutive failed authentication attempts,

- An Administrator specified a number of authentication failures against an administrative user identifier

known to indicate a potential security violation.

b) [assignment: *any other rules*[31]].

[29] **Application Note (ST):** The TOE may not be able to identify the subject identity associated with an event. For example: For all events occurring before the authentication part of the TOE has been successfully performed, the TOE is only able to audit a claimed ID of the subject.

[30] **Application Note (BIO):** The intent of this requirement is that an alarm is generated (FAU_ARP.1) once the threshold for the event in (a) is met. Once the alarm has been generated it is assumed that the "count" for that event is reset to zero. An administrator settable number of authentication failures in (a) is intended to be the same value as specified in the iterations of FIA_AFL.1.

Dependencies: FAU_GEN.1 Audit data generation

5.1.1.2 User data protection (FDP)

The current definition of the FDP class of requirements can be interpreted to accommodate the definitions of user data protection requirements as they relate to biometrics. This class defines a significant set of functional requirements for a biometric system in terms of protecting user data within the biometric system (e.g. during import, export and storage, as well as security attributes directly related to user data).

- **Access Control Policy (FDP_ACC)**

FDP_ACC.1: Subset Access Control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*[32]] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

Dependencies: FDP_ACF.1 Security attribute based access control

- **Access Control Functions (FDP_ACF)**

FDP_ACF.1[33]**: Security attribute based access control**

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment*: rules, based on security attributes that explicitly deny access of subjects to objects*].

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

---

[31] **Application Note (ST):** e.g. any failure of TSF self-tests or any detection of physical tampering (In this case relevant functional requirements are necessary (e.g. FPT_PHP.3; FPT_TST.1), but due to applicableness/flexibility not explicit considered in this part of the PP.

[32] **Application Note (ST):** The ST author is in charge of fixing the SFP for access control.

[33] **Application Note (ST):** The ST author is in charge of performing the assignments in this family. Due to this a maximum flexibility is given to develop conformant TOEs

- **Residual information protection (FDP_RIP)**

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

5.1.1.3 Identification and authentication (FIA)

The requirements of class FIA are used in two different directions in this PP: First to describe the biometric verification mechanism and second to describe the authentication mechanism for the administrator.

The current definition of the FIA class of requirements can be interpreted to accommodate the definitions of identification and authentication as they relate to biometrics. It represents requirements to establish the claimed identity of each user and verify that each user is indeed who he/she is claimed to be.

- **Authentication failures (FIA_AFL)**

FIA_AFL.1:	**Authentication failure handling**
Hierarchical to:	No other components.
FIA_AFL.1.1:	The TSF shall detect when an administrator configurable positive integer within [assignment: *range of acceptable values*[34]]" unsuccessful authentication attempts occur related to [assignment: *list of authentication attempts*]"[35].
FIA_AFL.1.2:	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *block any further authentication attempts related to that*

[34] **Application Note (ST):** The ST author is in charge of defining the range of acceptable values because this range depends on the used biometric technology.

[35] **Application Note (ST):** The TOE administrator shall specify the number of unsuccessful authentication attempts allowed before the TOE takes action and the Security Target shall explain how the TOE allows the TOE administrator to set the maximum number.

For biometric verification systems, there are three main circumstances which may constitute unsuccessful authentication attempts (same biometric template is used to attack a single user identification; different biometric templates are used to attack a single user identification; same biometric templates is used to attack different user identifications.

Additionally this element is added as a result of CC Final Interpretation for RI #111.

user until a defined time period has elapsed, as specified by the TOE administrator and [assignment: *additional measures*][36].

Dependencies: FIA_UAU.1 Timing of authentication

- **User attribute definition (FIA_ATD)**

FIA_ATD.1: User attribute definition

Hierarchical to: No other components.

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

a) Identifying name or number

b) Unique physical or behavioural characteristic

c) Role

d) [assignment: *other attributes specific to the particular biometric system*][37].

Dependencies: No dependencies.

[36] **Application Note (ST):** This security functional requirement needs to be interpreted in the light of the circumstances, which apply to FIA_AFL.1.1 previously. If the TOE does not detect multiple unsuccessful authentication attempts, then this should be indicated by completing the first assignment with “until the next authentication attempt”. This effectively reduces the SFR to a null requirement on the TOE. As with FIA_AFL.1.1 this should be clearly explained in the ST.

For a verification system, the various circumstances delineated previously need further clarification, possibly by iteration of FIA_AFL.1.2. In the circumstance that single user identification is subject to repeated unsuccessful authentication attempts (using the same or different biometric templates), further attempts to authenticate against that user shall be blocked.

The time period referred to in the first assignment will need clarification in the ST in the event that the TOE implements a more complex time-out scheme for the blocking of unsuccessful authentication attempts.

The TOE may take additional measures when repeated unsuccessful authentication attempts occur, e.g. raising an alarm to an authorised administrator. These measures should be stated in the ST by completing the second assignment. If no additional measures are taken then an assignment of “none” should be indicated by deleting the second assignment and the preceding “and”.

Under all circumstances auditing is to be performed in accordance with FAU requirements. If the TOE does not check for multiple authentication failures then the auditing requirement reduces to the need to record unsuccessful authentication attempts.

Clarification may be required in the ST to specify the criteria for time-outs and blocking or re-enabling of authentication attempts against users.

[37] **Application Note (ST):** It is permissible for an assignment of "none" to be made to complete the assignment. In this case list item d) may be omitted for clarity in the Security Target.

- **User authentication (FIA_UAU)**

FIA_UAU.2: User authentication before any action[38]

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1: The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

The biometric verification function that is used for this authentication has to reach the maximum value for FAR as demanded in OSP.FAR.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.3: Unforgeable authentication[39]

Hierarchical to: No other components.

FIA_UAU.3.1: The TSF shall detect and prevent use of authentication data that has been forged by any user of the TSF[40].

FIA_UAU.3.2: The TSF shall detect and prevent use of authentication data that has been copied from any other user of the TSF[41].

---

[38] **Application Note (ST):** 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. It is therefore conceivable that there are no functions provided for the user other than authentication, or the single function of controlling access to a facility or information system, which does not form part of the TOE itself. This security functional requirement (SFR), therefore, expresses the prime objective of the TOE.

[39] **Application Note (BIO):** This functional requirement includes aspects of the minimum quality of the used TSF-data, because the minimum quality aspect is not compatible with unforgeable authentication.

[40] **Application Note (ST):** In this context, forgery generally refers to the use of an artefact such that the biometric system is spoofed into accepting the artefact as coming from a live human being. It is not possible to make definitive statements on the potential for forging of biometric characteristics. Most biometric characteristics could, in principle, be forged given sufficient resources and justification. The ease or otherwise will depend on the nature of the biometric, the inherent characteristics of the biometric capture device and intentional countermeasures implemented in the TOE.

