CERTIFICATION REPORT

Certification file:	**TUVIT-DSZ-CC-9224**
Product / system:	biometric authentication system in software Authentication Engine of VOICE.TRUST Server, Version 4.1.2.0
Product manufacturer:	VOICE.TRUST.AG Geisenhausener Straße 15-17 81379 München
Customer:	see above
Evaluation facility:	TÜViT, evaluation body for IT security
Evaluation report:	*Version 2 as of 2005-05-19* Document-number: *20609936_TÜViT_14.2* Author: Christoph Zurheiden
Result:	EAL2
Evaluation stipulations:	none
Certifier:	Dr. Christoph Sutter
Certification stipulations:	none

Essen, 2005-05-20

Dr. Ernst-Hermann Gruschwitz Dr. Christoph Sutter

Contents

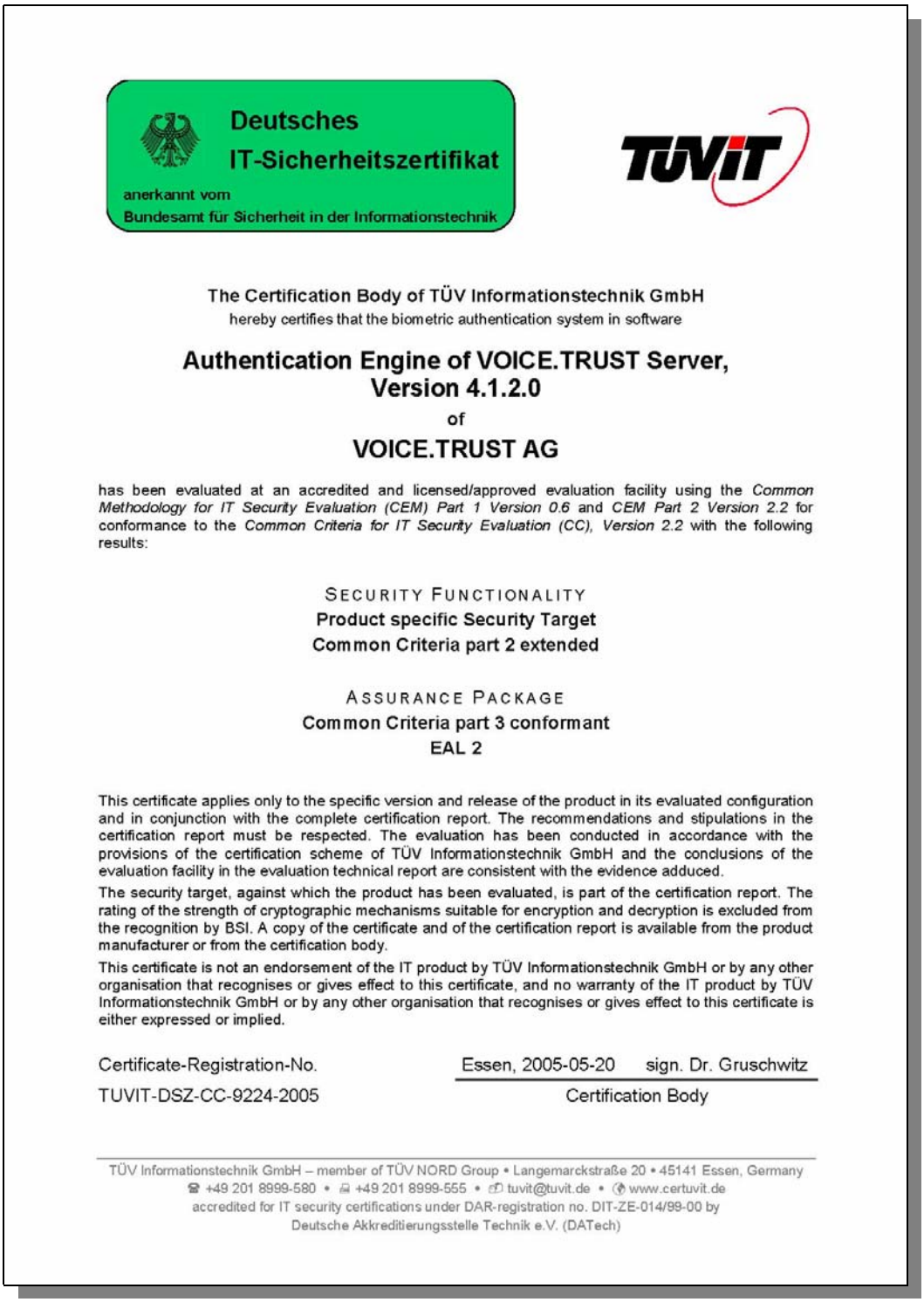
Part A

Certificate and Background of the Certification

Part A presents a copy of the issued certificate and summarizes

- information about the certification body,
- the certification procedure, and
- the performance of evaluation and certification.

1 The Certificate



Deutsches
IT-Sicherheitszertifikat
anerkannt vom
Bundesamt für Sicherheit in der Informationstechnik

The Certification Body of TÜV Informationstechnik GmbH
hereby certifies that the biometric authentication system in software

Authentication Engine of VOICE.TRUST Server, Version 4.1.2.0
of
VOICE.TRUST AG

has been evaluated at an accredited and licensed/approved evaluation facility using the *Common Methodology for IT Security Evaluation (CEM) Part 1 Version 0.6* and *CEM Part 2 Version 2.2* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.2* with the following results:

SECURITY FUNCTIONALITY
Product specific Security Target
Common Criteria part 2 extended

ASSURANCE PACKAGE
Common Criteria part 3 conformant
EAL 2

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The recommendations and stipulations in the certification report must be respected. The evaluation has been conducted in accordance with the provisions of the certification scheme of TÜV Informationstechnik GmbH and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The security target, against which the product has been evaluated, is part of the certification report. The rating of the strength of cryptographic mechanisms suitable for encryption and decryption is excluded from the recognition by BSI. A copy of the certificate and of the certification report is available from the product manufacturer or from the certification body.

This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate is either expressed or implied.

Certificate-Registration-No.
TUVIT-DSZ-CC-9224-2005

Essen, 2005-05-20 sign. Dr. Gruschwitz
Certification Body

TÜV Informationstechnik GmbH – member of TÜV NORD Group • Langemarckstraße 20 • 45141 Essen, Germany
☎ +49 201 8999-580 • 🖷 +49 201 8999-555 • 🖂 tuvit@tuvit.de • 🌐 www.certuvit.de
accredited for IT security certifications under DAR-registration no. DIT-ZE-014/99-00 by
Deutsche Akkreditierungsstelle Technik e.V. (DATech)

2 Certification Body – CERTÜVIT

CERTÜViT, the Certification Body of *TÜV Informationstechnik GmbH*[1] – a member of TÜV NORD Group – was established in 1998 and offers a variety of services in the context of security evaluation and validation.

CERTÜViT was accredited in September 1999 for certification of IT security products according to ITSEC and Common Criteria by *Deutsche Akkreditierungsstelle für Informations- und Telekommunikationstechnik (Dekitz)* now *Deutsche Akkreditierungsstelle Technik e.V. (DATech), Frankfurt/Main* under DAR-registration no. DAT-ZE-014/99-01 and performs its projects under a quality management system certified against ISO 9001 by *Germanischer Lloyd, Hamburg*.

CERTÜViT is accredited by *Bundesamt für Sicherheit in der Informationstechnik*[2] to issue the "German IT Security Certificate" which is recognised by BSI as equivalent to the "German IT Security Certificate" of BSI.

3 Specifications of the Certification Procedure

The certification body conducts the certification procedure according to the criteria laid down in the following:

- DIN EN 45011
- TÜViT Certification Scheme
- TÜViT Certification Conditions
- Regulations on the "German IT Security Certificate" issued by the BSI and accepted in the contract of BSI and TÜViT as of November 20, 2002.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, version 2.2, January 2004.
- Common Methodology for Information Technology Security Evaluation (CEM) part 1, version 0.6, January 1997.
- Common Methodology for Information Technology Security Evaluation (CEM) part 2, version 2.2, January 2004.
- Application Notes and Interpretations of the Scheme (AIS), published by BSI.

[1] in the following termed shortly TÜViT

[2] in the following termed shortly BSI

4 Recognition Agreements

In order to avoid multiple certification of the same product by different certification bodies a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC – under certain conditions was agreed. CERTÜViT certificates are German IT Security Certificates recognized by BSI – the national German certification body in international agreements – to be equivalent to its own certificates but they are not part of these international agreements.

4.1 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4 was signed between the national participants of Australia and New Zealand, Austria, Canada, Czech Republic, Finland, France, Germany, Greece, Hungary, Israel, Italy, Japan, The Netherlands, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom and the United States.

4.2 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. The arrangement on the mutual recognition of IT security certificates based on the CC was extended by these participants up to and including the evaluation assurance level EAL7.

5 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The biometric authentication system in software *Authentication Engine of VOICE.TRUST Server, Version 4.1.2.0* has undergone the certification procedure at TÜViT certification body. It was an initial certification.

The evaluation of the biometric authentication system in software Authentication Engine of VOICE.TRUST Server, Version 4.1.2.0 was conducted by the evaluation body for IT-security of TÜViT and concluded on May 19, 2005. The TÜViT evaluation facility is recognised by BSI.

The sponsor as well as the developer is VOICE.TRUST.AG. Distributor of the product is VOICE.TRUST.AG.

The certification was concluded with

- the comparability check and
- the preparation of this certification report.

This work was concluded on May 20, 2005. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stipulations regarding generation, configuration and operation, as given in part B of this report, are observed,
- the product is operated – where indicated – in the environment described.

This certification report applies only to the version of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

With regard to the meaning of the evaluation assurance levels (EAL) and the strength of function (SoF), please refer to part C of this report.

6 Publication

The following Certification Results consist of pages B-1 to B-17. The product Authentication Engine of VOICE.TRUST Server, Version 4.1.2.0 will be included in the BSI list of certified products which is published at regular intervals (e. g. in the Internet at http://www.bsi.bund.de) and the TÜViT certification lists (http://www.certuvit.de).

Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form at the internet address of CERTÜViT as stated above.

