BSI-DSZ-CC-1081-V3-2025

for

**Trusted Audio Switch with fiber optic (TAS-FO)
Version 2.0**

from

Rohde & Schwarz Topex S.A.

BSI-DSZ-CC-1081-V3-2025 (*)

Network Device

Trusted Audio Switch with fiber optic (TAS-FO)
Version 2.0

from	Rohde & Schwarz Topex S.A.
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4
valid until:	14 August 2030

SOGIS
Recognition Agreement

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), CEM:2022 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), CC:2022. 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.

Bonn, 15 August 2025

For the Federal Office for Information Security

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

Sandro Amendola   L.S.
Director-General

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

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 licensing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), CC:2022[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), CC:2022 [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 under SOGIS-MRA for all assurance components selected.

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 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 and ALC_FLR components.

---

4   Proclamation of the Bundesamtes für Sicherheit in der Informationstechnik vom 14. April 2023 auf https://www.bsi.bund.de

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 Trusted Audio Switch with fiber optic (TAS-FO), Version 2.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1081-V2-2020. Specific results from the evaluation process BSI-DSZ-CC-1081-V2-2020 were re-used.

The evaluation of the product Trusted Audio Switch with fiber optic (TAS-FO), Version 2.0 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 22 July 2025. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Rohde & Schwarz Topex S.A..

The product was developed by: Rohde & Schwarz Topex S.A..

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 evaluated guidance documentation and in the following report, are observed,

- the product is operated in the environment 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. 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. Therefore the BSI reserves the right to revoke the certificate, especially if a exploitable vulnerability of the certified product gets to known.

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 15 August 2025 is valid until 14 August 2030. Validity can be re-newed by re-certification.

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

---

[5]   Information Technology Security Evaluation Facility

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 Trusted Audio Switch with fiber optic (TAS-FO), Version 2.0 has been included in the BSI list of certified products, which is published regularly in the listing found at the BSI Website https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Further information can be obtained from BSI-Infoline +49 (0)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]   Rohde & Schwarz Topex S.A.
       9-9A Dimitrie Pompeiu Blvd, Iride Business Park, Building 19, ground floor, 1st, 2nd and 3rd floor, 2nd District
       020335 Bucharest
       Romania

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 a Trusted Audio Switch (TAS) as the key element in securing RED (CLASSIFIED) audio communication by keeping the RED and the BLACK (UNCLASSIFIED) network separated, while at the same time allowing the CWP (Controller Working Position) to work in a secure way with both RED and BLACK signals and media. This is visualized in Figure 1 "TOE Overview" of the Security Target [5].

The Security Target [5] 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.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [5], chapter 8.1. They are all selected from Common Criteria Part 2. Thus the claimed set of SFRs in the ST is CC Part2 conformant.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
TSF.VFC Voice Information Flow Control	Routing of CLASSIFIED / UNCLASSIFIED voice information from / to SECURE / UNSECURE domain to / from TAS-FO accessories
TSF.MNI Management Interface	Trusted status interface to the user
TSF.DFC User Interface Data Flow Control	Filter functionality for incoming and outgoing user data
TSF.PRT Protection of the TSF	Addresses fail security measures

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [5], chapter 9.

The assets to be protected by the TOE are defined in the Security Target [5], chapter 6.1. 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 [5], chapter 6.4, 6.5 and 6.6.

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:

