



Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0619-2012

for

**Secure Audio Switch (iSAS),
Version 1.0**

from

Frequentis Nachrichtentechnik GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111



Deutsches IT-Sicherheitszertifikat

erteilt vom



Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0619-2012

Secure Audio Switch (iSAS)

Version 1.0

from Frequentis Nachrichtentechnik GmbH
PP Conformance: None
Functionality: Product specific Security Target
Common Criteria Part 2 conformant
Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by ASE_TSS.2, ADV_INT.3 and
AVA_VAN.5



Common Criteria
Recognition
Arrangement
for components up to
EAL 4



The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

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.

Bonn, 27 July 2012

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.



This page is intentionally left blank.

Preliminary Remarks

Under the BSIG¹ 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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification.....	7
1 Specifications of the Certification Procedure.....	7
2 Recognition Agreements.....	7
2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA).....	7
2.2 International Recognition of CC – Certificates (CCRA).....	8
3 Performance of Evaluation and Certification.....	8
4 Validity of the Certification Result.....	9
5 Publication.....	9
B Certification Results.....	10
1 Executive Summary.....	11
2 Identification of the TOE.....	12
3 Security Policy.....	13
4 Assumptions and Clarification of Scope.....	13
5 Architectural Information.....	14
6 Documentation.....	14
7 IT Product Testing.....	15
7.1 TOE test configuration.....	15
7.2 Developer tests.....	15
7.3 Independent evaluator tests.....	15
7.4 Penetration tests.....	16
8 Evaluated Configuration.....	16
9 Results of the Evaluation.....	16
9.1 CC specific results.....	16
9.2 Results of cryptographic assessment.....	17
10 Obligations and Notes for the Usage of the TOE.....	17
11 Security Target.....	17
12 Definitions.....	17
12.1 Acronyms.....	17
12.2 Glossary.....	18
13 Bibliography.....	19
C Excerpts from the Criteria.....	21
D Annexes.....	31

A Certification

1 Specifications of the Certification Procedure

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

- BSIG²
- BSI Certification Ordinance³
- BSI Schedule of Costs⁴
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1⁵ [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

² Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

³ Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 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 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at <https://www.bsi.bund.de/zertifizierung>.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: <http://www.commoncriteriaportal.org>.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

This evaluation contains the components ASE_TSS.2, ADV_INT.3 and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

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 Secure Audio Switch (iSAS), Version 1.0, has undergone the certification procedure at BSI.

The evaluation of the product Secure Audio Switch (iSAS), Version 1.0, was conducted by the Technical Center for Information Technology and Electronics - Test Center for IT-Security of the Bundeswehr. The evaluation was completed on 11 June 2012. The Technical Center for Information Technology and Electronics - Test Center for IT-Security of the Bundeswehr is an evaluation facility (ITSEF)⁶ recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Frequentis Nachrichtentechnik GmbH.

The product was developed by: Frequentis Nachrichtentechnik GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

⁶ Information Technology Security Evaluation Facility

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. 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, as specified in the following report and in the security target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the security target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product Secure Audio Switch (iSAS), Version 1.0, has been included in the BSI list of certified products, which is published regularly (see also Internet: <https://www.bsi.bund.de> and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer⁷ of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

⁷ Frequentis Nachrichtentechnik GmbH
Robert-Bosch-Straße 11B
63225 Langen
Germany

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.

1 Executive Summary

The target of evaluation (TOE) is the Secure Audio Switch (iSAS), Version 1.0.

The TOE is installed in settings where a user needs to operate CLASSIFIED and UNCLASSIFIED voice communication via a common user interface and the same set of audio devices. The user can rely on the TOE unique architecture to keep the CLASSIFIED and UNCLASSIFIED voice information completely separate.

The CLASSIFIED and UNCLASSIFIED voice information is processed by dedicated, physically separated voice communication systems (RED and BLACK VCS – not part of the TOE) and transmitted via secure (in the case of CLASSIFIED information) or insecure (in the case of UNCLASSIFIED information) communication channels (not part of the TOE). The TOE and the VCSs are installed in a physically protected operations site.

In operation, the user can control the voice transmission path (microphone inputs) separately from the voice reception path (earpiece outputs).

The TOE connects the microphone inputs to either the RED VCS or the BLACK VCS. To switch between RED and BLACK VCS the user must perform some specific action (e.g. push a button, turn a knob, etc.). The TOE then visually indicates whether the microphone inputs are connected to the BLACK or RED VCS.

