Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0619-V2-2022

for

iSAS Release 1.0

from

Frequentis AG

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0619-V2-2022 (*)

Netzwerk- und Kommunikationsprodukte

iSAS
Release 1.0

from	Frequentis AG
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

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

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 Scheme Interpretations and 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. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 5.

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.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 2 March 2022

For the Federal Office for Information Security

Matthias Intemann
Head of Branch

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - 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

This page is intentionally left blank.

Contents

A. Certification

1. 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.

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

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

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. 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.

3.1. European Recognition of 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 SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the components ASE_TSS.2, ADV_INT.3 and AVA _VAN.5 that are not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL 4 components of these assurance families are relevant.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://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 related bodies

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

4. 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 iSAS, Release 1.0 has undergone the certification procedure at BSI. Since the previous evaluation was carried out by a different evaluation facility, no results were re-used.

The evaluation of the product iSAS, Release 1.0 was conducted by Deutsche Telekom Security GmbH. The evaluation was completed on 3 February 2022. Deutsche Telekom Security GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

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

The product was developed by: Frequentis AG.

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

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is 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 components and assurance levels please refer to CC itself. Detailed references are listed in part C of this 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-assessment or 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 order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 2 March 2022 is valid until 1 March 2027. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

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.

6. Publication

The product iSAS, Release 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 developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Frequentis AG
Innovationsstraße 1
1100 Wien
Österreich

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 iSAS, also referred to as Secure Audio Switch in the guidance documentation, Release 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.

The TOE is intended for use with Frequentis Voice Communication System (VCS). The digital format of the audio signal as well as other control signals are not intended for connection with general purpose voice communication systems. Additionally, the TOE requires the following non-TOE hardware:

- Audio device(s)
- RED VCS including the user interface (e.g. touch entry device)
- BLACK VCS
- Power supply

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 [8], 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 Functionality:

TOE Security Functionality	Adressed Issue
Voice Information Flow Control (TSF.VFC)	Each audio device has its dedicated PTT input. Inactive microphone inputs are disconnected. One common TX selector switches the microphone inputs either to the secure VCS interface or to the insecure VCS interface. Routing of received voice information to secure or to insecure outputs (earpiece). If selected, the received voice information can be selected even both. Current selection of voice information routing is indicated to the user.
Management Interface (TSF.MNI)	Assured indication of the state of the Voice Information Flow Control using LEDs. Setting the state of TX-, RX-selectors and PTT, as well as indicating the states to the user by the remote control device.
User Interface Data Flow Control (TSF.DFC)	Firewall mediating for data between the secure and insecure interfaces to prevent the user interface connection from being misused to bypass the voice information flow.
Protection of TSF (TSF.PRT)	Disconnection all audio devices and stopping of voice information routing in case of a power failure. A single failure will not result in an insecure state.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [8], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6] and [8], chapter 3.1. Based on these assets, the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [8], chapters 3.4, 3.5 and 3.6.

This certification covers the configurations of the TOE as outlined in chapter 8.

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 BSIG 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:

iSAS, Release 1.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	MOD iSAS-P	1.0	Separate unit in a closed case
2	HW	HOD iSAS-RC 02	1.0	Separate unit in a closed case

No	Type	Identifier	Release	Form of Delivery
3	DOC	Secure Audio Switch Preparative Procedures, EWSE23EN50003, V1.5, 29-07-2021, Frequentis AG [11] SHA256-sum: 0f50d3bc4a6abfe40236a3468127f8fb8f4e221e6bdc3051e1439628281d2292	V1.5	Paper or PDF file
4	DOC	Secure Audio Switch Operational User Guidance, EWSE23EN50004, V1.4, 26-07-2021, Frequentis AG [10] SHA256-sum: 6822235c296f5cfc873d8bfdece97636cd395b8a1b8b36df2d1d9c9f3dba70fc	V1.5	Paper or PDF file

Table 2: Deliverables of the TOE

The TOE is prepared for delivery within a secure environment. The preparation includes the final test in the secured production area, attachment of the security seal, and storage in a secure environment.

