Table of Contents

1 PP Introduction 4
1.1 PP Overview 4
2 TOE Description 6
2.1 Biometric Processes and terminology 7
2.2 The base TOE 13
2.3 Functional package: Biometric Verification 13
2.4 Functional Package: PAD 13
2.5 Functional Package: Identification and Authentication for administrators 14
2.6 Functional Package: Enrolment protection 14
2.7 TOE configuration and TOE environment 14
2.8 TOE boundary 15
3 Conformance Claims 17
3.1 Conformance statement 17
3.2 CC Conformance Claims 17
3.3 PP Claim 17
3.4 Package Claim 17
4 Security Problem Definition 18
4.1 External entities 18
4.2 Assets 18
4.3 Assumptions 19
4.4 Threats 20
4.5 Organizational Security Policies 21
5 Security Objectives 22
5.1 Security Objectives for the TOE 22
5.2 Security objectives for the operational environment 22
5.3 Security Objectives rationale 24
6 Extended Component definition 26
6.1 Presentation attack detection (FPT_PAD) 26
6.2 Biometric Verification (FIA_BVR) 28
6.3 Enrolment of biometric reference (FIA_EBR) 31
7 Security Requirements 34
7.1 Security Functional Requirements for the TOE 34
7.2 Security Assurance Requirements for the TOE 39
7.3 Security Requirements rationale 40
8 Functional Packages 43
8.1 Overview and allowed combinations of functional packages 43
8.2 Functional Package: Biometric Verification 44
8.3 Functional Package: PAD 49
8.4 Functional Package: Identification and Authentication for administrators 53
8.5 Functional Package: Enrolment Protection 56
Reference Documentation 60

Figures

Figure 1: TOE Overview....5
Figure 2: FPT_PAD.1 Presentation attack detection, detects presentation attacks for biometrics....24
Figure 3: Component leveling FIA_BVR....25
Figure 4: Component leveling for FIA_EBR....29

Tables

Table 1: Identification of PP....5
Table 2: Biometric Processes....8
Table 3: Terms and Definitions....9
Table 4: Overview of important error rates....12
Table 5: Security Objectives Rationale....23
Table 6: Security Functional Requirements....32
Table 7: Assurance Requirements....34
Table 8: Security Functional Requirements Rationale Overview....36
Table 9: Dependencies of functional requirements for base PP....36
Table 10: Dependencies of assurance components....37
Table 11: Possible combinations of functional packages....39
Table 12: Identification of Functional Package Biometric Verification....40
Table 13: Security Objectives Rationale for functional package biometric verification....42
Table 14: Security Functional Requirements Rationale Overview....43
Table 15: Dependencies of functional requirements for functional package “Biometric Verification”....44
Table 16: Identification of Functional Package: PAD....44
Table 17: Security Objectives Rationale for functional package PAD....46
Table 18: Dependencies of functional requirements for functional package “Presentation Attack Detection” 47
Table 19: Identification of Functional Package: Identification and Authentication for administrators....47
Table 20: Dependencies of functional requirements for functional package “Identification and Authentication for Administrators”....49
Table 21: Identification of Functional Package: Enrolment Protection....50
Table 22: Security Objectives Rationale for functional package biometric verification....51
Table 23: Security Functional Requirements Rationale Overview....52
Table 24: Dependencies of functional requirements for functional package “Enrolment Protection”....52

1 PP Introduction

Table 1: Identification of PP

Title:	Biometric Mechanisms Protection Profile (BMPP)
Version:	2.0
Date:	October, 8th 2021
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Editor:	Nils Tekampe, konfidas GmbH
Registration:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Certification-ID:	BSI-CC-PP-0118
CC-Version:	3.1 Revision 5
Keywords:	biometric; fingerprint-recognition; Protection Profile; presentation attack detection; PAD

1.1 PP Overview

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

Thereby, the Protection Profile utilizes a modular approach that allows the description of the major functionality that can make up a biometric system by means of Common Criteria. This specifically includes the biometric verification mechanism on the one hand and a mechanism for Presentation Attack Detection (PAD) on the other hand.

Therefore, this Protection Profile is structured into the following areas:

- **The base PP** contains all threats, OSPs, assumptions, objectives and SFRs that concern the biometric system in general. The base PP must not to be used alone but only in combination with at least one of the additional functional packages. With other words: The base PP must not be used alone but each Security Target claiming compliance to this Protection Profile shall at least use one of the following functional packages.
- **A functional package for biometric verification:** The package for biometric verification contains all threats, OSPs, assumption, objectives and SFRs that shall be used if a biometric verification mechanism is part of the TOE.
- **A functional package for PAD:** The package for PAD contains all threats, OSPs, assumption, objectives and SFRs that shall be used if Presentation Attack Detection is part of the TOE.
- **A functional package for enrolment protection**: The package for enrolment protection contains assumptions, threats, objectives and SFRs that shall be used if the biometric system shall contain functionality to protect its enrolment process against certain attacks.

- **A functional package for I&A:** This package contains functionality for the authentication of the administrator and the role management for users. It shall be used if the TOE supports functionality for the authentication of the administrator.

2 TOE Description

The Target of Evaluation (TOE) described in this PP is a biometric system. Depending on the use of the functional packages of this PP, the TOE may provide biometric verification and/or functionality for Presentation Attack Detection. The biometric functionality may be augmented by functionality for the identification and authentication of administrators or for the protection of the enrolment process.

In addition, the TOE must provide the functionality from the base PP that includes

- Security Management,
- Audit and
- Residual Information Protection

The following figure shows the overall architecture of the TOE. It should be noted that this figure displays a TOE with the use of all functional packages.

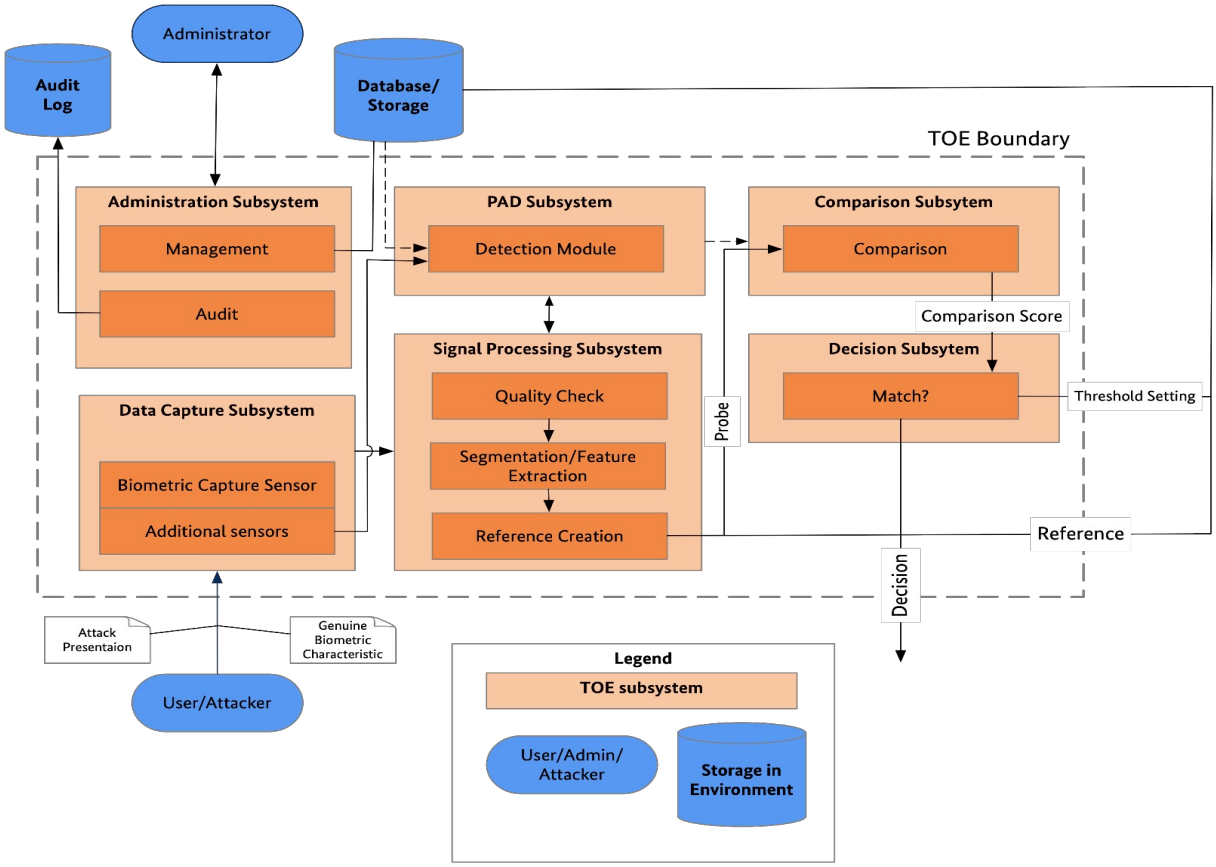

Figure 1: TOE Overview

The basis of the design of the TOE as described in Figure 1 has been borrowed from [ISO19989-1] and [ISO30107-1]. It has been adopted to the needs of this document by assigning the functional units to the packages/structure of this Protection Profile and by augmenting it by aspects of the immediate environment of the base PP.

The **Administration Subsystem** is responsible for providing the basic supporting functionality, specifically audit and security management. It represents the functionality that is defined in the base PP of this document.

The **Data Capture Subsystem** that primarily comprises the sensor devices, is the primary point of contact of the TOE with the user. The system acquires the biometric information about the biometric characteristic of the user (or the attacker) and turns it into a signal usable by the rest of the system.

The **Signal Processing Subsystem** belongs to the functional area of biometric verification. It includes functionality like quality check and biometric feature extraction but also the functionality for enrolment of users (i.e. reference creation).

The **Presentation Attack Detection Subsystem** comprises the functionality to detect whether an attempt to the system is a genuine attempt or a presentation attack.

The **Comparison Subsystem** compares the biometric reference information of a user with the information extracted from the biometric characteristic of a verification attempt. The outcome of this subsystem is usually a similarity score that describes, how similar both records are.

The **Decision Subsystem** takes the outcome of the comparison subsystem and decides whether reference record and data extracted from the verification attempt are similar enough for a successful verification. For this decision, the subsystem utilizes information that is typically referred to as threshold setting.

