Common Criteria Security Target

For

VoiceIdent Unit 2.0

Version:	***2.0.7***
Certification ID:	***BSI-DSZ-CC-0469***
Date:	***2008-04-21***

Revision History

Version	*Date*	*Description*
0.1	*2005-11-01*	*First Draft*
0.8	*2005-11-15*	*Draft for Kick-Off with all CC aspects*
0.9	*2005-11-16*	*Figure 3 updated*
0.95	*2005-12-19*	*Rationale completed*
0.96	*2005-12-20*	*updated: Figure 3, Table 1, Sections 2.5, 2.6, 5.1.3.2.1, 6.1, 8.1.3*
0.97	*2006-01-19*	*updated:Table 1,* *2.4 Section “Capture Device”,* *2.5,* *5.1.1.4.2”FMT_MSA.3*
1.0	*2006-01-23*	*new subchapters 8.3.3 and 8.3.4; minor editorial changes*
1.1	*2006-02-16*	*Changes concerning the BSI comment "threshold settings"*
1.2	*2006-03-14*	*Changes concerning the BSI comment in FMT_MOF.1.1#1; FMT_MSA.1.1*
1.3	*2006-05-05*	*Changes concerning the BSI comments from 21.04.2006*
1.4	*2006-07-27*	*Changes concerning the BSI comments from 18.07.2006*
1.5	*2006-08-24*	*Changes concerning the RNG and BSI comments*
1.6	*2006-09-14*	*Changes concerning the BSI comments from 04.09.2006*
1.7	*2006-09-29*	*Update of the software versions*
2.0	*2007-06-01*	*Changes concerning the VoIP extension for the purpose of the re-evaluation* *added extensions:* • *EW01: Extension for the VoIP telephony* • *EW02: Update the “nuance” versions, ASR (Automatic Speech Recognition) and SV (Speech Verification)* • *EW03: Extension for the implementation of IBM data base*
2.0.2	*2007-07-27*	*Changes concerning VoIP interface and new databases*
2.0.3	*2007-08-08*	*Insert certification-ID*
2.0.4	*2007-12-11*	*Resetting the version of the Nuance Verifier*
2.0.5	*2008-03-17*	*Update of the software versions*
2.0.6	*2008-03-31*	*Update of the software versions*
2.0.7	*2008-04-21*	*Changes concerning the BSI comments from 18.04.2008*

TABLE OF CONTENTS

LIST OF TABLES

List of Figures

DOCUMENT INTRODUCTION

This Security Target was developed based on the Protection Profile for Biometric Verification Mechanisms (BSI-PP-0016) published by the German Federal Office for Information Security (BSI) and the Security Target for VoiceIdent Unit 1.0 (BSI-DSZ-CC-0359) [ST_V1.0].

For VoiceIdent Unit 1.0 it was agreed upon the following arrangement: All text, which is taken from the PP, is in blue *colour. New text specific to this ST is in black colour and additionally in Italics.*

For VoiceIdent Unit 2.0 only the extensions between the versions are highlighted.

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

A Acknowledgement

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

B Application notes

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

Application notes are divided into:

- General **Application Note (GEN)** - explains basic principles of the approach and provides general information.
- [CC] explanatory **Application Note (CC)** - provides details of Common Criteria definitions and usage; regarding biometric practitioners.
- Biometric **Application Note (BIO)** - provides details of biometric definitions and usage; applicable to [CC] practitioners.

C Notations

The notation, formatting, and conventions used in this *ST* are consistent with those used in the Common Criteria, Version 2.3, August 2005 [CC].

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

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

D Abbreviations

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

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

E References

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

F Terminology

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

1. *SECURITY TARGET* INTRODUCTION

This chapter contains the following sections:

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

1.1 Identification

Title:	*Security Target* for *VoiceIdent Unit 2.0*
ST Version:	*2.0.7*
ST Date:	*2008-04-21*
Author:	*T-COM*
Developer:	*T-Systems*
Product:	*VoiceIdent Unit 2.0*
TOE-name:	*VoiceIdent Unit 2.0*
TOE-version:	*2.0*
Product Type:	*biometric authentication system*
Certification Authority:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security
Certification ID:	*BSI-DSZ-CC-0469*
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 [CC]
Keywords:	authentication; biometric; identification; Protection Profile; verification; voice-recognition

1.2 Overview

The scope of this *Security Target* is to describe the functionality of *the VoiceIdent Unit* biometric verification system in terms of [CC] and to define functional and assurance requirements for *this system*.

Therewith the major mean of *the VoiceIdent Unit* biometric verification system is to verify or reject the claimed identity of a human being using *his voice as a* unique characteristic of his body.

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

1.3 Common Criteria conformance

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

The assurance level for this *Security Target* is EAL2, augmented with ADV_SPM.1 and the minimum strength of function level is SOF-*medium*. Additional information related to [CC] biometric system evaluations are referenced in the Biometric Evaluation Methodology supplement [BEM]. For the pure biometric verification process, the strength of function is defined in terms of the FAR (see Annex A)[1].

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

This ST conforms to the "Protection Profile for Biometric Verification Mechanisms" (BSI-PP-0016) published and registered by the German Federal Office for Information Security (BSI).

1.4 Related documents

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

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

1.5 Organisation

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

- **Chapter 2:** The TOE description provides general information about the TOE, its generic structure and boundaries.
- **Chapter 3**: The TOE security environment describes security aspects of the environment in which the TOE is intended to be used and the manner in which it is intended to be employed. The TOE security environment includes assumptions regarding the TOE's intended usage and environment of use (chapter 3.2), threats relevant to secure TOE

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

operation (chapter 3.3) and organisational security policies (chapter 3.4), which must be complied by the TOE.

- **Chapter 4:** The statement of security objectives defines the security objectives for the TOE (chapter 4.1) and for its environment (chapter 4.2).
- **Chapter 5:** The IT security requirements are subdivided into TOE security requirements (chapter 5.1) and security requirements for the environment (chapter 5.2).
- ***Chapter 6:*** *The TOE summary specification provides a description of the TOE security functions in narrative form.*
- ***Chapter 7:*** *The PP claims section states conformance to Protection Profiles.*
- **Chapter *8*:** The rationale presents evidence that the security objectives satisfy the threats and policies. This chapter also explains how the set of requirements is complete relative to the security objectives and presents a set of arguments that address dependency analysis and Strength of Function.

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

2. TOE DESCRIPTION

This chapter TOE Description contains the following sections:

Description of biometric processes (2.1)
Wording in context of Common Criteria (2.2)
TOE configuration and TOE environment (2.3)
Generic design of a biometric system (2.4)
TOE boundary (2.5)

In terms of [CC], the VoiceIdent Unit 2.0 is a product which provide*s* a verification process to verify the claimed identity of a human being using *his voice as* a unique characteristic of his body. In comparison with the product *VoiceIdent Unit 1.0 the following changes took place:*

- Extension for the VoIP telephony (ERW01 in [IAR])
- Update the “nuance” version ASR (Automatic Speech Recognition) (ERW02 in [IAR])
- Extension for the implementation for IBM and MS SQL data base (ERW03 in [IAR])

The basic processes of *the* biometric verification system[2] are described in chapter 2.1.

This *ST* describes a biometric system that works in a verification mode. Biometric Identification is not addressed within this *ST*. Furthermore the enrolment process is out of scope of this *ST* and it is assumed that all authorized users have been enrolled. Last but not least a biometric verification system that is conformant with this *ST* has to verify the identity of a user for the purpose of controlling access to a portal[3].

Beside the biometric verification process every biometric system that is conformant to this *ST* includes a mechanism to identify and authenticate an administrator of the system with other means[4] than biometrics and to enforce an access control for the objects of the TOE. This is

[2] Here and further, the word "system" is used in general sense and is not used in terms of [CC].

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

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

especially important to limit the ability to change the threshold settings for the biometric verification process to an authorized administrator.

2.1 Description of biometric processes

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

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

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

2.1.1 Enrolment

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

During the enrolment process the system captures the biometric characteristic of a user and extracts the features it is working with. This feature vector is then combined with the identity of the user to a Biometric Identification Record (BIR) and stored in a database. The BIR is also called template.

The quality of the biometric template has to be assured and quality proofed. In the case of inadequate biometric characteristics or lower template quality, the person to be enrolled, has to repeat the process or is not possible to be enrolled. Additionally it is useful to be able to update a user biometric template regarding to possible physiology changes.

Only an administrator is allowed to start the enrolment process. He has to observe the whole process to ensure a correct enrolment. Furthermore the administrator has to ensure that the user claims his correct identity to the system during the enrolment process.

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

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

2.1.2 Verification

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

Therefore the user has to claim an identity to the system. The system then gets the BIR associated with this identity from the database and captures the biometric characteristic of the user.

If the Biometric Live Record (BLR) that is extracted from the characteristic and the BIR from the database are similar enough, the claimed identity of the user is verified. Otherwise or if no BIR was found for the user, the claimed identity is refused.

The matching component of a biometric system that decides whether a BIR and BLR are similar enough usually uses a threshold value for this decision that can be configured by an administrator. If the matcher finds that the BLR and the BIR are more similar than demanded by the threshold, it returns successful verification, otherwise failed verification.

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

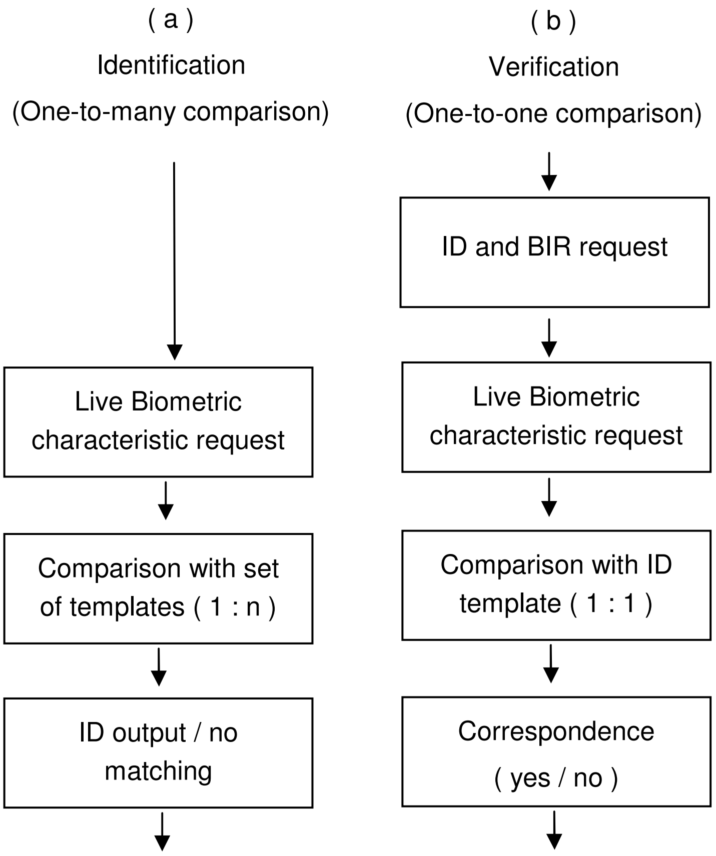
(a)
Identification
(One-to-many comparison)
Live Biometric characteristic request
Comparison with set of templates (1 : n)
ID output / no matching
(b)
Verification
(One-to-one comparison)
ID and BIR request
Live Biometric characteristic request
Comparison with ID template (1 : 1)
Correspondence (yes / no)

Figure 1: Identification / Verification flowchart

2.1.3 Identification

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

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

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

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

2.2 Wording in context of Common Criteria

In context of [CC] identification usually means the statement of a claimed identity while authentication means the confirmation of this identity. In context of biometric technology identification usually means a process as described in chapter 2.1.3. Because biometric identification is out scope of this *ST* there should not be a conflict in wording. To avoid any misunderstanding: the wording in this *ST* is as follows:

1. Identification: As defined in [CC]
2. Authentication: As defined in [CC]
3. Verification: biometric verification as described in chapter 2.1.2

2.3 TOE configuration and TOE environment

The PP [PP-BSI-BV] discusses two possible configurations of a biometric system:

- **A Stand-alone solution**

  The stand-alone solution is not integrated into another network and works with one database

- **A Network-integrated solution**

  The network-integrated solution is embedded in an existing network.