Part B

Certification Result

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the Certification Result

1 Executive Summary

1.1 Target of Evaluation and Evaluation Background

The target of evaluation (TOE) is the biometric authentication system in software ***Authentication Engine of VOICE.TRUST Server, Version 4.1.2.0***. The TOE is part of the product VOICE.TRUST Server 4.1 and contains software for decision management and interactive voice response-, mail-, text to speech-, database-, encryption-, and password reset- interfaces. This is illustrated in the following figure:

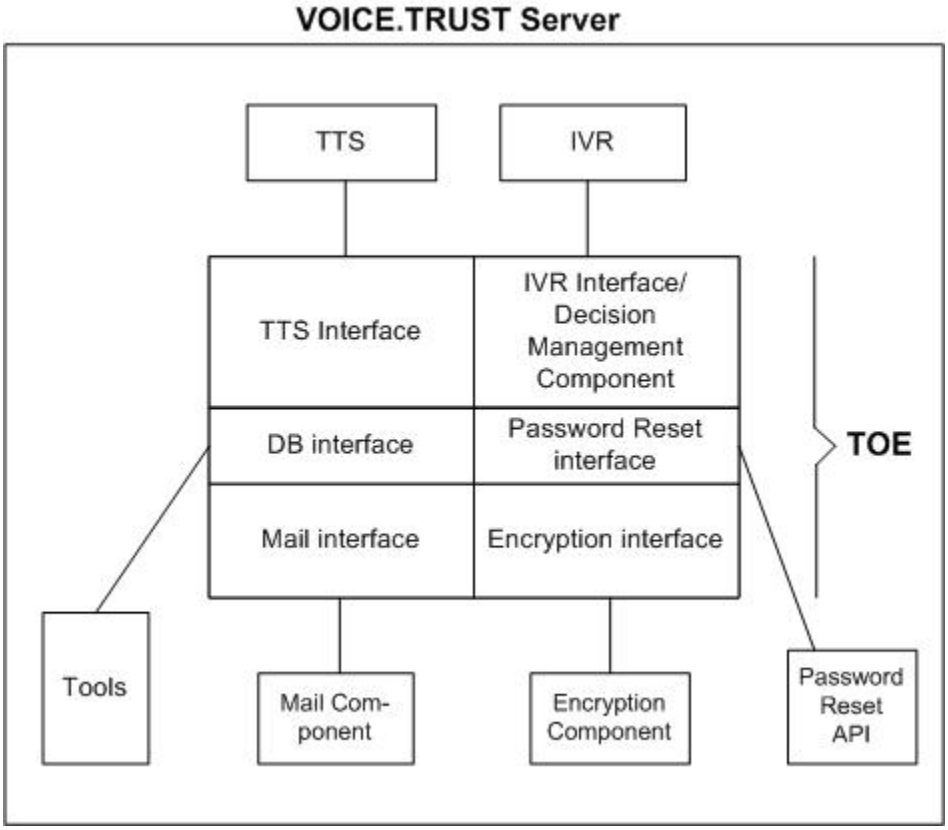


Figure 1: Overview about the VOICE.TRUST Server

A description of the components/interfaces of figure 1 can be found in chapter 5 of this report and in section 2.2 of the public ST, which is attached as part D of this certification report.

The TOE allows authenticating a user using the characteristics of his voice via standard telephone equipment and provides the possibility to reset passwords in target systems based on the result of the biometric authentication process.

The VOICE.TRUST Server (VTS) includes the interface to the telephone via the interactive voice response (IVR) system and allows the interactive (user) dialog with the help of the text to speech system (TTS) software. The VOICE.TRUST Server also communicates to the database, to the Password Reset systems and initiates the sending of e-mails. Figure 2 below gives an overview about the scope of the VOICE.TRUST Server and shows the application flow for a password reset.

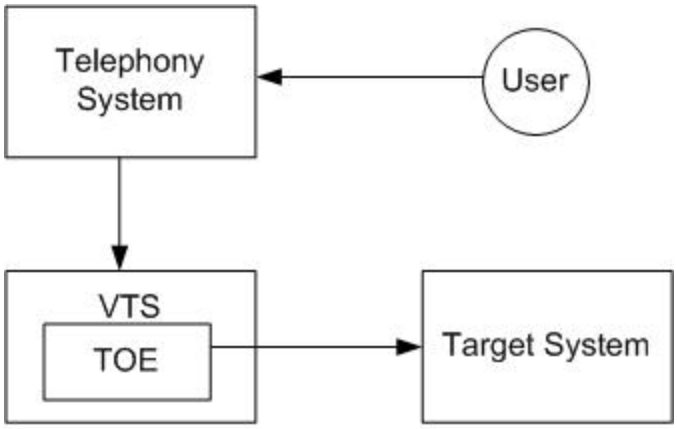


Figure 2: Schematic System Description

The TOE provides the following security features:

1. **Access for registered users only.** A user has to be registered by the administrator of the TOE. A not registered person whose unique user ID is not known to the system cannot be enrolled.
2. **User Identification before enrolment.** A user has to be identified personally by his Super User before he is allowed to provide his speech data to the TOE. That way, a recursive trust chain is established. Additionally, personal supervision by an experienced person improves the quality of the provided speech data.
3. **Claimed ID determination by Automated Speech Recognition (ASR).** A user's identity has to be clearly recognized by automated speech recognition (ASR) at the stage of login.
4. **Multi level authentication.** The user will be guided from the TOE through an authentication process consisting of several steps (levels).
5. **No status information during authentication sessions.** The user has to follow the multi level authentication process up to the end. Only then, he will get the information if he is successfully authenticated or not.

6. **Fault-tolerant speech data collection.** Whenever a user provides an utterance that is inadequate for verification, the user gets a second chance to speak the required phrase.

The TOE stores user data, as well as the platform access credentials necessary for the service applications like password reset, in an external database. All security relevant data are encrypted.

For authenticated users the service application (password reset) is called. In a dialogue driven process, the user is prompted for the target systems on which he wants to reset his password. The connectivity between the TOE and the target platforms uses the protection mechanisms provided by the target platform. The Application Program Interface (API) of an administration client on the target is used for password reset purposes. It is recommended that this API is installed on the same machine as the TOE.

1.2 Assurance Package

The TOE security assurance requirements are based entirely on the assurance components and classes defined in Part 3 of the Common Criteria (see part C of this report or [CC] Part 3 for details). The TOE meets the assurance requirements of assurance level EAL 2 (Evaluation Assurance Level 2).

1.3 Strength of Functions

The TOE‘s strength of functions is rated “medium” (SOF-medium). The strength of functions rating does not include cryptographic algorithms for encryption and decryption. For more details see also chapter 9 of this report.

1.4 Functionality

Except the functional requirement FIA_ENR.1 (Enrolment) the TOE security functional requirements were taken from CC part 2 (i. e. the set is CC part 2 extended) [CC]. They can be categorized into the following five functional classes:

1. security audit,
2. user data protection,
3. identification and authentication,
4. security management, and
5. TOE access.

Chapter 9 lists the security functional requirements in more detail. They are met by four suitable TOE security functions (TSF):

TSF	Short Description
AUDIT&REACTION	generates audit records for the enrolment and the identification and authentication process and stores this audit information within the database of the environment
ENROL	ensures the enrolment of a user into the TOE and the quality of the acquired data
I&A	verifies the identity of a user using the characteristics of his voice and comparing it to acquired data during enrolment
ROLES_ACCESS	manages the roles “Normal User” and “Super User” and the attributed access rights “reset passwords on target systems” and “start enrolment process for other users”

A more detailed description of the TOE security functions can be found in section 6.1 of the public ST, which is attached as part D of this certification report.

1.5 Summary of Threats and Organisational Security Policies (OSPs)

The primary asset for the TOE is the functionality to reset passwords on user systems. Secondary assets are used by the TOE for authentication and access control of the users and include: voice prints, access rights of users, and threshold setting for the authentication mechanism.

The attacker may be any person that attacks the TOE via the telephone interface to get access or to enhance its privileges. Remark: direct attacks – either physical or logical via a network – on the computer where the TOE is installed were not considered in this certification due to the assumptions A.EQUIPMENT and A.PHYSICAL.

The 4 threats deal with impersonation of users, enhancing of privileges and replay or reproduction of the voice of an enrolled user to get illegal access.

The organisational security policy contains the requirement, that all users must be enrolled previously.

A more detailed description of the threats and organisational security policies can be found in sections 3.3 and 3.4 of the public ST, which is attached as part D of this certification report.

1.6 Special Configuration Requirements

The TOE is delivered in one fixed configuration. The software VOICE.TRUST Server 4.1 including the TOE can be installed on a single machine or on multiple machines. Only the single machine installation is part of this certification.

1.7 Assumptions about the Operating Environment

The TOE (Authentication Engine of VOICE.TRUST Server, Version 4.1.2.0) is part of the VOICE.TRUST Server 4.1 (VTS) that is its direct operating environment (see figure 2). The VOICE.TRUST Server is based on a Win2000 Server machine (Pentium P4 3GHz, HT, 2GB RAM, 60 GB HD, NIC) and an ISDN AVM B1 or C4 controller. The VTS needs further a database to store user data, connections to a telephony system for speech entry, and via LAN network to at least one target system to reset passwords. According to the assumptions A.EQUIPMENT and A.PHYSICAL (see section 4.2), this operating environment including the telephone system, the database, and the network is sufficiently protected against direct attacks (see also section 1.5 above).

Further assumptions about the environment of use are contained in chapter 4.

1.8 Independence of the Certifier

Within the last two years, the certifier did not render any consulting- or other services for the company ordering the certification and there was no relationship between them that might have an influence on his assessment.

The certifier did not participate at any time in test procedures for the product, which forms the basis of the certification.

1.9 Disclaimers

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept with regard to generation, configuration and operation as detailed in this certification report. This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is the biometric authentication system in software Authentication Engine of VOICE.TRUST Server, Version 4.1.2.0. It is delivered on a CD-ROM and personally handed over to the customer and installed at customer's site. The CD contains the installation program (Setup.exe), the Microsoft Windows Installer Database (VOICE.TRUST Server.msi), a ZIP Archive that contains all necessary files for VTS including the TOE, the guidance documentation (see chapter 6), and additional files with licenses and sample data.

3 Security Policy

Within the security target one single security policy is defined:

Policy Name	Description
DAC SFP	only the Super User is allowed to start an enrolment process and a (authenticated) normal user is allowed to perform a password reset on a target system if it is explicitly allowed in the access control list

A more detailed description of the security policy can be found in section 5.1.2.2 of the public ST, which is attached as part D of this certification report.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The only assumptions defined in the ST are assumptions about the environment of use (see following section). There is no usage assumption defined in the ST.

4.2 Environmental Assumptions

The following four assumptions about the environment of use are defined in the ST and must be regarded when using the TOE.

Assumption	Description
A.ADMINISTRATION	The administrator and the Super Users are well trained and can be trusted. The administrator reads the guidance documentation carefully, understands the details of them and informs the trustworthy Super User about the secure usage of the TOE. Moreover the administrator is responsible to oversee the system requirements and also has to oversee the rates for false acceptance and false rejection to guarantee the keeping. A Super User is responsible to ensure the correct enrolment of each user.
A.EQUIPMENT	The necessary infrastructure like telephone set and LAN network are available. In the telephony network only voice services are allowed (no data services). It is assumed that the LAN network to which the TOE is connected is secure. The network to which the TOE is connected is internal and protected from unspecific access. LAN's with internet connections are protected, appropriate firewalls are installed. Therefore unauthorised access from the external networks is prevented. In addition, no users, unauthorised users or attackers

Assumption	Description
	can perform the direct attacks against the internal network such as eavesdropping of packets. It is assumed that the telephones that are used for enrolment are secured and securely connected to the TOE so that a sniffing of the enrolment process is not possible. It is assumed that the environment provides a database to be used by the TOE to store TSF data in. It is assumed that at least one Super User has been enrolled to the TOE before the operation of the TOE starts. The external database has to have the same level of protection as the TOE. Furthermore it is assumed that the database provides an identification/authentication mechanism and an access control mechanism to ensure that only the administrator is able to edit the TSF data within the database.
A.FALLBACK	It is assumed that any alternative or fallback identification/ authentication system, used when the TOE is not in operation, offers adequate protection of the assets. However the security of the fallback system is outside the scope of the evaluation. This means that even if the scope of the TOE is, to perform actions that are usually done by a callcenter/helpdesk, a helpdesk is still needed. The helpdesk is then responsible to handle the requests of the users who are not able to use the TOE or were rejected by the TOE or of all users if the TOE is out of order.
A.PHYSICAL	Physical access to the hardware is not allowed for unauthorised users (only administrator). The TOE is physically protected, firewall protected and state of the art protected against sniffing and malware.

4.3 Clarification of Scope

The software VOICE.TRUST Server 4.1 including the TOE can be installed on a single machine or on multiple machines. The installation on multiple machines is not part of this certification.