It should be noted that this overall architecture is described on a generic level and independent of any specific implementation. Thus, it should not be seen as a mandatory architecture of a TOE seeking compliance to this Protection Profile. It falls into the responsibility of the ST author to provide an architecture specific to the TOE. The following paragraphs provide more information on how the subsystems of the overall architecture relate to the functional packages of this Protection Profile.

The requirements from the **base PP** are reflected in the Administration subsystem. The Administration subsystem is also responsible for the requirements from the **functional package for Identification and Authentication for administrators**.

The requirements from the **functional package for PAD** are reflected in the PAD Subsystem (for the actual PAD functionality) and the Data Capture Subsystem for the acquisition of the information about the biometric modality. Depending on the specific implementation, the Signal Processing Subsystem may be needed or not.

The requirements from the **functional package for biometric verification** are reflected in the Data Capture Subsystem for the acquisition of the information about the biometric modality, the Signal Processing Subsystem, the Comparison Subsystem and the Decision Subsystem.

The requirements from the **functional package for biometric verification and integrated PAD** are reflected in all Subsystems of the overall architecture. The same holds for the **functional package for biometric verification, integrated PAD and enrolment protection.**

2.1 Biometric Processes and terminology

The following subchapters provide information on the biometric processes and terminology that are used in the context of this PP.

2.1.1 Biometric Processes

The following table provides an overview over the relevant biometric processes.

Table 2: Biometric Processes

Process	*Definition*
Enrolment (adopted from [ISO2382-37])	Act of creating and storing a biometric enrolment data record in accordance with an enrolment policy In enrolment, a transaction by a user is processed by the system in order to generate and store a biometric template for that individual. Enrolment typically involves: • biometric sample acquisition, • segmentation and biometric feature extraction, • quality checks, (which may reject the sample/features as being unsuitable for creating a template, and require acquisition of further samples), • biometric template creation (which may require features from multiple samples), possible conversion into a biometric data interchange format and storage, • test verification or identification attempts to ensure that the resulting enrolment is usable • and should the initial enrolment be deemed unsatisfactory, repeat enrolment attempts may be allowed (dependent on the enrolment policy).
Biometric Verification (adopted from [ISO2382-37])	Process of confirming a biometric claim through biometric comparison. In a biometric verification, a transaction of a user is processed by the system in order to verify a positive specific claim about the users enrolment (e.g. “I am enrolled as subject X”). Biometric verification will either accept or reject the claim. The verification decision outcome is considered to be erroneous if either a false claim is accepted (false accept) or a true claim is rejected (false reject). Biometric verification typically involves: • biometric sample acquisition, • segmentation and biometric feature extraction, • quality checks, (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples), • comparison of the sample features against the biometric template for the claimed identity producing a similarity score, • judgment on whether the sample features match the biometric template based on whether the similarity score exceeds a threshold, and • a verification decision based on the match result of one or more attempts as dictated by the decision policy.
Presentation Attack Detection ([ISO2382-37])	Automated discrimination between bona-fide and biometric presentation

Application Note 1

It should be noted that the list of typical steps involved in biometric enrolment and biometric verification is present for explanatory reasons and should not be seen as a requirements for a TOE claiming compliance to this Protection Profile. Alternative processes and steps are possible.

2.1.2 Terms and Definitions

The following table provides an overview over the relevant biometric processes.

Table 3: Terms and Definitions

Term	*Source*	*Definition*
artefact	[ISO30107-1]	artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns
biometric features	[ISO2382-37]	numbers or labels extracted from biometric samples and used for comparison
biometric impostor attack	[ISO2382-37]	presentation of biometric characteristics to impersonate another individual
biometric sample	[ISO2382-37]	analog or digital representation of biometric characteristics prior to biometric feature extraction
biometric template	[ISO2382-37]	set of stored biometric features comparable directly to probe biometric features
bona-fide presentation	[ISO2382-37]	biometric presentation without the goal of interfering with the operation of the biometric system
capture attempt	[ISO2382-37]	actions by the biometric capture subject interacting with the biometric capture subsystem with the intent of producing a captured biometric sample
capture transaction	[ISO19795-1]	one or more capture attempts with the intent of acquiring all of the biometric data from a biometric capture subject necessary to produce either a biometric reference or a biometric probe
comparison score	[ISO2382-37]	numerical value (or set of values) resulting from a comparison
confidence interval	[ISO19795-1]	a lower estimate L and an upper estimate U for a parameter x such that the probability of the true value of x being between L and U is the stated value (e.g. 95 %)
presentation attack	[ISO30107-1]	presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system
presentation attack instrument	[ISO2382-37]	biometric characteristic or object used in a biometric presentation attack
test subject	[ISO19795-1]	user whose biometric data is intended to be enrolled or compared as part of the evaluation
variance	[ISO19795-1]	measure of the spread of a statistical distribution

2.1.3 Error Rates

It is well known that biometric processes have associated error rates. These error rates are important in the context of a security evaluation as they can be used as a metric that describes, how likely an attacker has success. It should be noted however, that the concept of error rates can also be misleading.

Often, concrete and also impressive numbers for error rates are reported and discussed without consideration of important side aspects. Most of the error rates of biometric systems correlate with an antagonistic error rate via a threshold setting of the system. For example, the FMR rate of a biometric system can easily be tuned close to zero as long as one accepts that the FNMR (which is the antagonistic error rate in this case) raises.

Also, testing of error rates at low values requires a high amount of independent attempts to the system during the testing phase. However, as testing is expensive, tests of biometric systems often do not reach the size and therewith do not reach the confidence that would be desired.

More details on these questions, are provided and discussed in [PADEG]. The following table provides an overview over the error rates that are of specific importance in the context of this PP.

Table 4: Overview of important error rates

Error Rate	***Source***	***Definition***
false match rate (FMR)	[ISO19795-1]	The false match rate is the proportion of a specified set of completed non-mated comparison trials that result in a comparison decision of “match”.
false non match rate (FNMR) 19795	[ISO19795-1]	The false non-match rate is the proportion of completed mated comparison trials that result in a comparison decision of “non-match”.
false reject rate (FRR)	[ISO19795-1]	The false reject rate is the proportion of a specified set of verification transactions with true biometric claims erroneously rejected. A transaction may consist of one or more attempts depending on the decision policy.
false accept rate (FAR)	[ISO19795-1]	The false accept rate is the proportion of a specified set of transactions with false biometric claims erroneously accepted. A transaction may consist of one or more attempts depending on the decision policy.
attack presentation classification error rate (APCER)	[ISO30107-3]	proportion of attack presentations using the same PAI species incorrectly classified as bona-fide presentations by a PAD subsystem in a specific scenario
bona fide presentation classification error rate (BPCER)	[ISO30107-3]	proportion of bona-fide presentations incorrectly classified as presentation attacks in a specific scenario
attack presentation non-response rate (APNRR)	[ISO30107-3]	proportion of attack presentations using the same PAI species that cause no response at the PAD subsystem or data capture subsystem
bona fide presentation non-response rate (BPNRR)	[ISO30107-3]	proportion of bona fide presentations that cause no response at the PAD subsystem or data capture subsystem
Failure-to-enrol rate (FTER)	[ISO19795-1]	The failure-to-enrol rate is the proportion of the population for whom the system fails to complete the enrolment process. The failure-to-enrol rate shall include: • those unable to present the required biometric characteristic; • those unable to produce a sample of sufficient quality at enrolment; and • those who cannot reliably produce a match decision with their newly created template during attempts to confirm the enrolment is usable.

It should be noted that the error rates listed in table 4 are only an excerpt of important error rates and do not claim to provide a complete overview. Please refer to [ISO19795-1] and [ISO30107-1] for more details.

It should also be noted that this Protection Profile does not follow the complete approach for testing (based on metrics) as outlined in [ISO30107-3]. This decision has been deliberately taken as metrics are not suitable for a security certification as described by the methodology behind this Protection Profile. The introduction of [ISO30107-3] contains some valuable information on the reasons behind this decision.

2.2 The base TOE

The base TOE that is described in this Protection Profile forms the basis for functionality of biometric verification and/or Presentation Attack Detection. It ensures that the TOE provides all the general functionality that is required.

This functionality specifically includes:

- **Security Management:** the base TOE provides functionality to manage relevant TSF data. This specifically (but not only) refers to the parameters that are involved in biometric verification and/or Presentation Attack Detection. The TOE ensures that only secure values are accepted for those parameters
- **Residual Information Protection:** in order to prevent the leakage of information the TOE deletes relevant information if not longer in use.
- **Audit:** the TOE produces audit events for security relevant events.

Application Note 2

It should be noted that the base TOE as described in this Protection Profile must not be used in isolation. The author of the ST shall use at least one of the functional packages that are defined in chapter 8. The allowed combinations of the base PP with the packages are defined in chapter 8.1

2.3 Functional package: Biometric Verification

Products claiming to be conformant to the functional package for biometric verification as described in this Protection Profile shall provide a biometric verification process for the claimed identity of a user using a unique characteristic of their body.

The functional package covers the biometric verification process on a generic level and should be applicable to any biometric verification system. Development of conformant products should be possible for various IT environments.

The functional package describes a biometric system that operates in a verification mode only. Biometric identification is not addressed within this PP.

A biometric verification system that is conformant to this PP aims to verify the identity of a user for the purpose of controlling access to a portal. Such a portal can be a physical or logical point beyond which information or assets are protected by the biometric system. With failed verification, the portal stays closed for the user.

Only after successful verification, the portal will be opened. Therefore, such a portal requires one of two states after biometric verification: failed or successful authentication of the user. The final decision on the claimed identity of the user (resulting from a biometric probabilistic message into a boolean value) is considered to be part of the TOE.

In order to allow for a biometric verification a TOE claiming conformance to this functional package shall also provide the required functionality for the biometric enrollment of users. In enrolment, a transaction by the user is processed by the TOE in order to generate and store a biometric template for that individual.

Everything beyond the portal and the control of the portal itself (i.e. which users have access to the portal) is out of the scope of the TOE.