Though VoiceIdent Unit includes several computers connected by a local network, it is a Stand-alone solution in the sense of this discussion, because

- *all computers belonging to VoiceIdent Unit are located in the same secure environment and*
- *VoiceIdent Unit uses one database located in the same secure environment.*

The performance of biometric systems (especially the capture device) depends on physical environmental conditions in its environment. The environmental factors that could influence a biometric system are dependent on the used biometric characteristic and on the used capture device. *VoiceIdent Unit uses VoIP-devices or normal telephones as input devices and a system called "Voice Gateway", which transforms the digital data from the telephone line to data for the VoiceIdent Unit. Telephone and Voice Gateway together can be considered as capturing device. According to the PP the capturing device is not part of the TOE but is assumed to work within acceptable ranges. However, the VoiceIdent Unit does not rely on specific acceptable operating conditions for the telephone or VoIP-device used as voice input: Bad environmental conditions may cause voice samples to be useless, but can not help an attacker to claim a false identity. Therefore VoiceIdent needs no specific assumptions (in the sense of the CC) for the telephone and VoIP devices used for voice input.*

2.4 Generic design of a biometric system *and the VoiceIdent Unit*

This chapter provides a general description of the main and necessary components of a biometric verification system. *In addition the specific construction of the VoiceIdent system is described.*

The following figure *2* shows a simplified biometric verification system *as defined in the [PP-BSI-BV]. The next figure 3 shows the specific function of the VoiceIdent Unit. The* *components of the generic system and their realisation in the VoiceIdent Unit are described in the paragraphs following after that.*

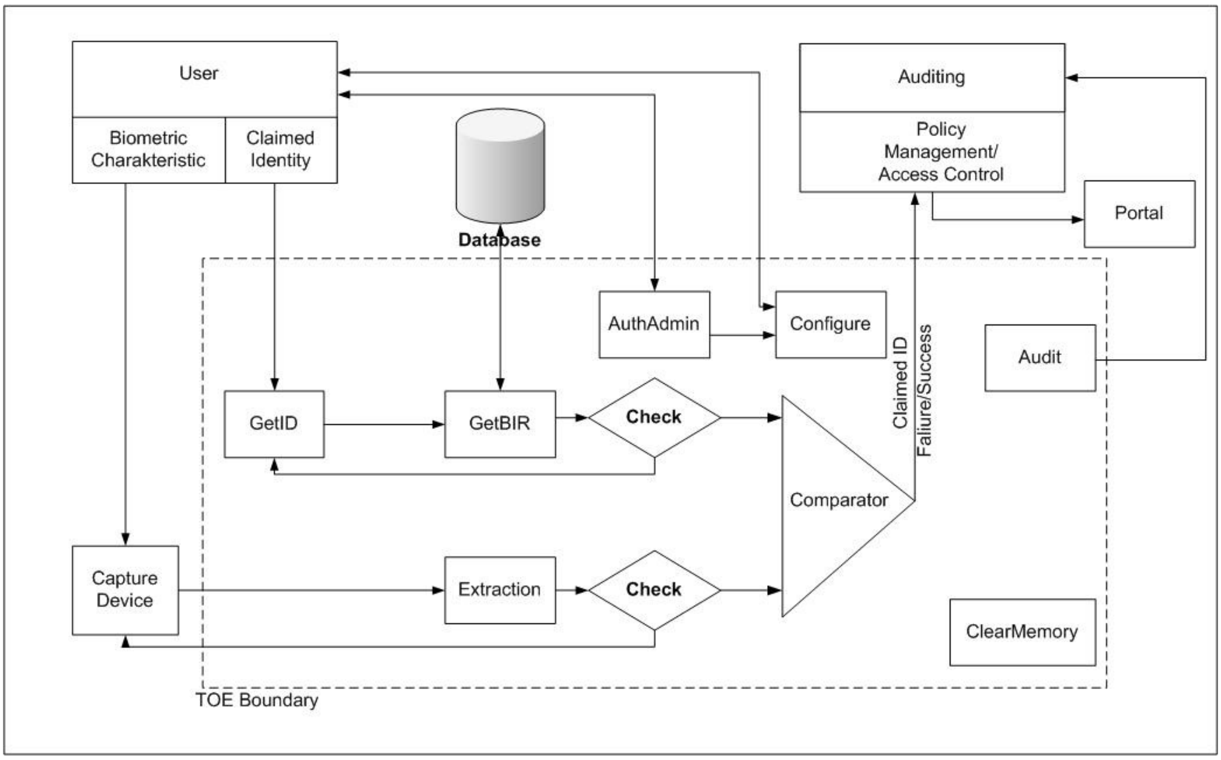

Figure 2: Simplified biometric verification system

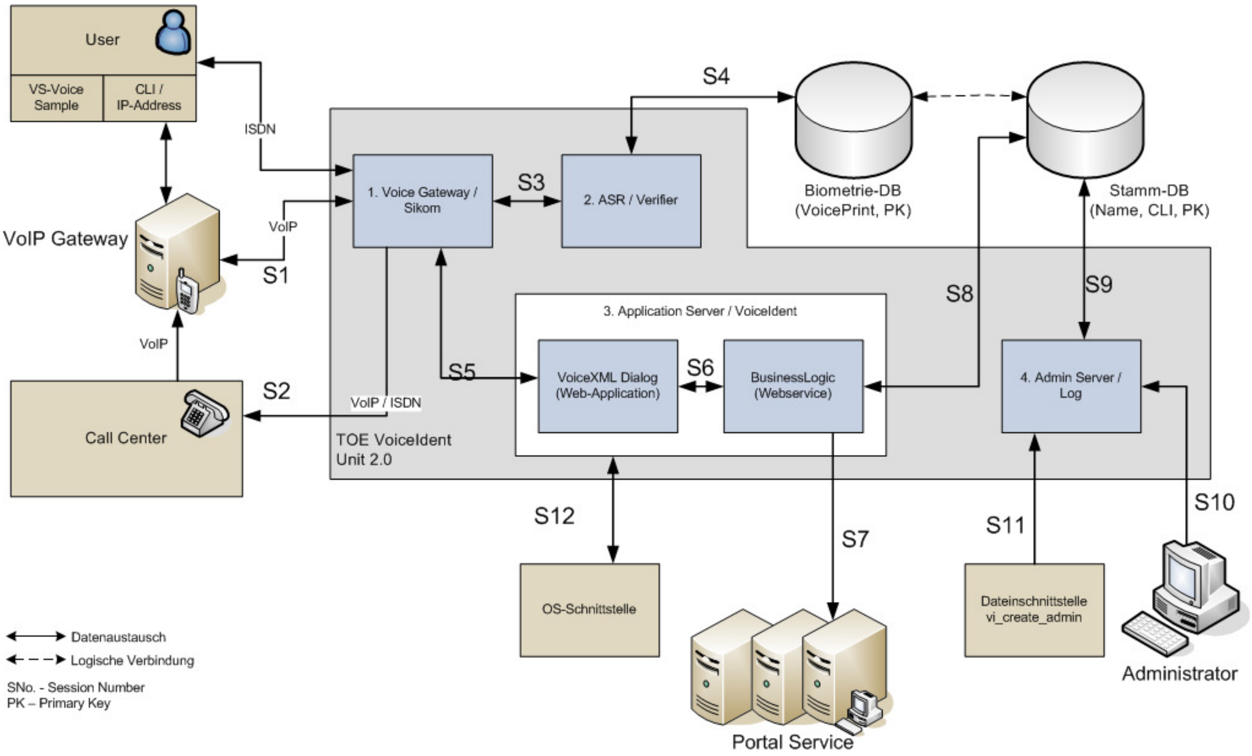

Figure 3: VoiceIdent Unit 2.0 voice verification system

- **Get ID:** This component is responsible for getting the user's claimed identity. Its functionality is security relevant because the system uses the claimed ID to determine, which BIR has to be used for comparison. Furthermore this component provides an obligatory user visible interface.

  In the VoiceIdent Unit this component is realised by a subsystem called “Voice Gateway / Sikom”, which is a component responsible for the communication with the user. At the start of the authentication each user must announce the User-ID. The voice gateway provides a serial number to identify the session.

- **Get BIR:** This component is responsible for getting the stored (already enrolled) biometric identification record (BIR) related to one claimed user's identity.

  In VoiceIdent this is realised by a subsystem called "ASR/Verifier”, which reads user identity data and the BIR from the database with help of the User-ID. The database program is outside of the TOE. It will probably be realised by two parts as indicated in the picture, however this is not relevant for the function of the TOE.

- **Extraction:** In preparation of the verification a feature vector has to be extracted from the captured data. This is the objective of this component. Optionally, the biometric data can be compressed.

  This is done by the “ASR/Verifier” too. In the VoiceIdent Unit the extraction is done in the same subsystem as the verification.

- **Check:** This component ensures the minimum quality requirements regarding the biometric templates (BIR; BLR). However, it can be differentiated between integrity and authenticity check during the process of getting the BIR as well as the quality check during the processing of the live biometric characteristics.

  Integrity and authenticity of the BIR as taken from the database is provided by the environment. Moreover the quality check for the BIR was already done during enrolment, so no explicit quality check of the BIR is necessary during operation of the TOE. The (biometric) quality check of the BLR is done in the “ASR/Verifier” subsystem.

- **AuthAdmin:** This component is responsible for identification and authentication of the administrator with other means than the biometric verification mechanism itself. This mechanism is a classical identification and authentication component that could for example be realized via a SmartCard/PIN based mechanism. It is especially necessary to authenticate an administrator before he is allowed to configure the thresholds of the system.

  This component is realised by the fourth subsystem “Admin Server” in the VoiceIdent Unit. Authentication of the TOE-Administrator is provided by username/password.

- **Configure**: This component provides an interface for the administrator to set security relevant TOE parameters. This component is especially used to configure the threshold setting for the comparator component and to determine audit events[5].

[5] The ability to review audit information is arranged via the TOE environment.

The configuration of the system is part of the "Admin Server". This also includes configuration of the data base.

- **Comparator** (also called Matcher): This is an important component regarding the scope of this *Security Target*. It compares the enrolled Biometric Identification Record (BIR) with the Biometric Live Record (BLR) and includes the determination whether these records match or not.
  Usually a comparator returns a value that shows how well the BIR and BLR match. To get a successful/failed return value from the biometric system, the comparator considers a threshold during the matching process. If the BIR and the BLR are more similar than demanded by the threshold, the return value is success, otherwise it is fails.

  "Exact match" comparison should not result in a positive verification as it may be a replay attempt and should be recorded in the audit log.

  This functionality is realised by the "ASR/Verifier" subsystem.

- **Clear memory:** In order to protect against attacks, this component clears the content of memory after using.
  The information that has to be cleared is not limited to the verification result but especially includes the BIR, BLR or any biometric raw data as well as authentication data for the administrator authentication. Because the memory that has to be cleared could belong to every other component no lines are signed in the picture before to or from this component.

  Clearing of sensitive memory areas is done by all subsystems of VoiceIdent as appropriate.

- **Audit:** This component of the TOE records security relevant events to ensure that information exists to support effective security management (e.g. verification protocol, retry counter, etc.).

  Logging data are produced by all subsystems of the VoiceIdent Unit as appropriate. The possibility to check these data (auditing) is provided by the "Admin Server" subsystem.

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

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

  The capture device is realised by a normal telephone, which transmits the Voice Data to the TOE. A prevention of the replay of voice data is included in the Voice Gateway (from Sikom Software GmbH) subsystem of the TOE.

- **Result passing on:** The verification result as Boolean value (verification successful or fail) is passed on via the policy management to the portal. Furthermore the claimed ID of the user is forwarded. The last decision, whether a user gets access to a portal is therefore done in the environment based on the biometric verification result.

