



<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

# Security Target NAVICS MLS Boundary Protection System Operational Software

Subject to  
change  
without notice

Document Title:  
Security Target NAVICS MLS Boundary Protection System Operational Software  
Order Customer: Rohde & Schwarz SIT GmbH  
Contract Number: 3MT 2340/08.08

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 1 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

**Table of Contents**

1 Introduction..... 4

1.1 Change History ..... 4

1.2 Referenced Documents ..... 7

1.2.1 General Referenced Documents ..... 7

1.2.2 Supporting, Project Specific Referenced Documents ..... 7

1.3 Abbreviations ..... 7

2 ST Introduction ..... 10

2.1 ST Reference ..... 10

2.2 TOE Reference ..... 10

2.2.1 TOE Identification..... 10

2.2.2 Development Site ..... 11

2.3 TOE Overview ..... 11

2.3.1 Required non-TOE hardware/firmware/software ..... 12

2.3.2 Major security features ..... 13

2.4 TOE Description ..... 14

2.4.1 Physical Scope of the TOE ..... 15

2.4.2 Logical Scope of the TOE ..... 18

3 Conformance Claims..... 22

4 Security Problem Definition..... 22

4.1 Threats ..... 23

4.2 Organisational Security Policies ..... 23

4.3 Assumptions..... 23

5 Security Objectives ..... 24

5.1 Security Objectives for the TOE..... 24

5.2 Security Objectives for the Operational Environment ..... 25

5.3 Security Objectives Rationale ..... 26

5.3.1 Security Objectives counter Threats ..... 27

5.3.2 Security Objectives for the environment uphold Assumptions..... 28

6 Extended Components Definition ..... 28

7 Security Requirements ..... 29

7.1 Security Functional Requirements (SFRs)..... 29

7.1.1 FCS\_COP.1 Cryptographic operation..... 29

7.1.2 FDP\_ITC.1 Import of user data without security attributes ..... 29

7.1.3 [TFM]FDP\_IFC.1 Subset information flow control [iteration for Trusted Filter Management (TFM)] ..... 30

7.1.4 [TFM]FDP\_IFF.1 Simple security attributes [iteration for Trusted Filter Management (TFM)] ..... 31

7.1.5 [TFV]FDP\_IFC.1 Subset information flow control [iteration for Trusted Filter Voice (TFV)] ..... 33

7.1.6 [TFV]FDP\_IFF.1 Simple security attributes [iteration for Trusted Filter Voice (TFV)] ..... 33

7.1.7 [VT]FDP\_IFC.1 Subset information flow control [iteration for Voice Terminal Security Module (VTSM)] ..... 35

7.1.8 [VT]FDP\_IFF.1 Simple security attributes [iteration for Voice Terminal Security Module (VTSM)] ..... 36

7.1.9 FDP\_ITT.2 Transmission separation by attribute ..... 38

7.1.10 FMT\_SMF.1 Specification of Management Functions ..... 38

7.1.11 FPT\_RCV.1 Manual recovery ..... 39


7.2 Security Assurance Requirements (SARs) ..... 40

7.3 Security Requirements Rationale ..... 41

7.3.1 Justification of SFR/SAR dependencies ..... 41

Subject to  
change  
without notice

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 2 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	
-------------------	--	---

7.3.2 SFRs trace to and meet all security objectives for the TOE .....42

7.3.3 Explanation of the chosen SARs .....43

8 TOE Summary Specification .....44

8.1 Management Traffic Filtering SFP (<sup>[TFM]</sup>FDP\_IFC.1, <sup>[TFM]</sup>FDP\_IFF.1, FMT\_SMF.1).....44

8.2 Voice Traffic Filtering SFP (<sup>[TFV]</sup>FDP\_IFC.1, <sup>[TFV]</sup>FDP\_IFF.1, FMT\_SMF.1) .....44

8.3 Voice Traffic Authorisation SFP (<sup>[VT]</sup>FDP\_IFC.1, <sup>[VT]</sup>FDP\_IFF.1, FMT\_SMF.1) .....45

8.4 Internal TOE transfer protection (FDP\_ITT.2, FCS\_COP.1, FDP\_ITC.1) .....45

8.5 Secure State (FMT\_SMF.1, FPT\_RCV.1) .....45

**List of Figures**

Figure 1: Simplified illustration of NAVICS MLS Boundary Protection System..... 12

Figure 2: R&S TF5900M Trusted Filter IP ..... 13

Figure 3: R&S GB5900SM Voice Terminal Softkey ..... 13

Figure 4: Boundary protection system elements in the NAVICS MLS network ..... 14

Figure 5: Block diagram of non-TOE Voice Terminal Softkey (VT) with embedded VTSM ..... 16

Figure 6: Non-TOE hardware, platform software (PFSW) and crypto application software (CApp) parts of VTSM indicating the software modules that implement SEF in operational mode ..... 16

Figure 7: Basic architecture of non-TOE Trusted Filter IP based on R&S SITLine IP ..... 17

Figure 8: Non-TOE hardware, platform software (PFSW) and crypto application software (CApp) parts of TFMSM in Trusted Filter Voice resp. Trusted Filter Management (without CMAC verification) indicating the software modules that implement SEF in operational mode ..... 17

Figure 9: Payload paths within Trusted Filter Voice (TFV)..... 19

Figure 10: Block diagram of voice traffic filtering ..... 20

Figure 11: Payload paths within Trusted Filter Management (TFM) ..... 21

Figure 12: Block diagram of management traffic filtering ..... 21

Subject to change without notice

**List of Tables**

Table 1: Change History ..... 6

Table 2: General referenced documents ..... 7

Table 3: Supporting, project-specific referenced documents ..... 7

Table 4: Abbreviations ..... 9

Table 5: Tracing of Security Objectives to Security Problem Definition ..... 26

Table 6: List of subjects, information, and operations covered by Management Traffic Filtering SFP ..... 31

Table 7: Rules of the Management Traffic Filtering SFP for permitting an information flow ..... 32

Table 8: List of subjects, information, and operations covered by Voice Traffic Filtering SFP ..... 33

Table 9: Rules of the Voice Traffic Filtering SFP for permitting an information flow ..... 35

Table 10: List of subjects, information, and operations covered by Voice Traffic Authorisation SFP ..... 36


Table 11: Rules of the Voice Traffic Authorisation SFP for permitting an information flow ..... 37

Table 12: Security Assurance Requirements (EAL4 augmented with AVA\_VAN.4) ..... 40

Table 13: SFR dependencies justification ..... 41

Table 14: Tracing of SFRs to TOE Security Objectives ..... 42

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 3 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---


## 1 Introduction

### 1.1 Change History

Version	Date	Author	Remark
09.00	2022-11-03	Ms. Joeckel (SIT)	5.2: OE.SecureRules extended
08.00	2022-08-04	Mr. Vogt (DFKI)	2.2.1: Manual versions updated 2.4.2.3: Rephrased SEF.Management.Protocol_Check to be consistent with Table 7 (drop [protocol]) 5.1: Rephrased OT.TrustedFilterManagement to be consistent with Table 7 (drop [protocol]) 7.1.10: Added refinement to FMT_SMF.1.1
07.00	2022-07-19	Mr. Vogt (DFKI)	5.2: OE.SecureRules extended 7.3.1: Dependency on FCS_CKM.4 addressed by OE.SecureRules 7.3.1: Minor corrections
	2022-07-19	Mr. Dischinger (SIT)	Table 7: Rephrasing of drop [protocol]
	2022-07-18	Mr. Joeckel (SIT)	2.1: Title adapted 7.1.1 deleted All: References to FCS_CKM4. removed
	2022-07-15	Ms. Joeckel (SIT)	2.2.1: Manual versions updated
06.00	2022-06-01	Mr. Vogt (DFKI)	8.1, 8.2: Added: protocol filter configuration implemented by SEF.Policy_Management
05.00	2022-05-25	Mr. Vogt (DFKI)	2.4.2, 8.1, 8.2, 8.5: Clarification: Removal of filter configuration and security attributes 2.4.2.2, 8.2,: Clarification: Detachment of tag 5.1: Clarification: OT.SecureState: Cause of leaving operational state 7.1.1: Clarification: Removal from storage 7.1.10, 8.1, 8.2, 8.5: Clarification: deletion -> removal
04.00	2022-02-02	Mr. Joeckel (SIT)	Sec. 2.2.1, Table 4: Difference software version - PDM PCI added
03.00	2021-12-17	Mr. Vogt (DFKI)	Sec. 2.3.2, 2.4, 2.4.2.1, 2.4.2.2, 5.1, 5.2, 7.1.5, Table 9, Table 10, Table 11, 7.1.9, 7.3.2: Clarification regarding usage of different cryptographic keys and network segments Sec. 7.1.2, 7.1.11, 7.3.1, Table 14, 8.4: FDP_ITC.2 replaced by FDP_ITC.1

Subject to  
change  
without notice


R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 4 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