The TOE is delivered to the customer by one of following three customer-selectable options:

- Hand carry by Frequentis employee,
- Hand carry by customer, and
- Trusted Carrier Service

The customer is responsible for applying the acceptance procedures as described in [11] sec. 2. If any step of the acceptance procedures fails, the customer shall reject the delivery of the TOE. If all acceptance steps are successful, the customer has to sign the pack list and send it back to Frequentis.

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:

- Voice Information Flow Control,
- User Interface Data Flow Control,
- Management Interface, and
- Protection of security functions.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies 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:

- A.Physical_Protection (Physical Protection): The TOE and the RED and BLACK VCS are installed in a physically protected area (operations site), at least approved for the highest security level of information handled in the TOE.
- A.TEMPEST_Facility (Tempest Facility Zone): The TOE is operated in a TEMPEST facility zone that allows the use of COTS products for the processing of the highest security level of information handled in the TOE.
- A.TEMPEST_Evaluation (Prevention of compromising emanation): The TOE is subject to a TEMPEST evaluation, which is carried out independent of the Common Criteria certification.
  The TEMPEST evaluation of the TOE prevents unacceptable compromising electromagnetic emissions and ensure that the interface to the BLACK VCS does not contain unintentional CLASSIFIED voice information.
- A.Training (User Training): All users are trained in the correct use of the TOE and VCS and follow the operational guidelines.
- A.Clearance (User Clearance): All users have a minimum clearance for the highest security level of information handled in the TOE and are authorized for all information handled by the TOE.
  User activity shall be monitored to the extent that sanctions can be applied when malfeasance occurs.
- A.Installation (TOE Installation and Maintenance): The TOE is installed and maintained according to the installation and maintenance guidelines.
- A.Headset (Headsets devices): Appropriate headsets and associated cables prevent unacceptable acoustic coupling between:
  - Earpiece and microphone of the audio device.
  - Ambient noise and microphone

  Note: This assumption does not hold for the handset and handheld.
- A.VCS (Separation of RED and BLACK VCS): The voice information transmitted by the RED VCS is strictly separated from the voice information transmitted by the BLACK VCS. Vulnerabilities associated with the VCS or its connections to the TOE are a concern of the application scenario and not the TOE.
  All communication channels of the RED VCS that leave the operations site are either encrypted with approved crypto devices or implemented as approved circuits (secure channels). Vulnerabilities associated with the RED communication channels are a concern of the application scenario and not the TOE.
- A.RED_VCS_Accreditation (Accreditation of RED VCS): The RED VCS is accredited for the highest security classification processed in the system.

Details can be found in the Security Target [6] and [8], chapter 3.4.

5. Architectural Information

The TOE controls the voice information flow received and sent to the Voice Communication Systems (VCS) that are provided by the developer and part of the operational environment of the TOE. Information received from and sent to the VCSs are considered as CLASSIFIED (RED VCS) and UNCLASSIFIED (BLACK-VCS). The TOE process the CLASSIFIED and UNCLASSIFIED information completely separated. Except

for its user guidance documents and required hardware within the operational environment, the TOE consists of two hardware parts “MOD iSAS P” and remote control part “MOD iSAS RC 02”. “MOD iSAS P” fulfills the functionality of the TOE itself. Therefore the remote control part is optional. It is mostly used in cases where the TOE is installed in a location inaccessible to the operator.

The architecture comprises two subsystems, the main system “MOD iSAS P” and the optional remote system “MOD iSAS RC 02”.

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

The developer performed extensive tests to verify the functionality of the TOE. The developer specified 27 tests that cover all Security Features described in the ST [6] and [8], subsection 1.3.1 and all SFR-Enforcing interfaces. The tests covered all configurations outlined in chapter 8. The developer provided the evaluator with a testing environment.