The security target [6] is the basis for this certification. It is not based on a certified protection profile.

The TOE security assurance requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the evaluation assurance level EAL 4 augmented by ASE_TSS.2, ADV_INT.3 and AVA_VAN.5.

The TOE security functional requirements (SFR) relevant for the TOE are outlined in the security target [6] and [7], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

The TOE security functional requirements are implemented by the following TOE security functions:

TOE Security Functions	Addressed issue
TSF.VFC	Voice Information Flow Control
TSF.DFC	User Interface Data Flow Control
TSF.MNI	Management Interface
TSF.PRT	Protection of TSF

Table 1: TOE Security Functionalities

For more details please refer to the security target [6] and [7], chapter 7.1.

The assets to be protected by the TOE are defined in the security target [6] and [7], chapter 3.1. Based on these assets the TOE security problem is defined in terms of assumptions and threats. This is outlined in the security target [6] and [7], chapter 3.4 and 3.5.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSI Section 9, Para. 4, Clause 2).

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:

Secure Audio Switch (iSAS), Version 1.0

The following table outlines the TOE deliverables:

No	Type	Identifier	SAP-No. / Revision	Form of Delivery
1	HW	MOD iSAS-P 01	30-0803100 / 05	Sealed housing
2	HW	MOD iSAS-RC 01	30-0803300 / 03	Sealed housing
3	HW	MOD iSAS-RC 02	30-0901400 / 03	Sealed housing
4	FW	Firmware of the PLD in MOD iSAS-P	08026 / 028	Installed on MOD iSAS-P 01
No	Type	Identifier	Version / Date	Form of Delivery
5	DOC	Preparative Procedures [11]	1.1 / 2012-05-10	Hardcopy or PDF
6	DOC	Operational User Guidance [12]	1.1 / 2010-11-09	Hardcopy or PDF

Table 2: Deliverables of the TOE

To preserve the integrity of iSAS during delivery, security seals are glued on the housing of MOD iSAS-P 01, MOD iSAS-RC 01 and MOD iSAS-RC 02 after the final test at the production site. The security seals shall be visible for inspection. The user guidance [11] describes how to check the seals.

This allows applying standard delivery procedure for iSAS. The iSAS will be physically delivered from the production site directly to the customer inclusive appropriate packaging by forwarding agency or courier service.

The iSAS identification can be verified by the customers based on the serial number on the iSAS housing and the delivery note. The user guidance [11] describes how to check the serial numbers. The integrity of the iSAS can be verified on behalf of the seals on the iSAS housings.

3 Security Policy

The security policy is expressed by the set of security functional requirements and implemented by the TOE. It covers the following issues:

- Indication of the transmission and receive status (to/from BLACK or RED VCS) to the user.
- Separation of CLASSIFIED and UNCLASSIFIED voice information and reliable routing of the voice information.
- Prevention of acoustic coupling.
- Mediation of the information flow between the RED VCS and the BLACK VCS in order to prevent the user interface connection from being misused.
- Providing a fail secure behaviour in the event of a single failure of the TSF.

4 Assumptions and Clarification of Scope

The assumptions defined in the security target and some aspects of the threats are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-environment. The following topics are of relevance:

Physical protection of operations site, tempest facility zone, prevention of compromising emanation, physical access to the TOE, clearance of TOE users, installation and maintenance of the TOE, user training, use of appropriate headsets, prevention of acoustic coupling from neighbouring users, separation of RED and BLACK VCS and accreditation of RED VCS.

Details can be found in the security target [6] and [7], chapter 4.2.

5 Architectural Information

The TOE consists of the HW-parts MOD iSAS-P 01, which implements the main security functionality and the Remote Control Devices MOD iSAS-RC 01 and MOD iSAS-RC 02.

In the environment of the TOE the audio devices are used to send and receive voice information by the users. The BLACK VCS and the RED VCS are used to send UNCLASSIFIED resp. CLASSIFIED information over insecure resp. secure communication channels. A common user interface (e.g. touch entry device) is integrated into the RED VCS.

The TOE and the VCSs are installed in a physically protected operations site.

Figure 1 shows the overall architecture of the TOE and its environment.

