

# Certification Report

**BSI-DSZ-CC-1081-V2-2020**

for

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

from

**Rohde & Schwarz Topex S.A.**

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-1081-V2-2020 (\*)**

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



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), Version 3.1 extended by Scheme Interpretations 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.

Bonn, 18 August 2020

For the Federal Office for Information Security

Sandro Amendola  
Head of Division

L.S.



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



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.....	6
1. Preliminary Remarks.....	6
2. Specifications of the Certification Procedure.....	6
3. Recognition Agreements.....	7
4. Performance of Evaluation and Certification.....	8
5. Validity of the Certification Result.....	8
6. 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.....	16
6. Documentation.....	17
7. IT Product Testing.....	17
8. Evaluated Configuration.....	20
9. Results of the Evaluation.....	20
10. Obligations and Notes for the Usage of the TOE.....	21
11. Security Target.....	21
12. Definitions.....	21
13. Bibliography.....	23
C. Excerpts from the Criteria.....	24
D. Annexes.....	25

## A. Certification

### 1. Preliminary Remarks

Under the BSIG<sup>1</sup> 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<sup>1</sup>
- BSI Certification and Approval Ordinance<sup>2</sup>
- BMI Regulations on Ex-parte Costs<sup>3</sup>
- 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]

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

<sup>2</sup> 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

<sup>3</sup> 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 Criteria for IT Security Evaluation (CC), Version 3.1<sup>4</sup> [1] also published as ISO/IEC 15408.
- 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 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.

<sup>4</sup> Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

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 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-1081-2020. Specific results from the evaluation process BSI-DSZ-CC-1081-2020 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 13 August 2020. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)<sup>5</sup> 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 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 18 August 2020 is valid until 17 August 2025. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

<sup>5</sup> Information Technology Security Evaluation Facility

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 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 (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<sup>6</sup> of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

<sup>6</sup> Rohde & Schwarz Topex S.A.  
71-73 Nicolae Caramfil Street, 2nd Floor, 1st District  
014142 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 [6].

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.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 8.1. 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	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 [6], chapter 9.

The assets to be protected by the TOE are defined in the Security Target [6], 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 [6], chapters 6.4 to 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"	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.1-2003.1012.02_v17.pdf  SHA-256: A332FA6CF4467D4B 33D7B50F4A906634 CEBC749E4EBBF836 F311C921D886A980	v.1 rev.17 02.04.2020	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.1-2003.1012.02_v1.7.pdf  SHA-256: 4992B471909009E8 862489EB5A680A14 AA9ED64CF30E602F E48ABE43027A40D4	v.1 rev.7; 08.07.2020	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 Document [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
- Protection of the TSF

Specific details concerning the above mentioned security policies can be found in Chapter 8 of the Security Target [6].

### 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: The TOE and the RED/BLACK Processing Unit are installed in a physically protected area (operational environment) during operation which is approved for the highest security level of information handled by the TOE.
  - OE.Physical\_Protection: The operation site shall have physical protection, which is at least approved for the highest level of information handled in the TOE.
  - OE.Physical\_Access: Only authorized persons shall be given physical access to the TOE, PU\_RED and Recording Storage device.
  - OE.Installation: The TOE shall be installed and maintained according to the installation and maintenance guidelines. The installation shall assure that the status domain of the TOE is visible to the operator and also the Red Lamp Indicator is visible to the neighbouring operators.
  - OE.Rec: The Recording Storage device connected to the PU\_RED shall be accredited for the highest security classification processed in the system.

The Recording Storage device connected to the PU\_RED shall have physical protection, which is at least approved for the highest level of information handled in the TOE.

The logical access to the Recording Storage device connected to the PU\_RED shall be protected but also the confidentiality during different life cycles of stored data (i.e. audio play, secure deletion).