2.4 Functional Package: PAD

Biometric systems are often subject to a well known and easy kind of attack: Attackers can use artefacts (e.g. fingers built out of gummy or silicone) that carry the characteristics of a known user in order to get recognized by a biometric system. As an alternative a user of a biometric system may use an artefact in order

to disguise their identity. Countermeasures against those attacks may be implemented by a set of dedicated hardware and software, the so called Presentation Attack Detection (PAD).

The functional package for PAD as defined in this PP describes a system that provides Presentation Attack Detection. The TOE that is conformant to this functional package determines whether an attempt to the biometric system is a bona-fide presentation or a presentation attack.

For this purpose the TOE acquires PAD evidences for a presented biometric characteristic using a sensor device. This sensor can either be part of the capture device that is used to capture the biometric sample of the user (or even be identical to it) or be a separate sensor device (or more than one) that is completely dedicated to PAD.

The services that are defined in this functional package can either be provided in order to protect the TOE against presentation attacks (which means that a biometric verification is part of the TOE) or can be used to protect a biometric system in the environment of the TOE.

2.5 Functional Package: Identification and Authentication for administrators

This functional package shall be used if the TOE provides functionality for the identification and authentication of administrators.

The functional package contains requirements

- for the timing of identification and authentication and
- the management of Security Roles

2.6 Functional Package: Enrolment protection

According to the description in the functional package biometric verification (see chapter 8.2), the TOE described in this document relies on the environment to ensure that the enrolment is sufficiently secured. This way specific attacks that are directed against the enrolment process are mitigated by the environment.

This specifically includes (but is not limited to) the environment ensuring that

- The biometric reference and the biometric samples that are used to create it, belong to the correct user identity,
- the biometric sample that is used to create the reference does not contain any information from other user(s),
- the biometric reference is of sufficient quality.

While a biometric system will always have to rely on the environment to secure certain aspects of the enrolment process, a TOE can also contribute to this by implementing or contributing to two items from the aforementioned list and ensuring that

- the biometric sample that is used to create the reference does not contain any information from other user(s),
- the biometric reference is of sufficient quality.

The functionality of the TOE that protects these aspects of the enrolment process is described by this functional package.

2.7 TOE configuration and TOE environment

A biometric system in general could be realized in two major configurations:

- **An integrated solution:** All relevant parts of the TOE are integrated into one physical unit.
- **A distributed solution:** Relevant parts of the TOE are implemented in physically separated parts.

This PP (i.e. the base PP and the functional packages) describes a TOE as an integrated solution but should be applicable to distributed solutions as well. However, if applied to a distributed TOE additional aspects of security shall be considered by the author of the Security Target in form of:

- assumptions for the TOE environment,
- requirements for additional functionality: e. g. encrypted transmission.

It is known that environmental factors may influence the performance and therewith the protection provided by a biometric system. Therefore the author of a Security Target claiming compliance to this PP shall clearly identify the relevant environmental factors and their acceptable range for the operation of the TOE.

2.8 TOE boundary

A basic design of the TOE and its boundaries is shown in Figure 1. The following chapters provide more details about the physical and logical boundaries of the TOE.

2.8.1 Physical boundary

Depending on the use of its functional packages, this PP defines functionality for

- biometric verification and/or
- Presentation Attack Detection,
- Enrolment protection
- the identification and authentication of administrators.

The TOE shall comprise all parts of a product (hardware and software) that contribute to this functionality or any of the additional functionality outlined in chapters 2.3 to 2.6. In particular these are:

- the capture device for biometric acquisition,
- additional sensor devices for acquisition of PAD evidences (if applicable),
- necessary software.

The TOE shall be able to generate audit data. This audit data can be used for security audit, quality assurance or statistics. However, functionality for storage, protection and review of audit records is assumed to be provided by the environment of the TOE.

In its environment, the TOE relies on the typical services of an operating system. Please refer to chapter 5.2 for more details.

2.8.2 Logical boundary

The logical boundaries of the TOE can be defined by the functionality that it provides. This functionality depends on the use of the functional packages as defined in this Protection Profile as follows.

2.8.2.1 For the Base-PP

- **Security Management:** the TOE provides functionality to manage its relevant parameters. This specifically (but not only) refers to the parameters that are involved in the biometric verification and/or PAD. The TOE ensures that only secure values for those parameters are accepted to ensure the constant operation of the primary functionality.
- **Residual Information Protection:** in order to prevent the leakage of information the TOE deletes relevant information if not longer in use.
- **Audit:** the TOE produces audit events for security relevant events.

2.8.2.2 For biometric verification

- **Biometric verification:** the TOE provides functionality to verify the claimed identity of the user based on a biometric characteristic.
- **Biometric enrolment:** the TOE provides functionality to enroll users into the TOE. In enrolment, a transaction by the user is processed by the TOE in order to generate and store a biometric template for that individual. Storage of the biometric template is handled by the environment of the TOE.

2.8.2.3 For PAD

- **PAD:** the TOE provides a functionality for the automated detection of a presentation attack. It should be clearly mentioned that in the context of this PP a TOE is always required to decide about the presented characteristic in form of a yes/no decision. It is not considered to be sufficient if a TOE would return a value that would need further interpretation by the environment.

2.8.2.4 For Identification and authentication for administrators

- **I&A:** the TOE provides functionality for the secure authentication of administrators that is distinct from the biometric verification. The TOE also provides functionality to distinguish separate roles for users.

2.8.2.5 For Enrolment protection

- **Enrolment protection:** the TOE provides functionality to protect the enrolment process against certain attacks and does not solely rely on the environment for this aspect.

2.8.2.6 From the environment

The following functionality shall be provided by the environment to support the operation of the TOE:

- **Access control:** the environment provides access control for primary and secondary assets and any software parts of the TOE.
- I**dentification and Authentication:** The environment provides a mechanisms for the secure authentication of administrators and to distinguish separate roles for users. Please note that this functionality may also be provided by the TOE in form of the functional package for identification and authentication.
- **Transmission / Storage:** the environment provides a secure communication and storage for data where security relevant data is transferred to or from the TOE.
- **Auditing:** the environment may provide additional audit functionality. In any case it will provide reliable time stamps for auditing, storage for the audit records that are produced by the TOE and mechanisms for review of audit logs. The developer will probably have to consider privacy concerns (in case that personal information is part of the audit logs). Applicable data protection laws and protection mechanisms might have to be considered.

3 Conformance Claims

3.1 Conformance statement

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

3.2 CC Conformance Claims

- This PP has been developed using Version 3.1 R5 of Common Criteria ([CC])
- The conformance of this Protection Profile is Common Criteria ([CC]) Part II conformant
- The conformance of this Protection Profile is Common Criteria ([CC]) Part III conformant

Application Note 3

Please note that this PP uses functional packages that refer to extended components. As such, it is likely that a Security Target claiming compliance to this Protection Profile will have an extended conformance claim with respect to Common Criteria ([CC]) Part II.

3.3 PP Claim

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

3.4 Package Claim

This PP does not claim conformance to any assurance package (i.e. EAL) as defined in Common Criteria ([CC]) Part III. Instead, this PP defines an explicit assurance package that bases on EAL 2. However, in contrast to EAL 2 as defined in Common Criteria ([CC]) Part III , the assurance package in this PP does not contain any AVA_VAN component. It further includes the assurance component ALC_FLR.1.

This explicit assurance level allows a purely functional evaluation. Such an evaluation will allow to determine whether the functionality of a biometric system is sufficient to with respect to the defined Security Functional Requirements.

An evaluation using this explicit assurance level is deliberately ignoring the fact that an attacker could try to circumvent the functionality of the TOE (e.g. by using different/innovative presentation attacks in addition to the predefined set used for ATE_IND.1) and focuses on the basic functionality of the TOE. A system claiming compliance to this Protection Profile is therefore suitable for the use in application cases in which an assurance about the basic functionality of a system is sufficient.

The complete list of the assurance components of the explicit assurance package can be found in chapter 7.2.

It should further be noted that this Protection Profile heavily utilizes the concept of functional packages. Indeed, it shall not be possible to use this Protection Profile without one or more additional functional packages. Please refer to chapter 8.1 for an overview over the available functional packages and the possible combinations.

integrity and confidentiality of these parameters shall be protected. PAD is only relevant if the functional package for PAD has been chosen.

- PAD evidence (PADE): This data is acquired by the capture device and/or separated dedicated sensor devices for the purpose of PAD. The TOE decides about an attempt being a presentation attack instrument (PAI) or bona-fide presentation based on this data. The integrity and confidentiality of this data have to be protected. PAD evidence is only relevant if the functional package for PAD has been chosen.
- Audit data (AD): This data comprises the audit information that is generated by the TOE. The integrity, confidentiality and authenticity of the information has to be protected. AD is relevant for all available combinations of functional packages.
- Biometric sample: analog or digital representation of biometric characteristics prior to biometric feature extraction. The biometric sample shall be – per minimum – integrity protected. Biometric sample is only relevant if the functional package for biometric verification has been chosen.
- Biometric template: set of stored biometric features comparable to a biometric sample. The biometric template shall be – per minimum – integrity protected. Biometric template is only relevant if the functional package for biometric verification has been chosen.

4.3 Assumptions

4.3.1 A.ADMINISTRATION

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

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

4.3.2 A.CAPTURE

- It is assumed that all environmental factors (e.g. lightning) are appropriate with respect to the used capture device and biometric modality.
- Furthermore, it is assumed that bypassing the capture device in a technical manner is not possible.

4.3.3 A.ENVIRONMENT

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

Specifically the following aspects are assumed:

- It is assumed that the direct environment of the TOE supports the functionality of the biometric system. Regarding the request of the claimed identity, which is necessary for the biometric verification, the environment offers the possibility to integrate a claimed identity into the biometric verification process.
- The TOE environment provides a database for the biometric reference of enrolled users, audit information and other TSF data, whereby integrity and authenticity are ensured.
- The environment ensures a secure communication of security relevant data from and to the TOE.
- The environment ensures that no residual information remains on the sensor device that may be usable by an attacker.
- It is assumed that the environment provides reliable time stamps for audit logs, a functionality to review the audit information of the TOE and to ensures that only authorized administrators have access to the audit logs.
- It is assumed that the TOE environment is free of viruses, trojans, and malicious software

4.3.4 A.I&A

It is assumed that the environment provides functionality that allows the TOE to distinguish roles of different users. This also includes that the environment is assumed to provide a secure authentication mechanism for the administrator.