5 Architectural Information

The TOE can be divided into 6 components/interfaces shown in figure 1 above:

name	description
Text To Speech (TTS) Interface	contains the speech component and deals with the transformation of text fragments into speech
IVR Transaction Interface/Decision Management Component	contains the interactive dialog for enrolment and authentication as well as the decision procedures for speaker verification and resulting actions
Database (DB) Interface	communicates to an external data component
Mail Interface	sends e-mails using an external mail component
Password Reset Interface	includes all data manipulation logic up to the usage of target system APIs
Encryption interface	connects the TOE with components in the environment that are used for encryption

6 Documentation

The following documentation is provided with the product by the developer to the consumer:

- Administration Guide for Authentication Engine of VOICE.TRUST Server 4.1, version 0.11, 2005-05-18,
- Super User Guide for Authentication Engine of VOICE.TRUST Server 4.1, version 0.6, 2004-12-03,
- User Guide for Authentication Engine of VOICE.TRUST Server 4.1, version 0.10, 2005-05-19,
- Installation Guide for Authentication Engine of VOICE.TRUST Server 4.1, version 0.6, 2005-05-19,
- Backup- and Recovery- Guide for Authentication Engine of VOICE.TRUST Server 4.1, version 0.4, 2004-12-06,
- External Agent Guide for Authentication Engine of VOICE.TRUST Server 4.1, version 0.4, 2004-07-21,
- Release Notes for VOICE.TRUST Server 4.1, version 0.4, 2004-12-06, and
- Database Guide for Authentication Engine of VOICE.TRUST Server 4.1, version 0.5, 2005-01-15.

7 IT Product Testing

The developer tested the TOE with the overall objectives to verify that the TOE Security Functions (TSF) satisfy the requirements as specified in the Functional Specifications (FSP). Overall 29 test cases with 97 test steps were applied on all TSF. No errors or other flaws occurred with regard to the security functionality defined in the Security Target and FSP. Consequently, the test results demonstrate that the behaviour of the security functions is as specified.

Furthermore, the developer used 250 voice templates to conduct statistical tests according to [BEM] and determined that the False Acceptance Rate (FAR) of the biometric verification mechanism is less or equal 1:10,000.

The evaluation body repeated the functional tests of the developer and performed independent penetration testing. The testing confirmed that all obvious vulnerabilities were considered and that these vulnerabilities are non-exploitable in the intended operational environment of the TOE with respect to low attack potential.

8 Evaluated Configuration

The TOE is delivered in one fixed configuration and no further generation takes place. Therefore the evaluated configuration is identical to the TOE, which can be identified as described in chapter 2 of this certification report.

9 Results of the Evaluation

The Evaluation Technical Report [ETR] was provided by TÜViT's evaluation body according to the requirements of the Scheme, the Common Criteria [CC], the Methodology [CEM] and the Application Notes and Interpretations of the Scheme [AIS].

The verdicts for the CC, part 3 assurance classes and components (according to EAL2 and the class ASE for the Security Target Evaluation) are summarised in the following table:

Assurance classes and components		**Verdict**
Security Target evaluation	**CC Class ASE**	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration Management	**CC Class ACM**	PASS
Configuration items	ACM_CAP.2	PASS
Delivery and operation	**CC Class ADO**	PASS
Delivery procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	**CC Class ADV**	PASS
Informal functional specification	ADV_FSP.1	PASS
Descriptive high-level design	ADV_HLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	**CC Class AGD**	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Tests	**CC Class ATE**	PASS
Evidence of coverage	ATE_COV.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	**CC Class AVA**	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

All assurance components were assessed with the verdict PASS. This includes that all evaluator action elements being part of the assurance components are also assessed with PASS. Therefore, the TOE as defined in the security target is considered to be Part 3 conformant.

Section 5.1 of the public ST, which is attached as part D of this certification report, lists the following TOE security functional requirements.

ID	**Class**/Component
FAU	**Security audit**
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAA.1	Security audit analysis

ID	**Class**/Component
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA	**Identification and authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UAU.3	Unforgeable authentication
FIA_UAU.7	Protected authentication feedback
FIA_UID.2	User identification before any action
FIA_ENR.1	*Enrolment*
FMT	**Security management**
FMT_SMR.1	Security roles
FTA	**TOE access**
FTA_SSL.3	TSF-initiated termination

Apart from FIA_ENR.1 all security functional requirements were taken from [CC] part 2, i. e. the TOE is [CC] part 2 extended.

The evaluation performed in accordance to EAL2 has shown that the TOE security functional requirements are correctly realised by the TOE security functions. Thus, in realising these functional requirements, it is assured that the TOE will meet the security objectives claimed in the ST.

The TOE Security Function *I&A* fulfils the SOF-rating medium (SOF-medium).

The sponsor must advise the certification authority about any modification of the TOE or its guidance documentation. The certification authority will then check whether the certification results are still valid and, if necessary, initiate all further steps concerning a re-evaluation. The results of the evaluation are only applicable to the product "*Authentication Engine of VOICE.TRUST Server, Version 4.1.2.0*". The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

10 Evaluation Stipulations, Comments, and Recommendations

There are no evaluation stipulations, comments, or recommendations.

11 Certification Stipulations and Notes

There are no certification stipulations or notes.

12 Security Target

The public version [ST-lite] of the security target [ST] for *Authentication Engine of VOICE.TRUST Server, Version 4.1.2.0* is included in part D of this certification report.

13 Definitions

13.1 Acronyms

ACL	Access Control List
ADM	Administrator Guidance
API	Application Programming Interface
ASR	Automated Speech Recognition
BEM	Biometric Evaluation Methodology Supplement (see [BEM])
CC	Common Criteria for Information Technology Security Evaluation (referenced to as [CC])
CEM	Common Methodology for Information Technology Security Evaluation (referenced to as [CEM])
CM	Configuration Management
DAC	Discretionary Access Control
DB	Data Base
EAL	Evaluation Assurance Level
FAR	False Acceptance Rate
FRR	False Rejection Rate
FSP	Functional Specification
HLD	High-level Design
IF	Interface
IGS	Installation, Generation and Start-up
IVR	Interactive Voice Response
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SIF	Sub-interface
SOF	Strength of Function
SS	Sub-system
ST	Security Target
TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Function Interfaces
TSP	TOE Security Policy
TTS	Text to Speech System

USR	User Guidance
VLA	Vulnerability Analysis
VTS	VOICE.TRUST Server

13.2 Glossary

Augmentation – The addition of one or more assurance component(s) from Part 3 to an EAL or assurance package.

Extension – The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

Formal – Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal – Expressed in natural language.

Object – An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile – An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function – A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target – A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal – Expressed in a restricted syntax language with defined semantics.

Strength of Function – 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.

SOF-basic – A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium – A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high – A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject – An entity within the TSC that causes operations to be performed.

Target of Evaluation – An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions – A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy – A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control – The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[AIS] Application Notes and Interpretations of the Scheme (AIS), published by BSI

[BEM] Biometric Evaluation Methodology Supplement, Version 1.0, August 2002, Author: Common Criteria Biometric Evaluation Methodology Working Group (remark: This is no official document of the German Certification Scheme.)

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004,
Part 1: Introduction and general model
Part 2: Security functional requirements
Part 3: Security assurance requirements

[CEM] Common Methodology for Information Technology Security Evaluation,
Part 1: Introduction and general model, version 0.6, revision 11.01.1997,
Part 2: Evaluation Methodology, Version 2.2, January 2004

[ETR] Evaluation Technical Report, TÜV Informationstechnik GmbH,
version 2, 2005-05-19, document-number: 20609936_TÜViT_14.2

[ST] Security Target for Authentication Engine of VOICE.TRUST Server 4.1,
Version 1.1, 2005-02-17
confidential document

[ST-lite] Security Target Lite for Authentication Engine of VOICE.TRUST Server 4.1,
Version 1.2, 2005-05-19
public version of the Security Target [ST]

Part C

Excerpts from the Criteria

The excerpts from the criteria are dealing with

- conformance results
- assurance categorization
- evaluation assurance levels
- strength of security function
- vulnerability analysis

CC Part 1:

Conformance results (section 5.4 of CC part 1 with final interpretation 008)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

> **Part 2 conformant** - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2.
>
> **Part 2 extended** - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2.

plus one of the following:

> **Part 3 conformant** - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3.
>
> **Part 3 extended** - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

> ***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
>
> ***Package name* Augmented** - A PP or TOE is an augmentation of a predefined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.“

CC Part 3:

Assurance categorisation

The assurance classes, families, and the abbreviation for each family are shown in *Table 1*.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 1: Assurance family breakdown and mapping

Evaluation assurance levels (chapter 6)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances.

Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility."

Evaluation assurance level (EAL) overview

„Table 2 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i. e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i. e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of "augmentation" allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an "EAL minus a constituent assurance component" is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration Management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and Operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_IMT					**1**	**2**	***3***
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance Documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life Cycle Support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability Assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Table 2: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested

“EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay. An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested

"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.

EAL2 is therefore 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."

Evaluation assurance level 3 (EAL3) - methodically tested and checked

"EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed

"EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL5) - semiformally designed and tested

"EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.“

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested

“EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.“

Evaluation assurance level 7 (EAL7) - formally verified design and tested

“EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF)

AVA_SOF Strength of TOE security functions

“Strength of function analysis addresses TOE security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function). Even if such functions cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat them by direct attack. A level or a specific metric may be claimed for the strength of each of these functions. Strength of function analysis is performed to determine whether such functions meet or exceed the claim. For example, strength of function analysis of a password mechanism can demonstrate that the password function meets the strength claim by showing that the password space is sufficiently large.”

Three levels exist: SOF-basic, SOF-medium, and SOF-high.

Vulnerability analysis (AVA_VLA)

AVA_VLA Vulnerability analysis

"Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: (1) the completeness of the TSF (does the TSF counter all the postulated threats?) and (2) the dependencies between all security functions. These potential vulnerabilities are assessed through penetration testing to determine whether they could, in practice, be exploitable to compromise the security of the TOE."

Application notes

"A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.

The intent of the developer analysis is to confirm that no identified security vulnerabilities can be exploited in the intended environment for the TOE and that the TOE is resistant to obvious penetration attacks.

Obvious vulnerabilities are considered to be those that are open to exploitation that requires a minimum of understanding of the TOE, skill, technical sophistication, and resources. These might be suggested by the TSF interface description. Obvious vulnerabilities include those in the public domain, details of which should be known to a developer or available from an evaluation authority.

Performing a search for vulnerabilities in a systematic way requires that the developer identify those vulnerabilities in a structured and repeatable way, as opposed to identifying them in an ad-hoc fashion. The associated evidence that the search for vulnerabilities was systematic should include identification of all TOE documentation upon which the search for flaws was based.

Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential. To accomplish this intent, the evaluator first assesses the exploitability of all identified vulnerabilities. This is accomplished by conducting penetration testing. The evaluator

should assume the role of an attacker with a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential when attempting to penetrate the TOE. Any exploitation of vulnerabilities by such an attacker should be considered by the evaluator to be “obvious penetration attacks” (with respect to the AVA_VLA.*.2C elements) in the context of the components AVA_VLA.2 through AVA_VLA.4.”