Version	Date	Author	Remark
02.00	2021-11-15	Mr. Joeckel (SIT)	Sec. 2.1: Reference and date updated Sec. 1.3; 2.2.1: TFSM introduced Sec. 2.3; 2.4: TFSM included; TOE Boundary in Figure 1 and Figure 2 deleted Sec. 2.2.1: Voice Terminal Softkey User Manual, Part Number and Version updated Figures 7, 9, 10, 11, 12: RSM changed to TFSM
01.17	2021-03-22	Mr. Joeckel (SIT)	Sec. 2.1: Reference and date updated Sec. 2.2.1: Versions updated Sec. 2.3; 2.4: Adapted to Security Architecture latest issue Figure 1; Figure 4: Adapted to Security Architecture latest issue Sec. 7.1.10: Textual correction
01.16	2020-12-17	Mr. Vogt (DFKI)	Sec. 2.4.1 and 2.4.2: Minor corrections
01.15	2020-12-11	Mr. Vogt (DFKI)	Sec. 2.2.1: Added preparative guidance to the TOE parts Sec. 2.4.1 and 2.4.2: Clarified physical/logical scope
01.14	2020-11-23	Dr. Dischinger (SIT)	Sec. 2.3.1: TFM and TFV can be combined on one device Sec. 2.3: Added NAT Sec. 2.4: TFM and TFV are different only in config.
01.13	2020-11-18	Mr. Vogt (DFKI)	Change of the TOE boundary: TF / VTSM software only Exclude tamper protection from the TSF Sec. 2.2.1: TOE reference identifies NAVICS MLS operational software for multi-purpose platform Sec. 2.2.2: Removed production site Sec. 2.3.1: Description of non-TOE multi-purpose platform Sec. 2.4.1: Physical scope refers to NAVICS MLS operational software for multi-purpose platform Sec. 5.2 and 5.2: Extended objectives and rationale for security features of the multi-purpose platform All sections: Update of text and figures to the change of the TOE boundary
01.12	2020-08-25	Mr. Vogt (DFKI)	Correction of abbreviation RSM Sec. 2.2: Added identification of two TOE configurations Sec. 2.4.1: Correction of method of delivery (electronic shipment of user manuals)
01.11	2020-06-30	Mr. Vogt (DFKI)	Further update of some Figures. Clarification of DMS scope (devices/protocols supported)
01.10	2020-06-29	Mr. Vogt (DFKI)	Update of Figures. Completion of list of abbreviations. Identification of supported management protocols.
01.09	2020-06-23	Mr. Vogt (DFKI)	Minor changes according to BSI review. Change of the TOE boundary: VTSM instead of VT.

Subject to  
change  
without notice

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 5 of 45


<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

Version	Date	Author	Remark
01.08	2020-03-03	Mr. Vogt (DFKI)	Security Functional Requirements (Sec. 7.1): Corrections in Voice Traffic Authorisation SFP ( <sup>[VT]</sup> FDP_IFC.1 and <sup>[VT]</sup> FDP_IFF.1), and SFR elements FDP_IFF.1.5 (all iterations) and FMT_SMF.1.1, according to evaluation findings. Renamed SEF.Management to SEF.Policy_Management for disambiguation. Adaptation of dependent sections according to the changes indicated above.
01.07	2020-02-11	Mr. Vogt (DFKI)	Corrections in ST introduction (Sec. 2), Security Objectives (Sec. 5), Security Functional Requirements (Sec. 7.1) and TOE Summary Specification (Sec. 8) according to evaluation findings
01.06	2020-02-10	Mr. Vogt (DFKI)	Corrections in ST introduction (Sec. 2) and Security Functional Requirements (Sec. 7.1) according to evaluation findings
1.05	2020-01-27	Mr. Vogt (DFKI)	Restructuring of TOE description. Corrections in TOE summary specification
1.04	2020-01-22	Mr. Vogt (DFKI)	Changes in all sections according to evaluation findings. FDP_ITT.4 removed (already covered by Voice Traffic Filtering/Autorisation SFPs) FPT_FLS.1 removed (not adequate) FMT_SMF.1 added
1.03	2019-10-14	Mr. Kraxberger	Changes to the lifecycle description, added figure for payload paths for TFM, minor corrections. Changes to figures and description to include boundaries and names of SFs.
1.02	2019-07-11	Mr. Schütze (SIT)	Section 2.4.2.2: explain different payload paths, small fix in Figure 6 (one SLE78 removed), new Figure 7. Change SEF.SIP.Voice.Deep_Packet_Inspection to SEF.Voice.Deep_Packet_Inspection as DPI is for RTP, too. Change description and rulesets.
1.01	2019-06-28	Mr. Vogt (DFKI) Mr. Schütze (SIT)	OE.PROTECTEDTRANSMISSION reformulated. SFR components added: FCS_CKM.4, FCS_COP.1, FDP_ITC.2, FPT_TDC.1 Explain NetworkID
1.00	2019-04-12	Mr. Schütze (SIT) Mr. Vogt (DFKI)	Initial version

Subject to  
change  
without notice

Table 1: Change History

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 6 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	--

## 1.2 Referenced Documents

### 1.2.1 General Referenced Documents

Document	Remark / Description
NIST SP 800-38B	NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005 (updated 10-06-2016) <a href="https://doi.org/10.6028/NIST.SP.800-38B">https://doi.org/10.6028/NIST.SP.800-38B</a>
FIPS PUB 197	NIST Federal Information Processing Standards Publication 197 Advanced Encryption Standard (AES) November 26, 2001 <a href="https://doi.org/10.6028/NIST.FIPS.197">https://doi.org/10.6028/NIST.FIPS.197</a>

Table 2: General referenced documents

### 1.2.2 Supporting, Project Specific Referenced Documents

Document	Remark / Description
[1] Glossary	Project-specific Glossary for NAVICS MLS Boundary Protection, part number 5414.8533.92


Table 3: Supporting, project-specific referenced documents

## 1.3 Abbreviations

See also the project's central list of abbreviations [1].

Abbreviation/term	Description
AES	Advanced Encryption Standard
AVA	Antenna Distributor product of Active Antenna Systems GmbH
Capp	Crypto Application
CHM	Central Health Management
CIK	Crypto Ignition Key (in smart card form factor)
CMAC	Cipher-based Message Authentication Code
COM	Computer-on-Module

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 7 of 45


<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

Abbreviation/term	Description
DMS	Device Management System
EM	Encryption Module
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
GA-205	Time Division Multiplexer product of DRS Technologies
GB2PP	GB2 Platform Protocol, remote control protocol for R&S radios
GPP	General Purpose Processor
IP	Internet Protocol
LED	Light Emitting Diode
Mgmt	Management
MGW	Navics Media Gateway
MLS	Multi-Level Security
NAT	Network Address Translation
NIC	Network Interface Card
NIST	[U.S.] National Institute of Standards and Technology
NPM	Not Protectively Marked
PCI	Product Change Index
PFSW	Platform Software
PTT	Push To Talk
RM6-A	Data modem of Rapid Mobile Ltd.
RSM	Radio Security Module
RTP	Real-time Transport Protocol (typically used to transport VoIP voice data)
RTSP	Real Time Streaming Protocol (typically used for VoIP)
ST	Security Target
SEF	Security Enforcing Function(s)
SFP	Security Functional Policy

Subject to  
change  
without notice

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 8 of 45




<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	--

Abbreviation/term	Description
SIP	Session Initiation Protocol (typically used for VoIP)
SMS	Security Management System
SNMP	Simple Network Management Protocol
SNR	HF/VHF/UHF Modem of Rockwell Collins
SoC	System on Chip
SP	Special Publication
SW	Software
TCP	Transmission Control Protocol
TF	Trusted Filter
TFM	Trusted Filter Management
TFSM	Trusted Filter Security Module
TFV	Trusted Filter Voice
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
VoIP	Voice-over-IP
VT	Voice Terminal Softkey
VTSM	Voice Terminal Security Module
XK4100	HF radio of R&S
XT4400	VHF/UHF radio of R&S

Table 4: Abbreviations

Subject to  
change  
without notice

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 9 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	--

## 2 ST Introduction

### 2.1 ST Reference

Title: Security Target NAVICS MLS Boundary Protection System Operational Software

Part Number: 5416.2803.92

Change Index (Version): 09.00

Date: 2022-11-03

Author(s): Marcel Dischinger, Stefan Kraxberger, Torsten Schütze,  
Peter Jöckel, Teresa Jöckel, Roland Vogt (DFKI)

### 2.2 TOE Reference

#### 2.2.1 TOE Identification

The TOE is an application-specific software on the multi-purpose system platform

*NAVICS MLS Boundary Protection System*

consisting of the following two platform configurations

- (1) Management configuration
  - R&S TF5900M Trusted Filter IP configured as Trusted Filter Management (TFM)
- (2) Voice configuration
  - R&S TF5900M Trusted Filter IP configured as Trusted Filter Voice (TFV)
  - R&S GB5900SM Voice Terminal Softkey

Both platform configurations can be operated in mixed mode. In mixed management/voice configuration the Trusted Filter IP is configured as Trusted Filter Management (TFM) and as Trusted Filter Voice (TFV).