Application Note 4

The assumption A.I&A shall be removed from the base PP if the functional package for I&A has been chosen, as it will be replaced by a respective OSP.

4.3.5 A.PHYSICAL

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

4.3.6 A.FALLBACK

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

4.4 Threats

4.4.1 T.TSFDATA

An attacker may try to modify TSF data like the parameters used for PAD or biometric verification in order to compromise the functionality of the TOE.

Such an attack could compromise the integrity of secondary assets resulting in an incorrect operation of the TOE and therewith allowing the attacker to overcome or bypass another security function.

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

It should be noted that many attack paths for this threat are already countered by assumptions for the environment of the TOE. However, the author of the PP decided to add this threat following the philosophy of “defense in depth”.

4.4.2 T.RESIDUAL

An attacker may try to take advantage of unprotected residual security relevant data (e.g. PAD parameters and PAD evidences) that remain in the memory of the TOE from a previous usage.

In this way the attacker tries to get access to information about a user or the security relevant settings of the TOE. Such information may contain sensitive information or can be used to prepare an attack.

This kind of attack usually presupposes that the attacker has further knowledge about the TOE and may require special equipment in order to perform the attack via a visible interface of the TOE.

It should be noted that many attack paths for this threat are already countered by assumptions for the environment of the TOE. However, the author of the PP decided to add this threat following the philosophy of “defense in depth”.

4.5 Organizational Security Policies

4.5.1 OSP.AUDIT

In order to

- generate statistics that can be used to adjust the parameters for better quality (maintenance),
- trace modification, and
- trace possible attacks

the TOE shall record security-relevant events.

- The environment shall ensure that no residual information remains on the sensor device that may be usable by an attacker.
- The environment shall ensure a secure communication of security relevant data from and to the TOE.
- The environment shall provide reliable time stamps for audit logs, functionality to review the audit information of the TOE and to ensures that only authorized administrators have access to the audit logs.
- The TOE environment is free of viruses, trojans, and malicious software

5.2.4 OE.I&A

The environment shall provide functionality that allows the TOE to distinguish roles of different users. This also includes that the environment shall provide a secure authentication mechanism for the administrator.

Application Note 5

This security objective shall be removed from the base PP if the functional package for the identification and authentication of administrators has been chosen, as it will be replaced by a security objective for the TOE by this package.

5.2.5 OE.PHYSICAL

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

5.2.6 OE.FALLBACK

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

5.3 Security Objectives rationale

5.3.1 Overview

Table 5: Security Objectives Rationale

	O.AUDIT	*O.RESIDUAL*	*O.MANAGEMENT*	*OE.ADMINISTRATION*	*OE.CAPTURE*	*OE.ENVIRONMENT*	*OE.I&A*	*OE.PHYSICAL*	*OE.FALLBACK*
T.TSFDATA			X	X		X			
T.RESIDUAL		X				X			
OSP.AUDIT	X								
A.ADMINISTRATION				X					
A.CAPTURE					X				
A.ENVIRONMENT						X			
A.I&A							X		
A.PHYSICAL								X	
A.FALLBACK									X

5.3.2 Justification for coverage of assumptions

A.ENVIRONMENT is fulfilled by **OE.ENVIRONMENT** as directly follows.

A.ADMINISTRATION is fulfilled by OE.ADMINISTRATION as directly follows.

A.CAPTURE is fulfilled by OE.CAPTURE as directly follows.

A.I&A is fulfilled by **OE.I&A** as directly follows.

A.PHYSICAL is fulfilled by **OE.PHYSICAL** as directly follows

A.FALLBACK is followed by **OE.FALLBACK** as directly follows.

All security objectives for the environment are a direct and 1:1 re-instantiation of their corresponding assumptions so that the coverage is obvious.

5.3.3 Justification for coverage of threats

The threat **T.TSFDATA** which describes that an attacker may try to modify TSF data is mitigated by **O.MANAGEMENT** which restricts management of TSF data to authorized administrators. **OE.ADMINISTRATION** and **OE.ENVIRONMENT** also contribute towards the mitigation of this threat. **OE.ADMINISTRATION** is required as the administrator has to be well trained and non-hostile in order to mitigate **T.TSFDATA**. In addition, the secure environment of the TOE as described in **OE.ENVIRONMENT** is a prerequisite to mitigate this threat.

The threat **T.RESIDUAL** which describes that an attacker may take advantage of residual information is directly and completely mitigated by **O.RESIDUAL** as the objective ensures that no residual information will be existing in memory. The aspect of **T.RESIDUAL** that addresses residual information on the sensor device is mitigated by **OE.ENVIRONMENT** as the environment ensures that no residual information is existing.

5.3.4 Justification for coverage of OSPs

OSP.AUDIT is fulfilled by **O.AUDIT** as directly follows.

6 Extended Component definition

The following chapters contain the definition of the extended components that have been used in the context of this PP. These definitions have been taken from [ISO19989-1]. In accordance with the typographic conventions used in this document, the names of the SFRs in this chapter have been marked by the suffix "-EXT" compared to [ISO19989-1].

6.1 Presentation attack detection (FPT_PAD)

6.1.1 Family behaviour

This family defines functional requirements to detect biometric presentation attacks.

6.1.2 Component leveling:

Figure 2: FPT_PAD.1 Presentation attack detection, detects presentation attacks for biometrics.

6.1.3 Management: FPT_PAD-EXT.1

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

a) management of the parameters used for presentation attack detection.

6.1.4 Audit: FPT_PAD-EXT.1

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

a) Basic: presentation attack detected

b) Basic: no presentation attack detected

6.1.5 Presentation Attack Detection (FPT_PAD-EXT.1)

Hierarchical to:	No other components
Dependencies:	FMT_MTD.3 Secure TSF data FMT_SMF.1 Specification of Management Functions
FPT_PAD-EXT.1.1	The TSF shall be able to distinguish between bona-fide presentations and attack presentations for [assignment: *presentation attack instrument*].
FPT_PAD-EXT.1.2	If a presentation attack is detected, the following action(s) shall be performed: [assignment: *list of actions*].
FPT_PAD-EXT.1.3	If no presentation attack is detected, the following action(s) shall be performed: [assignment: *list of actions*].
FPT_PAD-EXT.1.4	Along with the feedback about presentation attack status, detected or not detected, the TOE shall deliver the following information: [assignment: *list of information*].

6.1.6 Justification for the definition of functional family FPT_PAD

PAD functionality describes mechanisms that protect biometric verification systems against specific threats. It therefore provides protection of the TSF which is subject of the functional class FPT.

There is no family in FPT that deals with detection of presentation attacks or biometric functionality at all, therefore a new family has been defined.

6.2 Biometric Verification (FIA_BVR)

6.2.1 Family behaviour

This family defines biometric verification mechanisms supported by the TSF. This family also defines the required attributes on which the biometric verification mechanisms must be based.

6.2.2 Component leveling:

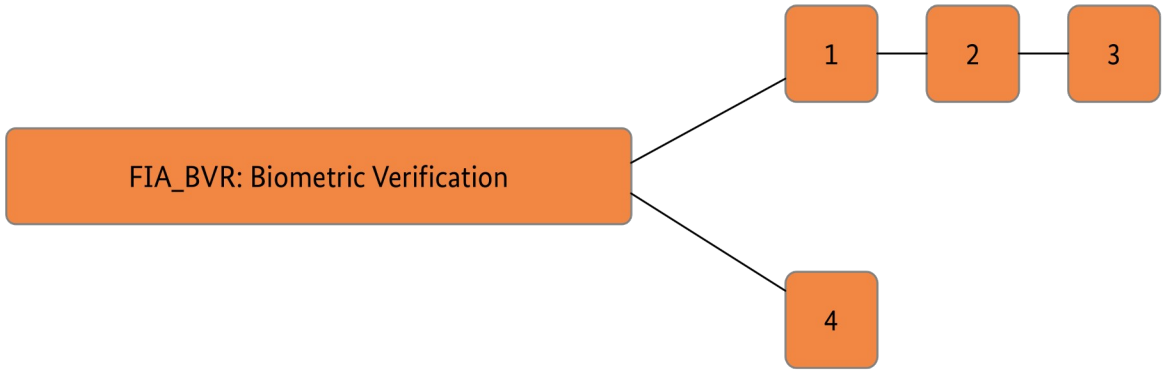

Figure 3: Component leveling FIA_BVR

FIA_BVR-EXT.1 Biometric verification with high performance, requires the TSF to limit FAR and FRR respectively within a specified rate.

FIA_BVR-EXT.2 Timing of the user authentication with biometric verification, allows a user to perform certain actions prior to the user authentication with biometric verification of the user's identity.

FIA_BVR-EXT.3 User authentication with biometric verification before any action, requires that users are authenticated with biometric verification before any other action will be allowed by the TSF.

FIA_BVR-EXT.4 Biometric verification not accepting presentation attack instruments, requires the biometric verification mechanism to be able to prevent the successful use of presentation attack instrument in a verification attempt.

Application Note 6

It should be highlighted here that FIA_BVR-EXT.1 does only require the TOE to provide a biometric verification mechanism. However, in contrast to other requirements from the class FIA, FIA_BVR-EXT.1 does not act in any way based on the result of the biometric verification. The decision about what follows out of the result of a biometric verification is left to another part of the TOE or the environment.

6.2.3 Management of FIA_BVR-EXT.1

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

a) the management of the TSF data (including the threshold values) by an administrator.

6.2.4 Management of FIA_BVR-EXT.2

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

a) the management of the TSF data (including the threshold values) by an administrator;

b) managing of the list of the actions that can be taken before the user is authenticated.

6.2.5 Management of FIA_BVR-EXT.3

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

a) the management of the TSF data (including the threshold values) by an administrator.

6.2.6 Management of FIA_BVR-EXT.4

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

a) the management of the TSF data (setting values for detecting artificial presentation attack instruments and for checking quality to generate biometric samples) by an administrator.

6.2.7 Audit of FIA_BVR-EXT.1

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

a) Minimal: Unsuccessful use of the biometric verification mechanism;

b) Basic: All use of the biometric verification mechanism;

c) Detailed: Identification of the changes to the TSF data (setting threshold values for biometric comparison scores used in biometric verification).