Part D

Security Target

Attached is the public version of the *Security Target for Authentication Engine of VOICE.TRUST Server 4.1*

Author: VOICE.TRUST.AG

Date: 2005-05-19

Version: 1.2

Security Target-lite
for
Authentication Engine of VOICE.TRUST Server 4.1

Version: 1.2

Date: May 19th, 2005

File Name: ST-LITE_1.2.DOC

Author(s): Bettina Stearn, VOICE.TRUST AG

Document Revision History

Version	Date	Author	Description
1.0	2005-05-13	Bettina Stearn, VOICE.TRUST AG	Initial document
1.1	2005-05-18	Bettina Stearn, VOICE.TRUST AG	Update
1.2	2005-05-19	Bettina Stearn, VOICE.TRUST AG	Update

Table of contents

1 ST introduction

1.1 ST identification

Title:	Security Target-lite for Authentication Engine of VOICE.TRUST Server 4.1
Version:	1.2
Date:	May, 19 th, 2005
Author:	Bettina Stearn, VOICE.TRUST AG
Developer:	VOICE.TRUST AG, Geisenhausener Str. 15-17, 81379 München, Germany
Product:	VOICE.TRUST Server 4.1
TOE-name:	Authentication Engine of VOICE.TRUST Server (VTS)
TOE-Version:	4.1.2.0
Product type:	biometric authentication system in software
CC used [CC]:	Common Criteria for Information Technology Security Evaluation, Version 2.1, Incorporated with interpretations as of 2003-12-31, (equivalent to Version 2.2), August 1999
EAL-level	2
SOF-claim	medium

1.2 ST overview

This document details the security target (ST) for the authentication engine of the "VOICE.TRUST Server 4.1 (VTS)", biometric authentication software via voice.

The TOE allows authenticating a user using the characteristics of his voice. The authentication process can be done using standard telephone equipment.

The TOE provides the possibility to reset passwords in target systems based on the result of the biometric authentication process.

This functionality is designed for large IT environments where passwords for systems (the target systems) are locked after a certain number of failures during authentication and where the reset of user passwords through a helpdesk produces substantial efforts.

1.3 CC conformance claims

This ST has been built with Common Criteria (CC) Version 2.1 (ISO/IEC 15408 Evaluation Criteria for Information Technology Security; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements including final interpretations until 12-31-2003). The TOE itself is CC part 2 extended because with FIA_ENR.1 as explicitly stated SFR is contained within this ST and conformant to part 3 of [CC].

This security target does not claim for compliance with any existing protection profile.

The assurance level for the TOE is **EAL 2,** the strength of function is **SOF Medium**.

2 TOE description

2.1 About the TOE

2.1.1 Definition of the VOICE.TRUST Server

The VOICE.TRUST Server (VTS) is the environment, in which the TOE with all its components is embedded. The VOICE.TRUST Server's hardware is based on a Win2000 Server machine (Pentium P4 3GHz, HT, 2GB RAM, 60 GB HD, NIC) and an ISDN AVM B1 or C4 controller (No. 2001778). Additional software components are necessary to support the functionality of the TOE; one of them is an Interactive Voice Response (IVR) system with its telephony interface.

Another software the VOICE.TRUST Server needs is a Text To Speech (TTS) system that allows the conversion from text into speech data.

A mail and database component is completing the environment of the VOICE.TRUST Server. As mail component, every SMTP compatible module can be used and integrated, as database client, the VOICE.TRUST Server can be installed with MySQL, MSDE, DB2 and Oracle. VOICE.TRUST provides tools that help to administrate the TOE data in the database.

Within huge companies, a help desk with human stuff is responsible for reset passwords for hundreds of persons a day, often it takes between 30 minutes and several hours for them to call the users back to give them the new passwords. So the companies makes loss because users cannot work for hours if they are having expired passwords or disabled accounts. To solve this problem, the use of the VOICE.TRUST Server is to automate password resets 24 hours a day, the only required hardware for this application on the users site is a telephone.

2.1.2 Definition of the TOE

The TOE contains a TTS interface, an IVR interface and a Decision Management Component, a Database interface, a Password Reset interface, a Mail interface and an Encryption interface.

These parts can also be seen as the core engine and the main security relevant section of the VOICE.TRUST Server, which is a biometric system for authentication via voice.

2.1.3 System Overview

During an interactive dialog via telephone a user is authenticated by biometric voice analysis, for which all telephone devices may be used. Users that have been authenticated successfully are allowed to use the service or portal application of the TOE, an automated password reset. A process description of how the password reset application within the TOE is taking place is: A user who is already enrolled in the TOE calls the TOE and says his user ID and several keywords. Following the system's prompts, the user is authenticated by the TOE using the characteristics of the voice of the user. The TOE then checks for authorization

and as a system with administration rights, completes the password reset online during the phone call and tells the new password to the user. With this password, the user may now log on to the required system and proceed working again.

The purpose of the TOE within the VOICE.TRUST Server is to authenticate the user. With scope of responsibility the VOICE.TRUST Server includes the interface to the telephone via the IVR system through the user is calling the TOE and allows the interactive dialog with the help of the TTS software. The VOICE.TRUST Server also communicates to the database, to the Password Reset systems and initiates the sending of e-mails. Figure 1 below gives an overview about the scope of the VOICE.TRUST Server and shows the application flow for a password reset.

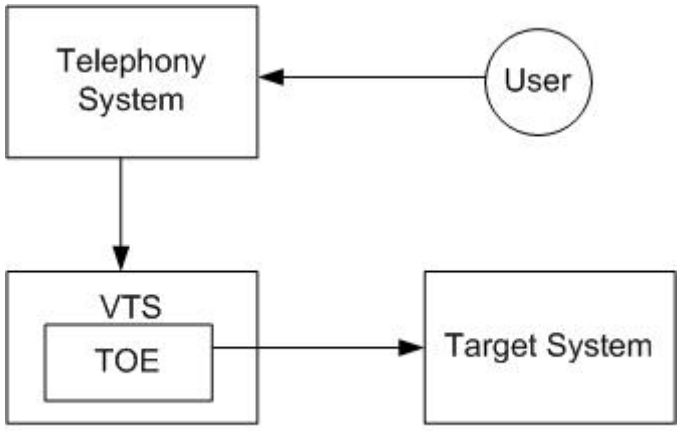


Figure 1: Schematic description of a password reset with the VOICE.TRUST Server in a single server installation. The TOE is shown as a part of the VOICE.TRUST Server as described in chapter 2.1.2.

Since the core security functions of the VOICE.TRUST Server are within the TOE itself, the following different techniques are used to achieve the highest possible level of security for the TOE:

1. **Access for registered users only.** A user has to be registered by the administrator of the TOE. A not registered person whose unique user ID is not known to the system cannot be enrolled.
2. **User Identification before enrolment.** A user has to be identified personally by his Super User before he is allowed to provide his speech data to the TOE. That way, a recursive trust chain can be established. Additionally, personal supervision by an experienced person improves the quality of the provided speech data.
3. **Claimed ID determination by Automated Speech Recognition (ASR).** A user's identity has to be clearly recognized by automated speech **recognition** (ASR) at the stage of login.
4. **Multi level authentication.** The user will be guided from the TOE through an authentication process with several steps.
5. **No status information during authentication sessions.** The user has to follow the multi level authentication process up to the end, only then he will get the information if he is succesfully authenticated or not.

6. **Fault-tolerant speech data collection.** Whenever a user provides an utterance that is inadequate for verification, the user gets a second chance to speak the required phrase.

The TOE stores the user data, as well as the platform access credentials necessary for the service applications like password reset, in an external database. All security relevant data are encrypted. For authenticated users the service application (password reset) is called. In a dialogue driven process, the user is prompted for the target systems on which he wants to reset his password. The connectivity between the TOE and the target platforms uses the protection mechanisms provided by the target platform. The Application Program Interface (API) of an administration client on the target is used for password reset purposes. It is recommended that this API is installed on the same machine as the TOE.

2.1.4 Roles

The following roles are important to mention for the rest of this ST.

- **Administrator**: The administrator is authorised to perform the administrative operations of the TOE. He manages the super users. The role of the administrator is not directly maintained by the TOE. It is part of the environment. The administrator administrates the TOE via the database in the environment.
- **Super user**: The super user has the permission to enrol other (normal) users.
- **Normal user**: The normal user is allowed to enrol himself in the TOE only if a super user initiates the call and forwards it to the normal user. After a successful authentication a normal user is allowed to perform password reset on the target platforms he is registered for.
- **Unauthorised user**: Users are not authorized as long as they are not known to the TOE or as long as they are not enrolled.
- **Attacker**: Person who want to be authenticated in order to get access unauthorized or to manipulate the TOE or its assets.

2.1.5 Configurations

The TOE within the VOICE.TRUST Server can be installed and used in two different configurations. In the single server installation, all components reside on a single machine, whereas the components in the multi server installation are distributed to several machines for scalability and redundancy reasons. Both solutions can be installed and managed by the same TOE version, but with different environment. Since the TOE will be evaluated in the single server configuration, the term VOICE.TRUST Server stands always for a single server installation including the data server component and the administration tools.

2.1.6 Range of Application

The authentication process is performed by the TOE via a telephone call. The generated authentication result can be used for various actions. Successfully authenticated users can

be transferred to any portal application with the help of an API. Therefore, multiple applications can use the Boolean results of the successful authentication.

The successful authentication result is used for a self service password reset. For this purpose the TOE is able to generate passwords which can be used to reset passwords on target systems.

With the automatic solution thereby the password reset mechanism of the target system is directly provided by the TOE. After the successful authentication and the examination of authorization for the target system, a password reset connector executes a fully automatic password reset for the appropriate target system. A fully automatic password reset means that the user gets the password from the TOE directly on the phone and can use it, what is the security relevant way of doing the password reset.

But with the TOE it is also possible to generate semi-automatic password resets. In this case an e-mail on the successful authentication and on the required platform is sent to the target platform administrator or to the help desk. The administrator can define for each target system, if an automatic or semi-automatic password reset should be possible.

The interface used for the integration to the target system is usually the API of an administration client provided by the target system. With a generic interface within the TOE, all target systems that can be integrated can be used for password reset, e.g. Windows, SAP or LDAP.

2.1.7 Processes: Enrolment, Authentication, Portal

Enrolment

The enrolment process is the basic process of the TOE and mandatory for every user and super user. Merely users enrolled in the TOE can use it later for password reset. Only authorised super users are allowed to initiate the enrolment process. After having verified himself, a super user hands over the call to the user to be enrolled.

By super user enrolment, a complete recursive trust chain can be guaranteed.

During the enrolment of an admitted person an interactive dialog assured the quality of the biometric template. Questions about individual parameters must be answered and get checked with respect to their quality.

A user is authorised for the use of the TOE after a successful enrolment procedure, when the biometric templates are stored as references for further authentications.

Authentication

When a user wants to initiate the authentication process the user has to dial the telephone number to be connected with the TOE. An interactive dialog starts. The user will be guided from the TOE through an authentication process with several steps, only in the end of these steps the user will get the information if he is succesfully authenticated or not.

2.2 Boundaries and logical interfaces

The following graphic (figure 2) shows the structure and the logical interfaces of the TOE with it's components within its environment.