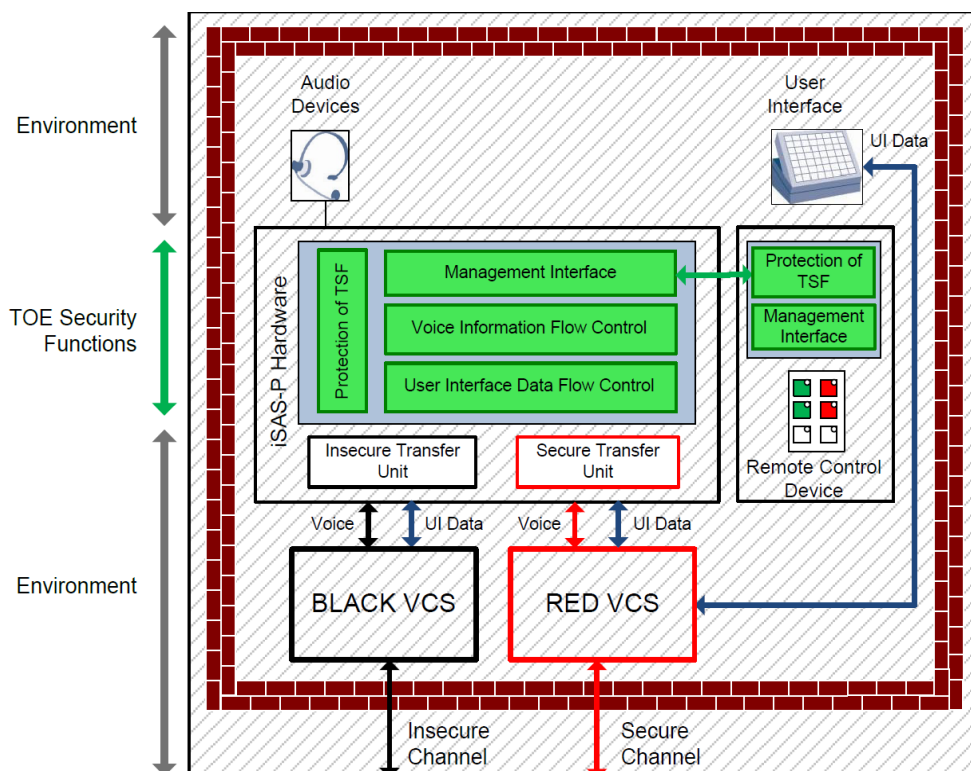


Figure1: TOE architecture

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the security target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

7.1 TOE test configuration

The TOE hardware and software parts used for testing were identical to the versions described in chapter 2 of this report.

The test configurations fulfilled all relevant assumptions for the environment of the TOE as described in the security target.

In one test configuration MOD iSAS-P 01 and Remote Control Device MOD iSAS-RC 02 were used. In a second test configuration MOD iSAS-RC 01 was used (please see chapter 8 of this report for the different possible combinations of the TOE parts). MOD iSAS-P 01 was connected with the Frequentis non-TOE products iPOS BLACK (embedded operator position for UNCLASSIFIED information) and iPOS RED (embedded operator position for CLASSIFIED information) over optical fibre cable. The iPOS BLACK/RED were connected to an IP phone and a radio tester.

The test environment was changed for only a few special tests based on automated test scripts. In these cases the iPOS BLACK or the iPOS RED were connected to a test PC.

7.2 Developer tests

The developer conducted manual and automated tests. For the manual tests the results were verified by visual and acoustical monitoring according to the corresponding user actions (executed keystroke on MOD iSAS-P 01, MOD iSAS-RC 02). The automated test cases were used to check the content and characteristics of all registers and several control functions of the implemented firewall (information flow control).

All modules of the hard- and software-subsystems itemized by the TOE-design were examined by developer tests. All test actual results match the expected ones.

7.3 Independent evaluator tests

The evaluators also used different test approaches during repeating developer tests and during performing independent evaluator tests.

Manual tests were performed via the demonstration method. In these cases the evaluators verified via optical and acoustical monitoring if for example routing of in- and outgoing audio signals or status displays of MOD iSAS-P 01, MOD iSAS-RC 02 work correctly according to the executed keystroke on MOD iSAS-P 01, MOD iSAS-RC 02.

A further test approach was to use test scripts and test programs. Therefore a PC was connected with iPOS BLACK respectively iPOS RED.

By this test approach the data content and the characteristics of all registers and the firewall control functions of the information flow between RED VCS and BLACK VCS were tested.

Altogether during the independent testing all important TSFI as well as all TSF hardware and software modules specified by the TOE-design were tested.

The results of all evaluator tests have shown that the expected and actual test results were consistent. Moreover, it was shown that the parts of the developer tests, which were repeated by the evaluators, didn't have any differences in comparison to the developers test results.

