Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0359-2007

for

VoiceIdent Unit 1.0

from

Deutsche Telekom AG / T-COM

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5455, Infoline +49 (0)3018 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom
Bundesamt für Sicherheit in der Informationstechnik

BSI
**Bundesamt für Sicherheit
in der Informationstechnik**

BSI-DSZ-CC-0359-2007

Biometric Verification System

VoiceIdent Unit 1.0

from

Deutsche Telekom AG / T-COM

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Version 2.3* (ISO/IEC 15408:2005) for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0016-2005**
Functionality:	**PP BSI-PP-0016-2005 conformant** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL 2 augmented by** **ADV_SPM.1 – Informal TOE Security Policy Model**

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 evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, January 10th, 2007

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT
Security
Certified

SOGIS - MRA

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- Biometrics Evaluation Methodology Supplement (BEM), version 1.0, August 2002
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product VoiceIdent Unit 1.0 has undergone the certification procedure at BSI.

The evaluation of the product VoiceIdent Unit 1.0 was conducted by SRC Security Research & Consulting GmbH. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

Deutsche Telekom AG / T-COM
Ollenhauerstraße 4
53113 Bonn

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on January 10th, 2007.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. 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.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-20.

The product VoiceIdent Unit 1.0 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Deutsche Telekom AG / T-COM
Ollenhauerstraße 4
53113 Bonn

B Certification Results

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 results

1 Executive Summary

The Target of Evaluation (TOE) is the product VoiceIdent Unit 1.0. The TOE consists of the Voice Gateway/Sikom (Sikom VoiceMan 7.0), the ASR/Verifier (Nuance ASR 8.5 / Verifier 3.5), the Application Server (Jakarta Tomcat 5.5, SV-VoiceDialog Version 1.5.0, SV-Webservice Version 1.2.0) and the Admin Server (SV-AdminSrv Version 1.0.9).

VoiceIdent Unit 1.0 provides a verification process to verify the claimed identity of a human being using his voice as a unique characteristic of his body. It enables operators of portals to uniquely authenticate their customers by means of a voiceprint. A portal in relation to the TOE is the physical or logical point beyond which information or assets are protected by a the TOE. With failed verification, the portal is closed for the user. Via successful verification, the portal is open.

The TOE is a biometric system that works in a verification mode. Biometric Identification is not addressed within the evaluation. Furthermore the enrolment process is out of scope of the evaluation and it is assumed that all authorized users have been enrolled. VoiceIdent Unit 1.0 verifies the identity of a user for the purpose of controlling access to a portal.

Beside the biometric verification process VoiceIdent Unit 1.0 includes a username/password mechanism to identify and authenticate an administrator of the system and enforces an access control for the objects of the TOE. This is especially important to limit the ability to change the threshold settings for the biometric verification process to an authorized administrator.

The IT product VoiceIdent Unit 1.0 (consisting of the Voice Gateway/Sikom, the ASR/Verifier, the Application Server and the Admin Server, see also chapter 2 of this report) was evaluated by SRC Security Research & Consulting GmbH. The evaluation was completed on December 15th, 2006. The SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

Deutsche Telekom AG / T-COM
Ollenhauerstraße 4
53113 Bonn

[8] Information Technology Security Evaluation Facility

1.1 Assurance package

The TOE Security Assurance Requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL 2 (Evaluation Assurance Level 2) augmented. The following table shows the augmented assurance components.

Requirement	**Identifier**
EAL 2	TOE evaluation: structurally tested
+: ADV_SPM.1	Development – Informal TOE security policy model

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 conformant as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	**Addressed issue**
FAU	**Security Audit**
FAU_ARP.1	Security alarms
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAA.1	Potential violation analysis
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_RIP.2	Full residual information protection
FIA	**Identification and authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UAU.3	Unforgeable authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.7	Protected authentication feedback
FIA_UID.2	User identification before any action

Security Functional Requirement	Addressed issue
FMT	**Security Management**
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_MTD.3	Secure TSF data
FMT_SMF.1	Specification of management function
FMT_SMR.1	Security roles
FPT	**Protection of the TOE Security Functions**
FPT_RPL.1	Replay detection

Table 2: SFRs for the TOE taken from CC Part 2

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [7], chapter 5.1.1.