6.2.8 Audit of FIA_BVR-EXT.2

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

a) Minimal: Unsuccessful use of the user authentication mechanism with biometric verification;

b) Basic: All use of the user authentication mechanism with biometric verification;

c) Detailed: Identification of the changes to the TSF data (setting threshold values for biometric comparison scores used in biometric verification) and all TSF mediated user actions performed before authentication with biometric verification of the user.

6.2.9 Audit of FIA_BVR-EXT.3

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

a) Minimal: Unsuccessful use of the user authentication mechanism with biometric verification;

b) Basic: All use of the user authentication mechanism with biometric verification.

c) Detailed: Identification of the changes to the TSF data (setting threshold values for biometric comparison scores used in biometric verification).

6.2.10 Audit of FIA_BVR-EXT.4

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

Biometric Mechanisms Protection Profile (BMPP)

a) Minimal: Rejection by the TSF of data that is checked as low quality or detected as artificial presentation attack instrument;

b) Basic: Rejection or acceptance by the TSF of data that is quality checked or input to presentation attack detection subsystem;

c) Detailed: Identification of the changes to the TSF data (setting threshold values for quality scores and detecting artificial presentation attack instruments).

6.2.11 FIA_BVR-EXT.1 Biometric verification with high performance

Hierarchical to:	No other components
Dependencies:	FIA_EBR-EXT.1 Check of biometric samples for enrolment FIA_EBR-EXT.2 Biometric enrolment with low failure to enroll rate
FIA_BVR-EXT.1.1	The TSF shall provide a biometric verification mechanism for [assignment: *biometric characteristic*] to the user with the [selection: *FMR, FAR*] not exceeding [assignment: *defined value*] and [selection: *FNMR, FRR*] not exceeding [assignment: *defined value*].

6.2.12 FIA_BVR-EXT.2 Timing of the user authentication with biometric verification

Hierarchical to:	FIA_BVR-EXT.1 High accuracy biometric verification
Dependencies:	FIA_UID.1 Timing of identification FIA_EBR-EXT.1 Check of biometric samples for enrolment FIA_EBR-EXT.2 Biometric enrolment with low failure to enroll rate
FIA_BVR-EXT.2.1	The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated with biometric verification based on [assignment: *biometric characteristic*].
FIA_BVR-EXT.2.2	The TSF shall provide a user authentication mechanism with biometric verification based on [assignment: *biometric characteristic*] to the user with the [selection: FMR, FAR] not exceeding [assignment: *defined value*] and [selection: *FNMR, FRR*] not exceeding [assignment: *defined value*] to require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.13 FIA_BVR-EXT.3 User authentication with biometric verification before any action

Hierarchical to:	FIA_BVR-EXT.2 Timing of the user authentication with biometric verification
Dependencies:	FIA_UID.1 Timing of identification FIA_EBR-EXT.1 Check of biometric samples for enrolment FIA_EBR-EXT.2 Biometric enrolment with low failure to enroll rate
FIA_BVR-EXT.3.1	The TSF shall provide a user authentication mechanism with biometric verification based on [assignment: *biometric characteristic]* to the user with the [selection: *FMR, FAR*] not exceeding [assignment: *defined value*] and [selection: *FNMR, FRR*] not exceeding [assignment: *defined value*] to require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.14 FIA_BVR-EXT.4 Biometric verification not accepting presentation attack instruments

Hierarchical to:	No other components
Dependencies:	FIA_EBR-EXT.1 Check of biometric samples for enrolment
FIA_BVR-EXT.4.1	The TSF shall prevent presentation of [assignment: *biometric characteristic*], which result in biometric samples of low quality from being successful in the biometric verification.
FIA_BVR-EXT.4.2	The TSF shall prevent use of artificial presentation attack instruments for [assignment: *biometric characteristic*] from being successfully verified.

6.2.15 Justification for the definition of functional family FIA_BVR

FIA_BVR describes mechanisms for biometric verification. Biometric verification is a mean for user authentication which is described in the class FIA.

There is no family in FIA that deals with biometric verification. Therefore, the new family has been defined within that class.

6.3 Enrolment of biometric reference (FIA_EBR)

6.3.1 Family behaviour

This family defines enrolment mechanisms for biometric verification supported by the TSF. This family also defines the required attributes on which the biometric enrolment mechanisms must be based.

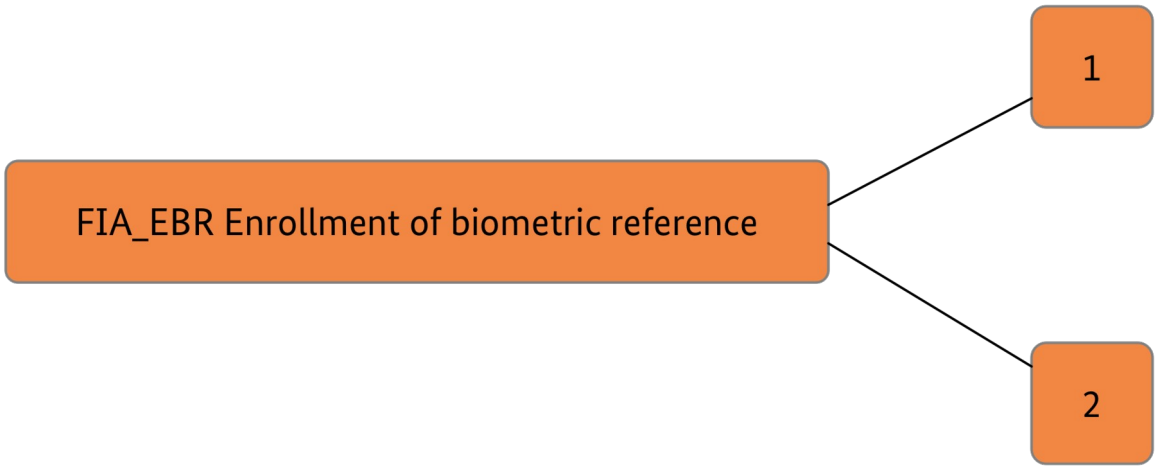

Figure 4: Component leveling for FIA_EBR

6.3.2 Component leveling:

FIA_EBR.1 Quality check of biometric samples for enrolment, requires the TSF to prevent enrolment if artificial presentation attack instruments are presented or biometric characteristics are presented in such a way that the biometric characteristics result in biometric samples of low quality. FIA_EBR.2 Biometric enrolment with low failure to enroll rate, requires the TSF to ensure enrolling only such biometric references of extremely good quality in order to achieve apparent good performance in biometric verification afterwards.

6.3.3 Management of FIA_EBR-EXT.1

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

a) the management of the TSF data (setting threshold values for quality scores to generate biometric reference) by an administrator;

b) the management of the TSF data (setting values for detecting artificial presentation attack instruments) by an administrator.

6.3.4 Management of FIA_EBR-EXT.2

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

a) the management of the TSF data (setting threshold values for quality scores to generate biometric reference) by an administrator.

6.3.5 Audit of FIA_EBR-EXT.1

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

a) Minimal: Rejection by the TSF of data that is checked as low quality or detected as artificial presentation attack instrument;

b) Basic: Rejection or acceptance by the TSF of data that is quality checked or input to presentation attack detection subsystem;

c) Detailed: Identification of the changes to the TSF data (setting threshold values for quality scores and detecting artificial presentation attack instruments).

6.3.6 Audit of FIA_EBR-EXT.2

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

a) Minimal: rejection by the TSF of data that is checked as low quality;

b) Basic: Rejection or acceptance by the TSF of data that is quality checked;

c) Detailed: Identification of the changes to the TSF data (setting threshold values for quality scores of biometric data for enrolment).

6.3.7 FIA_EBR-EXT.1 Check of biometric samples for enrolment

Hierarchical to:	No other components
Dependencies:	FPT_PAD-EXT.1
FIA_EBR-EXT.1.1	The TSF shall prevent use of [assignment: *biometric characteristic*] which result in biometric samples of low quality for enrolment that has been presented by any user of the TSF.
FIA_EBR-EXT.1.2	The TSF shall prevent use of artificial presentation attack instruments for enrolment of [assignment: *biometric characteristic*] that has been presented by any user of the TSF.

6.3.8 FIA_EBR-EXT.2 Biometric enrolment with low failure to enroll rate

Hierarchical to:	No other components
Dependencies:	No dependencies
FIA_EBR-EXT.2.1	The TSF shall provide a mechanism to enroll biometric reference information for [assignment: *biometric characteristic*] with the FTER not exceeding [*assignment: defined value*].

6.3.9 Justification for the definition of functional family FIA_EBR

FIA_BVR describes mechanisms for biometric enrolment. Biometric enrolment is a supportive mean for user authentication which is described in the class FIA.

There is no family in FIA that deals with biometric enrolment. Therefore, the new family has been defined within that class.

7 Security Requirements

This chapter describes the security functional and the assurance requirements which have to be fulfilled by the TOE.

Those requirements comprise functional components from Common Criteria ([CC]) Part II and assurance components from Common Criteria ([CC]) part III.

The following notations are used to mark operations that have been performed:

- **Selection** operations (used to select one or more options provided by the [CC] in stating a requirement.) are denoted by underlined text
- **Assignment** operation (used to assign a specific value to an unspecified parameter, such as the length of a password) are denoted by italicized text.
- **Extended SFR** are marked by the suffix "-EXT"
- No **Refinements** have been performed
- No **Iterations** have been performed.

7.1 Security Functional Requirements for the TOE

The following table summarizes all security functional requirements of this PP:

Table 6: Security Functional Requirements

Class FAU: Security Audit	
FAU_GEN.1	Audit Data Generation
Class FDP: User Data Protection	
FDP_RIP.2	Full residual information protection
Class FMT: Security Management	
FMT_MTD.3	Secure TSF data
FMT_SMF.1	Specification of Management Functions

7.1.1 Security audit (FAU)

7.1.1.1 Security audit data generation (FAU_GEN)

FAU_GEN.1	Audit data generation
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [basic] level of audit; and c) [assignment: *other specifically defined auditable events*].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].
Hierarchical to:	No other components
Dependencies:	FPT_STM.1

Application Note 7

The audit events that shall be recorded by the TOE depend on the use of the functional packages as defined in this PP.