Trusted Audio Switch with fiber optic (TAS-FO), Version 2.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	The TOE's reference is shown on a sticker applied on the TOE as follows: "Trusted Audio Switch with Fiber Optics, TAS-FO V2, CP2045.16.3.1"	Trusted Audio Switch with Fiber Optics, TAS-FO V2, CP2045.16.3.1	The Trusted Audio Switch is delivered as entire device (packed together with its accessories).
2	DOC	AGD_PRE.1 Preparative procedures R&S Trusted Audio Switch TAS-FO; Rohde & Schwarz [8] Filename: RST-AGD_PRE.1-TAS-FO V2_V3.0.pdf SHA-256: bddd5310081846f1dfe6178 132ff845e84c68df8f50ef5db b4f2691f24dbb2f6	v.3 rev.0 14.04.2025	Guidance documentation is delivered in a secure way in electronic form by signed e-mail using S/MIME.
3	DOC	AGD_OPE.1 Operational user guidance R&S Trusted Audio Switch TAS-FO; Rohde & Schwarz [9] Filename: RST- RST-AGD_OPE.1- TAS-FO V2_V3.0.pdf SHA-256: 9d630b842e7e81eba250bca 286d8701d8995fb9a219fc4f 27b4ac28703257ea2	v.3 rev.0 14.04.2025	Guidance documentation is delivered in a secure way in electronic form by signed e-mail using S/MIME.

Table 2: Deliverables of the TOE

The TOE Trusted Audio Switch with fiber optic (TAS-FO) product code: CP2045.16.3.1 is an electronic device, consisting of hardware and firmware, and additionally of documentations.

The delivery of the TOE from the production facility to the customer is described briefly in the following:

The delivery items are secured during the logistic process from pick-up until delivery with a transfer security tape that indicates if the package was opened during the process by showing an "OPENED!" message if the tape was manipulated. The developer included pictures of broken and unbroken seals in the documentation. A tampered security label can be easily distinguished from an unbroken security label.

Guidance documentation is delivered in a secure way in electronic form by signed e-mail using S/MIME, table 2 shows the SHA-256 hash values for both documents.

For the delivery procedure, only special delivery services are used. Those have to provide certain security measures like a box-trailer or anti-slash-curtains, the driver has to undergo special training and be available permanently on his mobile phone. Further security measures are described and applied.

The transport is monitored and tracked during the whole delivery process.

Furthermore the customer is obligated to perform several acceptance checks ensuring the integrity and authenticity of the delivery. These specific checks are specified in Chapter 5 of the Preparative user guidance [8] (cf. also Table 2 No. 2).

3.   Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. The TOE implements user data protection based on information flow control policies addressing the separation of audio data flows. In addition, the TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Security Management
- the Protection of the TSF

Specific details concerning the above mentioned security policies can be found in Chapter 8 of the Security Target [5].

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: OE.Physical_Protection, OE.TEMPEST_Zone, OE.TEMPEST_Evalutation, OE.Physical_Access, OE.Training, OE.Authorization, OE.Installation, OE.Audio Devices, OE.Neighbour_Acoustic_Coupling, OE.PU, OE.RED_PU, OE.Video, OE.Cabling, OE.Rec.

Details can be found in the Security Target [5], chapter 7.2.

5.   Architectural Information

The TOE "Trusted Audio Switch with fiber optic (TAS-FO-V2) product code: CP2045.16.3.1" is a stand-alone product intended to be used in a wider network structure.

The physical scope comprises the Trusted Audio Switch itself together with its interfaces. Based on these physical interfaces the TOE is divided into the following four functional blocks:

1. The audio path, including the headset connectors, external speaker and footswitch PTT (digital plus analog signals), with RED and BLACK concept separation;

2. the video path, including the HDMI connector, with Red and Black separation;

3. the decision block, which is managing the switching action between RED (CLASSIFIED) and BLACK (UNCLASSIFIED) domains, including the USB touch connector and the external mechanical RED/BLACK selector switch;

4. the data filter, where the TOE protects communication with RED and BLACK Processing Units, including the Gigabit Fiber Optic Interfaces and the trusted filter block, which is performing deep inspection on the specific Ethernet packets that transit from one domain to another.

A general overview about the external equipment together with a sketched internal overview can be anticipated from the Security Target [5], Figure 1: TOE Overview.

All subsystems of the TOE are identified as TSF subsystems and the developer has distinguished four TSF subsystems:

- Data Filter Flow Control
- Video Data Flow Control
- Voice Data Flow Control
- State Control

This subsystems are realized as a combination of software and hardware, as follows:

- FPGA configured with logic blocks defined by the developer, supported by logic blocks provided by the FPGA supplier for generic functions (Ethernet connection, memory access and video output);
- circuits to drive external interfaces (network, audio, video);
- a microcontroller with firmware written by the developer using libraries provided by the supplier to drive the USB interface.