Depending on the technology used by the TOE it is possible that it is not possible for the TOE itself to fulfil this requirement because – for example – the capture device fulfils this requirement. If reasonable it is therefore possible for the ST author to define that this requirement has to be fulfilled by the environment.

The term "authentication data" also includes the biometric template, which may be supplied by the user, e.g. stored on a SmartCard. In such cases the TOE is required to detect and prevent the use of a template forged by an impostor.

This SFR does not explicitly require the ability to detect mimicry by an impostor, i.e. such attacks are not considered as "forgery" of authentication data. Rather, these attacks are countered by the TOE meeting the FAR requirements in accordance with OSP.FAR.

Note that this requirement is not limited to the biometric verification process but does also cover the authentication data for administrator.

[41] **Application Note (ST):** This SFR may overlap in some instances with FIA_UAU.3.1 in the case of biometric systems. The production of a forgery may also involve copying the biometric characteristics of an authorised user of a system (for example, lifting a latent fingerprint from a glass). Most biometric characteristics are not secret and may therefore be vulnerable to being copied. There will be varying degrees of difficulty involved. For example it may be hard to copy a retinal pattern. This form of copying requires the use of a forgery to exploit the copy.

Replay attacks are not covered by this SFR: FPT_RPL.1 addresses this form of attack.

Dependencies: No dependencies.

FIA_UAU.5: Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide *a biometric verification mechanism to authenticate users and a non biometric verification mechanism to authenticate administrators*[42] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the

[assignment: *rules describing how the multiple authentication mechanisms*

provide authentication[43]].

Dependencies: No dependencies

FIA_UAU.7: Protected authentication feedback[44]

Hierarchical to: No other components.

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

Dependencies: FIA_UAU.1 Timing of authentication

- **User identification (FIA_UID)**

FIA_UID.2: User identification before any action[45]

Hierarchical to: FIA_UID.1

FIA_UID.2.1: The TSF shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.

Dependencies: No dependencies.

5.1.1.4 Security management (FMT)

The current definition of the FMT class of requirements can be interpreted to accommodate the definitions of security management requirements as they relate to biometrics. This requirement defines the management of security attributes, and TSF data and functions. With respect to biometric systems, the management of security functions and attributes are especially relevant to the administration of

---

This SFR does not explicitly require the ability to detect mimicry by an impostor, i.e. such attacks are not considered as "copying" of authentication data. Rather, these attacks are countered by the TOE meeting the FAR requirements in accordance with OSP.FAR.

[42] **Application Note (ST):** The non biometric authentication mode has to be specified by the ST author.

[43] **Application Note (ST):** The ST author has to specify the rules for the biometric verification process and for the non biometric authentication process for administrators.

[44] **Application Note (ST):** This SFR means that the biometric system must not inform the user of any "score" against the threshold that might help the attacker to fool the device in subsequent verification attempts. Notification of the result of the attempt, or presenting the supplied biometric image to the user, is considered to be permitted feedback.

[45] **Application Note (ST):** This SFR is used to describe the identification during the biometric verification process as well as needed for the administrator authentication process. Both times the identification means to present a claimed id to the TOE to be verified against. If the identification that is used in context of biometric verification differs from the identification method that is used for the administrator authentication an iteration of this component should be considered by the ST author.

security policies and the establishment of threshold levels. These levels determine the closeness or score required between a sample and reference template in order to declare them a match. For verification, the setting of threshold levels determines the rates of false matches and false non-matches, and acceptance or rejection by the system.

These are unique considerations for biometric evaluations. Furthermore, it is suggested that these security functions apply for systems that also include capabilities of, for example, appending user rights and privileges related to an application.

- **Management of functions in TSF (FMT_MOF)**

FMT_MOF.1#1: Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1#1: The TSF shall restrict the ability to determine the behaviour of, disable, enable, modify the behaviour of the functions

- *Audit mechanisms,*
- *Thresholds*
- [assignment: *other functions*]

to *TOE administrators*[46].

FMT_MOF.1#2: Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1#2: The TSF shall restrict the ability to disable and enable the functions:

- *Perform maintenance,*
- *Perform manual access (e.g. fallback-system),*
- *Emergency start-up/shutdown*
- [assignment: *List of actions that need to be taken in case of repetitive penetration attempts*]

to *IT administrators*.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

- **Management of Security Attributes (FMT_MSA)**

FMT_MSA.1: Management of security attributes

Hierarchical to: No other components

FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP,*] to restrict the ability to change default, query, modify, delete, [assignment: *other operations*] the security attributes *user attributes as defined in FIA_ATD.1, threshold settings,* [assignment: *other security attributes*] to *administrators.*

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

[46] **Application Note (ST):** Equal requirements as for normal IT system audit logs and trails.

FMT_SMF.1

FMT_MSA.3: Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP*] to provide [selection: *choose one of: restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the *SFP*.

FMT_MSA.3.2 The TSF shall allow the *administrator* to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

- **Management of TSF data (FMT_MTD)**

FMT_MTD.1: Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1: The TSF shall restrict the ability to initialize, query, modify, delete, or clear the

- [assignment: list of security parameters which control the performance of the biometric system]

- [assignment: user security attributes]

- audit trail

-[assignment: *other attributes]*

to *TOE administrators*[47].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.3: Secure TSF data

Hierarchical to: No other components.

FMT_MTD.3.1: The TSF shall ensure that only secure values are accepted for TSF data.

Dependencies: ADV_SPM.1 Informal TOE security policy model
FMT_MTD.1 Management of TSF data

- **Specification of Management Functions (FMT_SMF)**

FMT_SMF.1: Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1: The TSF shall be capable of performing the following security management functions:

a) Control the operation of security-related aspects of the TOE (threshold control)

b) Control audit attributes

c) *Control authentication attributes.*

[47] **Application Note (ST):** The security performance of a biometric system is critically dependent of the adjustment of system parameters, typically threshold values for acceptance or rejection of user authentication attempts. The activity must be restricted to trusted staff (TOE administrators) and the TOE must enforce this restriction. Otherwise the system security will be compromised.

Dependencies: No dependencies.

- **Security management roles (FMT_SMR)**

FMT_SMR.1:	**Security roles**
Hierarchical to:	No other components.
FMT_SMR.1.1:	The TSF shall maintain the roles *authorised users, TOE administrators, and IT administrators*[48].
FMT_SMR.1.2:	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification

5.1.1.5 Protection of the TSF (FPT)

The current definition of the FPT class of requirements can be interpreted to accommodate the definitions of TSF protection requirements as they relate to biometrics.