The TOE is identified as


*NAVICS MLS Boundary Protection System Operational Software V01.00*

consisting of

- R&S TFSM Operational Software, Version 10.04.10 as integral part of R&S Trusted Filter IP Operational Software, Part Number 5414.8679.02, Version 10.04.10 (PDM PCI 13.00)<sup>1</sup> installed on R&S TF5900M Trusted Filter IP, Part Number 5416.2490.02, Version 08.03
- R&S TF5900M Trusted Filter IP User Manual, Part Number 6190.3078.02, Version 06
- Test Description Trusted Filter IP, Part Number 5416.2490.01 T, Version 03.01

<sup>1</sup> "Version" indicates the "real" version number of the software, whereas the PDM PCI value is the PDM-internal version number of this software version.

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 10 of 45

NAVICS MLS	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
------------	--	---

- R&S VTSM Operational Software, Part Number 5414.8685.02, Version 10.02.04 (PDM PCI 06.00)<sup>2</sup> installed on  
R&S RSM-S IP Voice Terminal Security Module, Part Number 5414.0310.05, Version 08.19 as integral part of  
R&S GB5900SM Voice Terminal Softkey, Part Number 6157.0180.02, Version 05.00
- R&S GB5900SM Voice Terminal Softkey User Manual, Part Number 6202.7625.02, Version 03
- Test Instruction Voice Terminal MLS, Part Number 6157.0415.01, Version 01.12

## 2.2.2 Development Site

ROHDE & SCHWARZ SIT GmbH  
 ROHDE & SCHWARZ GmbH & Co. KG  
 Hemminger Str. 41  
 70499 Stuttgart/Weilimdorf

## 2.3 TOE Overview

The TOE is a *boundary protection system* (TOE type) acting as a bidirectional stateless packet filtering gateway. Its purpose and usage is to enforce the separation of network segments of different classification levels by protecting their boundaries,

- ensuring no data to compromise a network segment of high classification level when passed from a network segment of any lower classification level;
- ensuring no data with high classification level to pass from a network segment of high classification level to a network segment of any lower classification level; and
- allowing certain data with lower classification level to pass from a network segment of high classification level to a network segment of any lower classification level.

The TOE is operated as application-specific software on a multi-purpose system platform (Trusted Filter IP and Voice Terminal Softkey) within a Naval Integrated Communications System (NAVICS) established on a Multi-Level Security (MLS) communication infrastructure that consists of physically separated IPv4 network segments as installed on a naval ship (see Figure 1 for a simplified illustration).

Within the NAVICS MLS communication infrastructure three different kinds of user data are to be passed across the boundaries between separated network segments of different classification levels:


1. encrypted user data,
2. (unencrypted) VoIP data (SIP, RTSP, RTP) as part of a VoIP session, and
3. (unencrypted) device management data exchanged between a Device Management System (DMS) and a managed device like e.g. radio or satellite gateway.

Although encryption/decryption and transmission of encrypted user data are an integral part of the network separation, these security features are *not* part of the TOE security functionality (TSF), but provided by other trusted IT products.

Furthermore, tamper/tempest protection, strict red/black separation and network address translation (NAT) may be expected from a boundary protection system. These security features are also *not* part of the TOE security functionality (TSF), but provided by the multi-purpose system platform.

<sup>2</sup> "Version" indicates the "real" version number of the software, whereas the PDM PCI value is the PDM-internal version number of this software version.

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 11 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

### 2.3.1 Required non-TOE hardware/firmware/software

The following multi-purpose system platform components (cf. Figure 1 and Section 2.2.1) and accessory components are required to operate the TOE:

- *R&S TF5900M Trusted Filter IP* (cf. Figure 2) with embedded Trusted Filter Security Module (TFSM) to protect the boundary between the high network segment and a low network segment. Since the protection of controlled user data is different, the *Trusted Filter IP (TF)* is configured as
  - *Trusted Filter Voice (TFV)* to control VoIP data (SIP, RTSP, RTP); or
  - *Trusted Filter Management (TFM)* to control device management data.
 Both configurations can be operated in mixed management/voice mode, where the Trusted Filter IP is configured as Trusted Filter Voice (TFV) and as Trusted Filter Management (TFM).
- *R&S RSM-S IP Voice Terminal Security Module (VTSM)* as integral part of the *R&S GB5900SM Voice Terminal Softkey* (cf. Figure 3) to handle VoIP audio frames.
- *CIK (Crypto Ignition Key)* in smart card form factor for initialisation and configuration of TFSM and VTSM.
- *TOM Security Management System* managing the security configuration of VTSM and TFSM. TOM is responsible for the
  - generation of CIKs (Crypto Ignition Keys) used to initialize VTSM and TFSM;
  - generation and distribution of policy rules used by VTSM and TFSM for filtering (communication matrix) and authorisation (CMAC keys); and
  - other administrative functions.
- *Device Management System (DMS)* managing the configuration of other devices like e.g. radio or satellite gateways.

Subject to change without notice

The *Trusted Filter IP (TF)* is technically based on R&S SITLine IP with embedded Radio Security Module (RSM), a device that is approved for a classification level of "VS – Nur für den Dienstgebrauch (VS-NfD)". The *Voice Terminal Security Module (VTSM)* as integral part of the *Voice Terminal Softkey (VT)* is technically based on the Trusted Filter Security Module (TFSM).

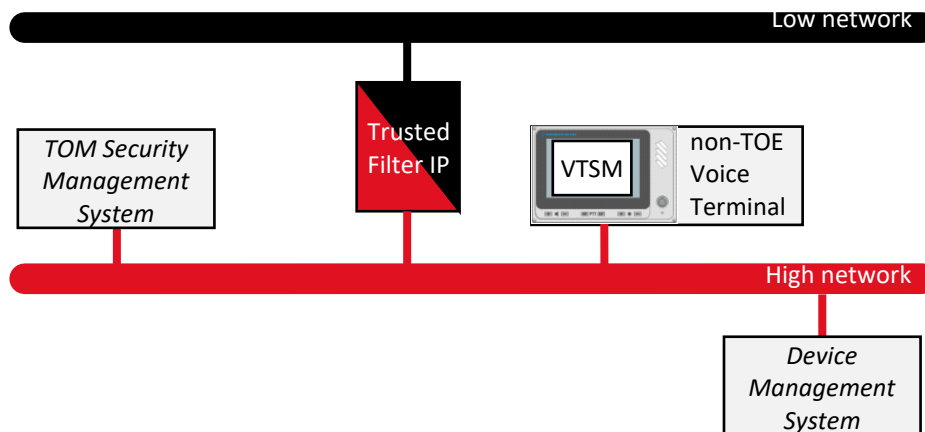


Figure 1: Simplified illustration of NAVICS MLS Boundary Protection System

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 12 of 45


<p><b>NAVICS MLS</b></p>	<p>Security Target NAVICS MLS Boundary Protection System Operational Software</p>	
--------------------------	---	---



Figure 2: R&S TF5900M Trusted Filter IP



Figure 3: R&S GB5900SM Voice Terminal Softkey

Subject to  
change  
without notice

### 2.3.2 Major security features

The transmission of (unencrypted) VoIP data (SIP, RTSP, RTP) and (unencrypted) device management data across the network segment boundaries is controlled by the TSF (information flow control) based on the following major security features.

- The operational software installed on the *Voice Terminal Security Module (VTSM)* as integral part of the Voice Terminal Softkey (VT) is operated in the high network segment (cf. Figure 1). It turns the VT into a trusted VoIP agent. Without the VTSM, the VT is not operable as it separates the audio processing from the VoIP implementation. The VT is transmitting/receiving VoIP data (SIP, RTSP, RTP). The TOE either indicates outgoing voice traffic to the user when it is targeted to a remote VoIP agent within the high network segment, or otherwise authorises outgoing voice traffic when it is targeted to a remote VoIP agent in a low network segment. The authorisation for transmission to a low network segment is based on CMAC generation: To each outgoing audio frame a cryptographic authorisation tag, i.e., a CMAC<sup>3</sup>, is attached. The separation of voice traffic is enabled by using different cryptographic keys.
- The TFSM operational software as integral part of the operational software installed on the *Trusted Filter IP (TF)* with embedded Trusted Filter Security Module (TFSM) is protecting the boundary between the high network segment and a low network segment (cf. Figure 1). It acts like an IPv4 router with additional filtering, deep packet inspection and CMAC verification (for outgoing RTP traffic only):
  - Filtering (protocol and communication matrix): For all user data types, i.e., VoIP data (SIP, RTSP, RTP) and device management data, a protocol check and a check of source and destination IPv4 addresses are performed. Only IPv4 packets of the specified protocols and authorised source/destination tuples are passed, all other IPv4 packets are dropped.

<sup>3</sup> Note that the CMAC is over the raw RTP data, i.e., no freshness or timeliness guarantees will be given.