  Inside of the TOE the result of the verifier is passed to the "Application Server" subsystem, which is that part of VoiceIdent responsible for general control functions. It also controls, *how many trials are allowed for a user. The result is not passed to the Portal Service (for example password reset) as a "Yes" or "No" message, but the portal is only invoked at all if the result is a "Yes". This is done for performance reasons: The portal service doesn't need to be activated at all, if a "No" is the result. Obviously the resulting behaviour of the overall system is logically equivalent to the model of the [PP-BSI-BV].*

If the result of voice comparison is negative, the Voice Gateway may either ask the user for a new try (if the allowed number of re-tries is not reached) or may transfer him to a Call Center for human assistance.

- **Policy manager**: The result of the biometric verification process is passed on to the policy manager of the environment. This component is responsible for checking the user's rights and opening the door if the user has enough privileges and was successfully verified by the TOE and is therewith realizing an access control mechanism for the portal.

  As mentioned before the VoiceIdent Unit only invokes the Portal Service after successful authentication of a user. All more specific decisions (whether a user with a specific identity has specific rights for the Portal Service) is up to the Portal Service itself. In this sense the Policy Manager is considered to be part of the Portal Service.

- **Storage:** The environment has to provide a database to the TOE. This is especially used to store the BIR of a user but it can be used to store additional information too.

  The database is provided by a database program outside of the TOE. It will probably be realised by two parts as indicated in the picture.

- **Portal**: The physical or logical point beyond which information or assets are protected by a biometric system is controlled by the TOE environment policy management, which gets the verification results (verification "failed" or "successful") related to the user identity from the TOE.

  As mentioned before the Voiceident Unit (more specifically the Application Server subsystem) informs the Portal Service only if the user authentication was successful. All further decisions are up to the Portal Service itself. The Portal Service may be a Password Reset Service, a Voice Mail System, a Ring-tone-Download service or any other service.

- **Auditing**: The environment may provide additional audit functionalities and has to provide a mechanism for audit review of the TOE audit logs.

  As mentioned before the "Admin Server" provides an interface for auditing purposes.

- **Transmission** / **Storage:** The environment cares for a secure communication and storing where security relevant data is transferred to or from the TOE.

  This assumption is also made for the VoiceIdent Unit.

2.5 TOE boundary

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

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

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

For the VoiceIdent the following more specific information can be given:

Physically the TOE consists of four software subsystems as described in the preceding subsection: Voice Gateway/Sikom, Application Server, ASR/Verifier, Admin Server. These four software subsystems may be installed on one machine or on an individual machine each.

The table of TOE deliverables can therefore be described as follows:

TOE Component	***description***	***Type***	***Transfer form***	***Requirements for Hardware Platform***
1.Voice Gateway	*Sikom VoiceMan 7.5,* *Version: 7.5.3.156* (ERW01 in [IAR])	*Software*	*Installed at the customer's site by technicians of the developer*	*Dual-Pentium Xeon 3.6GHz (4GB RAM, 2x73 GB HD with Raid1, NIC), Windows 2003 Server, ISDN Cards with CAPI for ISDN Connectivity (Eicon Diva Server 4BRI)*
2.ASR/Verifier	*Nuance ASR 9.0 / Verifier 3.5 Version 9.0 SP1* (ERW02 in [IAR])	*Software*	*Installed at the customer's site by technicians of the developer*	*Software runs on Voice Gateway server*
3.Application Server	*Jakarta Tomcat 5.5.26* *SV-VoiceDialog, Version 2.0 SV-Webservice, Version 2.0*	*Software*	*Installed at the customer's site by technicians of the developer*	*Software (runs on VoiceGateway server):* - *Jakarta Tomcat 5.5* *Random-generator: Implementation based on the Java library java.security.-SecureRandom*
4.Admin Server	*SV-AdminSrv, Version 2.0*	*Software*	*Installed at the customer's site by technicians of the developer*	*Software (runs on VoiceGateway server):* - *Jakarta Tomcat 5.5*
Administration	*Administration Guide*	*Paper and / or Online-*	*Handed personally resp.*	*--*

TOE Component	description	Type	Transfer form	Requirements for Hardware Platform
Handbook	VoiceIdent, Version 2.0.4	Dokumentation	Installed at the customer's site by technicians of the developer	

Table 1: TOE product scope

Logically the boundary of the TOE can be characterised by the following interfaces (compare figure 3 and the description in the preceding subsection):

- *The interface between the Voice Gateway and the telephone/VoIP-device, where claimed identity and the voice sample are transmitted to the TOE and where a negative result is returned in order to allow further actions (like switching the user to a Call center). For this purpose an interface exist between the Voice Gateway and the Call center.*
- *The interface to the database, where the BIR and user identification data are stored, comprises three interfaces: ASR/Verifier - Biometrie-DB, Application Server/VoiceIdent - Stamm-DB and Admin-Server/Log - Stamm-DB.*
- *The interface for the TOE-Administrator (for authentication, configuration and auditing purposes) to the Admin-Server and the file interface of the Admin-Server for the IT-Administrator (command line program).*
- *The interface to the Portal Service, which is invoked in case of positive verification.*
- *The interface between the application server and the operating system, in particular for providing random numbers and time stamps.*

The random number generator used by the application server (see Table 1) must be a cryptographically strong random number generator. It is recommended to use the random number generator, which is a part of the Java Runtime Environments.

System parts and players outside the TOE are the end user, the call center, the databases, the administrator of the supporting systems of the environment, and the portal services.

- *An end user can communicate with the TOE by telephone or VoIP-device only. The access within the TOE is technically provided by the VoiceGateway by 4 S0 Ports for the ISDN access and by support of the SIP protocol for IP-telephony. The VoiceGateway can be upgraded with additional ISDN interfaces if more than 4 ports are needed. During the enrolment process the telephone connection between the end user and the TOE is used to transfer the base data for the creation of the BIR and during the verification process it is used to transfer the BLR which is then compared to the BIR by the TOE.*
- *After an unsuccessful verification attempt the end user is connected to the call center The call center agent is informed about that fact before the connection is established.*

- *The databases are used to store the master data and the BIRs of the users and the configuration data of the TOE. An Oracle 9.2 DBMS is used together with Oracle SQL-Net for the interface. In addition the IBM DB2 and the Microsoft SQLServer are supported.* (ERW03 in [IAR]). For these databases other interfaces are used (instead of SQL-Net). For DB2 ODBC is used and for MS SQL Netlib/ODS over TDS are used.
- *The Admin Server has a webinterface which is used by the administrator of the TOE. The connection to the server is made via https. After a successful authentication, the TOE-administrator can view the logentries and configure the TOE.*
- *The portal services can be configured to get status information about end users from the TOE. (Examples for these informations are: "Is the access blocked for this user ?", "What is the maximum level of authentication for this user ?"). The retrieval of the data is done using a SOAP-based webservice. Within the TOE the details about what data is retrievable is configurable for the requesting user of the soap service based on the account name and the IP-address. (E. g. user X from IP-address Y may know which end users are blocked whereas user A from IP-address B is allowed to retrieve the authentication status of an end user). An application of this is the configuration of the rights for the call center agents resulting in an integration of the retrieved status information from the TOE into the screen masks used by the agents. Another application could be the integration of connectors to external systems to trigger actions based on a successful or unsuccessful authentication (e. g. a reset of a password after a successful authentication via telephone.)*

2.6 TOE Intended Usage

A very simple example, how the VoiceIdent Unit is used in operation is as follows:

> *Somebody wants to download a ring tone from a service provider selling ring tones. He calls the number of the service provider (*conventionally by telephone or VoIP device*). The call is answered by the voice gateway, which asks the caller to repeat some words (for example numbers or names of cities). These words are then used as a voice sample together with the User-ID, which is announced by start of the user authentication as claimed identity. The VoiceIdent Unit checks authenticity of the caller by comparing the voice sample with a sample taken fro the database. After successful authentication the caller is connected to the ring tone service, where he can download the ring tones of his choice.*

It is obvious from the example that the caller needs to be registered at the service and needs to have provided a voice sample at that time. However, this enrolment process is out of scope of this ST in accordance with the Protection Profile [PP-BSI-BV].

The following can be seen from this example:

The intended customer for the VoiceIdent Unit is not the End User, whose voice will be identified during operation of the TOE. Rather the customer will be a service provider as the following examples show:

- *The customer may be a telecommunication provider, who provides paid services like Voice mail to his customers*
- *Examples of the usage of VoiceIdent for access control are*
  - *User account management*
  - *Management of computer and data networks*
- *Within prisons the usage of telephones should be restricted in a personalized manner to the usage of a small set of dialable numbers only.*
- *Examples for the usage of VoiceIdent for Transaction authentication are*
  - *Toll fraud prevention*
  - *Telephone credit card purchases*
  - *Telephone brokerage*
  - *Voice Commerce*
- *VoiceIdent can be used to identify customers during their communication with call centers.*

The VoiceIdent Unit is installed at a computing centre of the customer, which is responsible for the secure environment required by the TOE. He then uses the VoiceIdent Unit to invoke his services for his customers.

Some remarks on user guidance and delivery:

As this discussion shows, the end user, who usually calls the system by telephone or VoIP-device, is the customer of the customer of TCOM/T-Systems. This is the reason that the user guidance in the sense of the CC will be no documentation for the end user but a documentation for the service provider and his administrators for the VoiceIdent unit.

If any security relevant hints are necessary for the end user, this will be described adequately in the user/administrator guidance for the service provider, so he can prepare information to his end customers.

Since the VoiceIdent Unit needs some specific technical support in the environment, like the specific database, the delivery method for the TOE will be personal delivery by technicians of the developer. They will help the customer not only to install the TOE but also to configure the computing and communication environment adequately.

3. TOE Security Environment

This chapter TOE Security Environment contains the following sections:

Assets and roles (3.1)

Assumptions (3.2)

Threats (3.3)

Organisational Security Policies (3.4)

Most of the text in this chapter is taken unchanged from the Protection Profile [PP-BSI-BV] because it is immediately valid for the VoiceIdent Unit. Only in some cases remarks for the specific situations were added.

3.1 Assets and roles

The following subchapters define assets and roles as follows:

3.1.1 Assets

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

Secondary assets: Assets (i.e. TSF data), which are generated by the TOE itself (e.g.: passwords to protect security relevant TOE settings and biometric templates). The following assets should be explicitly mentioned:

- **Biometric Identification Record (BIR):** This template includes the enrolled biometric data linked with the identity of a user. It is produced during the enrolment process and assumed to be given and quality checked.
- **Biometric Live Record (BLR):** This template includes the live (actual) biometric data (actual biometric characteristic and claimed user identity) to be verified against the BIR.
- **The claimed identity** of a user
- **User related security attributes** and authentication data for non biometric authentication

3.1.2 Roles

Roles are defined as follows:

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

IT administrator: The IT administrator installs the TOE and maintains the IT system (e.g. access control), but not the TOE itself[6].

[6] IT and TOE administrator could be the same person, but it is not necessary or obligatory.

The IT administrator is responsible for the maintenance of the hardware and software components (operation systems, data base, application server, Voice Gateway, ASR/Verifier and Admin-Server) and for the access control to the components. After log in on the subsystem "Admin-Server" (via operating system) with username/password the IT administrator is able to perform the necessary settings for access control of the TOE administrator. Administration of the TOE users and the biometric authentication process is not in responsibility of the IT administrator.

Developer-Administrator: *The Developer-Administrator is responsible for the TOE installation incl. one-time setting of the threshold value. The threshold parameters of the TOE can not be modified during operation. The Developer-Administrator has access to the system components of the TOE only during the installation phase. At the operational phase the activities of the Developer-Administrator are not needed.*

User: A person who wants access to the portal, which is protected by a biometric system.

Authorised user: An enrolled user with an assigned identity (BIR). He is allowed to get access to the protected portal.

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

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

3.2 Assumptions

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

A.ADMINISTRATION

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

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

A.CAPTURE[7]

The capture device as user visible interface operates inside its regular range and is suitable for the use with the TOE. Therefore, environmental influences must be assured regarding the operating environment. Furthermore it is assumed that a bypassing of the capture device in a technical manner is not possible. This assumption does not exclude the possibility to present an imitated or recorded biometric characteristic to the capture device because even in a

[7] As the discussion below this assumption shows, the VoiceIdent Unit doesn't really require security measures by the capture device. Therefore this assumption is kept only for formal compliance to the PP.

guarded environment (and the TOE is primarily unguarded) such a misuse of the system would be possible. Because the capture device is publicly available moderate physical robustness is presupposed.