For the base PP, the following events shall be audited:

- Every use of a management function (FMT_SMF.1),
- All parameters rejected by the management functions (FMT_SMF.3),

If the functional package for biometric verification is used, the following events shall be audited in addition:

- all use of the biometric verification mechanism; (FIA_BVR-EXT.1),
- rejection or acceptance by the TSF of data that is quality checked (FIA_EBR-EXT.2),

If the functional package for PAD is used, the following events shall be audited in addition:

- presentation attack detected (FPT_PAD-EXT.1),
- no presentation attack detected (FPT_PAD-EXT.1),

If useful in the context of a concrete technology the ST author should consider to audit additional information (e.g. a score or a claimed identity).

If the functional package for Identification and Authentication of administrators is used, the following events shall be audited in addition:

- All use of the authentication mechanism (FIA_UAU.1)
- All use of the user identification mechanism, including the user identity provided (FIA_UID.1)
- modifications to the group of users that are part of a role (FMT_SMR.1)

If the functional package for Enrolment Protection is used, the following events shall be audited in addition:

- Rejection or acceptance by the TSF of data that is quality checked or input to presentation attack detection subsystem (FIA_EBR-EXT.1)

7.1.2 User data protection (FDP)

7.1.2.1 Residual information protection (FDP_RIP)

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

7.1.3 Security management (FMT)

7.1.3.1 Management of TSF data (FMT_MTD)

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

Application Note 8

The assignment in FMT_MTD.3.1 shall be executed under consideration of the used functional package.

If the functional package for biometric verification is used, the second part of the assignment shall not be “none”.

If the functional package for PAD is used, the first part of the assignment shall not be “none”.

7.1.3.2 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1	Specification of Management Functions
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].
Hierarchical to:	No other components
Dependencies:	No dependencies

Application Note 9

The assignment in FMT_SMF.1.1 shall be executed under consideration of the used functional package.

If the functional package for biometric verification is used, the following management activities shall be considered:

- the management of the TSF data as used by FIA_EBR-EXT.2 (setting threshold values for quality scores to generate biometric reference) by an administrator,
- the management of the TSF data as used by FIA_BVR-EXT.1 (including the threshold values) by an administrator;

If the functional package for PAD is used, the following management activities shall be considered:

- management of the parameters used for presentation attack detection as defined in FPT_PAD-EXT.1

If the functional package for Identification and Authentication of administrators is used, the following management activities shall be considered:

- management of the authentication data by an administrator (FIA_UAU.1)
- management of the authentication data by the associated user (FIA_UAU.1)
- managing the list of actions that can be taken before the user is authenticated (FIA_UAU.1)
- the management of the user identities (FIA_UID.1)
- if an authorised administrator can change the actions allowed before identification, the managing of the action lists (FIA_UID.1)
- managing the group of users that are part of a role (FMT_SMR.1)

If the functional package for Enrolment Protection is used, the following management activities shall be considered:

- the management of the TSF data (setting threshold values for quality scores to generate biometric reference) by an administrator (FIA_EBR-EXT.1)

7.2 Security Assurance Requirements for the TOE

Due to the special character of the technology described in this PP, the following explicit assurance package has been defined for the TOE based on EAL 2. In contrast to EAL 2, it does not contain AVA_VAN.2 but is augmented by ALC_FLR.1. The following table lists the assurance components which are chosen for this PP.

Table 7: Assurance Requirements

Assurance Class	***Assurance Component***	***Title***
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic Design
Guidance documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.1	Basic flaw remediation
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended component definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample

Due to the special character of the technology described in this PP, the PAD Evaluation Methodology [PADEG] shall be applied during evaluation. This methodology will provide the evaluator with additional information and guidance for some assurance requirements.

7.3 Security Requirements rationale

7.3.1 Security Functional Requirements rationale

Table 8: Security Functional Requirements Rationale Overview

	O.AUDIIT	***O.RESIDUAL***	***O.MANAGEMENT***
FAU_GEN.1	X		
FDP_RIP.2		X	
FMT_SMF.1			X
FMT_MTD.3			X

O.AUDIT is directly and completely implemented by the use of **FAU_GEN.1**.

O.RESIDUAL is directly and completely implemented by the use of **FDP_RIP.2**.

O.MANAGEMENT has two major aspects. The aspect that the TOE shall provide the necessary management functionality is realized by the use of **FMT_SMF.1**. The fact that the TOE shall only accept secure values for TSF data is implemented by the use of **FMT_MTD.3**.

Application Note 10

FMT_MTD.3 and FMT_SMF.1 leave parts of their operations open to the ST author. This has been necessary as concrete aspects of the implementation may have an effect on the assignments. The aforementioned rationale has been written in a generic manner accordingly. However, as the ST author has to complete the assignments, they shall also specify the rationale for fulfilling the security objectives (specifically O.MANAGEMENT) in a more concrete manner (rather than simply referencing this Protection Profile).

7.3.1.1.1 Security Functional Requirements Dependency Rationale

Table 9: Dependencies of functional requirements for base PP

SFR	***Dependencies***	***Fulfilment***
FAU_GEN.1	FPT_STM.1	The requirements on FPT_STM.1 that requires the TOE to provide secure time stamps to be used in the context of its audit functionality is satisfied by the environment of the TOE (see A.ENVIRONMENT).
FDP_RIP.2	-	-
FMT_MTD.3	FMT_MTD.1	The TOE relies on its environment for storage and control of its TSF data. As such, the dependency on FMT_MTD.1 is not fulfilled by the TOE but by the environment.
FMT_SMF.1		

Application Note 11

This PP describes only the minimum requirements for a biometric system. Therefore, the TOE also relies on its environment and some of the dependencies from Common Criteria ([CC]) Part II are not met. The ST author shall therefore consider whether these requirements can be fulfilled by a concrete TOE. If this is the case, the SFRs that are needed to fulfill the dependencies shall be added to the ST.

7.3.2 Security Assurance Requirements rationale

Due to the special character of the technology described in this PP, an explicit assurance package has been defined for the TOE. It has been chosen for this Protection Profile as it should focus on application cases for which it is sufficient to determine whether the security functionality claimed by a TOE is working correctly without performing a dedicated vulnerability assessment.

The defined assurance package has been developed based on EAL 2. In contrast to EAL 2, it does not contain AVA_VAN.2 but has been augmented by the assurance component ALC_FLR.1. ALC_FLR.1 has been included as biometric systems are supposed to have flaws that will be found in future and that will then have to be addressed.

Additional guidance has been provided for some of the assurance components due to the special nature of the biometric technology in form of [PADEG].

7.3.2.1 Dependencies of assurance components

The dependencies of the assurance requirements are fulfilled as shown in table 10:

Table 10: Dependencies of assurance components

Assurance Class	***Assurance Component***	***Dependencies***	***Fulfilment***
Development	ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	ADV_FSP.2, ADV_TDS.1
	ADV_FSP.2	ADV_TDS.1	ADV_TDS.1
	ADV_TDS.1	ADV_FSP.2	ADV_FSP.2
Guidance documents	AGD_OPE.1	ADV_FSP.1	ADV_FSP.2
	AGD_PRE.1	No dependencies	-
Life-cycle support	ALC_CMC.2	ALC_CMS.1	ALC_CMS.2
	ALC_CMS.2	No dependencies	-
	ALC_DEL.1	No dependencies	-
	ALC_FLR.1	No dependencies	-
Security Target Evaluation	ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.2
	ASE_ECD.1	No dependencies	-
	ASE_INT.1	No dependencies	-
	ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1
	ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_OBJ.2, ASE_ECD.1
	ASE_SPD.1	No dependencies	-
	ASE_TSS.1	ASE_INT.1, ASE_REQ.1 ADV_FSP.1	ASE_INT.1, ASE_REQ.2 ADV_FSP.2
Tests	ATE_COV.1	ADV_FSP.2, ATE_FUN.1	ADV_FSP.2, ATE_FUN.1
	ATE_FUN.1	ATE_COV.1	ATE_COV.1
	ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1

8 Functional Packages

8.1 Overview and allowed combinations of functional packages

This Protection Profile utilizes the concept of functional packages . For the use of this PP, some limitations shall apply.

First of all, the base PP shall never be used alone and any functional package from this PP shall never be used without the base PP. Per minimum one functional package shall be used. The following table therefore identifies the combinations in which the functional packages can be used to achieve the description of certain use cases that have been considered during the development of this Protection Profile.

No other combinations than the ones identified in the following table must be used as only those combinations make sense. An “X” in the table stands for a mandatory use of a functional package for a certain use case while an “O” indicates an optional use.

Table 11: Possible combinations of functional packages

Use Case	***Functional Package***			
	Biometric Verification	***PAD***	***Enrolment Protection***	***I&A for Administrators***
TOE for presentation attack detection (PAD)		X		O
TOE for biometric verification	X			O
TOE for biometric verification and integrated PAD	X	X		O
TOE for biometric verification, integrated PAD and enrolment protection	X	X	X	O

8.2 Functional Package: Biometric Verification

8.2.1 Package Identification

Table 12: Identification of Functional Package Biometric Verification

Title:	Biometric Verification Functional Package
Version:	This functional package inherits the version of the base PP. Please refer to chapter 1.
Date:	This functional package inherits the date of the base PP. Please refer to chapter 1.
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Editor:	Nils Tekampe, konfidas GmbH
Registration/owner:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Certification-ID:	This functional package inherits the certification-ID of the base PP. Please refer to chapter 1.
CC-Version:	3.1 Revision 5
Conformance Claim:	• The conformance of this package is Common Criteria ([CC]) Part II extended • The conformance of this package is Common Criteria ([CC]) Part III conformant

8.2.2 Package Overview

This functional package shall be used if the TOE provides functionality for biometric verification as described in chapter 2.3.

8.2.3 Security Problem Definition

8.2.3.1 Assumptions

The following assumptions shall be added to the ST if this functional package is chosen.

8.2.3.1.1 A.PROTECTION

It is assumed that the immediate environment of the TOE ensures that presentation attacks against the biometric verification functionality of the TOE would be detected or are made impossible with a sufficient reliability.