These Security Functional Requirements are implemented by the TOE Security Functions:

TOE Security Function	Addressed issue
F.AUDIT_REACTION	Logging of security critical processes
F.ROLES_AND_ACCESS	Role based access control
F.BIO_VERIFICATION	Access control to a portal by biometric verification mechanism
F.AUTHADMIN	TOE administrator authentication
F.RESIDUAL	No residual data remaining
F.NO_REPRODUCE_OR_ RESIDUAL_CAPTURE	Prevention of re-use of recorded voice samples

Table 3: TOE Security Functions

For more details please refer to the Security Target [7], chapter 6.1.

1.3 Strength of Function

The TOE's strength of functions is claimed SOF-medium for the TOE Security Functions F.AUTHADMIN, F.BIO_VERIFICATION and F.NO_REPRODUCE_ OR_RESIDUAL_ CAPTURE (see Security Target [7], chapter 8.3.2).

In accordance with the BEM [3] the SOF for the biometric verification mechanism (F.BIO_VERIFICATION) is described in terms of FAR values. For SOF medium a FAR of less than 1 in 10000 is required.

1.4 Summary of Threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The following Threats and Organisational Security Policies are defined for the TOE:

Threat	Description
T.BRUTEFORCE	An attacker may use a brute force attack to find biometric data of a (e.g. randomly) chosen user's identity in order to get verified. During this attack a fraction of possible characteristics until one's matching is presented to the TOE.
T.MODIFY_ASSETS	An attacker may modify secondary assets like biometric templates or security-relevant system configuration data or settings. Such attacks could compromise the integrity of the user security attributes (e.g. BIR) resulting in an incorrect result that might give illegal access to the portal.
T.REPRODUCE	An attacker may try to record and replay, imitate, or generate the biometric characteristic of an authorised user. Therefore, the attacker could use technical equipment for analysing and generation of the biometric characteristics.
T.RESIDUAL	An attacker tries to take advantage of unprotected residual security relevant data (biometric data, templates, and settings) during a user's session or from a previous, already authenticated user.
T.ROLES	An already enrolled and authenticated user tries to exceed its authority.

Table 4: Threats

OSP	Description
OSP.FAR	As minimum requirement the TOE must meet recognised national and/or international criteria (see Annex A - BSI biometric performance standard) for false acceptance rate (FAR) as appropriate for the specified assurance level and strength of function claim.
OSP.USERLIMIT	Impostors must be prevented from gaining access to the portal by making repeated verification attempts using one or more claimed IDs.This organisational security policy shall establish the maximum number of unsuccessful verification attempts permitted by the biometric verification system.

Table 5: Organisational Security Policies (OSPs)

For more details please refer to the Security Target [7], chapter 3.3 and 3.4.

1.5 Special configuration requirements

Although VoiceIdent Unit includes several computers connected by a local network, it is a stand-alone solution in the sense of this discussion, because all computers belonging to VoiceIdent Unit are located in the same secure environment and VoiceIdent Unit uses one database located in the same secure environment.

VoiceIdent Unit uses normal telephones as input devices and a system called “Voice Gateway”, which transforms the digital data from the telephone line to data for the VoiceIdent Unit. Telephone and Voice Gateway together can be considered as capturing device. According to the PP the capturing device is not part of the TOE but is assumed to work within acceptable ranges. However, the VoiceIdent Unit does not rely on specific acceptable operating conditions for the telephone used as voice input: Bad environmental conditions may cause voice samples to be useless, but can not help an attacker to claim a false identity. Therefore VoiceIdent needs no specific assumptions (in the sense of the CC) for the telephone devices used for voice input.

1.6 Assumptions about the operating environment

The following assumptions for the environment of the TOE are made:

Assumption	**Definition**
A.ADMINISTRATION	Well trained administrators
A.CAPTURE	Regular operation of the capture device
A.ENROLMENT	Enrolment already performed in sufficient quality
A.ENVIRONMENT	TOE operating equipment and adequate infrastructure is available
A.PHYSICAL	TOE and its components are physically protected
A.FALLBACK	Fallback mechanism for the biometric verification system is available

Table 6: Assumptions for the TOE environment

Note: Only the titles of the assumptions are provided. For more details please refer to chapter 4 of this report and the Security Target [7], chapter 3.2.