- A.TEMPEST\_Zone: The TOE is operated in a TEMPEST zone that allows the use of commercial of the shelf products for the processing of the highest security levels of information handled by the TOE.
  - OE.TEMPEST\_Zone: The TOE shall be operated in a TEMPEST facility zone that allows the use of COTS products for the processing of highest security level of information handled in the TOE.
- A.TEMPEST\_Evaluation: The TOE is evaluated against TEMPEST attacks, which are out of scope of the CC evaluation.
  - OE.TEMPEST\_Evaluation: The TOE shall be a subject to a TEMPEST evaluation, which is carried out independent of Common Criteria certification.
- A.Training: All operators are trained in the correct use to the TOE and Processing Units and follow the operational guidelines.
  - OE.Training: The operators shall be trained to use the TOE. If the TOE is controlled via an external user interface, that is not part of the TOE, the operators shall be trained to check the assured status domain indication at the TOE.
- A.Authorization: All operators are authorized for all information handled by the TOE through the minimum level of clearance for the highest security level of information handled by the TOE.
  - OE.Authorization: All operators shall have a minimum clearance for the maximum-security level of information handled in the TOE. Operator activity shall be monitored and operator shall be accountable for their actions and follow the work instructions and operational guidance of the TOE.
  - OE.Rec: The Recording Storage device connected to the PU\_RED shall be accredited for the highest security classification processed in the system.

The Recording Storage device connected to the PU\_RED shall have physical protection, which is at least approved for the highest level of information handled in the TOE.

The logical access to the Recording Storage device connected to the PU\_RED shall be protected but also the confidentiality during different life cycles of stored data (i.e. audio play, secure deletion).

- A.Installation: The TOE is installed and maintained according to the installation and maintenance guidelines.
  - OE.Installation: The TOE shall be installed and maintained according to the installation and maintenance guidelines. The installation shall assure that the status domain of the TOE is visible to the operator and also the Red Lamp Indicator is visible to the neighbouring operators.
  - OE.Cabling: The Fiber Optic connection between Processing Units and TOE shall use the appropriate connectors:
    - PU\_RED shall be connected to “SECURE FO” Fiber Optic connector;

- PU\_BLACK shall be connected to “UNSECURE FO” Fiber Optic connector.
  - OE.Rec: The Recording Storage device connected to the PU\_RED shall be accredited for the highest security classification processed in the system.  
The Recording Storage device connected to the PU\_RED shall have physical protection, which is at least approved for the highest level of information handled in the TOE.  
The logical access to the Recording Storage device connected to the PU\_RED shall be protected but also the confidentiality during different life cycles of stored data (i.e. audio play, secure deletion).
- A.Audio\_Devices: Appropriate audio devices and associated cables prevent unacceptable acoustic coupling between:
  - Earpiece and microphone
  - Ambient noise and microphone

This does not hold up for the handset.

  - OE.Audio Devices: Appropriate Audio devices, Headsets or Handset, shall be used in order to prevent unacceptable acoustic coupling between:
    - Headset, when receiving CLASSIFIED voice information while transmitting UNCLASSIFIED voice information.
    - A neighbouring operator and the microphone of the operator, when the neighbouring operator is talking CLASSIFIED information while the operator transmits UNCLASSIFIED voice information.

To prevent neighbouring acoustic coupling, the operator shall ensure that the PTT is inactive if the TOE is in Unsecure state and External Red Lamp Indicator is On at the neighbour Operator.
- A.PU: Voice Information from the PU\_RED is separated from the PU\_BLACK. Vulnerabilities of the Processing Units or its Connections are not part of the TOE and its evaluation.  
PU\_RED communication channels that leave the operational environment are either encrypted with approved crypto devices or implemented as approved circuits (SECURE channels). Vulnerabilities of this out of bounds RED communication channels are not part of the TOE and its evaluation.
  - OE.PU: The voice information transmitted by the PU\_RED shall be strictly separated (logical or physical) from the voice information transmitted by the PU\_BLACK. All communication channels of the PU\_RED that leave the operational environment either shall be encrypted with approved crypto devices or implemented as approved circuits (SECURE channels).
- A.RED\_PU: The PU\_RED is accredited for the highest security classification processed in the system.
  - OE.RED\_PU: The PU\_RED shall be accredited for the highest security classification processed in the system.
  - OE.Rec: The Recording Storage device connected to the PU\_RED shall be accredited for the highest security classification processed in the system.

The Recording Storage device connected to the PU\_RED shall have physical protection, which is at least approved for the highest level of information handled in the TOE.

The logical access to the Recording Storage device connected to the PU\_RED shall be protected but also the confidentiality during different life cycles of stored data (i.e. audio play, secure deletion).

- A.Video: The TED displays the RED/BLACK video streams provided by the TOE separated in such a way that it is visible that the TOE is operating in the intended transfer mode SECURE/UNSECURE.
  - OE.Video: The Touch Entry Displays that are used to connect to the TOE and provide separated touch areas are only operated in the SECURE physical operational environment to assure only accountable personnel is using the TED and the displays are not manipulated.
- OE.Neighbour\_Acoustic\_Coupling: Each operator is made unambiguously aware of the CLASSIFIED/UNCLASSIFIED voice information status of a neighbouring operator by watching the Red Lamp Indicator.