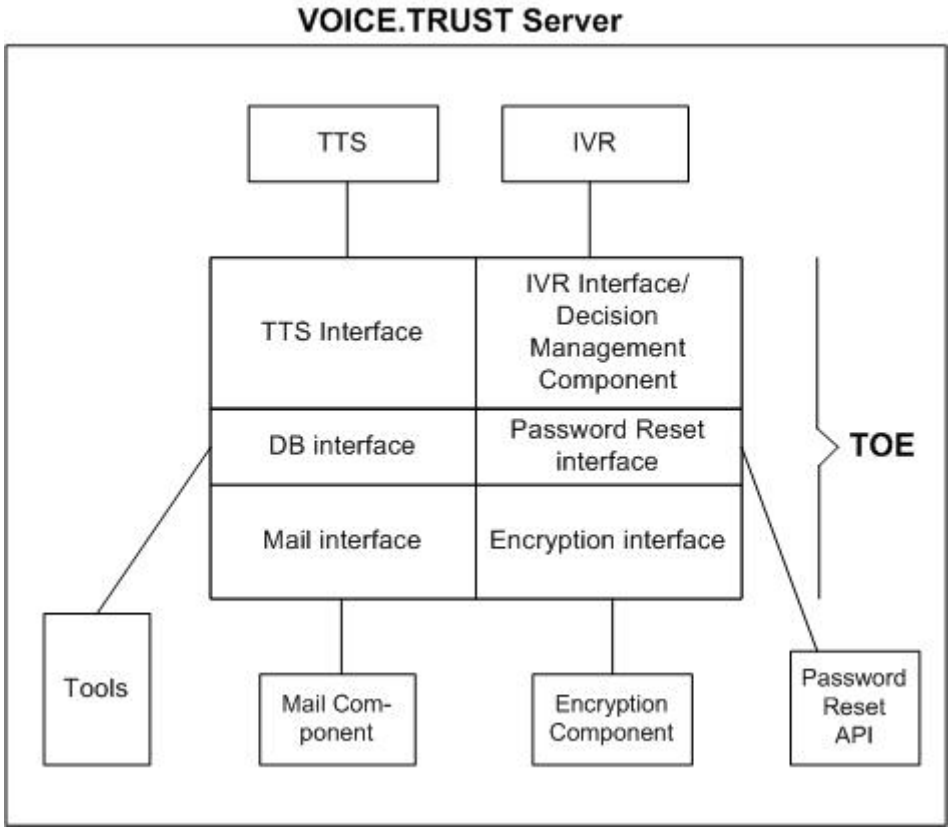


Figure 2: Overview about the role of the TOE in the VOICE.TRUST Server. The main modules of the TOE are a TTS interface, an IVR interface and a Decision Management Component, a Database interface, a Password Reset interface, a Mail interface and an Encryption interface.

In this section, all the modules of the TOE are described shortly to present the full functionality of the TOE.

Text To Speech (TTS) interface contains the Speech component and deals with the transformation of text fragments into speech.

Interactive Voice Response (IVR) interface and Decision Management Component contains the interactive dialog for enrollment and authentication.

The **Database Interface** is used by the TOE to communicate to an external data component and to the tools.

The **Mail Interface** is used by several other modules to send e-mails with an external mail component.

The **Password Reset Interface** includes all data manipulation logic up to the usage of target system APIs.

The **Encryption interface** connects the TOE with components in the environment that are used for encryption. Outside of the TOE but within the VOICE.TRUST Server there are Tools for the visualization of database content, a Mail Component for the mail function, a Password Reset API for connecting the target systems and an Encryption Component for the data security part.

The TTS module, a software for producing speech data out of text input, and an IVR software that initializes the telephony interface and talks to the TOE with the IVR interface/Decision Management Component of the TOE are also part of the VOICE.TRUST Server.

2.2.1 Differentiation

- The TOE does not protect database access connections or other connections of the TOE to applications outside the TOE by TOE means. To protect these connections, database means or protection means of the connected application are used.
- The TOE is not a password synchronization tool. Even if it is possible to reset several passwords in one session, the TOE will not reset a password on a platform that is not available in the moment the reset is attempted. When the platform is up and running again, the password will not be set because the user cancelled the call and the session is closed.
- The focus of the TOE with respect to the security of the password reset ends at the border of the TOE, the password reset interface. The TOE ensures that the required parameters for the target system are sent by an request from the password reset interface to the target system API. The TOE does not secure the password reset method call to the target system itself.
- The passwords the TOE generates are dependent from the password policy of the company that is using the TOE for password reset. Rules for the password constitution are stored in the database and may be adapted via scripts from the administrator.
- The TOE is not responsible for the authentication of the administrator.

3 TOE security environment

3.1 Assets

The primary asset of the TOE is the functionality to reset passwords on target systems.

The secondary assets are used by the TOE for authentication and access control of the users. This does especially cover (but is not limited to)

1. VoicePrints
2. UserData
3. Threshold settings for the authentication mechanism

3.2 Assumptions

The following conditions are assumed to exist in the operational environment of the TOE.

A.ADMINISTRATION

The administrator and the Super Users are well trained and can be trusted. The administrator reads the guidance documentation carefully, understands the details of them and informs the trustworthy Super User about the secure usage of the TOE. Moreover the administrator is responsible to oversee the system requirements and also has to oversee the rates for false acceptance and false rejection to guarantee the keeping.

A superuser is responsible to ensure the correct enrolment of each user.

A.EQUIPMENT

The necessary infrastructure like telephone set and LAN network are available. In the telephony network only voice services are allowed (no data services).

It is assumed that the LAN network to which the TOE is connected is secure. The network to which the TOE is connected is internal and protected from unspecific access. LAN's with internet connections are protected, appropriate firewalls are installed. Therefore unauthorised access from the external networks is prevented. In addition, no users, unauthorised users or attackers can perform the direct attacks against the internal network such as eavesdropping of packets.

It is assumed that the telephones that are used for enrolment are secured and securely connected to the TOE so that a sniffing of the enrolment process is not possible.

It is assumed that the environment provides a database to be used by the TOE to store TSF data in.

It is assumed that at least one superuser has been enrolled to the TOE before the operation of the TOE starts.

The external database has to have the same level of protection as the TOE. Furthermore it is assumed that the database provides an identification/authentication mechanism and an

access control mechanism to ensure that only the administrator is able to edit the TSF data within the database.

A.FALLBACK

It is assumed that any alternative or fallback identification/authentication system, used when the TOE is not in operation, offers adequate protection of the assets. However the security of the fallback system is outside the scope of the evaluation.

This means that even if the scope of the TOE is, to perform actions that are usually done by a callcenter/helpdesk, a helpdesk is still needed. The helpdesk is then responsible to handle the requests of the users who are not able to use the TOE or were rejected by the TOE or of all users if the TOE is out of order.

A.PHYSICAL

Physical access to the hardware is not allowed for unauthorised users (only administrator). The TOE is physically protected, firewall protected and state of the art protected against sniffing and malware.

3.3 Threats

The following threats are addressed either by the TOE or the environment or by a combination of them.

T.IMPERSONATION

Description

An attacker tries to get verified by the TOE as another user. Therefore he just claims the user ID of another (enrolled) user to the TOE but uses his own voice to get verified. The attacker may also uses other persons' voice (by convincing/bribing/extorting other persons to help him) and tries to attack more than one enrolled users of the TOE.

The attacker does only need to have public knowledge about the TOE for this attack but of course he has to know a valid user ID. It is also well known that even authorised users sometimes try to get authorised as another user just because of their curiosity about the reliability of the TOE. Therefore such an attack could also be performed without any real hostile intention of the attacker.

Aim

The aim in this attack is to reset a password on a target system where the attacked user has rights on.

T.ENHANCE_PRIV

Description

An enrolled user tries to enhance his privileges after he was successfully verified by the TOE. No special but only general knowledge of the TOE is necessary to plan and perform this kind of attack. After a successful verification process each user is asked for which

system he would like to reset a password and each user can try to reset a password on a system where he has no rights on.

Aim

This attack could have two aims:

1. A user tries to reset a password on a target system where he has no rights on
2. A user tries to become a super user and therewith tries to get able to start the enrolment procedure for another user although is not allowed to start this process.

The scope of an attacker in this threat of this threat is not to get verified with a wrong identity but to enhance his privileges after he has been verified with his own identity. This threat therefore does not address the biometric verification part of the TOE but the functionalities that are used to allow an authorized user to reset passwords or to start enrolment processes after they have been successfully authenticated.

T.REPLAY

Description

An attacker tries to record a verification session of an enrolled user and uses this recorded speech data to get verified as the attacked user. This threat is quite similar to T.IMPERSONATION but the attacker needs to have another background to perform this attack because he has to be able to record a verification session of another user.

No special but only general knowledge is needed to plan/perform such an attack. It is obviously that this threat exists on a speech based system. The attacker needs some technical equipment to record the voice of an authorized user but in general each voice recorder is sufficient.

Aim

The aim in this attack is to reset a password on a target system where the attacked user has rights on.

T.REPRODUCE

Description

An attacker tries to imitate the voice of an enrolled and authorised user to get verified as the attacked user.

Due to the fact that voice imitation (especially of politicians) is well known today, no special knowledge is needed to identify and plan this threat. But of course imitating the voice of another user needs much exercise and some voice examples of this user for exercising.

Aim

The aim in this attack is to reset a password on a target system where the attacked user has rights on.

3.4 Organisational security policies

The TOE must comply by the following organisational security policies:

OSP.ENROL

Each biometric verification process requires that the user whose identity should be verified has been enrolled previously. The generic description of such an enrolment process can be found in chapter 2.1.7.

In order to use the TOE each user has to go through an enrolment process. Therefore the TOE has to provide an enrolment mechanism. The TOE has to ensure that only voice data with sufficient quality is used for the enrolment process.

Furthermore the TOE has to ensure that only users can be enrolled whose data has been added to the external database by an administrator before and that the process of enrolment is only performed by a user while observed by a super user.

4 Security objectives

4.1 Security objectives for the TOE

O.AUDIT_REACTION

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

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

Messages can be sent to authorised users and the administrator (monitoring and reaction in case of unwanted authorisation). 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,

- Replay or brute force attacks against the same identity. This means that the reaction part of this objective should realize a mechanism through which more than an administrator defined number of unsuccessful verification attempts with the same claimed identity are blocked.
- Less quality: This means that the verification process should be stopped if the voice data does not have sufficient quality
- Session termination: If a user is not reacting to questions of the TOE during a session for a certain time period, this session will be terminated.

O.I&A (Identification & Authentication)

The TOE shall provide a biometric verification mechanism using voice data to ensure access to the primary assets

- The TOE shall process only its own templates from the enrolment process (consideration of integrity and authenticity).
- The templates as well as the recorded voice data during the verification shall suffice minimum quality standards and be compatible among each other.

The TOE shall meet national and/or international criteria for false acceptance rate (FAR) (see [BEM]).

O.ENROL

To provide a biometric verification mechanism this process is needed in the TOE.

The user that has to be enrolled presents his user ID to the TOE and after this the TOE acquires the voice data from the user and “learns” to link the user’s identity with the characteristic of his voice.

The TOE shall provide such an enrolment process. The voice data acquired from a user during the enrolment process has to be checked with respect to consistency before a template is generated.

O.ROLES_ACCESS

The TOE has to maintain the roles of

- users,
- super users and
- administrators.

The TOE shall limit the ability to reset a password in a target system to a user who has sufficient privileges, who is enrolled and who gets authenticated by the TOE.

Additionally the TOE has to limit the ability to start an enrolment process to a super user who was authenticated by the TOE and the TOE has to ensure that only a user whose data has been added to the database in the environment before is allowed to be enrolled.

4.2 Security objectives for the environment

OE.ADMINISTRATION

The administrator and the super users are well trained and can be trusted. The administrator reads the guidance documentation carefully, understands the details of them and informs the trustworthy super user about the secure usage of the TOE. Moreover the administrator is responsible to oversee the system requirements and also has to oversee the rates for false acceptance and false rejection to guarantee the keeping.

A superuser is responsible to ensure the correct enrolment of each user.

OE.EQUIPMENT

The necessary infrastructure like telephone set and LAN network are available. In the telephony network only voice services are allowed (no data services).

It is assumed that the LAN network to which the TOE is connected is secure. The network to which the TOE is connected is internal and protected from unspecific access. LAN's with internet connections are protected, appropriate firewalls are installed. Therefore unauthorised access from the external networks is prevented. In addition, no product users, unauthorised users or attackers can perform the direct attacks against the internal network such as eavesdropping of packets.

It is assumed that the telephones that are used for enrolment are secure and securely connected to the TOE so that a sniffing of the enrolment process is not possible.

The environment provides a reliable time stamp mechanism.

It is assumed that the environment provides a database to be used by the TOE to store TSF data in.