For the VoiceIdent system the capture device consists of a normal telephone or VoIP-device, which can be located anywhere, which transfers the voice data to the TOE. For the microphone there are no other specific requirements for its operating range than for any telephone/VoIP-device (fixed or mobile network). If the quality of the voice sample is not adequate this can only lead to a false rejection but not to a false acceptance of a user by the TOE. Therefore no specific security requirements are necessary for the telephone/VoIP-device. Since the TOE implements measures to recognise replay of recorded voice samples, also no specific requirements for the security of the telephone line between VoIP-device or telephoneand Voice gateway are necessary.

A.ENROLMENT

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

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

For the VoiceIdent System it is assumed that integrity and authenticity of all data in the database (which include the voice samples) is provided by physical and organisational protection in the environment.

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).

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

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

  For the VoiceIdent Unit it can be assumed that the complete TOE including all underlying software and hardware is located in a secured environment, which already prevents unauthorised access.

- *Random Number Generator (RNG): The TOE environment provides the TOE with random numbers which are used for the challenge-response-mechanism of the user authentication. It is assumed that the library "Java Runtime Environments" is installed and the RNG based on the library is used.*

- Storage: The TOE environment provides a database for the already enrolled biometric templates, whereby integrity and authenticity are guaranteed. The storage is a secure IT-product (e.g. SmartCard or hard disk in a secure area) and provides an access interface for the TOE.

  In case of user supplied templates (e.g. stored on SmartCard or token), measures exist to protect the authenticity and integrity of the template.

  For the VoiceIdent system it can be assumed that the database is located in a physically secured environment together with the TOE, such that only administrators can get access to the database. All data in the database are therefore protected by these physical measures.
- Transmission: The environment takes care for a secure communication of security relevant data from and to the TOE.

  For the VoiceIdent system it can be assumed that all interfaces to the TOE except the phone line are located in the same secure environment as the TOE itself and are physically protected.
- Audit: It is assumed that the environment provides a functionality to review the audit information of the TOE and to ensures that only authorized administrators are able to do this.

  For VoiceIdent again physical protection by a secure environment can be assumed.
- Beside this it is assumed that the surrounding TOE environment is Virus, Trojan, and malicious software free.

A.PHYSICAL

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

A.FALLBACK

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

3.3 Threats

General threats that need to be considered are described as follows[8]:

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

T.BRUTEFORCE

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

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

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

T.MODIFY_ASSETS

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

Such attacks could compromise the integrity of the user security attributes (e.g. BIR) resulting in an incorrect result that might give illegal access to the portal. This threat covers a number of distinct types of attacks:

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

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

T.REPRODUCE

An attacker may try to record and replay, imitate, or generate the biometric characteristic of an authorised user. Therefore, the attacker could use technical equipment for analysing and generation of the biometric characteristics[9].

[9] **Application Note (BIO):** Fingerprint and hand geometry systems are known to be vulnerable to artefacts. The setup costs are often low making the production of artefacts worthwhile for impostors for common use biometric technologies.

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

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

T.RESIDUAL

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

- An attacker takes advantage of the verification memory content (e.g. by reading the memory content, cache or relevant temporary data).
- An attacker may take advantage of residual images at the capture device. These are likely to be limited to cases where physical contact with the biometric capture device is involved, the obvious case are fingerprints.

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

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

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

T.ROLES

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

Two types of this threat are possible within the scope of this *ST*:

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

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

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

3.4 Organisational security policies

The TOE must comply with the following organisational security policies:

OSP.FAR[10]

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

OSP.USERLIMIT[11]

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

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

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

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

4. SECURITY OBJECTIVES

This chapter Security Objectives contains the following sections:

Security objectives for the TOE (4.1)

Security objectives for the environment (4.2)

Most of the text in this chapter is taken unchanged from the Protection Profile [PP-BSI-BV] because it is immediately valid for the VoiceIdent Unit. Only in some cases remarks for the specific situations were added.

4.1 Security objectives for the TOE

O.AUDIT_REACTION

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

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

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

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

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

O.ROLES_AND_ACCESS

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

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

O.BIO_VERIFICATION

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

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

Exact match comparison: An “Exact match” comparison should not activate the portal as it may be a replay attempt and should be recorded in the audit log.

The TOE shall meet national and/or international criteria for false acceptance rate (FAR) (see Annex A - BSI biometric performance standard or [BEM]) in accordance with OSP.FAR[12].

O.AUTHADMIN

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

O.RESIDUAL

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

O.NO_REPRODUCE

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

Note: For the VoiceIdent system the following more specific security features can be described: The Voice Gateway uses a kind of challenge-response protocol: The end user is asked to repeat a word (or a series of words) provided by the system. This prevents re-use of old voice samples whether recorded acoustically, from the user’s telephone or from the telephone line.

O.RESIDUAL_CAPTURE

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

See Note above.

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

4.2 Security objectives for the environment

OE.ADMINISTRATION

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

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

OE.CAPTURE[13]

The capture device as user visible interface operates inside its regular range and is suitable for the use with the TOE. Therefore, environmental influences must be assured regarding the operating environment. Furthermore a bypassing of the capture device in a technical manner is not possible. This does not exclude the possibility to present an imitated or recorded biometric characteristic to the capture device because even in a guarded environment (and the TOE is primarily unguarded) such a misuse of the system would be possible. Because the capture device is publicly available moderate physical robustness is presupposed.

For the VoiceIdent system the capture device consists of a normal telephone or VoIP-device, which can be located anywhere and transfers the voice data to the TOE. For the microphone there are no other specific requirements for its operating range than for any telephone (fixed or mobile network). If the quality of the voice sample is not adequate this can only lead to a false rejection but not to a false acceptance of a user by the TOE. Therefore no specific security requirements are necessary for the telephone. Since the TOE implements measures to prevent replay of recorded voice samples, also no specific requirements for the security of the telephone line between telephone and Voice gateway are necessary.

OE.ENROLMENT

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

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

For the VoiceIdent System it is required that integrity and authenticity of all data in the database (which include the voice samples) is provided by physical and organisational protection in the environment.

[13] As the discussion below this objective shows, the VoiceIdent Unit doesn't really require security measures by the capture device. Therefore this objective is kept only for formal compliance to the PP.

OE.ENVIRONMENT

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

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

  The OS has to provide a reliable time stamp mechanism to be used by the TOE.

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

  For the VoiceIdent Unit it has to be assured that the complete TOE including all underlying software and hardware is located in a secured environment, which already prevents unauthorised access.
- *Random Number Generator (RNG): It has to be assured that the library "Java Runtime Environments" is installed and the RNG based on the library is used.*
- Storage: The TOE environment provides a database for the already enrolled biometric templates, whereby integrity and authenticity are guaranteed. The storage is a secure IT-product (e.g. SmartCard or hard disk in a secure area) and provides an access interface for the TOE.

  In case of user supplied templates (e.g. stored on SmartCard or token), measures exist to protect the authenticity and integrity of the template.

  For the VoiceIdent system it must be assured that the database is located in a physically secured environment together with the TOE, such that only administrators can get access to the database. All data in the database are therefore protected by these physical measures.
- Transmission: The environment takes care for a secure communication of security relevant data from and to the TOE.

  For the VoiceIdent system it has to be assured that all interfaces to the TOE except the telephone connection are located in the same secure environment as the TOE itself and are physically protected.
- Audit: The environment provides a functionality to review the audit information of the TOE and ensures that only authorized administrators are allowed to do this

  For VoiceIdent again physical protection by a secure environment has to be assured.
- The surrounding TOE environment is Virus, Trojan, and malicious software free.
- The environment cares for access control to the controlled portal(s) based on the verified id of a user.

OE.PHYSICAL

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

OE.FALLBACK

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

5. IT SECURITY REQUIREMENTS

The content of this chapter is mainly identical to the corresponding chapter of the PP [PP-BSI-BV]. The modifications for VoiceIdent (mainly closure of all open operations) are added where applicable.

5.1 TOE Security Requirements

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

5.1.1 TOE security functional requirements

The following Table 2: TOE security functional requirements summarises all TOE functional requirements to meet the security objectives:

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

No.	SFR	Dependency
	FPT	
22.	FPT_RPL.1	-

Table 2: TOE security functional requirements

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

To look up the different types of operations used in this *Security Target* see Document Introduction - C Notations.

5.1.1.1 Security audit (FAU)

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

5.1.1.1.1 Security audit automatic response (FAU_ARP)

FAU_ARP.1: Security alarms

Hierarchical to: No other components.

FAU_ARP.1.1: The TSF shall[14] ~~[one or more of the following actions:~~

a) Generate an alarm condition to the environment by e-mail to the TOE-Administrator,

b) Block any further authentication attempts if three consecutive attempts were unsuccessful until ~~an administrator defined time period has elapsed, or~~ an action is taken by the TOE-Administrator,

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

upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

[14] **Application Note (PP):** The word “take” has been deleted from FAU_ARP1.1 to achieve a better readability.
The omitted text is marked as crossed out here and in the following SFRs.

5.1.1.1.2 Security audit data generation (FAU_GEN)

FAU_GEN.1: Audit data generation

Hierarchical to: No other components.

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

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

b) All auditable events for the basic level of audit **plus events as defined in Table 3: Auditable events**~~; and~~

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

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

Table 3: 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[15] and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *additional information as defined in Table 3 and* ~~[assignment: *other audit relevant information specific to the particular biometric system*~~*none*~~]~~.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

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

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

5.1.1.1.3 Security audit analysis (FAU_SAA)

FAU_SAA.1: Potential violation analysis[16]

Hierarchical to: No other components.

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

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

a) Accumulation or combination of

- A TOE-Administrator specified a number of authentication failures against a single non-administrative user identifier,

- A TOE-Administrator specified a number of consecutive failed authentication attempts,

- An Administrator[17] *specified a number of authentication failures against a TOE administrative user identifier*

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

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

[17] The *number of authentication failures against a TOE administrative user identifier is specified (3) and is not changeable in the operational phase. (The Developer-Administrator is able to change this number only during the installation phase.)*

known to indicate a potential security violation.

b) ~~[assignment: *any other rules*~~*none*~~]~~.

Dependencies: FAU_GEN.1 Audit data generation

5.1.1.2 User data protection (FDP)

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

Security Function Policy for Access Control (AC_SFP)

Access controls ensure that information is read from, created in, or modified into the TOE only by those authorised to do so.

Subjects (Users) in accordance with the roles defined in 3.1.2:

- *User*
- *TOE administrator*
- *IT administrator*
- *Developer-Administrator*

Security attributes for subjects:

- *Role Attribute (User, TOE Administrator, IT Administrator, Developer-Administrator)*
- *Successful authentication (PIN verification or voice (biometric) verification)*
- *Number of consecutive unsuccessful attempts*

Objects in accordance with the assets defined in 3.1.1:

- *User data (behind a portal, not in TOE, but the TOE controls access to the portal)*
- *Biometric Identification Record (BIR)*
- *Biometric Live Record (BLR)*
- *User verification result*
- *Threshold parameter for the matching rate*
- *User identity data (CLI, name, ...)*

- *Administrator authentication data (Username/Password)*

Operations (Access Rules):

- *A User has access to the User data of portal only after successful voice verification and forwarding the claimed ID by the TOE.*
- *After the successful Username/Password authentication on the Admin-Server, the TOE administrator can*
  - administrate the users (store, change and delete of the User identity data and the BIR),
  - perform the TOE relevant settings and check the audit records,
  - reset the counter of consecutive unsuccessful attempts for the User,
  - change his own Username/Password.
- *After the successful Username/Password authentication on the operating system, the IT administrator can perform the necessary IT relevant settings.*
- *After the successful Username/Password authentication on the operating system the IT administrator has access to the subsystem "Admin-Server" via a command line program and can*

- administrate the TOE administrators incl. reset the counter of consecutive unsuccessful attempts for the TOE administrator,
- change his own Username/Password.