1.7 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 as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI 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 called:

VoiceIdent Unit 1.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Voice Gateway / Sikom Sikom VoiceMan 7.0	 Version: 7.0.30.99	Installed at the customer's site by technicians of the developer
2	SW	ASR/Verifier Nuance ASR 8.5 / Verifier 3.5	 Version: 8.5 SP050930	Installed at the customer's site by technicians of the developer
3	SW	Application Server Jakarta Tomcat 5.5 SV-VoiceDialog SV-Webservice	 Version 5.5.17 Version 1.5.0 Version 1.2.0	Installed at the customer's site by technicians of the developer
4	SW	Admin Server SV-AdminSrv	 Version 1.0.9	Installed at the customer's site by technicians of the developer
5	Paper and PDF	Administration Guide VoiceIdent	Version 1.2	Handed personally resp. installed at the customer's site by technicians of the developer

Table 7: Deliverables of the TOE

3 Security Policy

The TOEs Security Policy is to provide access to a portal to authorised users and to provide access to the TOEs management functions to authorised administrators.

Therefore the TOE enforces the following rules:

- A user has access to the user data of the portal only after forwarding the claimed ID to the TOE and successful voice verification.
- After the successful username/password authentication on the Admin-Server, the TOE administrator can
    - administrate the users (store, change and delete the user identity data and the BIR),
    - perform the TOE relevant settings and check the audit records,
    - reset the counter of consecutive unsuccessful attempts for the user,
    - change his own password.
- After the successful username/password authentication on the operating system the IT administrator has access to the subsystem "Admin-Server" via a command line program and can
    - administrate the TOE administrators incl. reset the counter of consecutive unsuccessful attempts for the TOE administrator,
    - change his own username/password.
- After the successful username/password authentication on the operating system the Developer-Administrator can perform the installation of the TOE with IT administrator supports and set (once) the threshold value for acceptance or rejection of user authentication attempts.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

The following assumptions regarding the user behaviour are defined:

A.ADMINISTRATION

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

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

4.2 Environmental assumptions

The following assumptions regarding the physical environment of the TOE are defined:

A.CAPTURE

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

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

A.ENROLMENT

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

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

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

A.ENVIRONMENT

It is assumed that necessary TOE operating equipment and adequate infrastructure is available (e.g.: operating system, Random Number Generator (RNG), storage, LAN, public telephone). For more details regarding the operating system, the RNG and the storage please refer to the Security Target [7], chapter 3.2.

The environment takes care for a secure communication of security relevant data from and to the TOE.
For the VoiceIdent system it can be assumed that all interfaces to the TOE except the phone line are located in the same secure environment as the TOE itself and are physically protected.

It is assumed that the environment provides a functionality to review the audit information of the TOE and to ensures that only authorized administrators are able to do this.
For VoiceIdent again physical protection by a secure environment can be assumed.

Beside this it is assumed that the surrounding TOE environment is Virus, Trojan, and malicious software free.

A.PHYSICAL

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

A.FALLBACK

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

4.3 Clarification of scope

The TOE is a biometric system that works in a verification mode. Biometric identification is not addressed within the evaluation. Furthermore the enrolment process is out of scope and it is assumed that all authorized users have been enrolled.

For correct operation the TOE needs cryptographically strong random numbers and reliable timestamps that are provided by the underlying plattform.

The biometric identification records that are produced during the enrolment process as well as all other user identification data are stored in two databases that are outside the TOE.

For more detailed information about the the TOE boundary see the following chapter in this report and the Security Target [7], chapter 2.5.

5 Architectural Information

The following diagram shows the TOE in its intended environment. The TOE consists of the four software subsystems Voice Gateway/Sikom, ASR/Verifier, Application Server (containing the VoiceXML Dialog and the BusinessLogic) and Admin Server that are marked by blue boxes and that implement the security functionality. The TOE boundary is shown by the light violett box which surrounds the subsystems. The black arrows named S1, S2, S4 and S7 – S12 indicate the external interfaces of the TOE. The black arrows named S3, S5, S6 indicate the internal interfaces of the TOE.