Application Note 12

The assumption A.PROTECTION shall only be added to the ST if the functional package for PAD as defined in chapter 8.2 cannot be chosen.

8.2.3.1.2 A.ENROLMENT

It is assumed that the environment ensures that the biometric reference that is created during enrolment is of sufficient quality and cannot be used for any attacks against the biometric system.

Specifically, it is assumed that

- The biometric reference and the biometric samples that are used to create it, belong to the correct user identity,
- the biometric sample that is used to create the reference does not contain any information from other user(s),
- the biometric reference is of sufficient quality.

It is assumed that these assumptions are either achieved by a supervised enrolment process or by having a certified enrolment system in the environment.

Application Note 13

> The assumption A.ENROLMENT shall only be added to the ST if the functional package for enrolment protection as defined in chapter 8.5 cannot be chosen, as it will be replaced by a similar assumption and functionality provided by the TOE.

8.2.3.2 Threats

The following threats shall be added to the ST if this functional package is chosen.

8.2.3.2.1 T.BRUTEFORCE

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

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

This threat considers two different threat agents and corresponding adverse actions:

- A not really hostile user who just tries to get verified with a wrong claimed identity a few times. The motivation of such a user is usually just curiosity. He does not need specific knowledge about the TOE to perform this attack.
- A real attacker who uses a large amount of biometric characteristics and who really wants to get unauthorized access to the portal. This type of threat agent is supposed to have further public knowledge on biometric verification systems.

8.2.3.3 OSP

This package does not contain any OSP.

8.2.4 Security objectives for the TOE

The following security objectives shall be added to the ST if this functional package is chosen.

8.2.4.1 O.BIO_VERIFICATION

The TOE shall provide a biometric verification mechanism to ensure access to a logical or physical portal with an adequate reliability[1].

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

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

8.2.4.2 O.ENROLMENT

The TOE shall provide a mechanism to enroll the biometric characteristic of a user into the system.

8.2.5 Security objectives for the environment

The following security objectives for the environment shall be added to the ST if this functional package is chosen.

8.2.5.1 OE.PROTECTION

The immediate environment of the TOE shall ensure that presentation attacks against the biometric verification functionality of the TOE would be detected or are made impossible with a sufficient reliability.

Application Note 14

OE.PROTECTION shall only be added to the ST if the functional package for PAD as defined in chapter 8.3 cannot be chosen, as it will be replaced by a similar objective for the environment and functionality provided by the TOE.

8.2.5.1.1 OE.ENROLMENT

The environment shall ensure that the biometric reference that is created during enrolment is of sufficient quality and cannot be used for any attacks against the biometric system.

Specifically, it shall be ensured that

- the biometric reference and the biometric samples that are used to create it, belong to the correct user identity,
- the biometric sample that is used to create the reference does not contain any information from other user(s),
- the biometric reference is of sufficient quality.

These objectives can either be achieved by a supervised enrolment process or by having a certified enrolment system in the environment.

Application Note 15

The objective OE.ENROLMENT shall only be added to the ST if the functional package for enrolment protection as defined in chapter 8.5 cannot be chosen.

1 The term „adequate reliability“ here refers to the error rates mentioned later in the objective and in the corresponding SFR.

8.2.6 Rationale for added assumptions, threats and objectives

Table 13: Security Objectives Rationale for functional package biometric verification

	O.BIO_VERIFICATION	***O.ENROLMENT***	***OE.PROTECTION***	***OE.ENROLMENT***
T.BRUTEFORCE	X	X		
A.PROTECTION			X	
A.ENROLMENT				X

T.BRUTEFORCE is mitigated by a combination of **O.BIO_VERIFICATION** and **O.ENROLMENT**. While **O.BIO_VERIFICATION** contains the definition of the biometric verification mechanism that works against the attack as described in **T.BRUTEFORCE, O.ENROLMENT** provides the necessary enrolment functionality as a pre-requisite for biometric verification.

A.PROTECTION is fulfilled by **OE.PROTECTION** as directly follows.

A.ENROLMENT is fulfilled by **OE.ENROLMENT** as directly follows.

8.2.7 Security Functional Requirements

The following Security Functional Requirements shall be added to the ST if this functional package is chosen.

8.2.7.1 FIA_BVR-EXT.1 Biometric verification with high performance

FIA_BVR-EXT.1.1	The TSF shall provide a biometric verification mechanism for [assignment: *biometric characteristic*] to the user with the [selection: *FMR, FAR*] not exceeding [assignment: *defined value*] and [selection: *FNMR, FRR*] not exceeding [assignment: *defined value*].
Hierarchical to:	No other components
Dependencies:	FIA_EBR-EXT.1 Check of biometric samples for enrolment FIA_EBR-EXT.2 Biometric enrolment with low failure to enroll rate

8.2.7.2 FIA_EBR-EXT.2 Biometric enrolment with low failure to enroll rate

FIA_EBR-EXT.2.1	The TSF shall provide a mechanism to enroll biometric reference information for [assignment: *biometric characteristic*] with the FTER not exceeding [assignment: *defined value*].
Hierarchical to:	No other components
Dependencies:	No dependencies

8.2.7.3 Security Functional Requirements Rationale

Table 14: Security Functional Requirements Rationale Overview

	O.BIO_VERIFICATION	*O.ENROLMENT*
FIA_BVR-EXT.1	X	
FIA_EBR-EXT.2		X

O.BIO_VERIFICATION is directly and completely implemented by the use of **FIA_BVR-EXT.1**.

O.ENROLMENT is directly and completely implemented by the use of **FIA_EBR-EXT.2**.

8.2.7.3.1 Security Functional Requirements Dependency Rationale

Table 15: Dependencies of functional requirements for functional package "Biometric Verification"

SFR	***Dependencies***	***Fulfilment***
FIA_BVR-EXT.1	FIA_EBR-EXT.1 FIA_EBR-EXT.2	The dependency of FIA_BVR-EXT.1 to FIA_EBR-EXT.1 shall prevent the use of biometric characteristics that would result in low quality templates and presentation attacks during enrolment. In the context of this PP, this is already fulfilled by the environment. Therefore, the dependency on FIA_EBR-EXT.1 is not met within the TOE itself. Please note that this can be changed by choosing the functional package from chapter 8.5 on enrolment protection. FIA_EBR-EXT.2
FIA_EBR-EXT.2	-	-

8.3 Functional Package: PAD

8.3.1 Package Identification

Table 16: Identification of Functional Package: PAD

Title:	Biometric Presentation Attack Detection Functional Package
Version:	This functional package inherits the version of the base PP. Please refer to chapter 1.
Date:	This functional package inherits the date of the base PP. Please refer to chapter 1.
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Editor:	Nils Tekampe, konfidas GmbH
Registration/owner:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Certification-ID:	This functional package inherits the certification-ID of the base PP. Please refer to chapter 1.
CC-Version:	3.1 Revision 5
Conformance Claim:	• The conformance of this package is Common Criteria ([CC]) Part II extended • The conformance of this package is Common Criteria ([CC]) Part III conformant

8.3.2 Package Overview

This functional package shall be used if the TOE provides functionality for presentation attack detection as described in chapter 2.4.

8.3.3 Security Problem Definition

8.3.3.1 Assumptions

The following assumptions shall be added to the ST if this functional package is chosen.

8.3.3.1.1 A.BIOMETRIC_SYSTEM

The PAD functionality described in this functional package is a protection mechanism for a specific threat against a biometric system. However, it can only address threats based on presentation attacks.

The biometric system that is protected by the TOE therefore ensures that all other threats that are not related to PAD are appropriately handled.

Further, the biometric system ensures that the functionality of the TOE is invoked/used in order to protected the biometric system against presentation attacks.

Application Note 16

The assumption A.BIOMETRIC_SYSTEM shall only be added to the ST if the functional package for biometric verification as defined in chapter 8.2 cannot be chosen. If the functional package for biometric verification is chosen, the aspects described in A.BIOMETRIC_SYSTEM shall be addressed by the TOE (based on the requirements from the functional package for biometric verification).

8.3.3.2 Threats

The following threats shall be added to the PP if this functional package is chosen.

8.3.3.2.1 T.PA

An attacker may try to use a Presentation Attack Instrument in order to circumvent the functionality of a biometric system. The protected system in this context may be an enrolment and/or verification system. This threat is directed against the primary asset of the TOE, namely the decision of the PAD function.

The concrete aim of the attacker is highly depending on the concrete application case but will usually be

- The impersonation of a specific user of the protected biometric system,
- The impersonation of any user of the protected system or
- A disguise of their own identity

As this kind of attack is directed against the primary functionality of the biometric system it does not require specific knowledge about the system to identify the possibility for such an attack. However, depending on the concrete aim the attacker may need specific knowledge, skills and equipment for preparing and performing this attack.

8.3.3.3 OSP

This package does not contain any OSP.

8.3.4 Security objectives for the TOE

The following security objectives shall be added to the ST if this functional package is chosen.

8.3.4.1 O.PAD

The TOE shall be able to detect whether an attempt to a biometric system is a presentation attack or a bona-fide presentation .

The PAD evidence may be extracted from the data provided by the same sensor that is used to acquire the biometric characteristic for verification, or it may be retrieved using sensors which are solely dedicated to PAD.

8.3.5 Security objectives for the environment

The following security objectives for the environment shall be added to the ST if this functional package is chosen.

8.3.5.1 OE.BIOMETRIC_SYSTEM

The PAD functionality described in this functional package is a protection mechanism for a specific threat against a biometric system. However, it can only address threats based on presentation attacks.

The biometric system that is protected by the TOE therefore shall ensure that all other threats that are not related to PAD are appropriately handled.

Further, the biometric system ensures that the functionality of the TOE is invoked/used in order to protected the biometric system against presentation attacks.

Application Note 17

OE.BIOMETRIC_SYSTEM shall only be added to the ST if the functional package for biometric verification as defined in chapter8.2 cannot be chosen. If the functional package for biometric verification is chosen, the aspects described in OE.BIOMETRIC_SYSTEM shall be addressed by the TOE (based on the requirements from the functional package for biometric verification).