- *After the successful Username/Password authentication on the operating system the Developer-Administrator can perform the installation of the TOE with IT administrator supports and set (once) the threshold value for acceptance or rejection of user authentication attempts.*

The TOE does not authenticate the Developer- and IT-Administrator. But for the sake of completeness and by reason that the TOE uses the files with settings and parameters for the TOE, the operations of Developer- and IT-Administrator are listed here. This files can be inserted only if Developer-Administrator has been authenticate via operating system.

5.1.1.2.1 Access Control Policy (FDP_ACC)

FDP_ACC.1: Subset Access Control

Hierarchical to: No other components.

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

Dependencies: FDP_ACF.1 Security attribute based access control

5.1.1.2.2 Access Control Functions (FDP_ACF)

FDP_ACF.1: Security attribute based access control

Hierarchical to: No other components.

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

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

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ~~[assignment:~~ ~~*rules, based on security attributes that explicitly authorise access of subjects to objects*~~*none*~~]~~.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the ~~[assignment~~~~*: rules, based on security attributes that explicitly deny access of subjects to objects*~~*none*~~]~~.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

5.1.1.2.3 Residual information protection (FDP_RIP)

FDP_RIP.2: Full residual information protection

Hierarchical to: FDP_RIP.1

FDP_RIP.2.1: The TSF shall ensure that any previous information content of a resource is made unavailable upon the ~~[selection:~~ allocation of the resource to~~deallocation of the resource from]~~ all objects.

Dependencies: No dependencies.

5.1.1.3 Identification and authentication (FIA)

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

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

5.1.1.3.1 Authentication failures (FIA_AFL)

FIA_AFL.1: Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1: The TSF shall detect when ~~an administrator configurable positive integer within [assignment: *range of acceptable values*]~~"[18] *exactly three* unsuccessful authentication attempts occur related to ~~[~~*consecutive failed authentication attempts*~~assignment: *list of authentication attempts*~~].

FIA_AFL.1.2: When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *block any further authentication attempts related to that user until the TOE-Administrator unblocks the authentication* ~~*defined time period has elapsed, as specified by the TOE administrator*~~ *and* ~~[assignment: *additional measures*~~*none*].

Dependencies: FIA_UAU.1 Timing of authentication

5.1.1.3.2 User attribute definition (FIA_ATD)

FIA_ATD.1: User attribute definition

Hierarchical to: No other components.

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

a) Identifying name or number

b) Unique physical or behavioural characteristic

c) Role

d) ~~[assignment: *other attributes specific to the particular biometric system*~~*none*].

Dependencies: No dependencies.

5.1.1.3.3 User authentication (FIA_UAU)

FIA_UAU.2: User authentication before any action

Hierarchical to: FIA_UAU.1

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

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

Dependencies: FIA_UID.1 Timing of identification

[18] The wording of the PP was modified because the administrator can not change the number of consecutive failed authentication attempts, it is always three.

FIA_UAU.3: Unforgeable authentication[19]

Hierarchical to: No other components.

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

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

Dependencies: No dependencies.

FIA_UAU.5: Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide *a biometric verification mechanism to authenticate users and a non biometric verification mechanism to authenticate TOE-Administrators* to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the *voice verification for users and Username/Password verification for TOE-Administrators*

~~[assignment: *rules describing how the multiple authentication mechanisms provide authentication*~~].

Dependencies: No dependencies

FIA_UAU.7: Protected authentication feedback

Hierarchical to: No other components.

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

Dependencies: FIA_UAU.1 Timing of authentication

5.1.1.3.4 User identification (FIA_UID)

FIA_UID.2: User identification before any action

Hierarchical to: FIA_UID.1

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

Dependencies: No dependencies.

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

5.1.1.4 Security management (FMT)

The current definition of the FMT class of requirements can be interpreted to accommodate the definitions of security management requirements as they relate to biometrics. This requirement defines the management of security attributes, and TSF data and functions. With respect to biometric systems, the management of security functions and attributes are especially relevant to the administration of security policies and the establishment of threshold levels. These levels determine the closeness or score required between a sample and reference template in order to declare them a match. For verification, the setting of threshold levels determines the rates of false matches and false non-matches, and acceptance or rejection by the system.

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

5.1.1.4.1 Management of functions in TSF (FMT_MOF)

FMT_MOF.1#1: Management of security functions behaviour

Hierarchical to: No other components.

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

- *Audit mechanisms,*

- *Thresholds*[20]

- ~~[assignment: *other functions*~~*none*~~]~~

to *TOE administrators*.

FMT_MOF.1#2: Management of security functions behaviour

Hierarchical to: No other components.

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

- *Perform maintenance,*

- *Perform manual access (e.g. fallback-system),*

- *Emergency start-up/shutdown*

- ~~[assignment: *List of actions that need to be taken in case of repetitive penetration attempts*~~*none*~~]~~

to *IT administrators*.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

[20] The threshold parameters of the TOE can not be modified during operation. The one-time setting of the threshold value occurs by Developer-Administrator.

5.1.1.4.2 Management of Security Attributes (FMT_MSA)

FMT_MSA.1: Management of security attributes

Hierarchical to: No other components

FMT_MSA.1.1 The TSF shall enforce the ~~[~~*AC_SFP*~~assignment: *access control SFP,*]~~ to restrict the ability to change default, query, modify, delete, ~~[assignment: *other operations*~~*none*] the security attributes *user attributes as defined in FIA_ATD.1, threshold settings,* [~~assignment: *other security attributes*~~*none*] to *administrators*.

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

FMT_SMR.1 Security roles

FMT_SMF.1

FMT_MSA.3: Static attribute initialisation

Hierarchical to: No other components.

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

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

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

5.1.1.4.3 Management of TSF data (FMT_MTD)

FMT_MTD.1: Management of TSF data

Hierarchical to: No other components.

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

- ~~*[assignment: list of security parameters which control the performance of the biometric system]*~~ *threshold value for acceptance or rejection of user authentication attempts* [21]

- ~~*[assignment:*~~ *user security attributes according to AC_SFP*~~*]*~~

- *audit trail*

~~-*[assignment: other attributes]*~~*none*

to *TOE administrators*.

Dependencies: FMT_SMF.1 Specification of management functions

[21] The threshold parameters of the TOE can not be modified during operation. The one-time setting of the threshold value occurs by Developer-Administrator.

FMT_SMR.1 Security roles

FMT_MTD.3: **Secure TSF data**

Hierarchical to: No other components.

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

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

5.1.1.4.4 Specification of Management Functions (FMT_SMF)

FMT_SMF.1: **Specification of Management Functions**

Hierarchical to: No other components.

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

a) *Control the operation of security-related aspects of the TOE (threshold control)*[22]

b) *Control audit attributes*

c) *Control authentication attributes*.

Dependencies: No dependencies.

5.1.1.4.5 Security management roles (FMT_SMR)

FMT_SMR.1: **Security roles**

Hierarchical to: No other components.

FMT_SMR.1.1: The TSF shall maintain the roles *authorised users, TOE administrators, IT administrators, and Developer-Administrator*.[23]

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

Dependencies: FIA_UID.1 Timing of identification

5.1.1.5 Protection of the TSF (FPT)

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

The biometric system that verifies a user for a resource does not automatically convey rights or privileges for that resource. For a system to support this capability, the template must be bound to a resource in such a way that a successful match will convey privileges over that

[22] The threshold parameters of the TOE can not be modified during operation. The one-time setting of the threshold value occurs by Developer-Administrator.

[23] IT- and Developer-Administrator have access to the TOE system files only via operating system.

resource. It is this concept that makes the FPT class of functional requirement applicable to biometric systems. Biometric data in the TOE should be regarded as TSF Data.

5.1.1.5.1 Replay detection (FPT_RPL)

FPT_RPL.1: Replay detection

Hierarchical to: No other components.

FPT_RPL.1.1: The TSF shall detect replay for the following entities: *biometric authentication data*.

FPT_RPL.1.2: The TSF shall[24] *ignore the replayed data* when replay is detected.

Dependencies: No dependencies.

5.1.2 Minimum strength of function claim

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

For the biometric verification mechanism the SOF level is measured in terms of FAR (according to [BEM]). For SOF medium a FAR of less than *1 in 10000* is required.

[24] The word “perform” has been deleted from FPT_RPL1.2 to achieve a better readability.

5.1.3 TOE security assurance requirements

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

Assurance class	ID	Assurance component	Refinement
Configuration management	ACM_CAP.2	Configuration items	no
Delivery & operation	ADO_DEL.1	Delivery procedures	no
	ADO_IGS.1	Installation, generation & start-up procedures	no
Development	ADV_FSP.1	Informal functional specification	no
	ADV_HLD.1	Descriptive high-level design	yes
	ADV_RCR.1	Informal correspondence demonstration	no
	ADV_SPM.1[25]	Informal TOE security policy model	no
Guidance documents	AGD_ADM.1	Administrator guidance	yes
	AGD_USR.1	User guidance	yes
Tests	ATE_COV.1	Evidence of coverage	no
	ATE_FUN.1	Functional testing	yes
	ATE_IND.2	Independent testing – sample	yes
Vulnerability assessment	AVA_SOF.1	Strength of TOE-security function evaluation	yes
	AVA_VLA.1	Developer vulnerability analysis	yes

Table 4: Assurance requirements (EAL2, augmented with ADV_SPM.1)

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

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

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

[25] ADV_SPM.1 is augmented and described in chapter 5.1.3.3.4. Thereby the need of an informal TOE security policy model results from a security management dependency (see chapter 5.1.1.4.3).

5.1.3.1 Configuration management (ACM)

5.1.3.1.1 ACM_CAP.2 - Configuration items

Dependencies: No dependencies.

Developer action elements:

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

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

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

Content and presentation of evidence elements:

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

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

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

ACM_CAP.2.4C: The configuration list shall uniquely identify all configuration items that comprise the TOE[26].

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

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

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

Evaluator action elements:

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

5.1.3.2 Delivery and operation (ADO)

5.1.3.2.1 ADO_DEL.1 - Delivery procedures

Dependencies: No dependencies.

Developer action elements:

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

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

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

Within VoiceIdent the integrity of the installed software configuration can be tested by the software itself. This is done at startup-time by querying the version numbers of the used components from these components and compare these values with the intended configuration.

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

Dependencies: AGD_ADM.1 Administrator guidance

Developer action elements:

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

Content and presentation of evidence elements:

ADO_IGS.1.1C: The installation, generation and start-up documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE[27].

Evaluator action elements:

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

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

5.1.3.3 Development (ADV)

5.1.3.3.1 ADV_FSP.1 - Informal functional specification

Dependencies: ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

Evaluator action elements:

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

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

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

5.1.3.3.2 ADV_HLD.1 - Descriptive high-level design

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

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

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

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

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

Evaluator action elements:

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

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

Refinements regarding ADV_HLD.1:

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

5.1.3.3.3 ADV_RCR.1 - Informal correspondence demonstration

Dependencies: No dependencies.

Developer action elements:

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

5.1.3.3.4 ADV_SPM.1 - Informal TOE security policy model[28]

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

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

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

Content and presentation of evidence elements:

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

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

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

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

Evaluator action elements:

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

[28] The need of an informal TOE security policy model results from a security management dependency (see chapter 5.1.1.4.3). Thereby the informal TSP model mainly has to describe the secure values for the TSF data.

5.1.3.4 Guidance documents (AGD)

5.1.3.4.1 AGD_ADM.1 - Administrator guidance

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

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

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

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

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

Evaluator action elements:

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

Refinements regarding AGD_ADM.1:

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

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

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

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

a) Biometric Privacy

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

b) Environmental influences

Biometric system operation is greatly affected by physical environmental influences (e.g. light and sound levels, dust, humidity, and cleanliness of the biometric capture device) and these can affect accuracy of the enrolment and verification processes. Hence, guidance documentation should include information on environmental influences and ways of minimising these influences.

c) Setting of thresholds

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

5.1.3.4.2 AGD_USR.1 - User guidance

Dependencies: ADV_FSP.1 Informal functional specification

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

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

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

Evaluator action elements:

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

Refinements regarding AGD_USR.1:

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

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

5.1.3.5 Tests (ATE)

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

Determining the effectiveness of the underlying security mechanisms in biometric systems is dependent on performance testing. The behaviour of a biometric system depends on components that include the capture device, the biometric algorithms, the environmental conditions, and also the user and impostor distribution. The statistics of these are not amenable to theoretical analysis within the current state of knowledge, and hence performance testing is necessary to determine the effectiveness of these biometric security mechanisms[29].