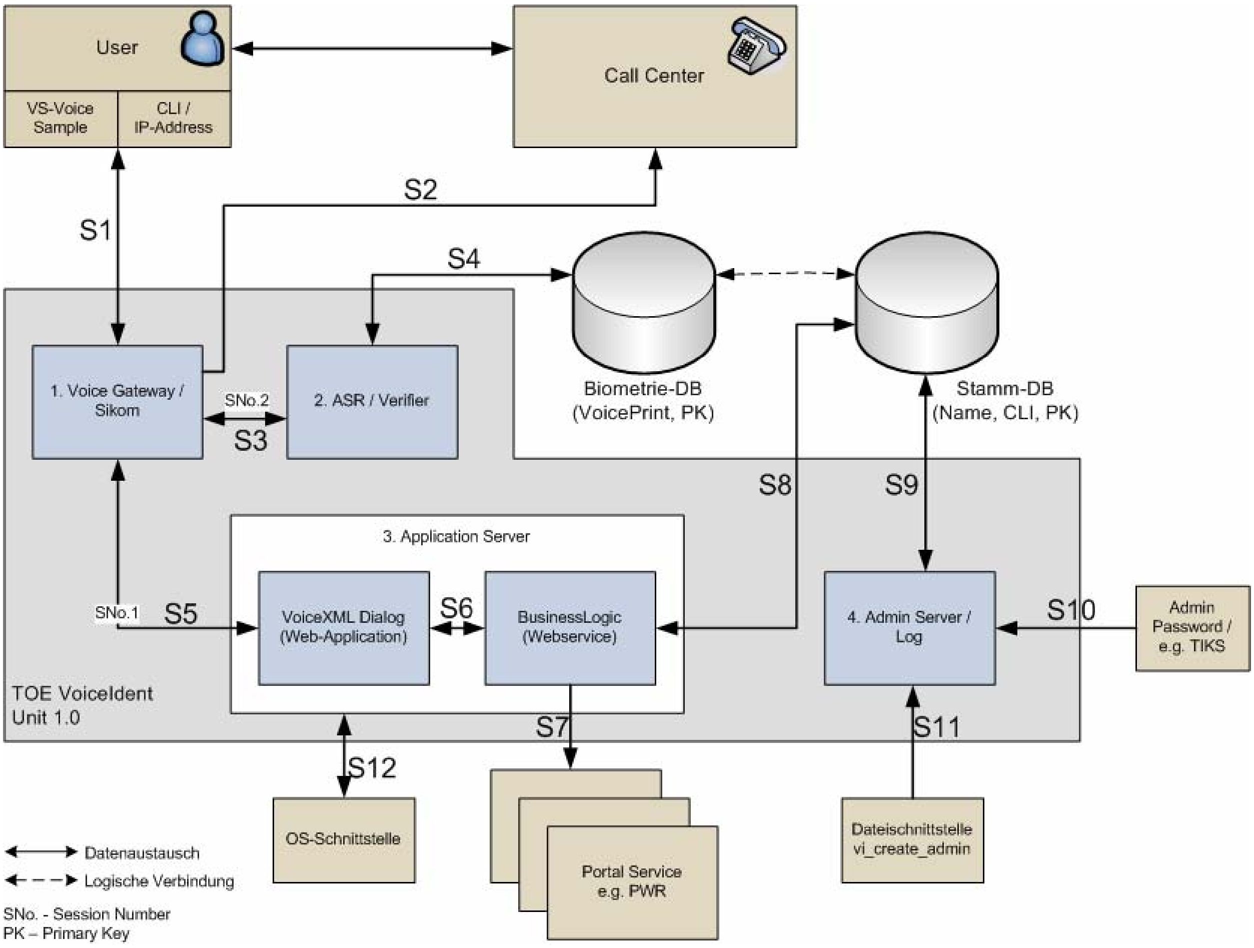

Figure 1: Architecture of the TOE

6 Documentation

The documentation consists of the Administration Handbook “Administration Guide VoiceIdent, Version 1.2 [10]” and is handed personally to the customer in paper form respectively installed in pdf-version at the customer’s site by technicians of the developer.

The documentation describes the secure usage of the TOE in accordance with the Security Target.

7 IT Product Testing

7.1 Test Configuration

The used test configuration was a VoiceIdent Unit 1.0 (subsystem versions and files in accordance with the configuration list) installed on one machine (a Fujitsu-Siemens RX200 S2 Server with 2 Intel Xeon 3,6 GHz prozessors, 4 GB RAM, 2 x 72GB harddisks and an Eicon Diva Server 4BRI-8M 2.0 ISDN card, operating system Windows Server 2003 Standard-Edition, Service Pack 1) and restricted to the local development network. That meant that no external email-addresses were available and in the verification process rejected users were not forwarded to a call centre. Except these restrictions the used test configuration was conform to the Security Target. But for all the restrictions complete testing of the TOE Security Functions was possible without any qualification.