The biometric system that verifies a user for a resource does not automatically convey rights or privileges for that resource. For a system to support this capability, the template must be bound to a resource in such a way that a successful match will convey privileges over that resource. It is this concept that makes the FPT class of functional requirement applicable to biometric systems. Biometric data in the TOE should be regarded as TSF Data.

- **Replay detection (FPT_RPL)**

FPT_RPL.1:	**Replay detection**[49]
Hierarchical to:	No other components.
FPT_RPL.1.1:	The TSF shall detect replay for the following entities: *biometric authentication data*.
FPT_RPL.1.2:	The TSF shall[50] *ignore the replayed data* when replay is detected.
Dependencies:	No dependencies.

5.1.2 Minimum strength of function claim

The minimum strength of function for the security functions that are fulfilling the functional security requirements is SOF-basic.

---

[48] **Application Note (ST):** It is permissible for a TOE to maintain more than one type of administrator role such as separating the template administration functions from general administration functions.

[49] **Application Note (ST):** If the connection between the biometric capture device and the authentication component can be intercepted, it may be possible to capture the data produced by the capture device and to later replay the data to the authentication component to effect a breach of security. The developer will need to indicate the countermeasures implemented by the TOE to resist this type of attack.

Part of detecting a replay attack is to detect e.g. when an "exact match" comparison against a reference template occurs.

[50] **Application Note (PP):** The word “perform” has been deleted from FPT_RPL1.2 to achieve a better readability.

For the biometric verification mechanism the SOF level is measured in terms of FAR (according to [BEM]). For SOF basic a FAR of less than 1 in 100 is required.

5.1.3 TOE security assurance requirements

The TOE assurance requirements for the TOE evaluation and its development and operating environment are taken from evaluation assurance level 2, augmented with ADV_SPM.1 as shown in the following table:

Assurance class	ID	Assurance component	Refinement
Configuration management	ACM_CAP.2	Configuration items	no
Delivery & operation	ADO_DEL.1	Delivery procedures	no
	ADO_IGS.1	Installation, generation & start-up procedures	no
Development	ADV_FSP.1	Informal functional specification	no
	ADV_HLD.1	Descriptive high-level design	yes
	ADV_RCR.1	Informal correspondence demonstration	no
	ADV_SPM.1[51]	Informal TOE security policy model	no
Guidance documents	AGD_ADM.1	Administrator guidance	yes
	AGD_USR.1	User guidance	yes
Tests	ATE_COV.1	Evidence of coverage	no
	ATE_FUN.1	Functional testing	yes
	ATE_IND.2	Independent testing – sample	yes
Vulnerability assessment	AVA_SOF.1	Strength of TOE-security function evaluation	yes
	AVA_VLA.1	Developer vulnerability analysis	yes

Table 3: Assurance requirements (EAL2, augmented with ADV_SPM.1)

The following subchapters describe the EAL2 (augmented with ADV_SPM.1) assurance requirements with respect to biometric systems. Refinements as well as application notes shall support the description and generally considered appropriate for biometric TOE's. Deviations regarding to the standard Common Criteria assurance requirements are added in form of refinements together with an introduction related to ADV_HLD, AGD_ADM, AGD_USR, ATE_FUN, ATE_IND, AVA_SOF, and AVA_VLA.

Additional descriptions related to the standard Common Criteria assurance components can be read in [CC], part3.

Note that many of the comments and refinements for the assurance classes are taken from [BEM]. Every evaluator should consider the current version of [BEM] for further guidance.

[51] **Application Note (PP; ST):** ADV_SPM.1 is augmented and described in chapter . Thereby the need of an informal TOE security policy model results from a security management dependency (see chapter).

5.1.3.1 Configuration management (ACM)

- **ACM_CAP.2 - Configuration items**

Dependencies: No dependencies.

Developer action elements:

ACM_CAP.2.1D: The developer shall provide a reference for the TOE.

ACM_CAP.2.2D: The developer shall use a CM system.

ACM_CAP.2.3D: The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C: The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C: The TOE shall be labelled with its reference.

ACM_CAP.2.3C: The CM documentation shall include a configuration list.

ACM_CAP.2.4C: The configuration list shall uniquely identify all configuration items that comprise the TOE[52].

ACM_CAP.2.5C: The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6C: The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.7C: The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.3.2 Delivery and operation (ADO)

- **ADO_DEL.1 - Delivery procedures**

Dependencies: No dependencies.

Developer action elements:

ADO_DEL.1.1D: The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D: The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C: The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

- **ADO_IGS.1 - Installation, generation and start-up procedures**

Dependencies: AGD_ADM.1 Administrator guidance

[52] **Application Note (CC):** This element is added as a result of CC Final Interpretation 003.

Developer action elements:

ADO_IGS.1.1D: The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C: The installation, generation and start-up documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE[53].

Evaluator action elements:

ADO_IGS.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E: The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.1.3.3 Development (ADV)

- **ADV_FSP.1 - Informal functional specification**

Dependencies: ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_FSP.1.1D: The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C: The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C: The functional specification shall be internally consistent.

ADV_FSP.1.3C: The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C: The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E: The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

- **ADV_HLD.1 - Descriptive high-level design**

Dependencies: ADV_FSP.1 Informal functional specification
ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_HLD.1.1D: The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C: The presentation of the high-level design shall be informal.

ADV_HLD.1.2C: The high-level design shall be internally consistent.

[53] **Application Note (CC):** This element is changed as a result of CC Final Interpretation 051.

ADV_HLD.1.3C: The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C: The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C: The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C: The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C: The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E: The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

Refinements regarding ADV_HLD.1:

Specifications of interfaces may be in term of defined biometric standards e.g. [BioAPI], [CBEFF], and [X9.84] as well as other developing standards.

- **ADV_RCR.1 - Informal correspondence demonstration**

Dependencies: No dependencies.

Developer action elements:

ADV_RCR.1.1D: The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C: For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

- **ADV_SPM.1 - Informal TOE security policy model[54]**

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_SPM.1.1D: The developer shall provide a TSP model.

[54] **Application Note (PP; ST):** The need of an informal TOE security policy model results from a security management dependency (see chapter). Thereby the informal TSP model mainly has to describe the secure values for the TSF data.

ADV_SPM.1.2D: The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C: The TSP model shall be informal.

ADV_SPM.1.2C: The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C: The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C: The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

ADV_SPM.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.1.3.4 Guidance documents (AGD)

- **AGD_ADM.1 - Administrator guidance**

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_ADM.1.1D: The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C: The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C: The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C: The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C: The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C: The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C: The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C: The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C: The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinements regarding AGD_ADM.1:

Administrator guidance should include guidance on environmental controls and on how environmental factors affect the security of the system.