5.1.3.5.1 ATE_COV.1 - Evidence of coverage

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

Developer action elements:

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

5.1.3.5.2 ATE_FUN.1 - Functional testing

Dependencies: No dependencies.

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

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

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

Developer action elements:

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

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

Content and presentation of evidence elements:

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

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

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

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

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

Evaluator action elements:

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

Refinements regarding ATE_FUN.1:

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

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

5.1.3.5.3 ATE_IND.2 - Independent testing - sample

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

Developer action elements:

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

Content and presentation of evidence elements:

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

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

Evaluator action elements:

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

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

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

Refinements regarding ATE_IND.2:

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

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

5.1.3.6 Vulnerability assessment (AVA)

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

5.1.3.6.1 AVA_SOF.1 - Strength of TOE security function evaluation

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

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

Developer action elements:

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

Content and presentation of evidence elements:

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

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

Evaluator action elements:

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

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

Refinements regarding AVA_SOF.1:

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

5.1.3.6.2 AVA_VLA.1 - Developer vulnerability analysis

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

Dependencies: ADV_FSP.1 Informal functional specification

ADV_HLD.1 Descriptive high-level design

AGD_AGD.1 Administrator guidance

AGD_USR.1 User guidance

Developer action elements[30]:

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

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

Content and presentation of evidence elements[31]:

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

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

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

Evaluator action elements:

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

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

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

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

Refinements regarding AVA_VLA.1:

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

5.2 TOE environment security requirements

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

R.ADMINISTRATION[32]

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

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

R.CAPTURE[33]

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

For the VoiceIdent system the capture device consists of a normal telephone or a VoIP-device, which can be located anywhere and transfers the voice data to the TOE. For the microphone there are no other specific requirements for its operating range than for any telephone or VoIP-device (fixed or mobile network). If the quality of the voice sample is not adequate this can only lead to a false rejection but not to a false acceptance of a user by the TOE. Therefore no specific security requirements are necessary for the telephone or VoIP-device. Since the TOE implements measures to prevent replay of recorded voice samples, also no specific requirements for the security of the line of communication between telephone / VoIP-device and Voice gateway are necessary.

[32] The requirements R.NO_REPRODUCE and R.RESIDUAL_CAPTURE which are defined in the PP are not necessary here because they are fulfilled by the TOE.

[33] As the discussion below this requirement shows, the VoiceIdent Unit doesn't really require security measures by the capture device. Therefore this requirement is kept only for formal compliance to the PP.

R.ENROLMENT

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

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

R.ENVIRONMENT

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

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

  The OS has to provide a reliable time stamp mechanism to be used by the TOE.

  Additional it has to be ensured that the operating system is able to protect itself and its own functionality (e.g.: policy management, access control, non-authenticated start-up).
- *Random Number Generator (RNG): The TOE environment has to provide the TOE with random numbers which are used for the challenge-response-mechanism of the user authentication. The RNG based on the library "Java Runtime Environments" is used.*
- Storage: The TOE environment hast to provide a database for the already enrolled biometric templates, whereby integrity and authenticity are guaranteed. The storage is a secure IT-product (e.g. SmartCard or hard disk in a secure area) and provides an access interface for the TOE.

  In case of user supplied templates (e.g. stored on SmartCard or token), measures have to exist to protect the authenticity and integrity of the template.
- Transmission: The environment hast to take care for a secure communication of security relevant data from and to the TOE.
- Audit: The environment provides a functionality to review the audit information of the TOE and ensures that only authorized administrators are allowed to do this
- The surrounding TOE environment is Virus, Trojan, and malicious software free.
- The environment cares for access control to the controlled portal(s) based on the verified id of a user.

R.PHYSICAL

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

R.FALLBACK

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

6. TOE SUMMARY SPECIFICATION

6.1 TOE Security Functions

This section defines the security functions of the TOE in a narrative way.

F.AUDIT_REACTION

The TOE supports security management by recording security relevant events in a way that all TOE users can subsequently be hold accountable for their security relevant actions.

The TOE will perform logging about all security critical processes according to the requirements FAU.GEN.1 and FAU.GEN.2 and inform about insecure states. This includes countered, unsuccessful attacks to the TOE.

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

The TOE shall react to,

a) Administrator's authentication: The TOE will audit the number of unsuccessful authentication attempts to one TOE administrator account and will lock the authentication mechanism if a configurable number of unsuccessful authentication attempts, namely three, has been reached.

b) Replay or brute force attacks against the same identity. This means that the TOE realizes a mechanism thru which access is blocked after three failed verification attempts with the same claimed identity.

c) The detection of attacks based on the use of residual information (as specified T.RESIDUAL).

d) Less quality: This means that the verification process will be stopped if the BLR does not have sufficient quality.

e) An unusual high amount of unsuccessful verification attempts against different identities could be caused by a brute force attack. Due to the fact that CLI spoofing can be done only using special hardware, such an attack has the form of a long sequence of tries with an invalid or unregistered CLI. Every attempt is detected by the system.

f) Modified installation: All installed files, the modules "ASR/Verifier and "Business Logic (Webservice)" consist of, are signed. On startup of theses modules the validness of the (public) certificate for the signatures and all the signatures are verified.

In the cases a), e) and f) the function initiate a mail sending to the addresses inserted from TOE-Administrator to inform the responsible persons, normally to all TOE-Administrators.

F.ROLES_AND_ACCESS

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

The TOE does not authenticate the Developer- and IT-Administrator. But for the sake of completeness and by reason that the TOE uses the files with settings and parameters for the TOE, the operations of Developer- and IT-Administrator are assign to this function. This files can be inserted only if Developer -Administrator has been authenticate via operating system.

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

In accordance with the AC_SFP the function is capable to perform the following security management functions:

- *Control the operation of security-related aspects of the TOE (threshold control)*[34]
- *Control audit attributes*
- *Control authentication attributes*.

F.BIO_VERIFICATION

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

- *The TOE will process only its own templates (respectively standardised) from the enrolment process as stored in the data base (consideration of integrity and authenticity). The selection occurs by means of the User-ID, which is announced by start of the user authentication.*
- *The BIR as well as the BLR shall satisfy minimum quality standards and will be compatible among each other.*
- *The TOE will count the number of unsuccessful authentication attempts.*
- *The TOE will provide only a message indicating that verification efforts are underway to the user while the biometric authentication is in progress.*

Exact match comparison: The comparison of the verification sample is not done directly to the sample of the enrolment. Instead, the result of the computation of the voice characteristics of the verification speaker is compared to the stored voice characteristics of the enrolment. The level of equality must exceed the decision threshold to accept a speaker, otherwise the speaker is rejected. To prevent attacks based on the replay of a verification voice sample or similar mechanisms, an additional "exact match threshold" is used, that is higher than usually reached equality values. Whenever the level of equality exceeds this value, it is assumed that an exact match attack is detected and the speaker is rejected.

[34] The threshold parameters of the TOE can not be modified during operation. The one-time setting of the threshold value occurs by Developer-Administrator.

The TOE meets the SOF-medium criteria for false acceptance rate (FAR) (see Annex A - BSI biometric performance standard) - maximum FAR of 0.0001.

F.AUTHADMIN

The TOE will provide a mechanism to authenticate a TOE administrator with other means than the biometric verification process. This authentication process will be realized thru a username/password mechanism. The TOE will count the number of unsuccessful authentication attempts.

F.RESIDUAL

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

F.NO_REPRODUCE_OR_RESIDUAL_CAPTURE

The TOE will implement measures to prevent that voice samples of a legitimate user, which were recorded by an attacker, can be used to get unauthorised access. The Voice Gateway uses a kind of challenge-response protocol: The end user is asked to repeat at least two series of numbers provided by the system with help of the external random number generator. This prevents re-use of old voice samples whether recorded acoustically, from the user's telephone or from the telephone line. The repetitions interpreted as responses are analysed to decide whether each response matches the challenge or not.

6.2 SOF Claim for TSF

According to Common Criteria Part 2 and Part 3, all TOE security functions which are relevant for the assurance requirement AVA_SOF.1 are identified in this section.

1. *The TSF F.BIO_VERIFICATION must reach SOF-medium. For the biometric verification mechanism the SOF level is measured in terms of FAR (according to [BEM]). For SOF medium a FAR of less than 1 in 10000 is required.*
2. *The TSF F.AUTHADMIN includes a probabilistic password mechanism for the authentication of the TOE-Administrator. The SOF F.AUTHADMIN must reach SOF-medium.*
3. *The TSF F.NO_REPRODUCE_OR_RESIDUAL_CAPTURE contains a Challenge-Response-Mechanism, which is of a probabilistic nature and must reach SOF-medium.*

6.3 Assurance Measures

To satisfy the security assurance requirements defined in chapter 5.1.3 suitable assurance measures are employed by the developer of the TOE. For the evaluation of the TOE, the developer provides suitable documents. The documents describe the measures and include *further information supporting the verification of the conformance of these measures against the claimed assurance requirements.*

The following table includes a mapping between the assurance requirements according to EAL 2 augmented with ADV_SPM.1 and the documents including the relevant information for the correspondent requirement. The developer of the TOE provide these documents.

Overview of Developer´s TOE related Documents		
Assurance Class	***Family***	***Document containing the relevant information***
ACM Configuration Management	*ACM_CAP.2*	*Document Configuration Management* *Document Life-Cycle Model*
ADO Delivery and Operation	*ADO_DEL.1*	*Document Life-Cycle Model*
	ADO_IGS.1	*Document Installation, Generation and Start-Up Procedures*
ADV Development	*ADV_FSP.1*	*Document Functional Specification*
	ADV_HLD.1	*Document High-Level Design* *Development documents like design specifications*
	ADV_RCR.1	*Document Functional Specification* *Document High-Level Design*
	ADV_SPM.1	*Document Security Policy Model*
AGD Guidance Documents	*AGD_ADM.1*	*Document Administrator guidance*
	AGD_USR.1	*Document User guidance*
ATE Tests	*ATE_COV.1*	*Document Test Documentation* *Detailed test documentation like test specifications*
	ATE_FUN.1	*Document Test Documentation* *Detailed test documentation like test specifications*
	ATE_IND.2	*Independent testing – sample*
AVA Vulnerability Assessment	*AVA_SOF.1*	*Document Security Function Evaluation*
	AVA_VLA.1	*Document Vulnerability Analysis*

Table 5: Overview of Developer´s TOE related Documents
(EAL2, augmented with ADV_SPM.1)

7. PP CLAIMS

This ST conforms to the “Protection Profile for Biometric Verification Mechanisms” (BSI-PP-0016) published and registered by the German Federal Office for Information Security (BSI).

8. RATIONALE

This chapter Rationale contains the following sections:

Security objectives rationale (8.1)

Coverage of the security objectives (8.1.1)

Coverage of the assumptions (8.1.2)

Countering the threats (8.1.3)

Coverage of the organisational security policies (8.1.4)

Security requirements rationale (8.2)

TOE security functional requirements (6.2.1)

Environment security requirements (6.2.2)

Assurance requirements rationale (6.2.3)

8.1 Security objectives rationale

8.1.1 Coverage of the security objectives

Table 4 below gives an overview, how the assumptions, threats, and organisational security policies are addressed by the security objectives. The text following after the table 4 together with the descriptions of the subchapter's 8.1.2, 8.1.3, and 8.1.4 justifies this more detailed.

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

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

Table 6: Assumptions/threats/OSP - security objectives mapping

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

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

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

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

The TOE security objective **O.ROLES_AND_ACCESS** (the TOE shall limit access to administrative functions) can be traced back to the threat T.ROLES as directly follows and to T.MODIFY_ASSETS as this objective realizes access control.

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

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

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

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

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

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

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

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

8.1.2 Coverage of the assumptions

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

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

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

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

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

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

For all assumptions, the corresponding objectives are stated in a way, which directly correspond to the description of the assumption (see chapter 3.2). It is clear from the description of each objective (see chapter 4.3), that the corresponding assumption is covered, if the objective is valid. Nevertheless some objectives exceed the statements of the assumptions they cover.