At least one superuser has been enrolled to the TOE before the operation of the TOE starts[1].

The external database has to have the same level of protection as the TOE. Furthermore it is assumed that the database provides an identification/authentication mechanism and an access control mechanism to ensure that only the administrator is able to edit the TSF data within the database.

OE.FALLBACK

The environment provides an alternative or fallback identification/authentication system that is used when the TOE is not in operation and that offers adequate protection of the assets. However the security of the fallback system is outside the scope of the evaluation.

This means that even if the scope of the TOE is, to perform actions that are usually done by a callcenter/helpdesk, a helpdesk is still needed. The helpdesk is then responsible to handle the requests of the users who are not able to use the TOE or were rejected by the TOE or of all users if the TOE is out of order.

OE.PHYSICAL

Physical access to the hardware is not allowed for unauthorised users (only administrator). The TOE is physically protected, firewall protected and state of the art protected against sniffing and malware.

OE.EQUIPMENT includes IT requirements for the environment (a reliable timestamp mechanism and the functions of the database). These requirements are described in chapter 5.3 more detailed. All the other objectives for the environment do only contain non IT requirements.

[1] Application Note: Furhter details will be given within the evidence documentation for ADO_IGS

5 IT Security Requirements

5.1 TOE security requirements

This chapter describes the security functional and the assurance requirements which have to be fulfilled by the TOE. The requirements consist of functional components from Part 2 of CC and an Evaluation Assurance Level (EAL2) which include components from Part 3 of the CC. Furthermore chapter 5.2 contains an extended functional requirement for the TOE.

5.1.1 TOE security functional requirements

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

No.	SFR	Dependency
	FAU	
1.	FAU_ARP.1	FAU_SAA.1
2.	FAU_GEN.1	FPT_STM.1
3.	FAU_GEN.2	FAU_GEN.1, FIA_UID.1
4.	FAU_SAA.1	FAU_GEN.1
	FDP	
5.	FDP_ACC.1	FDP_ACF.1
6.	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
	FIA	
7.	FIA_AFL.1	FIA_UAU.1, FPT_STM.1
8.	FIA_ATD.1	-
9.	FIA_UAU.1	FIA_UID.1
10.	FIA_UAU.3	-
11.	FIA_UAU.7	FIA_UAU.1
12.	FIA_UID.2	FMT_SMR.1
13.	FIA_ENR.1	FMT_SMR.1
	FMT	
14.	FMT_SMR.1	FIA_UID.1
	FTA	
15.	FTA_SSL.3	-

Table 1: TOE security functional requirements

The following subchapters describe the functional requirements with respect to the TOE and drawn from the standard set of functional components listed in CC part 2.

5.1.2 Security Audit (FAU)

5.1.2.1 Security audit automatic response (FAU_ARP)

FAU_ARP.1: Security alarms

Hierarchical to: No other components.

FAU_ARP.1.1 The TSF shall *inform an administrator and lock the user account that is related to the security violation* upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

5.1.2.2 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[2]; and

c) *none*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, 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, *none*

Dependencies: FPT_STM.1 Reliable time stamps

No.	SFR	Audit data	Remark
	FAU		
1.	FAU_ARP.1	Actions taken due to imminent security violations	-
2.	FAU_GEN.1	-	
3.	FAU_GEN.2	-	
4.	FAU_SAA.1	Automated response generated by the tool	It is not possible to disable the analyse mechanism. So this event is not audited.
	FDP		
5.	FDP_ACC.1	-	
6.	FDP_ACF.1	All requests to perform an operation on an object covered by the SFP	
	FIA		
7.	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	

[2] Application note: See also table 3

No.	SFR	Audit data	Remark
		(e.g. re-enabling of a terminal).	
8.	FIA_ATD.1	-	
9.	FIA_UAU.1	All use of the authentication mechanism	
10.	FIA_UAU.3		
11.	FIA_UAU.7	-	
12.	FIA_UID.2	All use of the user Identification mechanism, including the user Identity provided	
13.	FIA_ENR.1	The result of the enrolment process and the ID of the super user that allowed this process	
	FMT		
14.	FMT_SMR.1	Modifications to the group of users that are part of a role	
	FTA		
15.	FTA_SSL.3	Termination of an interactive session by the SF	

Table 2: Auditable events

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

5.1.2.3 Security audit analysis (FAU_SAA)

FAU_SAA.1: Potential violation analysis

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

- *Unsuccessful authentication attempts*

known to indicate a potential security violation;

b) *none*

Dependencies: FAU_GEN.1 Audit data generation

5.1.3 User data protection (FDP)

5.1.3.1 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 *DAC* on

- *Subjects: users (normal or super users)*
- *Object: enrolment process, password reset*
- *Operations: start, perform*

Dependencies: FDP_ACF.1 Security attribute based access control

5.1.3.2 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 *DAC* to objects based on *the following*:

- *The unique ID of the user who is performing a request to an object*
- *ACL (Access Control Lists)*
- *The role, the user belongs to (normal or super user)*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- *If the operation requested is to start an enrolment process:*
  - *Allow the request if the user requesting is a superuser*
  - *Else: Deny the request*
- *If the operation requested is to perform a password reset:*
  - *If the operation is explicitly allowed in an ACL, allow the operation*
  - *Else: deny the operation*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on *no further rules.*

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

5.1.4 Identification and authentication (FIA)

5.1.4.1 Authentication failures (FIA_AFL)

FIA_AFL.1: Authentication failure handling

Hierarchical to: No other components

FIA_AFL.1.1 The TSF shall detect when *3* unsuccessful authentication attempts occur related to *one user account since the last successful authentication attempt of this user or within the last 24 hours.*

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *lock the users account and inform an administrator.*

Dependencies: FIA_UAU.1 Timing of authentication

FPT_STM.1 Reliable time stamps[3]

5.1.4.2 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 unique identifier*
- *Counter of consecutive failed authentication attempts*
- *Flag whether this user object is disabled*
- *Flag whether a complete enrolment exists for this user*
- *The role, this user belongs to*
- *E-mail address to inform the user*

Dependencies: No dependencies

5.1.4.3 User authentication (FIA_UAU)

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow *the identification process* on behalf of the user to be performed before the user is authenticated.

[3] Application Note: The dependency to FPT_STM.1 has been added because of the second assignment in FIA_AFL.1.1. Without a reliable time stamp mechanism the TSF would not be able to determine the interval of 24 hours.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.3 Unforgeable authentication

Hierarchical to: No other components.

FIA_UAU.3.1 The TSF shall prevent use of authentication data[4] that has been forged by any user of the TSF.

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

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 that the authentication process has been started* to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

5.1.4.4 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

[4] Application Note: Where authentication data means the voice of the user.

5.1.5 Security management (FMT)

5.1.5.1 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

- *Super user*
- *User*

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

Dependencies: FIA_UID.1 Timing of identification

5.1.6 TOE Access (FTA)

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1 The TSF shall terminate an interactive session after *30 seconds.*

Dependencies: No dependencies

5.2 Extended TOE Functional Security Requirements

Biometric systems require an enrolment process for each user before they are able to verify the identity of a user.

5.2.1 Enrolment (FIA_ENR)[5]

FIA_ENR.1: Enrolment

Hierarchical to: No other components.

FIA_ENR.1.1: The TSF shall provide an enrolment mechanism to acquire *the voice data* of a user and associate this data with the identity of the user.

FIA_ENR.1.2 The TOE shall apply the following rules to determine that the acquired speech data has a sufficient quality to be used by the biometric verification mechanism of the TOE: *The rules addresses:*

- *Loud-/Quietness of signal space*
- *Duration of signal space*
- *Signal –to-Noise Ratio*
- *Consistency of the user's speech utterances*

The rules can be seen in detail in the corresponding confidential Security Target.

Dependencies: No dependencies

[5] Application Note: See also Chapter 9

5.3 Minimum strength of function (SOF) claim

The minimum level of strength of the security functions that are fulfilling the security requirements stated in chapter 5.1and 5.2 is to be **SOF-medium**.

5.4 Security requirements for the environment

The IT requirements as stated in OE.EQUIPMENT are described in this chapter using SFRs from part II of [CC]. The refinements in theses requirements are used to adopt the SFRs from part II of [CC] to the environment.

Because these requirements describe the environment of the TOE the dependencies of the SFRs are not considered.

5.4.1 Security management (FMT)

5.4.1.1 Management of security attributes (FMT_MSA)

FMT_MSA.1: Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The **database in the environment** shall enforce the *an appropriate access policy* to restrict the ability to change default, query, modify, delete, the security attributes

- *All data that is or will be used by the TOE esp.*
- *The unique ID of the user who is performing a request to an object*
- *ACL (Access Control Lists)*

to *administrators.*

Dependencies [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MSA.3: Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The **database in the environment** shall enforce *an appropriate access policy* to provide restrictive, default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The **database in the environment** 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

5.4.1.2 User authentication (FIA_UAU)

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU.1.1 The **database in the environment** shall allow *the identification process* on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The **database in the environment** shall require each user to be successfully authenticated before allowing any other **actions** on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

5.4.1.3 User Identification (FIA_UID)

FIA_UID.2: User Identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1 The **database in the environment** shall require each user to identify itself before allowing any other **actions** on behalf of that user.

Dependencies: No dependencies

5.4.2 Time Stamps (FPT_STM)

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The **environment** shall be able to provide reliable time stamps **to be used by the TOE**.

Dependencies: No dependencies

5.5 TOE security assurance requirements

The TOE is to fulfil the assurance requirements according to evaluation assurance level EAL2 as regards the functionality requirements. All these requirements are listed in the table shown below.

Assurance class	Components	Description
Security Target Evaluation	ASE_DES.1	TOE Description
	ASE_ENV.1	Security environment
	ASE_INT.1	ST Introduction
	ASE_OBJ.1	Security objectives
	ASE_PPC.1	PP claims
	ASE_REQ.1	IT security requirements
	ASE_SRE.1	Explicitly stated IT security requirements
	ASE_TSS.1	TOE summary specification
Configuration management	ACM_CAP.2	Configuration Items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation & start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE-security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 3: Assurance requirements for EAL2

6 TOE summary specification

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements as stated in the previous chapter.

6.1 Security functions

A description of each of the TOE security functions follows.

SF.AUDIT&REACTION

The TOE generates audit records for the enrolment and the identification and authentication process and stores this audit information within the database of the environment.

For each audit event the TOE saves information about date and time of the event, the type of the event, the result of this event and identity of the user that caused the event as far as this identity is already available. Furthermore this function audits the start up and shutdown of itself.

The reaction part of this SF terminates a call with a user if the user is not longer responding. The TOE also informs about security relevant actions by sending e-mails for different actions, so if an administrator, super user or user gets a mail for an action he never did, an impostor attack can be assumed. This gives the possibility to react adequately to these attacks.

We can classify this e-mail functionality into several groups:

The first group contains an e-mail for a successful enrolment to the user who enrolled in the system and the super user who enrolled the user.

Further the TOE initiates e-mails for a successful or failed password reset. For a successful password reset for a system the mail contains the status OK, for a failed reset an error message is given. This e-mail is sent to the enrolled user and the administrator.

This function also audits each unsuccessful authentication attempts against a users account. Therefore a third group of e-mails is sent by the TOE if a user gets rejected or disabled. The user and the administrator will get an e-mail that the users account is disabled.

SF.ENROL

The enrolment of a user into the TOE is the basic action for using the TOE for password reset.

To start this process the super user has to authenticate himself and is then able to start an enrolment procedure for another user and can handover the phone to the user.