Operational procedures, not technical solutions, shall regulate concurrent use of CLASSIFIED and UNCLASSIFIED conversations to prevent acoustic coupling of CLASSIFIED conversations to be transmitted on UNCLASSIFIED communication channels.

Please note that some security objectives for the operational environment cover more than one assumption. In such a case the security objective for the operational environment has been repeated several times in the list given above. For the security objective OE.Neighbour\_Acoustic\_Coupling no assumption is given because it is derived from the Threat T.Acoustic\_Coupling.

## 5. Architectural Information

The TOE “Trusted Audio Switch with fiber optic (TAS-FO) 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 analogical 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) domain and BLACK (UNCLASSIFIED) domain, 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 seen in the Security Target [6], 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);
- integrated 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 [6] 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 subsystem/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) [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.

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-1081-2020, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on

- the operation of the MIXED mode, where the reception of CLASSIFIED is now summed with UNCLASSIFIED voice information on the right ear and only CLASSIFIED voice information is on the left ear,
- the external Red Lamp indicator, which is now active only when the system is in SECURE state, the HDMI Display and Touch devices are detected and the Operator is successful is logged in,
- plus some bug fixes and smaller optimizations.

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

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.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

## 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. Definitions

### 12.1. Acronyms

<b>AIS</b>	Application Notes and Interpretations of the Scheme
<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
<b>BSIG</b>	BSI-Gesetz / Act on the Federal Office for Information Security
<b>CCRA</b>	Common Criteria Recognition Arrangement
<b>CC</b>	Common Criteria for IT Security Evaluation
<b>CEM</b>	Common Methodology for Information Technology Security Evaluation
<b>cPP</b>	Collaborative Protection Profile
<b>CWP</b>	Controller Working Position
<b>EAL</b>	Evaluation Assurance Level
<b>ETR</b>	Evaluation Technical Report
<b>FO</b>	Fiber Optic
<b>FPGA</b>	Field-Programmable Gate Array
<b>HW</b>	Hardware
<b>ID</b>	Identifier
<b>IT</b>	Information Technology
<b>ITSEF</b>	Information Technology Security Evaluation Facility

<b>IP</b>	Internet Protocol
<b>LED</b>	Light-Emitting Diode
<b>PP</b>	Protection Profile
<b>PTT</b>	Push To Talk
<b>PU</b>	Processing Unit
<b>PU_BLACK</b>	Processing Unit Black
<b>PU_RED</b>	Processing Unit Red
<b>RU</b>	Rack Unit
<b>SAR</b>	Security Assurance Requirement
<b>SFP</b>	Security Function Policy
<b>SFR</b>	Security Functional Requirement
<b>ST</b>	Security Target
<b>SW</b>	Software
<b>TAS</b>	Trusted Audio Switch
<b>TCP</b>	Transmission Control Protocol
<b>TED</b>	Touch Entry Device
<b>TOE</b>	Target of Evaluation
<b>TSF</b>	TOE Security Functionality
<b>USB</b>	Universal Serial Bus
<b>VLAN</b>	Virtual LAN

## 12.2. 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.

### 13. 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<sup>7</sup>  
<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/zertifizierungsberichte>
- [6] Security Target BSI-DSZ-CC-1081-V2-2020, Version 1.7, Revision 19, 2020-07-09, Security Target R&S Trusted Audio Switch, Rohde & Schwarz Topex S.A.
- [7] Evaluation Technical Report, Version 2.7, 2020-07-30, Evaluation Technical Report (ETR), SRC Security Research & Consulting GmbH (confidential document)
- [8] AGD\_PRE.1 Preparative procedures R&S Trusted Audio Switch TAS-FO, Version 1.17, 2020-04-02, Rohde & Schwarz
- [9] AGD\_OPE.1 Operational user guidance R&S Trusted Audio Switch TAS-FO, Version 1.7, 2020-07-08, Rohde & Schwarz

<sup>7</sup>specifically

- AIS 14, Version 7, 2010-08-03, Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC
- AIS 19, Version 9, 2014-11-03, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR für Evaluationen nach CC
- AIS 23, Version 4, 2017-03-15, Zusammentragen von Nachweisen der Entwickler
- 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 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.