7.1. Developer Testing

The developer performed extensive tests to verify the functionality of the TOE. The developer specified 27 tests. The tests performed by the developer can be divided into the following categories:

- Analysis: by technical/mathematical evaluation or simulation using mathematical representation, charts, graphs, circuit diagrams, etc. to verify that an item meets the specified requirement.
- Inspection: tests are performed by visual examination of the item according to descriptive documentation, and comparing the appropriate characteristics with a predetermined or referenced standard.
- Demonstration: tests are performed by operating the functions under a specific set of conditions. Visual witness of the demonstration is sufficient to judge success or failure.
- Measurement: tests are performed by systematic operation of the item under appropriate conditions to assure compliance with the requirements. Collection, analysis and evaluation of recorded data are mandatory to provide evidence that the requirement(s) has/have been met.

There were no deviations between the expected and the actual test results.

7.2. Independent Testing

The independent tests were performed using the testing environment provided by the developer and extended by additional testing equipment for data injection and extraction. A non-TOE touch entry device was connected to RED VCS to test control of the RED and BLACK VCS.

Routing of in- and outgoing audio signals and status displays of MOD iSAS-P 01 and MOD iSAS-RC 02 according to user input was verified via optical and acoustical monitoring.

The data content and the characteristics of all registers and the firewall control functions between RED VCS and BLACK VCS were tested using computers connected to the RED VCS and the BLACK VCS.

The TOE provides only one “normal” operating mode. However in normal mode the RX selector supports three different options “SECURE”, “INSECURE” and “BOTH”. All options were covered in the independent testing.

The tests showed that the TOE behaves as expected in all configurations that are considered as part of the evaluation. No deviation was found between the expected and the actual test results. The depth of testing is adequate for the evaluation assurance level chosen (EAL4+). The TOE has successfully passed independent testing.

7.3. Vulnerability Testing

No attack scenario with the attack potential High was actually successful in the TOE’s operational environment as defined in [6] and [8] provided that all measures required by the developer are applied.

8. Evaluated Configuration

The TOE consists of two hardware components as listed in chapter 2 of this report. These components are not configurable. The following configurations are possible and were evaluated:

- MOD iSAS-P as a standalone solution in the IT environment. It implements all security functionality.
- MOD iSAS-P with MOD iSAS-RC 02 where the MOD iSAS-RC 02 is used to operate the TOE remotely via cable connection.

The security target [6] and [8], 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) [7] 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 EAL 5 extended by advice of the Certification Body for components beyond EAL 5.

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.

Although the TOE has been evaluated before, the evaluation results were not available to the ITSEF. Therefore this evaluation was not a re-evaluation.

The evaluation has confirmed:

- 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 cryptographic mechanisms. 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.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. 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

cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
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
VCS	Voice Communication System

13.2. Glossary

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

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

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

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

Informal - Expressed in natural language.

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

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

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 - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

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.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-0619-V2-2022, Version 2.2, 19 January 2021, Secure Audio Switch Security Target, EWSE23EN90001 , FREQUENTIS AG (confidential document)

[7] Evaluation Technical Report, Version 1.20, 03 February 2022, Summary of Evaluation Technical Reports BSI-DSZ-CC-0619-V2, Deutsche Telekom Security GmbH (confidential document)

[8] Security Target BSI-DSZ-CC-0619-V2-2022, Version 2.1, 02 February 2022, Secure Audio Switch Security Target Lite, EWSE23EN90002, FREQUENTIS AG (sanitised public document)

[9] Configuration list for the TOE, Version 1.3, 08 October 2021, Secure Audio Switch Configuration List (confidential document)

[10] Guidance documentation for the TOE, V1.4, 26 July 2021, Secure Audio Switch Operational User Guidance, EWSE23EN50004, FREQUENTIS AG

[7] specifically

- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies

[11] Preparative Procedures for the TOE, V1.5, 20 July 2021, Secure Audio Switch Preparative Procedures, EWSE23EN50003, FREQUENTIS AG

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report