Together with the circuit board, which physically supports and connects the hardware components, and the casing, which makes the external interfaces and LEDs accessible to the user, these subsystems constitute the TOE.

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 TOE has only one configuration. Depending on each test case, the test environment can differ from one test case to another.

7.1. Test Configuration

The test configuration consists of the TOE with its accessories and a Test-Laptop connected to both Processing Units, PU_RED and PU_BLACK. See Figure 1 in the Security Target [5] for the setup without the Laptop.

The Laptop is used to write/build a test application and to access the PU_RED and PU_BLACK terminals. The network packets between the TOE and the PUs are 802.3 Ethernet packets without 802.1Q VLAN tag or IP headers. The test application uses raw sockets, with this the application gets control over all the headers i.e. Ethernet, TCP, IP etc. from the network and can inject packets with custom headers and data directly into the network. The test application can be run on PU_RED or PU_BLACK or both, depending on each test case.

The application sends frames from specific MAC source address (PUs) to specific MAC destination address (TOEs) with specific Ethertype and payload data (according to the chosen test case option / ID).

In order to analyse what frames are sent / received to / from the TOE the packet analyser tcpdump was used. It prints out a description of the contents of packets on a network interface. In the test cases it is specified on which processing unit (PU_RED or PU_BLACK) to start the tcpdump capture and what result to expect. The tcpdump packet analyser can be run from both sides of the connection between the TOE and the PUs either with specific filter or without any filter option to see all exchanging packets.

7.2.   Developer Tests

The developer defined several groups of TOE functionality requirements (HWx/SWx) and 93 test cases manually to run for all those functional requirements. Each requirement gives a statement about the behaviour of the TOE's subsystems, regardless if it is hardware or software, under a well-defined situation.

Each test case includes the purpose, a test pre-condition, the TOE functionality requirements (HWx/SWx) that would be tested, acceptance criteria, a step-by-step plan for the interactive test and expected behaviour of the subsystem or module for each step.

The developer specified and implemented test cases for each defined TSFI and each sub-system/module. Thus, all subsystems are covered by several test cases and each SFR-enforcing module is covered by at least one test case.

To ensure that the security functionality (SFRs) is completely covered by test cases, the developer also mapped all relevant test cases directly to SFRs.

Testing Results

All test cases were executed by the developer successfully and ended up with the expected result.

7.3.   Independent Evaluator Tests

For the independent testing the original test environment provided by the developer has been used at the evaluators site. Therefore the test configuration was the same as already reported in Chapter 7.1.

The evaluators have developed a sampling strategy to repeat selected developer tests from Chapter 7.2.

The reason why the evaluators repeated the sampled developer tests is that these tests are important for a correct implementation of the security relevant functionality of the TOE. As not all the developer tests are relevant for security aspects of the TOE, the developer tests have been chosen so that they cover all security functionality requirements, all subsystems of the TOE and additionally some not security relevant functional and hardware visual inspection was done.

Furthermore a set of 3 independent tests were developed and executed by the evaluators.

Testing Results

The overall test result is that no deviations were found between the expected and the actual test results.

7.4. Vulnerability Analysis

Having performed the vulnerability analysis, the evaluator determined that the TOE is free of exploitable or residual vulnerabilities under the claimed attack potential.

8. Evaluated Configuration

The TOE is integrated into a standard 1 RU chassis, secured by a Transfer Security Label covering the rear/left and rear/right chassis screws. The product label should show the following informations:

- The trade name: TAS-FO V2
- The trade description: Trusted Audio Switch with fiber optic (TAS-FO)
- The unique product code: CP2045.16.3.1

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [6] 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.

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)

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1081-V2-2020, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on a site audit for a changed development and production site as well as a new vulnerability analysis.