Any change to a matching threshold should be considered as a function that needs secure control.

Guidance on user behaviour may include the need for users to be monitored or supervised. The matching threshold must be considered to be a security parameter.

In scope of biometric systems the guidance documents have to pay special attention about:

a) Biometric Privacy

Personal and legal issues related to collecting and storing of biometric data should be documented.

b) Environmental influences

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 these can affect accuracy of the enrolment and verification processes. Hence, guidance documentation should include information on environmental influences and ways of minimising these influences.

c) Setting of thresholds

Where it is possible to change the matching thresholds used in the comparison process, documentation should include the effects of changing these thresholds, the means of changing these thresholds, and the importance of these thresholds in determining security.

- **AGD_USR.1 - User guidance**

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

AGD_USR.1.1D: The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C: The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C: The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C: The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C: The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C: The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C: The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinements regarding AGD_USR.1:

User guidance should include guidance for the capture process and for any relevant environmental considerations.

Guidance may also be given on personal issues, such as privacy.

5.1.3.5 Tests (ATE)

This assurance class defines the testing requirements to demonstrate that the Target of Evaluation Security Functions (TSF's) satisfies the security functional requirements. The concept of this class is to confirm, through developer and independent testing, that each TSF operates according to its specification.

Determining the effectiveness of the underlying security mechanisms in biometric systems is dependent on performance testing. The behaviour of a biometric system depends on components that include the capture device, the biometric algorithms, the environmental conditions, and also the user and impostor distribution. The statistics of these are not amenable to theoretical analysis within the current state of knowledge, and hence performance testing is necessary to determine the effectiveness of these biometric security mechanisms[55].

- **ATE_COV.1 - Evidence of coverage**

Dependencies: ADV_FSP.1 Informal functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.1.1D: The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C: The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

- **ATE_FUN.1 - Functional testing**

Dependencies: No dependencies.

Developer action elements:

[55] **Application Note (BIO):** The main performance parameters that determine the effectiveness of biometric mechanisms are False Acceptance Rate (FAR) and False Rejection Rate (FRR), which directly measure biometric recognition.

Testing of these rates must include an appropriate and statistically representative data set that validates the rates. Testing may be done from a collected biometric database or by enrolling and testing a representative sample population. When databases are used, the conditions under which the samples were collected must be considered carefully. Care must be taken in configuring the equipment, verifying its correct functioning and consistency in collection procedures.

[BPT] and [BEM] include some guidance on the quantity of tests required.

ATE_FUN.1.1D: The developer shall test the TSF and document the results.

ATE_FUN.1.2D: The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C: The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C: The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C: The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C: The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C: The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinements regarding ATE_FUN.1:

The tests must include statistic performance tests e.g. for FAR and FRR rates (for guidance on tests see [BPT, chapter 3.4]). Tests may also include the effects of physical environmental factors on the performance of the biometric system.

The interpretation of "configuration" should include the setting of environmental controls, where relevant.

- **ATE_IND.2 - Independent testing - sample**

Dependencies: ADV_FSP.1 Informal functional specification
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance
ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D: The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C: The TOE shall be suitable for testing.

ATE_IND.2.2C: The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E: The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E: The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

Refinements regarding ATE_IND.2:

The interpretation of "configuration" should include the setting of environmental controls, where relevant.

The tests will normally include statistical performance tests for FAR and FRR rates which could be realized by repeating the vendors tests with a partly changed set of test data.

5.1.3.6 Vulnerability assessment (AVA)

This assurance class defines requirements directed at the identification of exploitable vulnerabilities. It addresses those vulnerabilities introduced in the design, construction, operation, misuse or incorrect configuration of the Target of Evaluation (TOE).

- **AVA_SOF.1 - Strength of TOE security function evaluation**

Strength of function investigates the strength of the underlying security mechanism of the TOE and its vulnerability. With respect to biometric systems, the strength of function lies in the ability to correctly identify a user. For access control applications, this is measured through the FAR achieved in the operational environment. The FRR may be considered a measure of inconvenience, but it is also a measure of availability, and needs to be kept within acceptable limits for the intended application. Note that when the primary purpose is to detect people with multiple identities on the system, the most important parameter may be FRR. The strength of function for a biometric system is determined by the uniqueness of the biometric captured from a person and by the transformation of that biometric by the system into a measurable quantity.

Dependencies: ADV_FSP.1 Informal functional specification
ADV_HLD.1 Descriptive high-level design

Developer action elements:

AVA_SOF.1.1D: The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C: For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C: For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E: The evaluator shall confirm that the strength claims are correct.

Refinements regarding AVA_SOF.1[56]:

Guidance on FAR and FRR is available in [BPT] and [BEM].

- **AVA_VLA.1 - Developer vulnerability analysis**

Vulnerability analysis is an assessment to determine whether vulnerabilities identified during the evaluation of the development, construction and anticipated operation of the TOE could allow users to violate the TOE Security Policy. Vulnerability analysis of biometric systems has some features that distinguish it from normal IT vulnerability analysis. For a consideration of vulnerabilities specific to biometric systems, see [BEM, chapter 3.5].

Dependencies: ADV_FSP.1 Informal functional specification
ADV_HLD.1 Descriptive high-level design
AGD_AGD.1 Administrator guidance
AGD_USR.1 User guidance

Developer action elements[57]:

AVA_VLA.1.1D: The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D: The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements[58]:

AVA_VLA.1.1C: The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C: The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C: The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E: The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E: The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

Refinements regarding AVA_VLA.1:

Appropriate documentation on potential vulnerabilities for biometric systems should be considered; see [BEM, chapter 3.5].

---

[56] **Application Note (ST):** It is proposed that all biometric Security Targets (ST) should include a claim for SOF and a rationale to explain the claim. This rationale should include an estimate of FAR with a clear definition of the test procedures and algorithms behind the FAR claims.

[57] **Application Note (CC):** The following two elements are changed as a result of CC Final Interpretation 051.

[58] **Application Note (CC):** The following elements are replaced as a result of CC Final Interpretation 051.

5.2 TOE environment security requirements

This subchapter contains the requirements for the TOE environment. No requirements are taken from part 2 of [CC].

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

R.RESIDUAL_CAPTURE
It has to be assured that residual data that may be at a capture device after use could not be used to gain access.

R.ADMINISTRATION
The TOE- and IT-administrator are well trained have to be trusted (non hostile), read the guidance documentation carefully, completely understand and apply it.

Moreover, the TOE administrator has to be responsible to accompany the TOE installation and oversee the biometric system requirements regarding to the TOE as well as the TOE settings and requirements.