<p>R&amp;S Part Number: 5416.2803.92</p>	<p>Version: 09.00</p>	<p>Date: 2022-11-03</p>
<p>Rohde &amp; Schwarz SIT GmbH</p>		<p>Page 13 of 45</p>

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	
-------------------	--	---

- Deep packet inspection: For all user data types, i.e., VoIP data (SIP, RTSP, RTP) and device management data, a deep packet inspection is performed. The inspection is stateless, i.e., the decision whether an IPv4 packet may pass is not related to any previous or future packet. The checks of VoIP data (SIP, RTSP, RTP) are specifically designed for the actually used VoIP agents. The checks of device management data are specific to the actually used management protocols. Only IPv4 packets conforming to their respective inspection rules are passed, all other IPv4 packets are dropped.
- Authorisation (for outgoing voice traffic only): If an outgoing RTP packet has an attached cryptographic authorisation tag, the tag is detached and a CMAC verification using a single cryptographic key is performed. Using exactly one CMAC key ensures the separation from differently tagged voice traffic. Only RTP packets with correct CMAC tag are passed, all other RTP packets with an incorrect or missing cryptographic authorisation tag are dropped.
- If an IPv4 packet passes all of the above checks, it is forwarded to its destination.
- When the information flow control rules as described above are completely operational, the TSF is in its so-called *operational mode*. Caused by certain failure events occurring at VT or TF, the TSF enters a *maintenance mode* where any information flow is denied.

## 2.4 TOE Description

The NAVICS MLS communication infrastructure consists of at least two separated network segments of different security classification levels. A typical installation has three network segments, for example named "SECRET", "RESTRICTED" and "NPM" (Not Protectively Marked). For the purpose of the TOE description, the boundary between the network segment of high classification level (SECRET) and other network segments of any lower classification level is considered (cf. Figure 4).

Subject to change without notice

Since the protection of VoIP data (SIP, RTSP, RTP) and device management data is different, the *Trusted Filter IP* is typically configured to filter either voice traffic (*Trusted Filter Voice (TFV)*) or management traffic (*Trusted Filter Management (TFM)*).

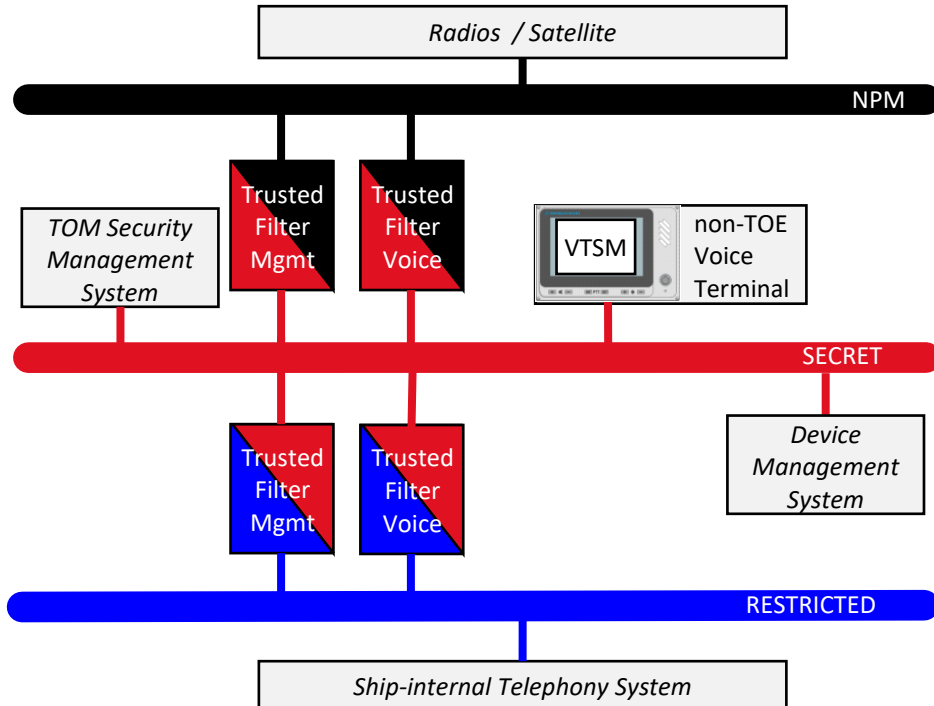



Figure 4: Boundary protection system elements in the NAVICS MLS network

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 14 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	--

## 2.4.1 Physical Scope of the TOE

The following physical parts constitute the TOE and are delivered to the customer:

- R&S TF5900M Trusted Filter IP Operational Software as integral part of the R&S Trusted Filter IP Operational Software (as identified in Section 2.2.1)
  - Method of delivery: Electronic shipment ready for installation on R&S TF5900M Trusted Filter IP
- R&S TF5900M Trusted Filter IP User Manual (as identified in Section 2.2.1)
  - Method of delivery: Electronic shipment
- Test Description Trusted Filter IP (as identified in Section 2.2.1)
  - Method of delivery: Electronic shipment to R&S site Memmingen
- R&S VTSM Operational Software (as identified in Section 2.2.1)
  - Method of delivery: Electronic shipment ready for installation on R&S RSM-S IP Voice Terminal Security Module (VTSM) as integral part of R&S GB5900SM Voice Terminal Softkey
- R&S GB5900SM Voice Terminal Softkey User Manual (as identified in Section 2.2.1)
  - Method of delivery: Electronic shipment
- Test Instruction Voice Terminal MLS (as identified in Section 2.2.1)
  - Method of delivery: Electronic shipment to R&S site Memmingen

Subject to  
change  
without notice

The following physical non-TOE parts are also delivered to the customer:


- R&S TF5900M Trusted Filter IP (as identified in Section 2.2.1)
  - Method of delivery: Integrated in its operational environment as ready-for-use device
- R&S GB5900SM Voice Terminal Softkey (as identified in Section 2.2.1)
  - Method of delivery: Integrated in its operational environment as ready-for-use device
- CIK (Crypto Ignition Key) in smart card form factor for initialisation of the VT, TFV and TFM
  - Method of delivery: Supply to individually authorised administrative personnel

### 2.4.1.1 Voice Terminal Softkey

The non-TOE Voice Terminal Softkey (VT) is a VoIP terminal equipment. Figure 5 shows a block diagram of the VT with embedded Voice Terminal Security Module (VTSM). On the audio side, microphone, speaker and headset are connected, the analogue audio signals are converted to digital data and vice versa, and the Audio FPGA processes the digital data of both directions, e.g., the digitalized voice signals are packetized for exchange with the VTSM. The network side consists of a COM Express Computer-on-Module, which implements the VoIP software stack and controls a display with softkeys for user control. Using the softkeys of the VT, a user configures the circuits for the two PTT buttons of the device.

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 15 of 45



<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	
-------------------	--	---

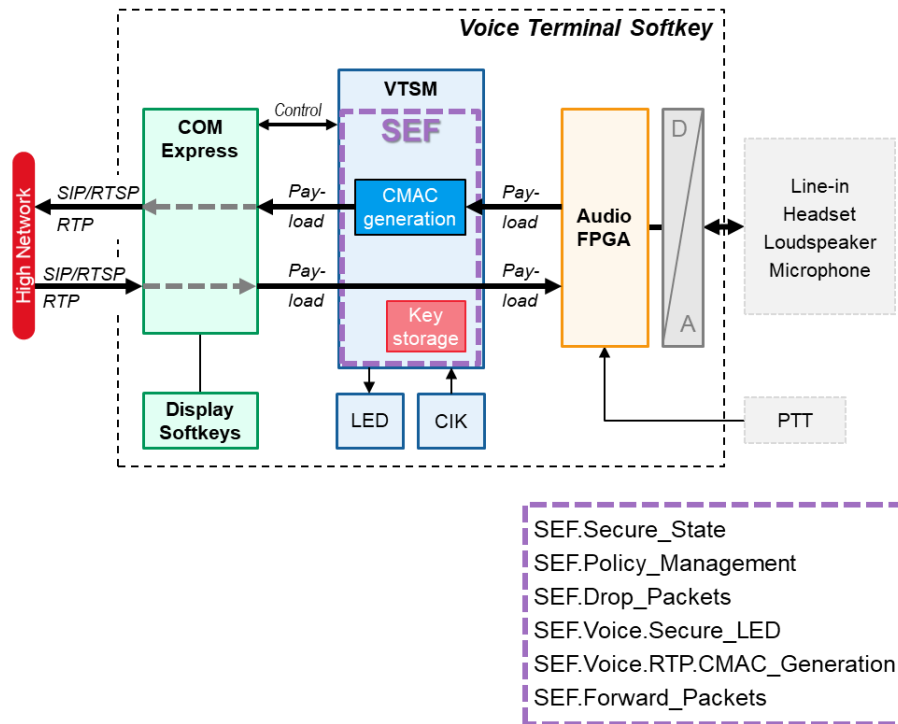


Figure 5: Block diagram of non-TOE Voice Terminal Softkey (VT) with embedded VTSM

Subject to change without notice

The VTSM is located between COM Express and Audio FPGA. All voice data (audio frames) going from the Audio FPGA side to the COM Express side or vice versa is passed through the VTSM. The VTSM is a radio security module as used in Trusted Filter IP (TFSM; cf. Figure 7). The architecture of the TFSM separates between non-TOE hardware, platform software (PFSW) and crypto application software (CApp). While the (uniform) TFSM hardware remains unchanged, the TFSM platform software (PFSW) is modified for integration into the VTSM. In Figure 6, the modules in the crypto application software (CApp), the platform software (PFSW) and the non-TOE hardware inside the VTSM are outlined, indicating the software modules that implement security enforcing functions (SEF).