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

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 [5] 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
FO	Fiber Optic
FPGA	Field-Programmable Gate Array
HW	Hardware
ID	Identifier
IT	Information Technology

ITSEF	Information Technology Security Evaluation Facility
IP	Internet Protocol
LED	Light-Emitting Diode
PP	Protection Profile
PTT	Push To Talk
PU	Processing Unit
PU_BLACK	Processing Unit Black
PU_RED	Processing Unit Red
RU	Rack Unit
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
SW	Software
TAS	Trusted Audio Switch
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus
VLAN	Virtual LAN

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.

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/CC
       ISO-Version:
       ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
       - Part 1: Introduction and general model
       - Part 2: Security functional components
       - Part 3: Security assurance components
       - Part 4: Framework for the specification of evaluation methods and activities
       - Part 5: Pre-defined packages of security requirements
       https://www.iso.org/standard/72891.html
       https://www.iso.org/standard/72892.html
       https://www.iso.org/standard/72906.html
       https://www.iso.org/standard/72913.html
       https://www.iso.org/standard/72917.html
       CCRA-Version:
       CC:2022 R1, Common Criteria for Information Technology Security Evaluation
       - Part 1: Introduction and general model
       - Part 2: Security functional components
       - Part 3: Security assurance components
       - Part 4: Framework for the specification of evaluation methods and activities
       - Part 5: Pre-defined packages of security requirement
       https://www.commoncriteriaportal.org

[2]   Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der
       Sicherheit von Informationstechnik (Common Methodology for Information
       Technology Security Evaluation (CEM), Evaluation Methodology
       ISO-Version:
       ISO 18045:2022: Information technology Security techniques Methodology for IT
       security evaluation
       https://www.iso.org/standard/72889.html
       CCRA-Version:
       CEM:2022 R1, Common Methodology for Information Technology Security
       Evaluation
       https://www.commoncriteriaportal.

[3]   BSI certification: Scheme documentation describing the certification process (CC-
       Produkte) and Scheme documentation on requirements for the Evaluation Facility,
       approval and licensing (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

---

[7]specifically

- AIS 1, Version 14, 2027-10-11, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers

[5]   Security Target BSI-DSZ-CC-1081-V3-2025, Edition 3.0, Revision 5, 2025-05-05, Security Target R&S Trusted Audio Switch, Rohde & Schwarz

[6]   Evaluation Technical Report, Version 2.9, 2025-06-30, Evaluation Technical Report (ETR), SRC Security Research & Consulting GmbH (confidential document)

[7]   Configuration list for the TOE, Edition 3, Revision 2, 2025-06-18, ALC_CMS.4 Problem tracking CM coverage R&S Trusted Audio Switch TAS-FO-V2, Rohde & Schwarz (confidential document)

[8]   Guidance documentation for the TOE, Edition 3, Revision 0, 2025-04-14, AGD_PRE.1 Preparative procedures R&S Trusted Audio Switch TAS-FO; Rohde & Schwarz

[9]   Guidance documentation for the TOE, Edition 3, Revision 0, 2025-04-14, AGD_OPE.1 Operational user guidance R&S Trusted Audio Switch TAS-FO; Rohde & Schwarz

- AIS 38, Version 2, 2007-09-28, Reuse of evaluation results

C.   Excerpts from the Criteria

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

- On conformance claim definitions and descriptions refer to CC:2022 part 1 chapter 10.5

- On the concept of assurance classes, families and components refer to CC:2022 Part 3 chapter 6.1

- On the concept and definition of pre-defined assurance packages (EAL) refer to CCRA CC:2022 Part 5.

- On the assurance class ASE for Security Target evaluation refer to CC:2022 Part 3 chapter 9

- On the detailed definitions of the assurance components for the TOE evaluation refer to CC:2022 Part 3 chapters 7 to 15

- The table 1 in CC:2022 part 5, Chapter 4.2 summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published as the CCRA Version at
https://www.commoncriteriaportal.org/cc/index.cfm

The CC are published as the ISO/IEC Version at
https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

D.   Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report