R.CAPTURE
The capture device as user visible interface has to operate inside its regular range and is suitable for the use with the TOE. Therefore, environmental influences must be assured regarding the operating environment. Furthermore a bypassing of the capture device in a technical manner must not be possible.

R.ENROLMENT
The enrolment has to be already performed and therefore, the BIR for each authorized user is given. The generated BIR has to suffice minimum quality standards and is linked with the correct user.

Additionally all biometric templates have to be protected stored and measures regarding to authenticity and integrity has to be available.

R.ENVIRONMENT
The necessary TOE operating equipment and adequate infrastructure has to be available (e.g.: operating system, database, LAN, public telephone, and guardian).

- Operating System: It has to be assumed that the biometric system underlying operating system compatibly supports the functionality of the biometric system (e.g.: GINA replacement, audit functionality). Regarding the request of the claimed identity, which is necessary for the biometric authentication, the underlying operating system offers the possibility to integrate a claimed identity into the biometric verification process.
  The OS has to provide a reliable time stamp mechanism to be used by the TOE.
  Additional it has to be ensured that the operating system is able to protect itself and its own functionality (e.g.: policy management, access control, non-authenticated start-up).
- Storage: The TOE environment hast to provide a database for the already enrolled biometric templates, whereby integrity and authenticity are guaranteed. The storage is a secure IT-product (e.g. SmartCard or hard disk in a secure area) and provides an access interface for the TOE.
  In case of user supplied templates (e.g. stored on SmartCard or token), measures have to exist to protect the authenticity and integrity of the template.
- Transmission: The environment hast to take care for a secure communication of security relevant data from and to the TOE.
- Audit: The environment provides a functionality to review the audit information of the TOE and ensures that only authorized administrators are allowed to do this
- The surrounding TOE environment is Virus, Trojan, and malicious software free.

- The environment cares for access control to the controlled portal(s) based on the verified id of a user.

R.PHYSICAL[59]

The TOE and its components have to be physically protected against unauthorized access or destruction. Physical access to the hardware that is used by the TOE is only allowed for TOE or IT administrators. This does not cover the capture device that has to be accessible for each user.

R.FALLBACK

A fallback mechanism for the biometric verification system has to be available that reaches at least the same security level as the biometric verification system does. This fallback system is used especially if an authorized user is rejected by the biometric verification system (False Rejection).

[59] **Application Note (ST):** The Security Target shall clarify the division of responsibility between the TOE and its environment. In case of capture device assignment to the TOE, additional functional requirements like e.g. FPT_PHP.3 and FPT_TST.1 are necessary. In comparison with SmartCard products the biometric capture device (sensor) does not include countermeasures as e.g. active shielding.

6 Rationale

This chapter Rationale contains the following sections:

Security objectives rationale (6.1)

- Coverage of the security objectives (6.1.1)
- Coverage of the assumptions (6.1.2)
- Countering the threats (6.1.3)
- Coverage of the organisational security policies (6.1.4)

Security requirements rationale (6.2)

- TOE security functional requirements (6.2.1)
- Environment security requirements (6.2.2)
- Assurance requirements rationale (6.2.3)

6.1 Security objectives rationale

6.1.1 Coverage of the security objectives

Table 4 below gives an overview, how the assumptions, threats, and organisational security policies are addressed by the security objectives. The text following after the table 4 together with the descriptions of the subchapter's 6.1.2, 6.1.3, and 6.1.4 justifies this more detailed.

	O.AUDIT_REACTION	**O.ROLES_AND_ACCESS**	**O.BIO_VERIFICATION**	**O.AUTHADMIN**	**O.RESIDUAL**	**OE.NO_REPRODUCE**	**OE.RESIDUAL_CAPTURE**	**OE.ADMINISTRATION**	**OE.CAPTURE**	**OE.ENROLMENT**	**OE.ENVIRONMENT**	**OE.PHYSICAL**	**OE.FALLBACK**
A.ADMINISTRATION								X					
A.CAPTURE									X				
A.ENROLMENT										X			
A.ENVIRONMENT											X		
A.PHYSICAL												X	
A.FALLBACK													X
T.BRUTEFORCE	X		X										
T.MODIFY_ASSETS	X	X		X									
T.REPRODUCE	X					X							
T.RESIDUAL	X				X		X						
T.ROLES	X	X		X							X		
OSP.FAR			X										

	O.AUDIT_REACTION	O.ROLES_AND_ACCESS	O.BIO_VERIFICATION	O.AUTHADMIN	O.RESIDUAL	OE.NO_REPRODUCE	OE.RESIDUAL_CAPTURE	OE.ADMINISTRATION	OE.CAPTURE	OE.ENROLMENT	OE.ENVIRONMENT	OE.PHYSICAL	OE.FALLBACK
OSP.USERLIMIT	X												

Table 4: Assumptions/threats/OSP - security objectives mapping

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 in O.AUDIT_REACTION.

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 directly follows.

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

The TOE security objective **O.ROLES_AND_ACCESS** (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 thjs objective realizes access control.

The TOE security objective **O.BIO_VERIFICATION** can be traced back to the threats T.BRUTEFORCE (to be resistant against brute force attacks) and OSP.FAR because O.BIO_VERIFCATION realizes the demanded limit for the FAR from OSP.FAR.

The TOE security objective **O.AUTHADMIN** (the TOE shall be able to authenticate an administrator with non biometric means) can be traced back to the threats T.ROLES because it helps to ensure that only authorised administrators are able to change security relevant data of the TOE and T.MODIFY_ASSETS because this objective is responsible for authentification of the administrator and the correct authentication of an administrator is needed to enforce the access control mechanisms to counter T.MODIFY_ASSETS.

The environment security objective **OE.ADMINISTRATION** (well trained and trusted administrator) can be traced back to the assumption A.ADMINISTRATION (well trained and trusted administrator).

The environment security objective **OE.CAPTURE** can be directly traced back to A.CAPTURE.

The environment security objective **OE.ENROLMENT** can be directly traced back to A.ENROLMENT

The environment security objective **OE.ENVIRONMENT** can be directly traced back to A.ENVIRONMENT. Furthermore it counters parts of T.ROLES because the environment ensures the access to the portal.

The environment security objective **OE.PHYSICAL** can be directly traced back to A.PHYSICAL.

The environment security objective **OE.FALLBACK** can be directly traced back to A.FALLBACK.

6.1.2 Coverage of the assumptions

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 (see chapter 3.2). It is clear from the description of each objective (see chapter 4.3), that the corresponding assumption is covered, if the objective is valid. Nevertheless some objectives exceed the statements of the assumptions they cover.

Each assumption is covered by one environmental security objective.

6.1.3 Countering the threats

The threat **T.BRUTEFORCE** (using a fraction 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 **one** impostor brute force attempt is less then the specified limit for SOF basic. 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 shutting down the system for a specific time or informing an administrator.