Another pre-condition for the ability of a user to enrol in the TOE is that his user ID is added to the TOE database in the environment. Without these two preconditions fulfilled a user' enrolment attempt will be rejected by the TOE. If a user ID of a user is not in the database and this user is calling the TOE, he is not able to enrol because the TOE cannot find his user ID. In these cases the TOE proposes another user ID to the user that sounds similar to the one the user said and asks the user whether this is his ID. The TOE is only doing this twice before the user is finally rejected for enrolment and he can try again later.

If the TOE found the user ID the user prompted, the application flow for the rest of the process is as follows:

1. The user is asked to say his user ID
2. The user has to repeat several keywords

If the TOE is not able to understand the user, he will ask the user to repeat the word. If the user is not repeating any more, the TOE will disconnect the call.

Before generating a template (which means to connect the ID of the user with his speech data) the consistency of the voice data is checked by the TOE. In this way it is ensured that the produced templates do have sufficient quality to be used by SF.I&A. The following techniques are used for quality assurance:

Loud-/Quietness of signal space

Duration of signal space

Signal –to-Noise Ratio

Consistency of the user's speech utterances

Furthermore the enrolment process is only allowed to be performed from a secure telephone as stated in A.EQUIPMENT.

SF.I&A

The SF.I&A is the core functionality of the TOE. It allows verifying the identity of a user using the characteristics of his voice. If a user likes to get identified and authenticated by the TOE he calls the TOE. During the process of authentication is running, no feedback (about the single steps) is given to the user. The user is informed about the result of the process after he performed all steps even if the system decides to reject the user after the first authentication step.

The overall False Acceptance Rate for this identification/authentication process is less than 1/10000.

Before a user gets rejected by the TOE, he can attempt 3 trials within 24 hours per standard. If the maximum number of attempts is reached, the user account is disabled and the user will not get the possibility to authenticate any more. He is asked to call again or will be transferred to the Help Desk.

SF.ROLES_ACCESS

The TOE maintains several different roles, the role of a user and of a super user.

For each user this SF maintains the following attributes:

- A unique identifier
- Counter of consecutive failed authentication attempts
- Flag whether this user object is disabled
- Flag whether a complete enrolment exists for this user
- The role this user belongs to
- E-mail address to inform the user

The role of (normal) users is the role with the least privileges. This role is allocated to all the users authenticating within the TOE via telephone for password reset without physical access to the TOE. This role contains the permission to enrol in the TOE only with the assistance of the super user through super user enrolment and to reset passwords in selected target systems for which they are having access permissions.

The role of super user includes in contrast to the role of normal users also the permission to enrol in the TOE on their own and to start the enrolment process for other users. Apart from that their role matches the role of the normal user.

So this SF ensures that a user is only able to enrol to the TOE with the assistance of a superuser. Furthermore this SF ensures that only a user whose ID exists in the database in the environment is allowed to enrol into the TOE.

The role of the administrator has the intention of administer and manage the TOE. But the maintenance of this role is done by the database in the environment.

Beside the management of these roles, the TOE ensures that a successfully authenticated user is only allowed to reset a password of a target system where he has the appropriate permissions for. This check is realized through access control lists (ACL) which are administrated in the environment. The TOE only checks if the ACL contains the permission for the user if a user tries to reset a password on a target system. If the ACL does not contain this permission, the request of the user is rejected.

This SF also ensures that a user is not allowed to perform any action before he has been successfully identified and authenticated by SF.I&A.

After a user has been successfully authenticated this function provides the possibility to reset a password on a target system if the user has the sufficient permission for this system.

6.2 Strength of function claims

Only SF.I&A is based on a probabilistic mechanism.

In accordance with the required minimum strength level, the strength of the security functions SF.I&A must reach SOF-medium and a maximum FAR of 1/10000 according to [BEM].

6.3 Assurance measures

The TOE is to fulfil the assurance requirements of assessment class ASE and of evaluation level EAL2. The present document "Security Target" serves to fulfil the requirements according to ASE. Besides the TOE (according to ATE_IND.2), the manufacturer will provide the following additional documents within the frame of the evaluation, to evidently prove the fulfilling of the requirements according to EAL2:

- Configuration management documentation (according to ACM_CAP.2)
- Delivery and operational documentation (according to ADO_DEL.1 and ADO_IGS.1)
- Informal functional specification (according to ADV_FSP.1)
- Security enforcing high-level design (according to ADV_HLD.1)
- Assignment description (according to ADV_RCR.1)
- Administrator and user guidance documentation (according to AGD_ADM.1 and AGD_USR.1)
- Test documentation (according to ATE_COV.1 and ATE_FUN.1)
- Vulnerability analysis (according to AVA_SOF.1 and AVA_VLA.1)

7 PP claims

There is **no** Protection Profile claimed to which this [ST] is conformant.

8 Rationale

8.1 Security objectives rationale

8.1.1 Coverage of the Security Objectives

In this section it is proven that the security objectives described in section 4 can be traced for all aspects identified in the TOE-security environment and that they are suited to cover them.

At least one security objective results from each assumption and each threat. At least one threat or assumption exists for each security objective.

	O.AUDIT_REACTION	O.I&A	O.ENROL	O.ROLES_ACCESS	OE.ADMINISTRATION	OE.EQUIPMENT	OE.FALLBACK	OE.PHYSICAL
A.ADMINISTRATION					X			
A.EQUIPMENT						X		
A.FALLBACK							X	
A.PHYSICAL								X
T.IMPERSONATION	X	X						
T.ENHANCE_PRIV				X				
T.REPLAY	X	X						
T.REPRODUCE	X	X						
OSP.ENROL			X					

Table 4: Assignment: assumptions / threats / OSP – security objectives

The security objective **O.AUDIT_REACTION** can be traced back to the threats **T.IMPERSONATION**, **T.REPLAY** and **T.REPRODUCE** because it detects insecure states of the TOE (esp. a configurable number of unsuccessful authentication attempts) and reacts in an appropriate way (by locking the user account)

The security objective **O.I&A** can be traced back to the threats **T.IMPERSONATION**, **T.REPLAY** and **T.REPRODUCE** as this objective describes that the authentication mechanism of the TOE has to resist these types of attacks.

The security objective **O.ROLES_ACCESS** can be traced back to the threats **T.ENHANCE_PRIV** as it describes the maintenance of roles and user based access rights in the TOE that counter **T.ENHANCE_PRIV**.

The security objective **O.ENROL** can directly be traced back to **OSP.ENROL** as **O.ENROL** defines that the TOE has to provide an enrolment mechanism that provides the functionality as demanded in **OSP.ENROL**.

The objective for the environment **OE.ADMINISTRATION** can be traced back to **A.ADMINISTRATION** as directly follows.

The objective for the environment **OE.EQUIPMENT** can be traced back to **A.EQUIPMENT** as directly follows.

The objective for the environment **OE.FALLBACK** can be traced back to **A.FALLBACK** as directly follows.

The objective for the environment **OE.PHYSICAL** can be traced back to **A.PHYSICAL** as directly follows.

8.1.2 Countering the Threats

Threat **T.IMPERSONATION** is fully countered by **O.AUDIT_REACTION** (because it locks accounts after a configurable number of unsuccessful authentication attempts) and **O.I&A** (as this objective describes the authentication mechanism of the TOE that has to be reliable enough.)

Threat **T.ENHANCE_PRIV** is fully countered by security objective **O.ROLES_ACCESS** as this objective describes the functionality to realize role and user based access control.

Threat **T.REPLAY** is countered by O.I&A as this objective describes that the authentication mechanism of the TOE has to resist a replay attack and **O.AUDIT_REACTION** because it locks accounts after a configurable number of unsuccessful authentication attempts.

Threat **T.REPRODUCE** is countered by **O.I&A** as this objective describes that the authentication mechanism of the TOE has to resist a mimic attack and **O.AUDIT_REACTION** because it locks accounts after a configurable number of unsuccessful authentication attempts.

8.1.3 Coverage of Organisational Security Policies

The organisational security policy **OSP.ENROL** is directly met by **O.ENROL** as **O.ENROL** defines that the TOE has to provide an enrolment mechanism that provides the functionality as demanded in **OSP.ENROL**.

8.1.4 Coverage of the Assumptions

A.ADMINISTRATION is covered by **OE.ADMINISTRATION** as directly follows.

A.EQUIPMENT is covered by **OE.EQUIPMENT** as directly follows.

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

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

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

8.2 Security requirements rationale

8.2.1 Fulfilment of TOE security objectives

This chapter proves that the set of security requirements (TOE) is suited to fulfil the security objectives described in chapter 4.1 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.I&A	O.ENROL	O.ROLES_ACCESS
FAU_ARP.1	X			
FAU_GEN.1	X			
FAU_GEN.2	X			
FAU_SAA.1	X			
FDP_ACC.1				X
FDP_ACF.1				X
FIA_AFL.1		X		
FIA_ATD.1		X		
FIA_UAU.1		X		
FIA_UAU.3		X		
FIA_UAU.7		X		
FIA_UID.2		X		
FIA_ENR.1			X	
FMT_SMR.1				X
FTA_SSL.3	X			

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

As shown in the previous table, every SFR adresses at least one objective.

The coverage of the objectives by the SFR is described in the following paragraphs.

O.AUDIT_REACTION

FAU_ARP.1 ensures that the TOE reacts in case of a potential security violation. **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 5.1.2.2) and **FAU_GEN.2** supports the user ID association in order to be able to hold users accountable for their actions. These two requirements fulfil the audit part of this objective.

	FTA_SSL.3 realizes the session termination after a certain period of user inactivity.
O.I&A	**FAU_AFL.1** ensures that a user account is locked after three unsuccessful authentication attempts. **FIA_ATD.1** describes the attributes, the TOE has to maintain for each user, **FIA_UAU.1** ensures that each user has to be authenticated before any other action than user identification is allowed, **FIA_UAU.7** ensures that no unnecessary information are given to a user during the authentication process and **FIA_UID.2** ensures that each user has to be identified before any other action is allowed. **FIA_UAU.3** ensures that the TOE is able to prevent forged and replayed speech data for authentication.
O.ENROL	**FIA_ENR.1** as explicitly stated SFR directly fulfils **O.ENROL**.
O.ROLES_ACCESS	**FDP_ACC.1** and **FDP_ACF.1** describe the access control functions of the TOE while **FMT_SMR.1** describes the roles the TOE has to know.

8.2.2 Fulfilment of TOE SFR dependencies

The following table shows that all dependencies among the chosen SFRs from part II of [CC] are satisfied.

No.	SFR	Dependency	Dependency Fulfilled?[6]
	FAU		
1.	FAU_ARP.1	FAU_SAA.1	YES
2.	FAU_GEN.1	FPT_STM.1	YES (E)
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 (E)
	FIA		
7.	FIA_AFL.1	FIA_UAU.1, FPT_STM.1	YES (E)
8.	FIA_ATD.1	-	
9.	FIA_UAU.1	FIA_UID.1	YES
10.	FIA_UAU.3	-	
11.	FIA_UAU.7	FIA_UAU.1	YES
12.	FIA_UID.2	-	
13.	FIA_ENR.1	-	
	FMT		
14.	FMT_SMR.1	FIA_UID.1	YES
	FTA		
15.	FTA_SSL.3	-	

Table 6: Fulfilment of the dependencies between the SFRs

8.2.3 Suitability of minimum strength of function (SOF) level

Against the background of the selected operational environment and the application case (password reset system), the chosen minimum strength level SOF-medium makes sense and is consistent with the security objectives.

To use a SOF level of medium even if the evaluation only includes AVA_VLA.1 makes sense because in a biometric system the SOF level is mainly influenced by the FAR of the biometric authentication system. The FAR is a very important quality aspect of each biometric system. Therefore the SOF-level of an evaluation of a biometric system should try to fulfil the highest SOF-level possible.