7.4 Penetration tests

The evaluators conducted a theoretical vulnerability analysis on the basis of the TOE architecture and a source code inspection and came to the conclusion that there are no potential vulnerabilities of the TOE to exploit. Therefore no penetration testing was performed by the evaluators.

8 Evaluated Configuration

The TOE consists of three hardware components and a firmware component. They are listed in chapter 2 of this report. These components are not configurable. They only can be used in different combinations:

- MOD iSAS-P 01 can be used as single TOE part together with the IT-environment of the TOE because it implements all necessary security functionality
- MOD iSAS-P 01 can be used together with the separated remote console MOD iSAS-RC 02 and the IT-environment of the TOE
- MOD iSAS-RC 01 can be used as single TOE part together with the IT-environment of the TOE as MOD iSAS-P 01 is integrated in the MOD iSAS-RC 01 housing.

The security target [6] and [7], chapter 1.4.1 describes the different possible combinations in more detail.

9 Results of the Evaluation

9.1 CC specific results

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 [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components up to EAL5 extended by advice of the Certification Body for components beyond EAL 5 [4] (AIS 34).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ASE_TSS.2, ADV_INT.3 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by ASE_TSS.2, ADV_INT.3 and AVA_VAN.5

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The TOE does not include cryptoalgorithms. Thus, no such mechanisms were part of the assessment.

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of assumptions, threats and OSPs as outlined in the security target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

11 Security Target

For the purpose of publishing, the security target [7] of the target of evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete security target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
iPOS	Embedded Operator Position
iSAS	Secure Audio Switch
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

TSFI	TSF Interface
VCS	Voice Communication System

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

BLACK VCS - Voice Communication System for UNCLASSIFIED voice information

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.

iPOS BLACK - Embedded Operator Position for UNCLASSIFIED information

iPOS RED - Embedded Operator Position for CLASSIFIED information

Object - An passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

RED VCS - Voice Communication System for CLASSIFIED voice information

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

13 Bibliography

- [1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009
- [3] BSI certification: Procedural Description (BSI 7125)
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE⁸.
- [5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website
- [6] Security Target BSI-DSZ-CC-0619-2012, Version 1.7, 2012-05-10, iSAS Security Target, Frequentis Nachrichtentechnik GmbH (confidential document)
- [7] Security Target BSI-DSZ-CC-0619-2012, Version 1.0, 2012-05-15, iSAS Security Target lite, Frequentis Nachrichtentechnik GmbH (sanitised public document)
- [8] Evaluation Technical Report, Version 2.1, 2012-06-04, Technical Center for Information Technology and Electronics - Test Center for IT-Security of the Bundeswehr (confidential document)
- [9] Configuration list for the TOE, Version 1.0, 2012-05-16, Documentation Status Accounting Report, Frequentis Nachrichtentechnik GmbH (confidential document)
- [10] Configuration list for the TOE, Version 1.0, 2012-05-08, Configuration Status Accounting Report, Frequentis Nachrichtentechnik GmbH (confidential document)
- [11] Secure Audio Switch iSAS 1.0, Preparative Procedures, Version 1.1, 2012-05-10, Frequentis Nachrichtentechnik GmbH
- [12] Secure Audio Switch iSAS 1.0, Operational User Guidance, Version 1.1, 2012-05-10, Frequentis Nachrichtentechnik GmbH

⁸specifically

- AIS 32, Version 7, 8 June 2011, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, 3 September 2009, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
 - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
 - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
 - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
 - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- **Package name Conformant** - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
 - the SFRs of that PP or ST are identical to the SFRs in the package, or
 - the SARs of that PP or ST are identical to the SARs in the package.
- **Package name Augmented** - A PP or ST is an augmentation of a predefined package if:
 - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
 - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- **PP Conformant** - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- **Conformance Statement (Only for PPs)** - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.”

“Each assurance class contains at least one assurance family.”

“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high- level design presentation

Assurance Class	Assurance Components	
AGD:	AGD_OPE.1 Operational user guidance	
Guidance documents	AGD_PRE.1 Preparative procedures	
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support	
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage	
	ALC_DEL.1 Delivery procedures	
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures	
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation	
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model	
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts	
	ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
		ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
		ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete		
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis	

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“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 8.1)

“Table 1 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 7 of this 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 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 augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)**“Objectives**

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)**“Objectives**

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)**“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target lite provided within a separate document.

This page is intentionally left blank.