Each assumption is covered by one environmental security objective.

8.1.3 Countering the threats

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

Within the VoiceIdent system the first variant is countered by the restriction of the possible successive false attempts for one id to a small number and blocking the id afterwards. The second variant is countered by a monitoring strategy: all acceptance events and rejection events are logged within the database. Based on this data the current average rate of rejection events is computed for constant, successive time-intervals. Whenever the average rate of rejection events exceeds an adminstrator-defined threshold, an appropriate action can be triggered (shutdown, administrator alarm, etc.)

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

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

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

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

8.1.4 Coverage of organisational security policies

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

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

Each OSP is covered by at least one security objective.

8.2 Security requirements rationale

8.2.1 TOE security functional requirements rationale

The following subchapters consider the TOE security requirements.

8.2.1.1 Fulfilment of TOE security objectives

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

	O.AUDIT_REACTION	O.ROLES_AND_ACCESS	O.BIO_VERIFICATION	O.AUTHADMIN	O.RESIDUAL	O.NO_REPRODUCE	O.RESIDUAL_CAPTURE
FAU_ARP.1	X						
FAU_GEN.1	X						
FAU_GEN.2	X						
FAU_SAA.1	X						
FDP_ACC.1		X					
FDP_ACF.1		X					
FDP_RIP.2					X		X
FIA_AFL.1			X	X			
FIA_ATD.1		X	X	X			
FIA_UAU.2			X	X			
FIA_UAU.3			X	X		X	
FIA_UAU.5			X	X			
FIA_UAU.7			X				
FIA_UID.2			X	X			
FMT_MOF.1#1		X					
FMT_MOF.1#2		X					
FMT_MSA.1		X					
FMT_MSA.3		X					
FMT_MTD.1		X					
FMT_MTD.3			X				
FMT_SMF.1		X					
FMT_SMR.1		X					
FPT_RPL.1			X			X	X

Table 7: SFR (TOE) - security objectives (TOE) mapping

O.AUDIT_REACTION **FAU_ARP.1** ensures that the TOE reacts in case of a potential security violation white **FAU_SAA.1** ensures that the potential security violation is detected. These both requirements fulfil the reaction part of this objective.

FAU_GEN.1 makes arrangements to generate records of security relevant events (see table in chapter 5.1.1.1.2) and **FAU_GEN.2** supports the user identity association in order to be able to hold users accountable for their actions. These two requirements fulfil the audit part of this objective.

O.ROLES_AND_ACCESS **FDP_ACC.1** realizes a general access control mechanism between subjects and objects of the TOE and **FDP_ACF.1** describes the attributes on which the access control is based on. **FIA_ATD.1** defines that the role of a user is a user attribute.

FMT_MOF.1#1 limits the ability to modify the behaviour of audit functions and system thresholds to an administrator.

FMT_MOF.1#2 limits the ability to disable/enable the functions Perform maintenance, Perform manual access and Emergency start-up/shutdown to IT-administrators

FMT_MSA.1 restricts the management of security attributes to an administrator while **FMT_MSA.3** enforces secure default values for security attributes and limits the ability to change these default values to administrators. **FMT_MTD.1** restricts the ability to control the performance of the system to administrators. **FMT_SMF.1** defines that the TOE has to provide some specific management functions to control the security relevant attributes and **FMT_SMR.1** ensures that the TOE maintains roles and that each user can be associated with a role.

O.BIO_VERIFICATION **FIA_AFL.1** ensures that reaching a threshold of unsuccessful authentication attempts is realized to be a security relevant state. **FIA_ATD.1** defines the user attributes that are also used for the biometric verification. **FIA_UAU.2** states that each user has to be successfully authenticated before performing any action and defines the maximum values for FAR and FRR. **FIA_UAU.3** ensures that no forged authentication data can be used for authentication. **FIA_UAU.5** defines that the TOE has another authentication mechanism beside the biometric verification process. **FIA_UAU.7** ensures that no authentication feedback is given to a potential attacker. **FIA_UID.2** states that the each user has to be identified before performing any action. **FPT_RPL.1** ensures that the TOE ignores replayed authentication data.

FMT_MTD.3 assures that only secure values are accepted for BIR and BLR during the biometric verification process.

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

FIA_UID.2 states that the each user has to be identified before performing any action.

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

O.NO_REPRODUCE This objective is completely covered by **FPT_RPL.1** and **FIA_UAU.3**. **FPT_RPL.1** ensures that the TOE ignores replayed authentication data. **FIA_UAU.3** ensures that no forged or copied authentication data can be used for authentication.

O.RESIDUAL_CAPTURE This objective is completely covered by **FPT_RPL.1** and **FDP_RIP.2**. **FPT_RPL.1** ensures that the TOE ignores replayed authentication data. **FDP_RIP.2** prevents reuse of residual data of the TOE itself.

8.2.1.2 Fulfilment of TOE SFR dependencies

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

The following Table 8 identifies the security functional requirements and their associated dependencies. It also indicates whether the *ST* explicitly addresses each dependency. For those cases where dependencies have not specifically been addressed, explanations of the rationale for excluding them are provided.

No.	SFR	Dependency	Dependency satisfied?
	FAU		
1.	FAU_ARP.1	FAU_SAA.1	yes
2.	FAU_GEN.1	FPT_STM.1	no[35]
3.	FAU_GEN.2	FAU_GEN.1, FIA_UID.1	yes
4.	FAU_SAA.1	FAU_GEN.1	yes
	FDP		
5.	FDP_ACC.1	FDP_ACF.1	yes
6.	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	yes
7.	FDP_RIP.2	-	-
	FIA		
8.	FIA_AFL.1	FIA_UAU.1	yes
9.	FIA_ATD.1	-	-
10.	FIA_UAU.2	FIA_UID.1	yes
11.	FIA_UAU.3	-	-
12.	FIA_UAU.5	-	-
13.	FIA_UAU.7	FIA_UAU.1	yes
14.	FIA_UID.2	-	-
	FMT		
15.	FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	yes
16.	FMT_MSA.1	[FDP_ACC.1 or FDP_ICF.1], FMT_SMR.1, FMT_SMF.1	yes (without the use of

[35] See - "Remarks on TOE functional requirements that are fulfilled by the TOE environment" under table 8.

No.	SFR	Dependency	Dependency satisfied?
			FDP_ICF.1)
17.	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	yes
18.	FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	yes
19.	FMT_MTD.3	ADV_SPM.1, FMT_MTD.1	yes
20.	FMT_SMF.1	-	-
21.	FMT_SMR.1	FIA_UID.1	yes
	FPT		
22.	FPT_RPL.1	-	-

Table 8: Fulfilment of SFR (TOE) dependencies

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

The functional component FAU_GEN.1 has an identified dependency on FPT_STM.1. This dependency is not satisfied by any TOE functional requirement, but by a security requirement for the TOE environment (see R.ENVIRONMENT, chapter 5.2). This is acceptable, because the time stamp functionality is required by the used, TOE underlying operating system. Therefore, the time stamp functionality is not needed within the TOE boundary and creates maximum flexibility to meet the developer needs.

8.2.1.3 Mutual support and internally consistency

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

8.2.1.4 Suitability of minimum SOF level

SOF-medium is chosen as minimum SOF level.

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

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

8.2.2 Environment security requirements

This *Security Target* provides security requirements for the TOE environment[36]. Thereby no functional requirements are taken from [CC], part 2.

[36] The requirements R.NO_REPRODUCE and R.RESIDUAL_CAPTURE which are defined in the PP are not necessary here because they are fulfilled by the TOE.

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

Table 9: Environment requirements - security objectives (environment) mapping

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

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

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

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

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

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

For all security objectives for the environment the corresponding security requirement is stated in a way, which directly correspond to the description of the objective (see chapter 4.1 and 4.2). It is clear from the description of each objective (see chapter 4.1 and 4.2), that the corresponding requirement is covered, if the objective is valid.

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

8.2.3 Assurance requirements rationale

The assurance level EAL2 is chosen with one augmentation (ADV_SPM.1) and additionally described with refinements (see chapter 5.1.3) due to the scope of biometric systems. EAL2 (augmented with ADV_SPM.1) and the relevant assurance requirements (see Table 4: Assurance requirements (EAL2, augmented with ADV_SPM.1)) provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

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

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

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

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

8.2.3.1 Dependencies, mutual support and internal consistency

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

8.3 TOE Summary Specification Rationale

8.3.1 TOE Security Functions Rationale

This chapter proves that the set of security functions is suited to meet the security functional requirements described in chapter 5.1.1 and that they can be traced back to the security functional requirements. At least one security functional requirement exists for each security function.

	F.AUDIT_REACTION	F.ROLES_AND_ACCESS	F.BIO_VERIFICATION	F.AUTHADMIN	F.RESIDUAL	F.NO_REPRODUCE_OR_.RESIDUAL_CAPTURE
FAU_ARP.1	X					
FAU_GEN.1	X					
FAU_GEN.2	X					
FAU_SAA.1	X					
FDP_ACC.1		X				
FDP_ACF.1		X				
FDP_RIP.2					X	X
FIA_AFL.1	X		X	X		
FIA_ATD.1		X	X	X		
FIA_UAU.2			X	X		
FIA_UAU.3			X	X		X
FIA_UAU.5			X	X		
FIA_UAU.7			X			
FIA_UID.2			X	X		
FMT_MOF.1#1		X				
FMT_MOF.1#2		X				
FMT_MSA.1		X				
FMT_MSA.3		X				
FMT_MTD.1		X				
FMT_MTD.3			X			
FMT_SMF.1		X				
FMT_SMR.1		X				
FPT_RPL.1			X			X

Table 10: SFR (TOE) - security functions mapping

FAU_ARP.1

*According to the requirements defined in the SFR FAU_ARP.1 the TSF **F.AUDIT_REACTION** audits the number of unsuccessful authentication attempts and locks the authentication mechanism if three consecutive attempts were unsuccessful or if either the BIR or the BLR do not have sufficient quality. The function initiate a mail sending to the TOE-Administrators if three unsuccessful authentication attempts to one TOE administrator account are occurred or if a brute force attack is identified.*

FAU_GEN.1

*According to the SFR FAU_GEN.1 the TSF **F.AUDIT_REACTION** audits all required events with corresponding information.*

FAU_GEN.2

According to the SFR FAU_GEN.2 the TSF ***F.AUDIT_REACTION*** *audits all required events with the identity of the user that caused the event.*

FAU_SAA.1

The TSF ***F.AUDIT_REACTION*** *locks the authentication mechanism for a user or a TOE administrator if three consecutive attempts were unsuccessful. The function initiate a mail sending to the TOE-Administrators if three unsuccessful authentication attempts to one TOE administrator account are occurred or if a brute force attack is identified.*

FDP_ACC.1

As required in the SFR FDP_ACC.1 the TSF ***F.ROLES_AND_ACCESS*** *enforces access control according to AC_SFP.*

FDP_ACF.1

FDP_ACF.1 is realised by the TSF ***F.ROLES_AND_ACCESS*** *which enforces access control according to AC_SFP.*

FDP_RIP.2

The TSF ***F.RESIDUAL*** *ensures that no residual or unprotected security relevant data remain after operations are completed. The TSF* ***F.NO_REPRODUCE_OR_RESIDUAL_CAPTURE*** *prevents an authentication with recorded voice samples by using a kind of challenge-response protocol.*

FIA_AFL.1

The TSF ***F.BIO_VERIFICATION*** *and the TSF* ***F.AUTHADMIN*** *count the number of unsuccessful authentication attempts. The TSF* ***F.AUDIT_REACTION*** *locks the authentication mechanism for a user or a TOE administrator if three consecutive attempts were unsuccessful.*

FIA_ATD.1

FIA_ATD.1 is realised by the TSF ***F.ROLES_AND_ACCESS*** *which enforces access control according to AC_SFP. The TSF* ***F.BIO_VERIFICATION*** *and the TSF* ***F.AUTHADMIN*** *use the defined attributes for the authentication.*