The explicit strength metrics in form of required FAR is determined using the specified international interpretations [BEM]. The FAR of the TOE has to be less than 1/10000.

8.2.4 Fulfilment of the objective for the environment

As described in chapter 4.2 **OE.EQUIPMENT** contains IT requirements for the environment that are described in form of SFRs in chapter 5.3.

OE.EQUIPMENT requires a time stamp mechanism which is sufficiently described by the use of **FPT_STM.1**

OE.EQUIPMENT requires that the database in the environment that is used by the TOE has the possibility to identify/authenticate an administrator what is sufficiently described by the use of **FIA_UAU.1** and **FIA_UID.2.** Furthermore **OE.EQUIPMENT** requires that only the administrator is able to change the behaviour of the functions of the TOE. This is adressed by the use of, **FMT_MSA.1** and **FMT_MSA.3.**

8.2.5 Assurance requirements rationale

To select the assurance class ASE is obligatory for the evaluation of a concrete TOE.

The selection of the EAL level will prove to be suitable, if the rating is appropriate to the assurance resulting here from. The selected level EAL2 ensures a medium 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 basic security requirements.

The selected level EAL2 includes the component AVA_VLA.1 which requires that the manufacturer identifies all evident weaknesses of the TOE and proves that these cannot be exploited. The evaluator checks this on the basis of a penetration test. In view of the operational environment, no explicit attack potential for exploiting the weaknesses of the TOE is utilized. A typical attacker starts at the telephone and directly attacks security function SF.I&A. For this reason, a SOF Claim of medium is postulated. Considering the fact that SOF-medium is postulated as minimum strength level of the security functions of the TOE, it is justified to have selected EAL2.

[6] (E) means that at least one dependency of this SFR is satisfied within the environment

Furthermore the selected Assurance Level EAL2 is applicable and appropriate for the explicitly stated SFR FIA_ENR.1. This follows out of the fact that the described enrolment process is needed to perform the functions for identification and authentication out of class FIA which are adequately addressed by the assurance requirements of EAL2. It is also shown by the fact this explicitly stated SFR belongs to the class FIA in its notation.

8.2.6 Dependencies and mutual support

The dependencies of the assurance requirements are fulfilled automatically, since no other had been selected than all components of assessment class ASE and all components of evaluation level EAL2 (within ASE and within EAL2 all dependencies are fulfilled).

8.3 TOE summary specification rationale

8.3.1 Coverage of the SFR by the SF

The following table and subclasses show which Security Functions of the TOE fulfil which SFRs.

	SF.AUDIT_REACTION	SF.I&A	SF.ENROL	SF.ROLES_ACCESS
FAU_ARP.1	X	X		
FAU_GEN.1	X			
FAU_GEN.2	X			
FAU_SAA.1	X			
FDP_ACC.1				X
FDP_ACF.1				X
FIA_AFL.1	X	X		
FIA_ATD.1				X
FIA_UAU.1				X
FIA_UAU.3		X		
FIA_UAU.7		X		
FIA_UID.2				X
FIA_ENR.1			X	
FMT_SMR.1				X
FTA_SSL.3	X			

Table 7: Coverage of the SFRs by SF

FAU_ARP.1 is realized in **SF.AUDIT_REACTION** as this SF audits each unsuccessful authentication attempt and informs an administrator about that.

FAU_ARP.1 is realized by **SF.I&A as this SF** realizes three unsuccessful authentication attempts and locks the related user account.

FAU_GEN.1 is realized by **SF.AUDIT_REACTION** as this SF audits the start up and shutdown of audit functions and all other required events and associates the required information with each audit event.

FAU_GEN.2 is realized by **SF.AUDIT_REACTION** as this SF links the identity of the user who caused an event to the audit event.

FAU_SAA.1 is realized by **SF.AUDIT_REACTION** as this SF realizes an unusual high amount of authentication attempts against a user account.

FDP_ACC.1 and **FDP_ACF.1** are realized by **SF.ROLES_ACCESS** as the access control is implemented there.

FIA_AFL.1 is realized by **SF.I&A** as this SF realizes three unsuccessful authentication attempts and locks the related user account.

FIA_AFL.1 is realized by **SF.AUDIT_REACTION** as this SF audits each unsuccessful authentication attempt and informs an administrator about that.

FIA_ATD.1 is realized by **SF.ROLES_ACCESS** as this SF maintains the required attributes for each user.

FIA_UAU.1 is realized by **SF_ROLES_ACCESS** as this SF requires each user to be successfully authenticated before allowing any other action than user identification.

FIA_UAU.3 is realized by **SF.I&A** as the SF counters replay attacks by asking for randomly chosen words.

FIA_UAU.7 is realized by **SF.I&A** as this SF describes that no feedback is given to the user about the results of authentication as long as this process is running.

FIA_UID.2 is realized by **SF.ROLES_ACCESS** as this SF requires each user to get identified before allowing any other action.

FIA_ENR.1 is realized by **SF.ENROL** as directly follows.

FMT_SMR.1 is realized by **SF.ROLES_ACCESS** as this SF describes the roles, the TOE knows for users.

FTA_SSL.3 is realized by SF.AUDIT_REACTION as directly follows.

8.3.2 Rationale for strength of functions claims

As shown in section 6.2, there is only one security function that has a permutational mechanism and this has the strength SOF-medium. On the other hand, as claimed in section 5.3, the minimum strength of function is SOF-medium. It is obvious that those claims are consistent.

8.4 PP claims rationale

Not required, as there is no reference to a PP.

9 Appendix A: Definition of FIA_ENR

Family behaviour:

Before biometric authentication systems are able to authenticate a user, each user has to perform a so called enrolment procedure. During this procedure the user presents the biometric characteristics (voice in this ST) to the TOE and the TOE links these unique characteristics of the user with the identity of the user.

Part II of [CC] does not provide a SFR that describes this functionality. Therefore an extended SFR has been defined in this family.

Class FIA has been used because the enrolment process is necessary to perform the biometric authentication later on.

Component levelling:

FIA_ENR.1 is used to describe the enrolment process.

Management: FIA_ENR.1

No actions could be considered for the management activities in FIA_ENR.1

Audit: FIA_ENR.1

The following actions should be auditable if FIA_ENR.1 is included in a ST/PP

a) Basic: The outcome of each enrolment process (success or failure)

FIA_ENR.1:	**Enrolment**
Hierarchical to:	No other components.
FIA_ENR.1.1:	The TSF shall provide an enrolment mechanism to acquire [*assignment: biometric data used by the TOE*] of a user and associate this data with the identity of the user.
FIA_ENR.1.2	The TOE shall apply the following rules to determine that the acquired speech data has a sufficient quality to be used by the biometric verification mechanism of the TOE: [*Assignment: Set of rules for quality control*]
Dependencies:	No dependencies

10 Glossary and abbreviations

A.xxx	Assumptions
ACL	Access Control List, see also DAC
Administrator	Person who is authorised to perform the administrative operations, that is able to use the administration tools and manage super users.
API	Application programming interface, the interface of a system that can be used by other programs to communicate.
ASR	See Automated Speech Recognition
Attacker	Person who wants to be authenticated in order to get access to the assets or to perform manipulation.
Authentication	Authentication is the confirmation of the identity of a person. In biometrics, authentication comes in two flavours: Identification and verification. Also see there.
Automated speech recognition	Conversion of speech into machine readable text
Biometric template	See Voiceprint
CC	Common Criteria
Connector Interface	Built-in software of the TOE that allows to access the API of a target platform using data structures that are provided by the TOE for the password reset functionality. Other functionality than password reset is possible, too.
DAC	Discretionary Access Control. Discretionary Access Control (DAC) is used to control access by restricting a subject's access to an object based on the identity of the subject. For the TOE in this ST, DAC means that the users access to the primary assets of the TOE (the possibility to reset a password) depends on the identity of the user. A user is only allowed to access the primary assets when an administrator added this permission for the user to an access control list (ACL) before.
EAL	Evaluation Assurance Level
Enrolment data	Reference data of a user that is stored in a raw format or in a pre-computed algorithm specific format that contains only the relevant extracted features of the raw data.
Enrolment	Process in which a user provides his reference data that can be used for biometric verifications and authentications.
FAR	False Acceptance Rate - The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor.

FRR	False Rejection Rate – The probability that a biometric system will fail to identify an enrolee, or to verify the legitimate claimed identity of an enrolee.
Identification	(Biometric) identification is the process that determines and verifies the identity of a person based on a template. No claim of identity is necessary. Technically seen, an identification is a one-to-many match in the template database.
Interactive Voice Response	Interactive Voice Response (IVR) systems allow callers to interact with a communications system over the telephone. IVR is used to enable the caller to retrieve information from a database, enter information into a database, or both.
IVR	See Interactive Voice Response
Life test	Biometric systems authenticate users after a presentation of a physical or behavioural property of that user. Obviously these properties cannot be secret. So it is necessary to prevent replay attacks with previously recorded properties. This is done with life tests.
Mimic attack	In a mimic attack, an attacker tries to imitate the voice of a person knowing that voice.
Multilevel authentication	The speech data that are collected in one short utterance often do not allow an authentication of the required quality. So several utterances should be collected. Furthermore, the collection of speech material in several portions allows smarter and more powerful decision algorithms than the collection in one attempt.
Normal user	A normal user is allowed to enrol himself in the TOE only after a successful super user authentication. Normal users or just users are that persons, that are allowed to reset password on target systems they are configured for.
O.xxx	Security objectives for the TOE
OE.xxx	Security objectives for the environment
OSP.xxx	Organisational security policies
PP	Protection Profile
Recognition	Recognition can be used in the sense of Automated Speech Recognition (see there) and of Speaker Recognition (see Speech Verification)
Replay attack	In a replay attack, an attacker uses recorded data from earlier authentication attempts to get access to a system.
SF.xxx	Security function
SNR	The Signal to Noise Ratio (SNR) measure estimates the ratio of the

	speech signal power to noise power in decibels (dB).
SOF	Strength of Function
Speaker Recognition	See Speech Verification
Speech Recognition	See Automated Speech Recognition
Speech template	See Voiceprint
Speech Verification	Speech Verification (SV) is a technique that is able to differentiate persons by their speech. Speech Verification can be performed text dependent (the user has to say a secret phrase), text independent (the user may say - technically seen - anything), and text prompted (the user has to repeat a given phrase). The TOE uses text prompted SV.
SR	See Speaker Recognition
ST	Security Target
Super user	A super user is a normal user that has additionally the permission to enrol other users as soon as he is enrolled by another super user.
SV	See Speaker Verification
T.xxx	Threats
Target system	IT system a password can be reset at. The TOE connects to a target system using the API of an admin client of the target system that is installed at the machine that hosts the TOE.
Template	See Voiceprint
Text to speech system	Program that is able to convert machine readable text into spoken language.
TOE	Target of Evaluation, Authentication Engine of VOICE.TRUST Server 4.1.2.0
Threshold	A predefined number, controlled by the administrator of the TOE, which establishes the degree of correlation necessary for a template comparison to be deemed a match.
TSF	TOE Security Functions
TTS	See Text to Speech system
Unauthorised user	A person that is not known to the TOE or that is not enrolled.
Verification	(Biometric) verification is the process that verifies the identity of a person based on a template and a claim of identity. Technically seen, an identification is a one-to-one match in the template database.
Voiceprint	File representation of the features extracted from speech material of a certain user that belongs to a certain spoken text. Voiceprints represent the enrolment data of a user_object.

VTS	VOICE.TRUST Server that includes the TOE
Zero effort attack	In a zero effort attack a user does not know anything about the account to be attacked. Here, the attacker does not know the voice of the person that own the user_object to be attacked.

11 References

A central reference document is available. See VT_REF_VERSION05.doc.