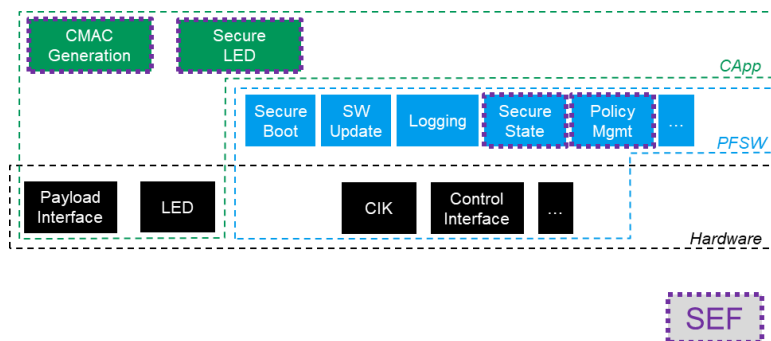



Figure 6: Non-TOE hardware, platform software (PFSW) and crypto application software (CApp) parts of VTSM indicating the software modules that implement SEF in operational mode

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 16 of 45



<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	
-------------------	--	---

### 2.4.1.2 Trusted Filter IP

The non-TOE Trusted Filter IP (TF) system platform is technically based on R&S SITLine IP with embedded Radio Security Module (RSM). The basic architecture of TF is shown in Figure 7. Payload (SIP, RTSP, RTP and device management protocols) has to pass all three modules, i.e., the High Network Module, the Trusted Filter Security Module (TFSM) and the Low Network Module. It propagates along two different, distinct paths: RTP is forwarded on the FPGA path, while all other traffic (SIP, RTSP and management protocols) is forwarded using the GPP path. The splitting is done in a non-TOE switch inside the FPAG of High and Low Network Module, respectively.

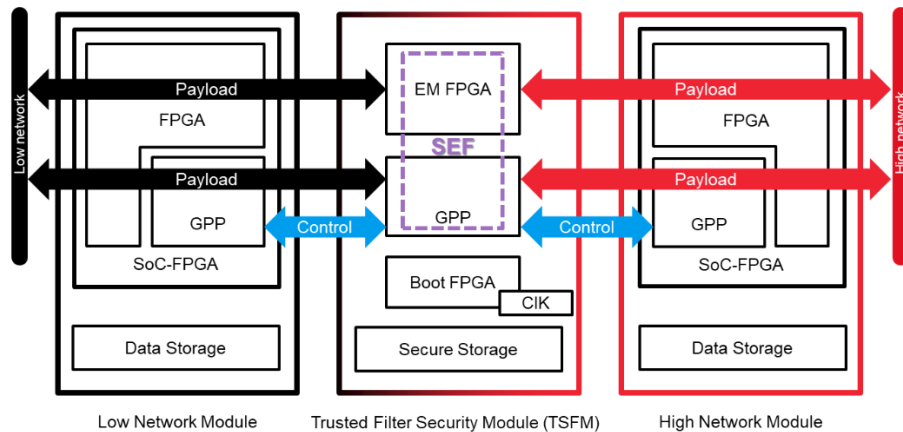


Figure 7: Basic architecture of non-TOE Trusted Filter IP based on R&S SITLine IP

Subject to change without notice

The TFSM is located between Low Network Module and High Network Module. All payload going from the low network to the high network or vice versa is passed through the TFSM. The architecture of the TFSM separates between non-TOE hardware, platform software (PFSW) and crypto application software (CApp). In Figure 8, the modules in the crypto application software (CApp), the platform software (PFSW) and the non-TOE hardware inside the TFSM are outlined, indicating the software modules that implement security enforcing functions (SEF).

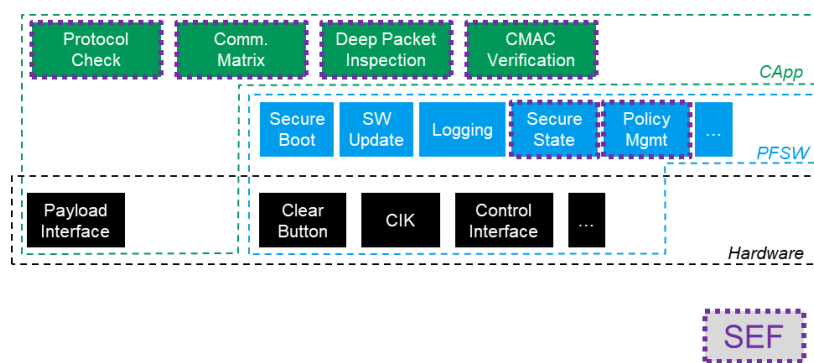



Figure 8: Non-TOE hardware, platform software (PFSW) and crypto application software (CApp) parts of TFSM in Trusted Filter Voice resp. Trusted Filter Management (without CMAC verification) indicating the software modules that implement SEF in operational mode

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 17 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

## 2.4.2 Logical Scope of the TOE

The TOE security functionality (TSF) is implemented as an application-specific software on the Voice Terminal Security Module (VTSM) and the Trusted Filter Security Module (TFSM). The VTSM and TFSM hardware (non-TOE) and platform software provide the following logical security features that are not part of the TSF:

- trigger mechanisms for handling failure events (declassification and emergency clear)
- protected channel for reception of the operational software, configuration settings, policy rules and their security attributes
- secure installation/update of the operational software
- secure storage of configuration settings, policy rules and their security attributes
- signalling of security alarms
- generation, storage and transfer of security audit records

Basic common TOE security functionality (SEF.Secure\_State) is

- secure initialisation of the Voice Terminal Security Module resp. Trusted Filter IP to operational mode using a CIK-mediated mechanism,
- preservation of a maintenance mode in case of a declassification event (Trusted Filter IP only), and
- preservation of a maintenance mode in case of an emergency clear event.

While in operational mode, the TOE security functionality (TSF) applies specific information control policies on the Voice Terminal Security Module operational software and the Trusted Filter Security Module operational software which are described in the following subsections. Common TOE security management functionality (SEF.Policy\_Management) consists of modification (reception and persistent storage) of the protocol filter configuration (TFM resp. TFV), policy rules and their security attributes, i.e. authorised communication partners and CMAC keys. When leaving the operational mode in case of some failure event (cf. SEF.Secure\_State), the protocol filter configuration, stored policy rules and their security attributes are removed (SEF.Policy\_Management). While in maintenance mode, the VTSM / TF operational software denies any information flow (SEF.Drop\_Packets).

Subject to  
change  
without notice


### 2.4.2.1 Voice Terminal Security Module (VTSM) Operational Software

The TOE security functionality (TSF) is capable to indicate to the user the classification level of transmitted audio frames and to authorise VoIP data (audio frames) that is to be transmitted to remote VoIP agents in a network segment of any lower classification level by attaching a cryptographic tag using CMAC. The CMAC tag is supposed to be verified by a Trusted Filter Voice (TFV) when crossing the boundary of the network segment of high classification level.

While in operational mode, the TOE security functionality (TSF) implements the following SEF:

- SEF.Voice.Secure\_LED: The TSF controls a LED which indicates to the user the classification level of the currently transmitted audio frames:
  - The LED is ON if the destination of outgoing audio frames is in the network segment of high classification level.
  - The LED is OFF if no audio frame is currently passing the VTSM or if the destination of outgoing audio frames is in a network segment of any lower classification level.
- SEF.Voice.RTP.CMAC\_Generation: The TSF generates and attaches an authorising 128bit CMAC tag (using AES-256) to an audio frame received from the Audio FPGA, if it is to be transmitted to a target network segment of any lower classification level. For enabling voice traffic separation, the TSF uses different cryptographic keys for the CMAC computation.
- SEF.Forward\_Packets: The TSF forwards each incoming audio frame to the Audio FPGA. The TSF forwards each outgoing audio frame (including CMAC tag, if applicable) to the COM Express.

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 18 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	
-------------------	--	---

### 2.4.2.2 Trusted Filter Security Module (TFSM) Operational Software (voice configuration)

The main purpose of the Trusted Filter Voice (TFV) configuration of the TOE is to check VoIP traffic transmitted between two network segments. The basic architecture and the data/payload paths of the Trusted Filter Voice (TFV) configuration are shown in Figure 9.

A functional block diagram of the SEF for voice traffic filtering is shown in Figure 10. Only IPv4 packets of protocol type SIP, RTSP or RTP are processed. The IP addresses of authorised communication partners are used in a communication matrix check. Finally, a deep packet inspection and a CMAC verification (outgoing RTP traffic only) is performed.