The threat **T_MODIFY_ASSETS** is countered by a combination of the objectives O.ROLES_AND_ACCESS, O.AUTHADMIN and O.AUDIT_REACTION. O.ROLES_AND_ACCESS is responsible to limit the access to security relevant objects of the TOE to authorized administrators. O.AUTHADMIN is responsible to authenticate an administrator. O.AUDIT_REACTION is logging the 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.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 the impostor attempt.

The threat **T.ROLES** is fully countered by a security objective combination of O.AUDIT_REACTION, O.ROLES_AND_ACCESS, O.AUTHADMIN and OE.ENVIRONMENT. O.AUTHADMIN ensures a secure authentication of administrators. O.ROLES_AND_ACCESS takes care 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.

6.1.4 Coverage of organisational security policies

The organisational security policy **OSP.FAR** (the TOE must meet criteria for FAR - see Annex A) is directly met by O.BIO_VERIFICATION as this objective describes that the biometric verification mechanism has to reach a FAR as specified in OSP.FAR.

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

Each OSP is covered by at least one security objective.

6.2 Security requirements rationale

6.2.1 TOE security functional requirements rationale

The following subchapters consider the TOE security requirements.

6.2.1.1 Fulfilment of TOE security objectives

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

	O.AUDIT_REACTION	**O.ROLES_AND_ACCESS**	**O.BIO_VERIFICATION**	**O.AUTHADMIN**	**O.RESIDUAL**
FAU_ARP.1	X				
FAU_GEN.1	X				
FAU_GEN.2	X				
FAU_SAA.1	X				
FDP_ACC.1		X			
FDP_ACF.1		X			
FDP_RIP.2					X
FIA_AFL.1			X	X	
FIA_ATD.1		X	X	X	
FIA_UAU.2			X	X	
FIA_UAU.3			X	X	
FIA_UAU.5			X	X	
FIA_UAU.7			X		
FIA_UID.2			X	X	
FMT_MOF.1#1		X			
FMT_MOF.1#2		X			

	O.AUDIT_REACTION	O.ROLES_AND_ACCESS	O.BIO_VERIFICATION	O.AUTHADMIN	O.RESIDUAL
FMT_MSA.1		X			
FMT_MSA.3		X			
FMT_MTD.1		X			
FMT_MTD.3			X		
FMT_SMF.1		X			
FMT_SMR.1		X			
FPT_RPL.1			X		

Table 5: SFR (TOE) - security objectives (TOE) mapping

O.AUDIT_REACTION
FAU_ARP.1 ensures that the TOE reacts in case of a potential security violation while **FAU_SAA.1** ensures that the potential security violation is detected. These both requirements fulfil the reaction part of this objective. **FAU_GEN.1** makes arrangements to generate records of security relevant events (see table in chapter) and **FAU_GEN.2** supports the user identity association in order to be able to hold users accountable for their actions. These two requirements fulfil the audit part of this objective.

O.ROLES_AND_ACCESS
FDP_ACC.1 realizes a general access control mechanism between subjects and objects of the TOE and **FDP_ACF.1** describes the attributes on which the access control is based on. **FIA_ATD.1** defines that the role of a user is a user attribute. **FMT_MOF.1#1** limits the ability to modify the behaviour of audit functions and system thresholds to an administrator. **FMT_MOF.1#2** limits the ability to disable/enable the functions Perform maintenance, Perform manual access and Emergency start-up/shutdown to IT-administrators. **FMT_MSA.1** restricts the management of security attributes to an administrator while **FMT_MSA.3** enforces secure default values for security attributes and limits the ability to change these default values to administrators. **FMT_MTD.1** restricts the ability to control the performance of the system 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_AFL.1 ensures that reaching a threshold of unsuccessful authentication attempts is realized to be a security relevant state. **FIA_ATD.1** defines the user attributes that are also used for the biometric verification. **FIA_UAU.2** states that each user has to be successfully authenticated before performing any action and defines the maximum values for FAR and FRR. **FIA_UAU.3** ensures that no forged authentication data can be used for authentication. **FIA_UAU.5** defines that the TOE has another authentication mechanism beside the biometric verification process. **FIA_UAU.7** ensures that no authentication feedback is given to a potential attacker. **FIA_UID.2** states that the each user has to be identified before performing any action. **FPT_RPL.1** ensures that the TOE ignores replayed authentication data. **FMT_MTD.3** assures that only secure values are accepted for BIR and BLR during the biometric verification process.

O.AUTHADMIN
FIA_AFL.1 ensures that reaching a threshold of unsuccessful authentication attempts is realized to be a security relevant state. **FIA_ATD.1** defines the user attributes that are also used for the authentication of an administrator. **FIA_UAU.2** states that each user has to be successfully authenticated before performing any action. **FIA_UAU.3** ensures that no forged authentication data can be used for authentication. **FIA_UAU.5** defines that the TOE has another authentication mechanism beside the biometric verification process. **FIA_UID.2** states that the each user has to be identified before performing any action.

O.RESIDUAL

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

6.2.1.2 Fulfilment of TOE SFR dependencies

The set of security functional requirements that are selected covers all the TOE security objectives as demonstrated in the previous chapter.

The following Table 6 identifies the security functional requirements and their associated dependencies. It also indicates whether the PP explicitly addresses each dependency. For those cases where dependencies have not specifically been addressed, explanations of the rationale for excluding them are provided.

No.	SFR	Dependency	Dependency satisfied?
	FAU		
1.	FAU_ARP.1	FAU_SAA.1	yes
2.	FAU_GEN.1	FPT_STM.1	no[60]
3.	FAU_GEN.2	FAU_GEN.1, FIA_UID.1	yes
4.	FAU_SAA.1	FAU_GEN.1	yes
	FDP		
5.	FDP_ACC.1	FDP_ACF.1	yes
6.	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	yes
7.	FDP_RIP.2	No Dependency	not applicable
	FIA		
8.	FIA_AFL.1	FIA_UAU.1	yes
9.	FIA_ATD.1	No Dependency	not applicable
10.	FIA_UAU.2	FIA_UID.1	yes
11.	FIA_UAU.3	No Dependency	not applicable
12.	FIA_UAU.5	No Dependency	not applicable
13.	FIA_UAU.7	FIA_UAU.1	yes
14.	FIA_UID.2	No Dependency	not applicable
	FMT		
15.	FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	yes
16.	FMT_MSA.1	[FDP_ACC.1 or FDP_ICF.1], FMT_SMR.1, FMT_SMF.1	yes (without the use of FDP_ICF.1)

[60] **Application Note (PP):** See - "Remarks on TOE functional requirements that are fulfilled by the TOE environment" under table 6.