8.3.6 Rationale for added assumptions, threats and objectives

Table 17: Security Objectives Rationale for functional package PAD

	O.PAD	***OE.BIOMETRIC_SYSTEM***
T.PA	X	
A.BIOMETRIC_SYSTEM		X

T.PA is countered by **O.PAD** as directly follows. The mechanism for PAD as described in **O.PAD** is the direct countermeasure to presentation attack as described in **T.PA**.

A.BIOMETRIC_SYSTEM is fulfilled by **OE.BIOMETRIC_SYSTEM** as directly follows.

8.3.7 Security Functional Requirements

The following Security Functional Requirements shall be added to the ST if this functional package is chosen.

8.3.7.1 Presentation Attack Detection (FPT_PAD-EXT.1)

FPT_PAD-EXT1.1	The TSF shall be able to distinguish between bona-fide presentations and attack presentations for [assignment: *presentation attack instrument*].
FPT_PAD-EXT.1.2	If a presentation attack is detected, the following action(s) shall be performed: [assignment: *list of actions*].
FPT_PAD-EXT.1.3	If no presentation attack is detected, the following action(s) shall be performed: [assignment: *list of actions*].
FPT_PAD-EXT.1.4	Along with the feedback about presentation attack status, detected or not detected, the TOE shall deliver the following information: [assignment: *list of information*].
Hierarchical to:	No other components
Dependencies:	FMT_MTD.3 Secure TSF data FMT_SMF.1 Specification of Management Functions

8.3.7.2 Security Functional Requirements Rationale

O.PAD is directly and completely implemented by the use of **FPT_PAD-EXT.1**

8.3.7.2.1 Security Functional Requirements Dependency Rationale

Table 18: Dependencies of functional requirements for functional package "Presentation Attack Detection"

SFR	***Dependencies***	***Fulfilment***
FPT_PAD-EXT.1	FMT_MTD.3 FMT_SMF.1	Both dependencies are contained in the required base PP.

8.4 Functional Package: Identification and Authentication for administrators

8.4.1 Package Identification

Table 19: Identification of Functional Package: Identification and Authentication for administrators

Title:	Identification and Authentication for Administrators Functional Package
Version:	This functional package inherits the version of the base PP. Please refer to chapter 1.
Date:	This functional package inherits the date of the base PP. Please refer to chapter 1.
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Editor:	Nils Tekampe, konfidas GmbH
Registration/owner:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Certification-ID:	This functional package inherits the certification-ID of the base PP. Please refer to chapter 1.
CC-Version:	3.1 Revision 5
Conformance Claim:	• The conformance of this package is Common Criteria ([CC]) Part II conformant • The conformance of this package is Common Criteria ([CC]) Part III conformant

8.4.2 Package Overview

This functional package shall be used if the TOE provides functionality for the identification and authentication as described in chapter 2.5.

8.4.3 Security Problem Definition

8.4.3.1 Assumptions

The assumption A.I&A from the base PP shall not be copied into an ST if this package is chosen.

8.4.3.2 Threats

This functional package contains no threats.

8.4.3.3 OSP

The following new OSP shall be added to the ST if this package is chosen.

8.4.3.3.1 OSP.I&A

The TOE shall provide functionality to distinguish roles of different users. This also includes that the TOE shall provide a secure authentication mechanism for the administrator.

8.4.4 Security objectives for the TOE

The following security objectives shall be added to the ST if this functional package is chosen.

8.4.4.1 O.I&A

The TOE shall provide functionality to distinguish roles of different users. This also includes that the TOE shall provide a secure authentication mechanism for the administrator.

8.4.5 Security objectives for the environment

The security objective **OE.I&A** from the base PP shall not be copied into an ST if this package is chosen.

8.4.6 Rationale for added assumptions, threats and objectives

Removing the assumption **A.I&A** and the corresponding objective for the environment is necessary as this objective describes the functionality which is now required by **O.I&A**.

O.I&A completely implements the functionality as required by **OSP.I&A**.

8.4.7 Security Functional Requirements

The following Security Functional Requirements shall be added to the ST if this functional package is chosen.

8.4.7.1 FIA_UAU.1: Timing of authentication

FIA_UAU.1.1	The TSF shall allow [assignment: *list of TSF mediated actions]* on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

8.4.7.2 FIA_UID.1: Timing of identification

FIA_UID.1.1	The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Hierarchical to:	No other components.
Dependencies:	No dependencies

8.4.7.3 FMT_SMR.1: Security Roles

FMT_SMR.1.1	The TSF shall maintain the roles [assignment: *the authorised identified roles*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

8.4.7.4 Security Functional Requirements Rationale

O.I&A is directly and completely implemented by the use of **FIA_UAU.1**, **FIA_UID.1** and **FMT_SMR.1**

8.4.7.4.1 Security Functional Requirements Dependency Rationale

Table 20: Dependencies of functional requirements for functional package "Identification and Authentication for Administrators"

SFR	***Dependencies***	***Fulfilment***
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UID.1	-	-
FMT_SMR.1	FIA_UID.1	FIA_UID.1

8.5 Functional Package: Enrolment Protection

8.5.1 Package Identification

Table 21: Identification of Functional Package: Enrolment Protection

Title:	Enrolment Protection Functional Package
Version:	This functional package inherits the version of the base PP. Please refer to chapter 1.
Date:	This functional package inherits the date of the base PP. Please refer to chapter 1.
Sponsor:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Editor:	Nils Tekampe, konfidas GmbH
Registration/owner:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security Germany
Certification-ID:	This functional package inherits the certification-ID of the base PP. Please refer to chapter 1.
CC-Version:	3.1 Revision 5
Conformance Claim:	• The conformance of this package is Common Criteria ([CC]) Part II extended • The conformance of this package is Common Criteria ([CC]) Part III conformant

8.5.2 Package Overview

This functional package shall be used if the TOE provides functionality for enrolment protection as described in chapter 2.6.

8.5.3 Security Problem Definition

8.5.3.1 Assumptions

The following assumptions shall be added to the ST if this functional package is chosen. It shall replace A.ENROLMENT from the functional package from biometric verification.

8.5.3.1.1 A.ENROLMENT

It is assumed that the biometric reference and the biometric samples that are used to create the biometric reference, belong to the correct user identity and that the biometric sample that is used to create the reference does not contain any information from other user(s).

8.5.3.2 Threats

The following threats shall be added to the ST if this functional package is chosen.

8.5.3.2.1 T.ENROLMENT

An attacker may perform an attack against the enrolment process. The overall objective of the attacker is to later attack the biometric verification decision but the attacker prepares this via an attack to the enrolment process.

This threat specifically covers

- An attacker trying to enroll an artefact into the biometric system
- an attacker trying to enroll a biometric sample that has carries characteristics from more than one user.

8.5.3.3 OSP

This package does not contain any OSP.

8.5.4 Security objectives for the TOE

The following security objectives shall be added to the ST if this functional package is chosen. This security objective replaces the objective O.ENROLMENT from the functional package for biometric verification as described in chapter 8.2.

8.5.4.1 O.ENROLMENT

The TOE shall provide a mechanism to enroll the biometric characteristic of a user into the system.

The TOE shall provide functionality to protect the enrolment process in cooperation with its immediate environment. Specifically, the TOE shall ensure that

- the biometric reference is of sufficient quality
- the biometric reference is not created from an artefact.

8.5.5 Security objectives for the environment

The following security objectives for the environment shall be added to the ST if this functional package is chosen. It replaces the objective OE.ENROLMENT from the package for biometric verification.

8.5.5.1 OE.ENROLMENT

It shall be ensured that the biometric reference and the biometric samples that are used to create the biometric reference belong to the correct user identity and that the biometric sample that is used to create the reference does not contain any information from other user(s).

8.5.6 Rationale for added assumptions, threats and objectives

Table 22: Security Objectives Rationale for functional package biometric verification

	O.ENROLMENT	***OE.ENROLMENT***
T.ENROLMENT	X	
A.ENROLMENT		X

T.ENROLMENT is mitigated completely by **O.ENROLMENT**.

A.ENROLMENT is fulfilled by **OE.ENROLMENT** as directly follows.

8.5.7 Security Functional Requirements

The following Security Functional Requirements shall be added to the ST if this functional package is chosen.

8.5.7.1 FIA_EBR-EXT.1 Check of biometric samples for enrolment

FIA_EBR-EXT.1.1	The TSF shall prevent use of [assignment: *biometric characteristic*] which result in biometric samples of low quality for enrolment that has been presented by any user of the TSF.
FIA_EBR-EXT.1.2	The TSF shall prevent use of artificial presentation attack instruments for enrolment of [assignment: *biometric characteristic*] that has been presented by any user of the TSF.
Hierarchical to:	No other components
Dependencies:	FPT_PAD-EXT.1

Application Note 18

It should be noted that the functionality as required by FIA_EBR-EXT.1 is explicitly expected to detect and prohibit so called morphing attacks in which an attacker tries to create a biometric template that matches multiple users.

8.5.7.2 Security Functional Requirements Rationale

Table 23: Security Functional Requirements Rationale Overview

	O.ENROLMENT
FIA_EBR-EXT.1	X

O.ENROLMENT is directly and completely implemented by the use of **FIA_EBR-EXT.1**.

8.5.7.2.1 Security Functional Requirements Dependency Rationale

Table 24: Dependencies of functional requirements for functional package "Enrolment Protection"

SFR	***Dependencies***	***Fulfilment***
FIA_EBR-EXT.1	FPT_PAD-EXT.1	FPT_PAD-EXT.1

Reference Documentation

CC	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and general model, dated April 2017, version 3.1 R5 • Part 2: Security functional requirements, dated April 2017, version 3.1, R5 • Part 3: Security assurance requirements, dated April 2017, version 3.1, R5
ISO19989-1	ISO/IEC 19989-1:2020 — Information technology — Security techniques — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework
ISO30107-1	ISO/IEC 30107 Information technology — Biometric presentation attack detection —Part 1: Framework
ISO19795-1	ISO/IEC 19795 Information technology — Biometric performance testing and reporting —Part 1: Principles and framework
ISO2382-37	ISO/IEC: ISO/IEC 2382-37 Information technology — Vocabulary — Part 37: Biometrics
PADEG	PAD evaluation guidance, BSI
ISO30107-3	ISO/IEC 30107 Information technology — Biometric presentation attack detection —Part 1: Framework