VoIP (SIP, RTSP, RTP) traffic is processed using the following SEF in operational mode:

- SEF.Voice.Protocol\_Check: Drop packets with transport protocol type other than UDP or that do contain messages with a protocol type other than SIP, RTSP or RTP.
- SEF.Voice.Communication\_Matrix: Drop SIP, RTSP or RTP packets with unauthorised tuple of source and destination IP addresses.
- SEF.Voice.Deep\_Packet\_Inspection: Drop SIP, RTSP or RTP packets failing a stateless deep packet inspection.
- SEF.Voice.RTP.CMAC\_Verification: For outgoing RTP traffic from the network segment of high classification level to a network segment of any lower classification level, drop RTP packets with incorrect or missing 128bit CMAC tag (using AES-256). The TSF uses exactly one CMAC key ensuring the separation from differently tagged voice traffic.

If an IPv4 packet passes all checks, i.e. is not dropped according to any of the above security functions, the TSF forwards it to its target network segment (SEF.Forward\_Packets). Before forwarding outgoing RTP packets, the CMAC tag is detached and the packet length field in the RTP header is updated (SEF.Voice.RTP.CMAC\_Verification).

Subject to change without notice

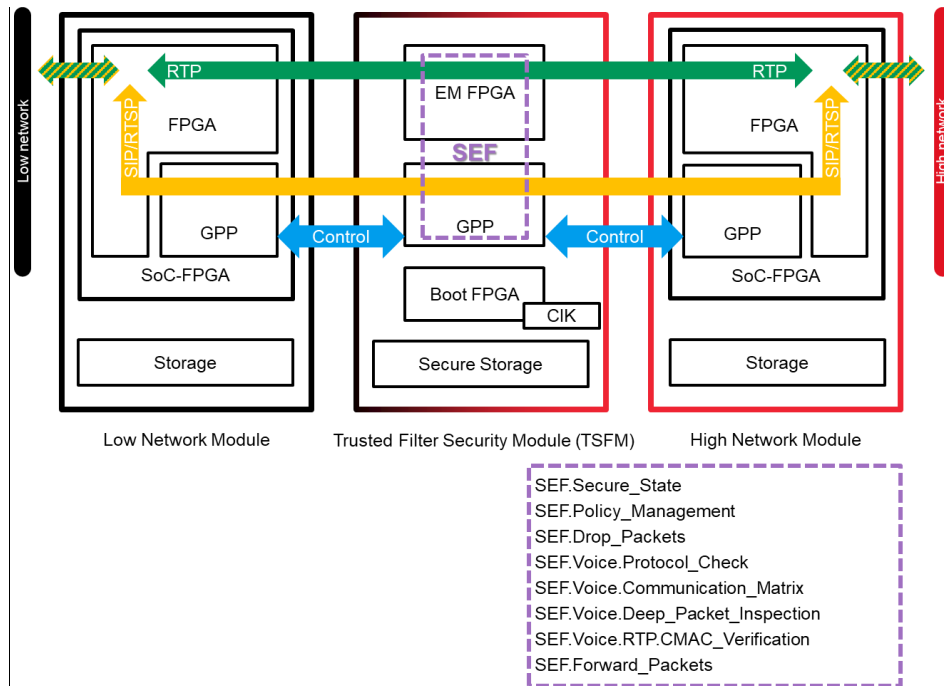



Figure 9: Payload paths within Trusted Filter Voice (TFV)

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 19 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

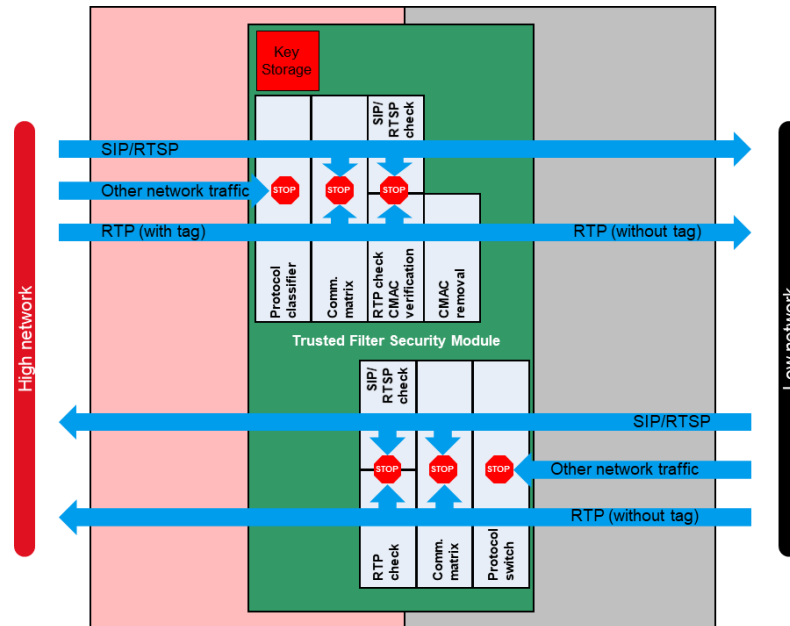


Figure 10: Block diagram of voice traffic filtering

Subject to  
change  
without notice

### 2.4.2.3 Trusted Filter Security Module (TFSM) Operational Software (management configuration)

The main purpose of the Trusted Filter Management (TFM) configuration of the TOE is to check device management traffic transmitted between two network segments. The basic architecture and the data/payload paths of the Trusted Filter Management (TFM) configuration are shown in Figure 11.


A functional block diagram of the SEF for management traffic filtering is shown in Figure 12. Only IPv4 packets of specific protocols are processed. The IP addresses of authorised communication partners are used in a communication matrix check. Finally, a deep packet inspection is performed.

Device management traffic is processed using the following SEF in operational mode:

- SEF.Management.Protocol\_Check: Drop packets with transport protocol type other than TCP or containing messages with a protocol type that is not configured for deep packet inspection.
- SEF.Management.Communication\_Matrix: Drop packets with unauthorised tuple of source and destination IP addresses.
- SEF.Management.Deep\_Packet\_Inspection: Drop packets failing a stateless deep packet inspection specific to the management protocol used.

If an IPv4 packet passes all checks, i.e. is not dropped according to any of the above security functions, the TSF forwards it to its target network segment (SEF.Forward\_Packets).

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 20 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	
-------------------	--	---

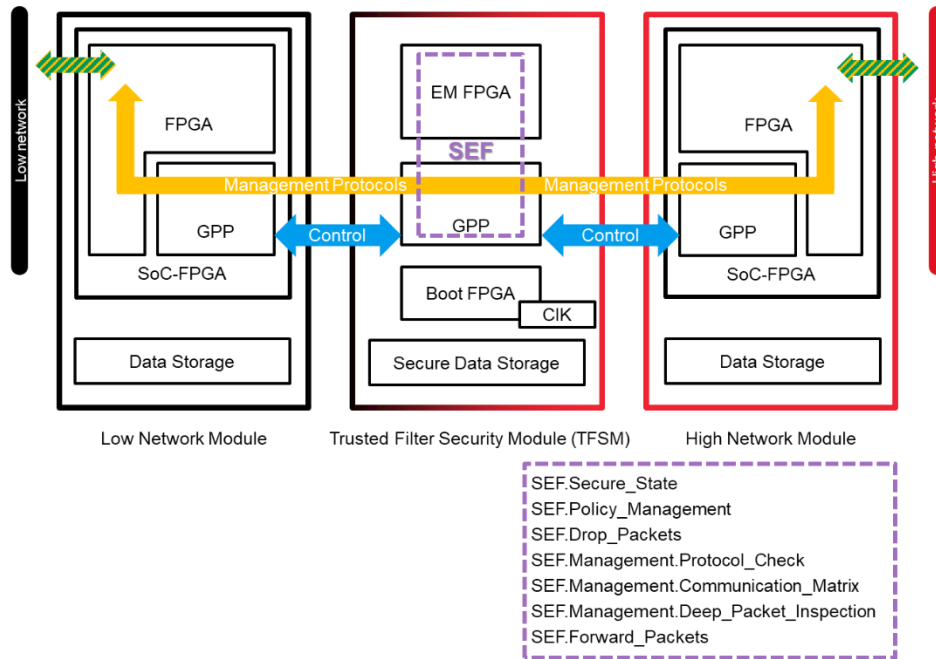


Figure 11: Payload paths within Trusted Filter Management (TFM)