No.	SFR	Dependency	Dependency satisfied?
17.	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	yes
18.	FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	yes
19.	FMT_MTD.3	ADV_SPM.1, FMT_MTD.1	yes
20.	FMT_SMF.1	No Dependency	not applicable
21.	FMT_SMR.1	FIA_UID.1	yes
	FPT		
22.	FPT_RPL.1	No Dependency	not applicable

Table 6: Fulfilment of SFR (TOE) dependencies

Remarks on TOE functional requirements that are fulfilled by the TOE environment:

The functional component FAU_GEN.1 has an identified dependency on FPT_STM.1. This dependency is not satisfied by any TOE functional requirement, but by a security requirement for the TOE environment (see R.ENVIRONMENT, chapter 4.3). This is acceptable, because the time stamp functionality is required by the used, TOE underlying operating system. Therefore, the time stamp functionality is not needed within the TOE boundary and creates maximum flexibility to meet the developer needs.

6.2.1.3 Mutual support and internally consistency

From the details given in the two previous chapters it becomes evident that the functional requirements form an integrated unity and, taken together, are suited to meet all security objectives. Requirements from [CC] part 2 are used to fulfil the security objectives. Since the individual requirements meet all dependencies that the [CC] are demanding, the proper combination of these requirements is ensured.

6.2.1.4 Suitability of minimum SOF level

SOF-basic as chosen minimum SOF level Nevertheless, if possible the TOE can fulfil higher SOF levels, but at minimum SOF-basic[61].

Against the background of the selected operational environment (and of the assurance level EAL2 augmented with ADV_SPM.1, too), the chosen minimum strength level SOF-basic makes sense and is consistent with the security objectives.

The explicit strength metrics in form of required FAR and FRR are determined by the specified national and international rules in accordance with OSP.FAR and this organisatorical security politic is covered by the security objective O.BIO_VERIFICATION (see Annex A).

6.2.2 Environment security requirements

This Protection Profile provides security requirements for the TOE environment. Thereby no functional requirements are taken from [CC], part 2.

[61] **Application Note (BIO):** According to the threat T.REPRODUCE the SOF level should be considered in context of the attack potential. Thereby vulnerabilities as e.g. artificial fingers are well known. However additional security measures as e.g. aliveness checks could be used.

	OE.NO_REPRODUCE	OE.RESIDUAL_CAPTURE	OE.ADMINISTRATION	OE.CAPTURE	OE.ENROLMENT	OE.ENVIRONMENT	OE.PHYSICAL	OE.FALLBACK
R.NO_REPRODUCE	X							
R.RESIDUAL_CAPTURE		X						
R.ADMINISTRATION			X					
R.CAPTURE				X				
R.ENROLMENT					X			
R.ENVIRONMENT						X		
R.PHYSICAL							X	
R.FALLBACK								X

Table 7: Environment requirements - security objectives (environment) mapping

OE.NO_REPRODUCE is covered by the environment security requirement R.NO_REPRODUCE as directly follows.

OE.RESIDUAL_CAPTURE is covered by the environment security requirement R._RESIDUAL_CAPTURE as directly follows.

OE.ADMINISTRATION is covered by the environment security requirement R.ADMINISTRATION as directly follows.

OE.CAPTURE is covered by the environment security requirement R.CAPTURE as directly follows.

OE.ENROLMENT is covered by the environment security requirement R.ENROLMENT as directly follows.

OE.ENVIRONMENT is covered by the environment security requirements R.ENVIRONMENT as directly follows.

OE.PHYSICAL is covered by the environment security requirement R.PHYSICAL as directly follows.

OE.FALLBACK is covered by the environment security requirement R.FALLBACK as directly follows.

For all security objectives for the environment the corresponding security requirement is stated in a way, which directly correspond to the description of the objective (see chapter 4.2 and 4.3). It is clear from the description of each objective (see chapter 4.2 and 4.3), that the corresponding requirement is covered, if the objective is valid.

Each security objective for the environment can be traced back to one environment functional requirement as well as each described environment functional requirement can be tracked back to one environment security objective.

6.2.3 Assurance requirements rationale

The assurance level EAL2 is chosen with one augmentation (ADV_SPM.1) and additionally described with refinements (see chapter 5.1.3) due to the scope of biometric systems. EAL2 (augmented with ADV_SPM.1) and the relevant assurance requirements (see Table 3: Assurance requirements (EAL2, augmented with ADV_SPM.1)) provides assurance by an analysis of the security functions, using a

functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain). The selected level EAL2 (augmented with ADV_SPM.1) includes the component AVA_VLA.1 that requires that the manufacturer identifies all evident weaknesses of the TOE and proves that these cannot be exploited. AVA_VLA.1 requires that the TOE is resistant to an attacker with a low-attack potential (this is consistent with SOF-basic). The evaluator has to check this on the basis of penetration tests. In view of the operational environment, no explicit attack potential for exploiting the weaknesses of the TOE is utilised.

EAL2 (augmented with ADV_SPM.1) also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures and EAL2 (augmented with ADV_SPM.1) represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis, and independent testing based upon more detailed TOE specifications.

Therefore, the selected level EAL2 (augmented with ADV_SPM.1) and related assurance requirements ensure a basic extent of confidence into the security examined by an independent authority. This assurance level is sufficient for the TOE, as it is conceived for operation in an environment with low or unspecified security requirements.

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time. Additionally EAL2 is applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

6.2.3.1 Dependencies, mutual support and internal consistency

The dependencies of the assurance requirements taken from EAL2 are fulfilled automatically. The sole augmentation (ADV_SPM.1) is also fulfilled, because its dependency (ADV_FSP.1) is part of EAL2.

Annex

This Annex contains the following sections:

A BSI biometric performance standard

B Abbreviations and glossary

C References

A BSI biometric performance standard

The following predefinition shows the SOF defined in terms of FAR:

SOF-basic = maximum FAR of 0.01 (1 in 100)

SOF-medium = maximum FAR of 0.0001 (1 in 10000)

SOF-high = maximum FAR of 0.000001 (1 in 1000000)

It is proposed that all biometric Security Targets should include a claim for SOF and a rationale to explain the claim. This rationale should include an estimate of FAR with a clear definition of the test procedures and algorithms behind the FAR claims.

B Abbreviations and glossary

The following glossary includes all used terms and abbreviations of this Protection Profile regarding to the Common Criteria as well as biometric and IT technology terms in alphabetical order. Most of the definitions were taken from [BEM].