7.2 Developer Testing

The developer specified and implemented test cases for each defined Security Function. Each test case covered one Security Function and the test procedures were based on the described behaviour of the Security Function. All Security Functions were covered and the actual test results were conform to the expected test results.

7.3 Evaluator Indenpendent Testing

The evaluators used the test configuration installed and used by the developer for the developer tests. The hardware and software used by the evaluators for testing were the same as the ones used by the developer, because the tests took place in the test environment of the developer.

Taking into account the results of the developer’s tests the evaluators specified tests by varying existing tests. Only for the residual tests the evaluators did not specify varying tests, because the tests of the developer are adequate to cover the Security Function behaviour. The evaluators conducted at least one test case for each Security Function. One evaluator test could be understood as penetration test for obvious attacks (a user trying to authenticate with a recorded voice sample). The evaluator recorded his own voice sample and used it for the authentication attempt. The authentication failed. All actual test results were conform to the expected test results.

8 Evaluated Configuration

The TOE is identified as VoiceIdent Unit 1.0.

The evaluated configuration was a VoiceIdent Unit 1.0 (subsystem versions and files in accordance with the configuration list) installed on one machine and restricted to the local development network.

For setting up and running the TOE according to the evaluated configuration all guidance documents (refer to chapter 6) and the implications given by the Security Target were followed. These implications can also be found in chapter 1.5, 1.6 and 4 of this report.

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [4] and all interpretations and guidelines of the Scheme (AIS) [5] as relevant for the TOE.

The Common Methodology for Information Technology Security Evaluation (CEM) [2] was used for those components identical with EAL 2 augmented.

In addition the Biometrics Evaluation Methodology Supplement (BEM) [3] was used for the evaluation of the biometric verification mechanism.

The verdicts for the CC, Part 3 assurance components (according to **EAL 2** augmented by ADV_SPM.1 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

Assurance classes and components		**Verdict**
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
Informal TOE security policy model	ADV_SPM.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

Table 8: Verdicts for the assurance components

The evaluation has shown that:

- the TOE is conform to the PP BSI-PP-0016-2005 [9]
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL 2 augmented by ADV_SPM.1.

The TOE Security Functions F.BIO_VERIFICATION, F.NO_REPRODUCE_OR_RESIDUAL_CAPTURE and F.AUTHADMIN fulfil the claimed Strength of Function of “SoF-medium“.

The results of the evaluation are only applicable to the TOE “VoiceIdent Unit 1.0” (for identification of the TOE components please refer to chapter 2 of this report).

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The operational document “Administration Guide VoiceIdent“ [10] contains necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the Security Target [7] of the Target of Evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

ASR	Automatic Speech Recognition
BEM	Biometrics Evaluation Methodology Supplement
BIR	Biometric Identification Record
BLR	Biometric Live Record
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FAR	False Accept Rate
FRR	False Rejection Rate
IT	Information Technology
LAN	Local Area Network
OSP	Organisational Security Policy
PP	Protection Profile
RNG	Random Number Generator
SF	Security Function
SFP	Security Function Policy

SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC 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

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

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

[4] BSI certification: Procedural Description (BSI 7125)

[5] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

[6] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[7] Security Target BSI-DSZ-0359-2007, Version 1.7, 29.09.2006 , Common Criteria Security Target for VoiceIdent Unit 1.0, Deutsche Telekom AG / T-COM

[8] Evaluation Technical Report, Version 1.2, 06.12.2006 (confidential document)

[9] Protection Profile BSI-PP-0016-2005, Version 1.04, 17.08.2005, Protection Profile for Biometric Verification Mechanisms

[10] Administration Guide VoiceIdent, Version 1.2, 15.09.2006, Administratorhandbuch, Deutsche Telekom AG / T-COM

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„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 CC Part 2 (functional requirements), CC 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:

a) **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.

b) **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

a) **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

b) **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC 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:

a) **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.

b) **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined 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.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

a) **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Assurance categorisation (chapter 7.5)

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

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
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)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
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 11)

“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 CC 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 (chapter 11.1)

“Table 6 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 in as much 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 7 of this 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 standard 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_INT					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 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

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 (chapter 11.4)

“Objectives

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 (chapter 11.5)

“Objectives

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 (chapter 11.6)

“Objectives

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 (chapter 11.7)

“Objectives

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 (chapter 11.8)

“Objectives

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 (chapter 11.9)

“Objectives

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) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"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.”

“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 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”