Subject to change without notice

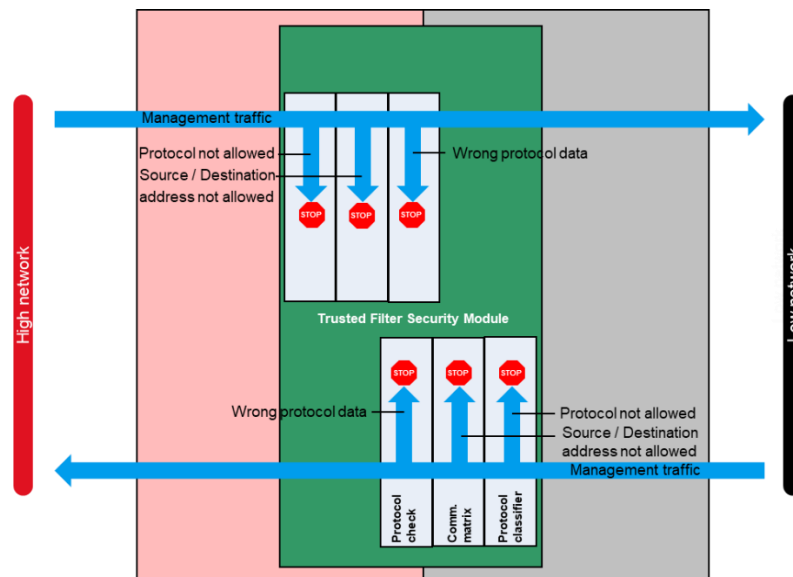



Figure 12: Block diagram of management traffic filtering

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 21 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

### 3 Conformance Claims

The Security Target (ST) and the Target of Evaluation (TOE) claim conformance with Common Criteria (CC) for IT Security Evaluation, Version 3.1, Revision 5, April 2017 consisting of

- Part 1: Introduction and general model, CCMB-2017-04-001
- Part 2: Security functional components, CCMB-2017-04-002
- Part 3: Security assurance components, CCMB-2017-04-003

The CC conformance claim consists of the following conformance statements.

- The ST and the TOE are **CC Part 2 conformant**.
- The ST and the TOE are **CC Part 3 conformant**.
- The ST and the TOE are **EAL 4 augmented** with component AVA\_VAN.4 “Methodical vulnerability assessment” (replacing AVA\_VAN.3).

The ST and the TOE do not claim conformance with any Protection Profile (PP).

Subject to  
change  
without notice

### 4 Security Problem Definition


The security problem focusses on the following assets:

- confidentiality and integrity of user data with high classification level while passing user data across the boundaries of IPv4 network segments of different classification levels.

The security problem considers threat agents who possess a moderate level of attack potential and

- do *not* have physical or logical access to the IPv4 network segments of high classification level;
- do have physical or logical access to IPv4 network segments of any lower classification level;
- do have logical access to TSF interfaces connected to IPv4 network segments of any lower classification level;
- do *not* have physical access to system platform components (Trusted Filter IP, Voice Terminal Softkey) or its interconnections;
- do *not* have physical or logical access to any management component (other trusted IT product) used for configuring or updating the TOE;
- are *not* able to decrypt encrypted user data with high classification level.

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 22 of 45

<p><b>NAVICS MLS</b></p>	<p>Security Target NAVICS MLS Boundary Protection System Operational Software</p>	
--------------------------	---	---

## 4.1 Threats

T.DISCLOSURE IPv4 packets passed across the boundary from the network segment of high classification to a network segment of any lower classification level may (be part of an attack to) disclose user data with high classification level. A threat agent having access to an IPv4 network segment of lower classification level may passively observe user data in IPv4 traffic. A threat agent having access to TSF interfaces connected to an IPv4 network segment of lower classification level may actively request user data to be transmitted.

T.MANIPULATION IPv4 packets passed across the boundary from a network segment of any lower classification level to the network segment of high classification level may (be part of an attack to) manipulate user data with high classification level. A threat agent having access to TSF interfaces connected to an IPv4 network segment of lower classification level may actively transmit malicious content.

## 4.2 Organisational Security Policies

The security problem is not defined in terms of organisational security policies.

## 4.3 Assumptions

A.HIGHNETWORKSECURITY The confidentiality and integrity of user data with high classification level is not compromised within the IPv4 network segment of high classification level. The system platform components (Trusted Filter IP, Voice Terminal Softkey) are deemed to be part of this network segment and protected in its operational environment against interference of its operational state and interconnections. This includes the protection of any management component (other trusted IT product) used for the administration of the TOE.


A.TRUSTEDUSERS User data with high classification level is securely processed by authorised external entities, including educated and trained human users.

A.TRUSTEDADMINISTRATORS The administration of the TOE is performed by authorised administrators who act in the best interest of security. This includes being appropriately educated and trained, following policy, and adhering to guidance for managing all administrative functions of the TOE.

Subject to  
change  
without notice

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 23 of 45



<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

## 5 Security Objectives

The definition of security objectives differentiates between Trusted Filter Security Functionality (TFSF) and Voice Terminal Security Functionality (VTSF).

### 5.1 Security Objectives for the TOE

**OT.TRUSTEDFILTERMANAGEMENT** The TFSF shall forward any IPv4 packet across the boundary between the network segment of high classification level and a network segment of any lower classification level, if it does not contain detectable user data with high classification level or detectable malicious content, i.e. if each of the following filter conditions is fulfilled:

- Its transport protocol type is TCP.
- A set of packet inspection rules corresponding to its protocol type is configured.
- Its source and destination IP addresses are configured as authorised communication partners.
- It passes a stateless deep packet inspection based on the configured set of packet inspection rules corresponding to its protocol type.

The TFSF shall drop any IPv4 packet, if one of the above filter conditions fails, i.e. if the TFSF detects the potential disclosure or manipulation of user data with high classification level.

**OT.TRUSTEDFILTERVOICE** The TFSF shall forward any IPv4 packet across the boundary between the network segment of high classification level and a network segment of any lower classification level, if it does not contain detectable user data with high classification level or detectable malicious content, i.e. if each of the following filter conditions is fulfilled:

- Its transport protocol type is UDP.
- Its protocol type is SIP, RTSP or RTP.
- Its source and destination IP addresses are configured as authorised communication partners.
- It passes a stateless deep packet inspection based on a configured set of SIP, RTSP or RTP packet inspection rules.
- In case of protocol type RTP: When it originates from the network segment of high classification level, a cryptographic authorisation tag can be detached and correctly verified using a single cryptographic key ensuring the separation from differently tagged voice traffic.

The TFSF shall drop any IPv4 packet, if one of the above conditions fails, i.e. if the TFSF detects the potential disclosure or manipulation of user data with high classification level.


**OT.VOICETERMINAL** The VTSF shall indicate outgoing voice traffic to the user when it is to be transmitted to a remote VoIP agent within the network segment of high classification level. The VTSF shall authorise outgoing voice traffic when it is to be transmitted to a remote VoIP agent in a network segment of any lower classification level. The authorisation shall be performed by attaching each outgoing audio frame with a cryptographic authorisation tag. For enabling voice traffic separation, the TFSF shall use different cryptographic keys for the CMAC computation.

**OT.SECURESTATE** When leaving the operational mode, caused by a declassification event or emergency clear event, the TFSF resp. VTSF shall enter a maintenance mode where the ability to return to a secure state is provided. When the TFSF resp. VTSF is not in operational mode,

- the TFSF shall disable filtering and deny the transmission/reception of any IPv4 packets across the boundary between a network segment of high classification level and a network segment of any lower classification level; resp.
- the VTSF shall deny the transmission/reception of any VoIP audio frame.

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 24 of 45



NAVICS MLS	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
------------	--	--

## 5.2 Security Objectives for the Operational Environment

OE.PROTECTEDTRANSMISSION The operational environment shall ensure that any IPv4 packet crossing the boundary between the network segment of high classification level and a network segment of any lower classification level passes either the TFSF trusted filtering procedure or a non-TOE trusted encryption/decryption procedure.

OE.SECURERULES The operational environment shall ensure that the policy rules and their security attributes for communication relationships, deep packet inspection and voice traffic separation are appropriate for protecting the confidentiality and integrity of user data with high classification level. In particular, cryptographic keys for voice traffic separation shall be unique per network boundary. The operational environment shall ensure that the policy rules and their attributes are configured as intended by the user using a trusted management component and are securely transmitted to the TOE using a protected communication channel. When a system platform component in voice configuration (Trusted Filter Voice or Voice Terminal Softkey) is taken out of service, all active cryptographic keys for voice traffic separation shall be decommissioned, i.e. replaced by new ones, in each of the remaining system platform components in the same voice configuration.

OE.SECUREPLATFORM The operational environment shall ensure that the system platform provides the following security features:

- trigger mechanisms for handling failure events (declassification and emergency clear)
- protected channel for reception of the operational software, policy rules and their security attributes
- secure installation/update of the operational software
- secure storage of policy rules and their security attributes
- signalling of security alarms
- generation, storage and transfer of security audit records


Subject to  
change  
without notice

OE.HIGHNETWORKSECURITY The operational environment shall protect the confidentiality and integrity of user data with high classification level within the IPv4 network segments of high classification level. The operational environment shall implement appropriate measures for the protection of the system platform components (Trusted Filter IP and Voice Terminal Softkey) in its operational environment against interference of its operational state and interconnections. This includes tamper/tempest protection and strict red/black separation. It also includes the protection of any management component (other trusted IT product) used for the administration of the TOE, i.e. managing secure policy rules, processing security alarms, transferring security audit records or updating the operational software.