Term	Description
Assets	Information or resources to be protected by the countermeasures of a TOE.
Assignment	The specification of an identified parameter in a component.
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.
Attribute	Security attribute: Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.
Augmentation	The addition of one or more assurance components(s) from [CC] part 3 to an EAL or assurance package.
Authentication	Testimony the 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 an enrolee or verify a claimed identity.
Biometric data	Extracted information taken from a biometric sample and used either to build a reference template on enrolment, or to compare against a previously created reference template.
Biometric feature	A representation from a biometric sample extracted by the extraction system.
Biometric sample	A biometric measure presented by the user and captured by the data collection system.
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 reference templates, 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.
BIR	Biometric Identification Record - A BIR includes the reference template and other data associated with the user. This is the saved reference data record against that the comparison is accomplished.
BLR	Biometric Live Record - This template includes the actual biometric data (actual biometric characteristic and user identity) to be verified with the biometric identity 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.
BSI	Bundesamt für Sicherheit in der Informationstechnik - Federal Office for Information Security BSI - Godesberger Allee 185-189 - D-53133 Bonn (Germany) Tel.: +49 (0) 1888 9582 0 - FAX: +49 (0) 1888 9582 400 http://www.bsi.bund.de
Capture	The process of taking a biometric sample via a sensor from a user.
CC	Common Criteria - Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology
CMOS	Complementary Metal Oxide Semiconductor
Comparison	The process of comparing biometric data with a previously stored BIR
EAL	Evaluation Assurance Level
Enrolee	A user with a stored biometric reference template on file.
Enrolment	See 2.1.1
FAR	False Accept Rate (FAR) - The probability that a biometric system will incorrectly identify an individual that is not authorised. For a positive (verification) system, it can be appraised from: (the number of false acceptances)/(the number of impostor verification attempts).

Term	Description
FRR	False Rejection Rate (FRR) - The probability that a biometric system will fail to identify a genuine enrolee. For a positive (verification) system, it can be estimated from: (the number of false rejects)/(the number of enrolee verification attempts). (Security attribute regarding to this PP)
GINA	Graphical Identification and Authentication as part of an operating system
Identification	See 2.2
Identification system	Biometric system that provides an identification function (see also identification)
ITSEF	IT Security Evaluation Facility (see TÜViT)
LAN	Local Area Network
Live processing	Direct enrolment/ identification of potential users via the normal biometric capture process. Compare off-line processing.
Matching Score	A measure of similarity or dissimilarity between the biometric data and a stored template, used in the comparison process.
Multimodal biometrics	A biometric system, which uses information from different biometrics - e.g. fingerprint and hand shape; or fingerprints from two separate fingers. All statistical analysis of multimodal systems should consider how the modes are combined in the comparison process.
one-to-many matching	See identification system.
one-to-one matching	See verification system.
OS	Operating system
OSP	Organisational Security Policy
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 TOE's that meet specific consumer needs.
Refinement	The addition of details to a component.
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.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Sensor	The physical hardware device used for biometric capture. Also called caputer device
SFR	Security Functional Requirement
SOF	Strength Of Function (SOF) - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms. The determination of an additional strength of function is an important part of the evaluation of a biometric product or system. In accordance with [BEM] the SOF for the biometric verification mechanism is described in terms of FAR values. It is proposed that all biometric Security Targets should include a claim for SOF and a rationale to explain the claim. This problematic arises due to the fact of probabilistic prediction of biometric systems. SOF-basic: A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential (SOF-basic defined in terms of FAR: 0,01).
ST	Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
SW	Software
Template	A user's stored reference measure based on biometric feature(s) extracted from biometric sample(s). It could differentiate in: Biometric Identification Record: see BIR Biometric Live Record: see BLR
Threat	An intended or unintended potential event that could compromise the security integrity of the system.
Threshold	A parametric value used to convert a matching score to a decision. A threshold change will usually change both FAR and FRR - as FAR decreases, FRR increases.

Term	Description
TOE	Target of Evaluation - An IT product or system (and its associated documentation) that is the subject of a Common Criteria evaluation.
TSF	TOE Security Functions
TSF data	Data created by and for the TOE that might affect the operating of the TOE.
TSP	TOE Security Policy
TÜViT	TÜV Informationstechnik GmbH - Division Information Security Langemarckstraße 20 - D-45141 Essen (Germany) Tel.: +49 (0) 201 8999 601 - FAX: +49 (0) 201 8999 666 http://www.tuvit.de
User	A person who requires access to the portal, which is protected by a biometric system.
User data	Data created by and for the user that does not affect the operation of the TSF.
Verification	See 2.1.2
Verification system	A biometric system that provides a verification functionality.
WAN	Wide Area Network
Weak Template	A template created from a noisy, poor quality, highly varying biometric sample.
WLAN	Wireless Local Area Network

Table 8: Abbreviations and Glossary

C References

[BEM] Biometrics Evaluation Methodology Supplement, Version 1.0, August 2002

[BioAPI] BioAPI Specification, Version 1.1, 16. March 2001, The BioAPI Consortium

[BPT] Best Practices in Testing and Reporting Performance of Biometric Devices, NPL Report CMSC 1402, Version 2, August 2002

[CBEFF] Common Biometric Exchange File Format (CBEFF), NIST, NISTIR6529, 03. January 2001

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.1, Annotated with interpretations as of 2003-12-31, August 1999
Part 1: Introduction and general model, CCIMB-99-031,
Part 2: Security functional requirements, CCIMB-99-032,
Part 3: Security Assurance Requirements, CCIMB-99-032.

[CEM] Common Methodology for Information Technology Security Evaluation,

Part 1: Introduction and general model, version 0.6, revision 11.01.1997,
Part 2: Evaluation Methodology, CEM-99/045, version 1.0, Annotated with interpretations as of 2003-12-31, August 1999.

[ISO15446] Information technology - Security techniques - Guide for the production of Protection Profiles and Security Targets, ISO/IEC PDTR 15446, 01. April 2000

[PP_UK_BD] Biometric Device Protection Profile (BDPP), UK Government Biometrics Working Group, Draft Issue 0.2, 05. September 2001

[PP_US_BS] Biometric System Protection Profile for Medium Robustness Environments, Department of Defense & Federal, Version 0.02, 03. March 2002

[PP_US_BV_BR] Biometric Verification Mode Protection Profile for Basic Robustness Environments, Biometrics Management Office and National Security Agency, Version 0.8, 08. June 2003

[PP_US_BV_MR] Biometric Verification Mode Protection Profile for Medium Robustness Environments, Information Assurance Directorate, Version 1.0, 15. November 2003

[PP_SCSUG] Smart Card Security User's Group - Smart Card Protection Profile (SCSUG-SCPP), Version 2.1d, 21. March 2001

[X9.84] Biometric Information Management and Security, American National Standards Institute, X9.84-2001