FIA_UAU.2

The TSF ***F.BIO_VERIFICATION*** *provides the user authentication via biometric verification with maximum FAR of 0.0001. The TSF* ***F.AUTHADMIN*** *provides the TOE administrator authentication through a username/password mechanism.*

FIA_UAU.3

FIA_UAU.3 is realised by the TSF ***F.BIO_VERIFICATION*** *which provides the user authentication via biometric verification and by the TSF* ***F.AUTHADMIN*** *which provides the TOE administrator authentication through a username/password mechanism. The TSF* ***F.NO_REPRODUCE_OR_RESIDUAL_CAPTURE*** *prevents an authentication with recorded voice samples by using a kind of challenge-response protocol (by asking for randomly chosen numbers).*

FIA_UAU.5

*FIA_UAU.5 is realised by the TSF **F.BIO_VERIFICATION** which provides the user authentication via biometric verification and by the TSF **F.AUTHADMIN** which provides the TOE administrator authentication through a username/password mechanism.*

FIA_UAU.7

*The TSF **F.BIO_VERIFICATION** does not give a feedback as long as the verification process is not finished.*

FIA_UID.2

*FIA_UID.2 is realised by the TSF **F.BIO_VERIFICATION** which provides the user authentication via biometric verification and by the TSF **F.AUTHADMIN** which provides the TOE administrator authentication through a username/password mechanism.*

FMT_MOF.1#1

*As required in the SFR FMT_MOF.1#1 the TSF **F.ROLES_AND_ACCESS** enforces access control for the TOE administrator according to AC_SFP.*

FMT_MOF.1#2

*As required in the SFR FMT_MOF.1#2 the TSF **F.ROLES_AND_ACCESS** enforces access control for the IT administrator according to AC_SFP.*

FMT_MSA.1

*FMT_MSA.1 is realised by the TSF **F.ROLES_AND_ACCESS** which restricts the management activities to the administrator according to AC_SFP.*

FMT_MSA.3

*FMT_MSA.3 is realised by the TSF **F.ROLES_AND_ACCESS** which enforces access control according to AC_SFP.*

FMT_MTD.1

*FMT_MTD.1 is realised by the TSF **F.ROLES_AND_ACCESS** which restricts the management of the user security attributes to the TOE administrator according to AC_SFP.*

FMT_MTD.3

*As required in the SFR FMT_MTD.3 the TSF **F.BIO_VERIFICATION** uses only its own templates (respectively standardised) from the enrolment process as stored in the data base.*

FMT_SMF.1

*The management functions of the SFR FMT_SMF.1 are directly part of the TSF **F.ROLES_AND_ACCESS**.*

FMT_SMR.1

*As required in the SFR FMT_SMR.1 the TSF **F.ROLES_AND_ACCESS** maintains the roles user, Developer-Administrator, TOE administrator and IT administrator according to AC_SFP.*

FPT_RPL.1

*FPT_RPL.1 is realised by the TSF **F.BIO_VERIFICATION** which provides the user authentication via biometric verification and by the TSF **F.NO_REPRODUCE_OR_RESIDUAL_CAPTURE** that prevents an authentication with recorded voice samples by using a kind of challenge-response protocol (by asking for randomly chosen numbers).*

8.3.2 Rationale for Strength of Function Claims

According to the section 6.2 there are three security functions (F.BIO_VERIFICATION, F.AUTHADMIN and F.NO_REPRODUCE_OR_RESIDUAL_CAPTURE) that must reach SOF-medium. As claimed in section 5.1.2, the minimum strength of function is SOF-medium. Those claims are consistent.

8.3.3 Mutual Support and Internal Consistency of the TOE Security Functions

The detailed description and analysis of the TOE Security Functions in chapter 6.1 demonstrate how the defined functions work together and support each other. Furthermore, this description shows that no inconsistencies exist. The analysis results in chapter 8.3.1 support this conclusion.

8.3.4 Assurance Measures Rationale

The assurance measures of the developer as mentioned in chapter 6.3 are considered to be suitable and sufficient to meet the CC assurance level EAL2 augmented by ADV_SPM.1 as claimed in chapter 5.1.3. Especially the documents listed in chap. 6.3 are seen to be suitable and sufficient to confirm the fulfilment of the assurance requirements.

8.4 PP claims rationale

According to chapter 7 this ST conforms to the "Protection Profile for Biometric Verification Mechanisms" (BSI-PP-0016) [PP_BSI_BV] published and registered by the German Federal Office for Information Security (BSI). As shown in the previous sections, this ST implements all of the requirements of the PP and hence no further rationale is necessary.

ANNEX

This Annex contains the following sections:

A BSI biometric performance standard
B Abbreviations and glossary
C References

A BSI biometric performance standard

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

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

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

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

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

B Abbreviations and glossary

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

Term	Description
ASR	*Automatic Speech Recognition*
Assets	Information or resources to be protected by the countermeasures of a TOE.
Assignment	The specification of an identified parameter in a component.
Attacker	An attacker is any individual who is attempting to subvert the operation of the biometric system. The intention may be either to subsequently gain illegal entry to the portal or to deny entry to legitimate users.
Attempt	The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.
Attribute	Security attribute: Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.
Augmentation	The addition of one or more assurance components(s) from [CC] part 3 to an EAL or assurance package.
Authentication	Testimony the authenticity; confirmation of the identity of a user. Generic term for the processes of the identification and verification.
Authentication data	*Information used to verify the claimed identity of a user.*
Authorised user	*A user who may, in accordance with TSP, perform an operation.*
Behavioural biometric	*A biometric which is characterised by a behavioural trait that is learned and aquired over time, e.g. signature. See also physical biometric.*
BEM	*Biometric Evaluation Methodology*
BIO API	*Biometric Application Programming Interface standard*
Biometric	A measurable physical characteristic or personal behavioural trait used to recognise the identity of an enrolee or verify a claimed identity.
Biometric data	Extracted information taken from a biometric sample and used either to build a reference template on enrolment, or to compare against a previously created reference template.
Biometric application	*The use to which a biometric system is put.*
Biometric feature	A representation from a biometric sample extracted by the extraction system.
Biometric sample	A biometric measure presented by the user and captured by the data collection system.
Biometric system	An automated system capable of capturing a biometric sample from a user, extracting biometric data from the sample, comparing the data with one or more reference templates, deciding on how well they match, and indicating whether or not an identification or verification of identity has been achieved. Note that in [CC] evaluation terms, a biometric system may be a product or part of a system.
BIR	Biometric Identification Record - A BIR includes the reference template and other data associated with the user. This is the saved reference data record against that the comparison is accomplished.
BLR	Biometric Live Record - This template includes the actual biometric data (actual biometric characteristic and user identity) to be verified with the biometric identity record.
Brute Force Attack	A brute force attack is an attack that requires trying all or a large fraction of all possible values until the right value is found.

Term	Description
BSI	Bundesamt für Sicherheit in der Informationstechnik - Federal Office for Information Security BSI - Godesberger Allee 185-189 - D-53133 Bonn (Germany) Tel.: +49 (0) 1888 9582 0 - FAX: +49 (0) 1888 9582 400 http://www.bsi.bund.de
Capture	The process of taking a biometric sample via a sensor from a user.
CBEFF	*Common Biometric Exchange File Format standard*
CC	Common Criteria - Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology
CLI	*Calling Line Identification*
CMOS	Complementary Metal Oxide Semiconductor
Comparison	The process of comparing biometric data with a previously stored BIR
DB	*Database*
EAL	Evaluation Assurance Level
Enrolee	A user with a stored biometric reference template on file.
Enrolment	See 2.1.1
FAR	False Accept Rate (FAR) - The probability that a biometric system will incorrectly identify an individual that is not authorised. For a positive (verification) system, it can be appraised from: (the number of false acceptances)/(the number of impostor verification attempts).
FRR	False Rejection Rate (FRR) - The probability that a biometric system will fail to identify a genuine enrolee. For a positive (verification) system, it can be estimated from: (the number of false rejects)/(the number of enrolee verification attempts). (Security attribute regarding to this *ST*)
GINA	Graphical Identification and Authentication as part of an operating system
Identification	See 2.2
Identification system	Biometric system that provides an identification function (see also identification)
IP	*Internet Protocol*
ITSEF	IT Security Evaluation Facility
LAN	Local Area Network
Live processing	Direct enrolment/ identification of potential users via the normal biometric capture process. Compare off-line processing.
Matching Score	A measure of similarity or dissimilarity between the biometric data and a stored template, used in the comparison process.
MS SQL	Microsoft Structured Query Language – database product of MS
Multimodal biometrics	A biometric system, which uses information from different biometrics - e.g. fingerprint and hand shape; or fingerprints from two separate fingers. All statistical analysis of multimodal systems should consider how the modes are combined in the comparison process.
Negative claim	*A claim by a user not to be enrolled in the biometric system. This may be needed to establish that double claims are not being made.*
one-to-many matching	See identification system.
one-to-one matching	See verification system.
OS	Operating system
OSP	Organisational Security Policy

Term	Description
Physical/Physiological biometric	*A biometric which is characterised by a physical characteristic. See also behavioural biometric.*
PK	*Primary Key*
Portal	The physical or logical point beyond which information or assets are protected by a biometric system.
PP	Protection Profile - An implementation-independent set of security requirements for a category of TOE's that meet specific consumer needs.
PWR	*Password Reset*
Refinement	The addition of details to a component.
Replay attack	An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of an impostor attack.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Scenario testing	*Testing a biometric system to measure its statistical properties (e.g. FAR and FRR) in an environment modelled to simulate a particular application.*
Security attribute	*Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.*
Sensor	The physical hardware device used for biometric capture. Also called caputer device
SFR	Security Functional Requirement
SOF	*Strength Of Function (SOF) - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.* *The determination of an additional strength of function is an important part of the evaluation of a biometric product or system. In accordance with [BEM] the SOF for the biometric verification mechanism is described in terms of FAR values. It is proposed that all biometric Security Targets should include a claim for SOF and a rationale to explain the claim. This problematic arises due to the fact of probabilistic prediction of biometric systems.*
ST	Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
SW	Software
Technology testing	*Testing one or more biometric systems to measure statistical properties (e.g. FAR and FRR) to compare various algorithms and technologies – usually achieved by off-line processing.*
Template	A user's stored reference measure based on biometric feature(s) extracted from biometric sample(s). It could differentiate in: Biometric Identification Record: see BIR Biometric Live Record: see BLR
Threat	An intended or unintended potential event that could compromise the security integrity of the system.
Threshold	A parametric value used to convert a matching score to a decision. A threshold change will usually change both FAR and FRR - as FAR decreases, FRR increases.
TIKS	*Telekom Internal Key Service*
TOE	Target of Evaluation - An IT product or system (and its associated documentation) that is the subject of a Common Criteria evaluation.
TSF	TOE Security Functions

Term	Description
TSF data	Data created by and for the TOE that might affect the operating of the TOE.
TSP	TOE Security Policy
User	A person who requires access to the portal, which is protected by a biometric system.
User data	Data created by and for the user that does not affect the operation of the TSF.
Verification	See 2.1.2
Verification system	A biometric system that provides a verification functionality.
VoIP	*Voice over IP*
VS	*Voice Sample*
WAN	Wide Area Network
Weak Template	A template created from a noisy, poor quality, highly varying biometric sample.
WLAN	Wireless Local Area Network
XML	*Extended Mark-up Language*

Table 11: Abbreviations and Glossary

C References

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

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

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

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

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Part 1: Introduction and general model,
Part 2: Security functional requirements,
Part 3: Security Assurance Requirements.

[CEM] Common Methodology for Information Technology Security Evaluation, CCIMB-2005-08-004, Version 2.3, August 2005

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

[PP_BSI_BV] "Protection Profile for Biometric Verification Mechanisms" (BSI-PP-0016), BSI, Version 1.04, 17. August 2005

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

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

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

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

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

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

[ST_V1.0]	Security Target for VoiceIdent Unit 1.0, Version 1.7, T-Systems International GmbH, 29.09.2006
[IAR]	Auswirkungsanalyse zur BSI-Re-Zertifizierung VoiceIdent Unit 2.0, T-Systems