OE.TRUSTEDUSERS The operational environment shall ensure that user data with high classification level is securely processed by authorised external entities, including educated and trained human users, i.e. they are processing user data in such a way that IPv4 packets do not contain any non-detectable user data with high classification level and non-detectable malicious content of IPv4 packets does not manipulate user data with high classification level.

OE.TRUSTEDADMINISTRATORS The operational environment shall ensure that the administration of the TOE is performed by authorised administrators who act in the best interest of security. This includes being appropriately educated and trained, following policy, and adhering to guidance for managing all administrative functions of the TOE.

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 25 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

### 5.3 Security Objectives Rationale


Each security objective traces back to the security problem definition (see Table 5).

	T.DISCLOSURE	T.MANIPULATION	A.HIGHNETWORKSECURITY	A.TRUSTEDUSERS	A.TRUSTEDADMINISTRATORS
<b>OT.TRUSTEDFILTERMANAGEMENT</b>	x	x			
<b>OT.TRUSTEDFILTERVOICE</b>	x	x			
<b>OT.VOICETERMINAL</b>	x				
<b>OT.SECURESTATE</b>	x	x			
<b>OE.PROTECTEDTRANSMISSION</b>	x	x			
<b>OE.SECURERULES</b>	x	x			
<b>OE.SECUREPLATFORM</b>	x	x			
<b>OE.HIGHNETWORKSECURITY</b>	x	x	x		
<b>OE.TRUSTEDUSERS</b>	x	x		x	
<b>OE.TRUSTEDADMINISTRATORS</b>	x	x			x

Table 5: Tracing of Security Objectives to Security Problem Definition

Subject to  
change  
without notice

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 26 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

### 5.3.1 Security Objectives counter Threats

The security objectives counter all threats.

T.DISCLOSURE IPv4 packets passed across the boundary from the network segment of high classification level to a network segment of any lower classification level may not disclose user data with high classification level due to the following reasons:


- OT.TRUSTEDFILTERMANAGEMENT, OT.TRUSTEDFILTERVOICE, OT.VOICETERMINAL:  
The TFSF and VTSF ensure that any IPv4 packet passing the TOE does not contain detectable user data with high classification level.
- OT.SECURESTATE: The TFSF ensures that no IPv4 packet passes the Trusted Filter IP (Voice / Management) operational software when it is not in operational mode.
- OT.SECURESTATE: The VTSF ensures that no RTP packet is transmitted by the Voice Terminal Security Module operational software when it is not in operational mode.
- OE.PROTECTEDTRANSMISSION: The operational environment ensures that no IPv4 packet bypassing the Trusted Filter Voice / Management is exposed to a disclosure attack since it is encrypted/decrypted.
- OE.TRUSTEDUSERS: The operational environment supports the TFSF and VTSF by ensuring that authorised users are processing user data in such a way that IPv4 packets do not contain any non-detectable user data with high classification level.
- OE.SECURERULES, OE.SECUREPLATFORM, OE.HIGHNETWORKSECURITY: The operational environment supports the TFSF and VTSF by ensuring a trusted configuration and operating environment.
- OE.HIGHNETWORKSECURITY, OE.TRUSTEDADMINISTRATORS: The operational environment supports the TFSF and VTSF by ensuring that the operational software of Voice Terminal Security Module resp. Trusted Filter IP is protected against interference of its operational state and interconnections with trusted management components used for authorised TOE administration.

Subject to  
change  
without notice

T.MANIPULATION IPv4 packets passed across the boundary from a network segment of any lower classification level to the network segment of high classification level may not (be part of an attack to) manipulate user data with high classification level due to the following reasons:

- OT.TRUSTEDFILTERMANAGEMENT, OT.TRUSTEDFILTERVOICE: The TFSF ensures that any IPv4 packet passing the TOE does not contain detectable malicious content.
- OT.SECURESTATE: The TFSF ensures that no IPv4 packet passes the Trusted Filter IP (Voice / Management) operational software when it is not in operational mode.
- OT.SECURESTATE: The VTSF ensures that no RTP packet is received by the Voice Terminal Security Module operational software when it is not in operational mode.
- OE.PROTECTEDTRANSMISSION: The operational environment ensures that no IPv4 packet bypassing the Trusted Filter Voice / Management is exposed to a manipulation attack since it is encrypted/decrypted.
- OE.TRUSTEDUSERS: The operational environment supports the TFSF and VTSF by ensuring that authorised users are processing user data in such a way that non-detectable malicious content of IPv4 packets does not manipulate user data with high classification level.
- OE.SECURERULES, OE.SECUREPLATFORM, OE.HIGHNETWORKSECURITY: The operational environment supports the TFSF and VTSF by ensuring a trusted configuration and operating platform.
- OE.HIGHNETWORKSECURITY, OE.TRUSTEDADMINISTRATORS: The operational environment supports the TFSF and VTSF by ensuring that the the operational software of Voice Terminal Security Module resp. Trusted Filter IP is protected against interference of its operational state and interconnections with trusted management components used for authorised TOE administration.

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 27 of 45

<p><b>NAVICS MLS</b></p>	<p>Security Target NAVICS MLS Boundary Protection System Operational Software</p>	 <p><b>ROHDE &amp; SCHWARZ</b></p>
--------------------------	---	---

**5.3.2 Security Objectives for the environment uphold Assumptions**

The security objectives uphold all assumptions.

A.HIGHNETWORKSECURITY The security objective OE.HIGHNETWORKSECURITY comprehensively upholds the corresponding assumption.

A.TRUSTEDUSERS The security objective OE.TRUSTEDUSERS comprehensively upholds the corresponding assumption.

A.TRUSTEDADMINISTRATORS The security objective OE.TRUSTEDADMINISTRATORS comprehensively upholds the corresponding assumption.

**6 Extended Components Definition**

The security requirements stated in Sections 7.1 and 7.2 are taken from CC Parts 2 and 3. They do not contain any extended security requirement. Therefore, no extended components are defined.

Subject to  
change  
without notice

<p>R&amp;S Part Number: 5416.2803.92</p>	<p>Version: 09.00</p>	<p>Date: 2022-11-03</p>
<p>Rohde &amp; Schwarz SIT GmbH</p>		<p>Page 28 of 45</p>

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

## 7 Security Requirements

### 7.1 Security Functional Requirements (SFRs)

The SFR components are taken from CC Part 2 and reproduced in alphabetical order of classes.

All operations on SFR elements are identified using leading superscripts in square brackets. In order to clearly indicate the tailoring, each identification refers to the specific performance of the operation.

#### 7.1.1 FCS\_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP\_ITC.1 Import of user data without security attributes, or  
FDP\_ITC.2 Import of user data with security attributes, or  
FCS\_CKM.1 Cryptographic key generation]  
FCS\_CKM.4 Cryptographic key destruction

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	list of cryptographic operations	<i>generation and verification of cipher-based message authentication codes</i>
[2]	assignment	cryptographic algorithm	<i>CMAC-AES256 (128 bit tag length)</i>
[3]	assignment	cryptographic key sizes	<i>256 bit (AES key)</i>
[4]	assignment	list of standards	<i>NIST SP 800-38B and FIPS PUB 197</i>

Subject to  
change  
without notice

**FCS\_COP.1.1** The TSF shall perform <sup>[1]</sup>*generation and verification of cipher-based message authentication codes* in accordance with a specified cryptographic algorithm <sup>[2]</sup>*CMAC-AES256 (128 bit tag length)* and cryptographic key sizes <sup>[3]</sup>*256 bit (AES key)* that meet the following: <sup>[4]</sup>*NIST SP 800-38B and FIPS PUB 197.*

#### 7.1.2 FDP\_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP\_ACC.1 Subset access control, or  
FDP\_IFC.1 Subset information flow control]  
FMT\_MSA.3 Static attribute initialisation

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	refinement (editorial)	the [assignment: access control SFP(s) and/or information flow control SFP(s)]	[assignment: access control SFP(s) and/or information flow control SFP(s)]
-----	---------------------------	---	---

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 29 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

[2] assignment	access control SFP(s) and/or information flow control SFP(s)	<i>no specific SFP(s)</i>
[3] refinement (editorial)	user data	<i>CMAC keys</i>
[4] refinement (editorial)	user data controlled under the SFP	<i>CMAC keys</i>
[5] assignment	additional importation control rules	<i>The TSF shall only accept exactly one CMAC key to be used by the Voice Traffic Filtering SFP</i>

**FDP\_ITC.1.1** The TSF shall enforce <sup>[1][2]</sup>*no specific SFP(s)* when importing <sup>[4]</sup>*CMAC keys* from outside of the TOE.

**FDP\_ITC.1.2** The TSF shall ignore any security attributes associated with the <sup>[3]</sup>*CMAC keys* when imported from outside the TOE.

**FDP\_ITC.1.3** The TSF shall enforce the following rules when importing <sup>[4]</sup>*CMAC keys* from outside the TOE: <sup>[5]</sup>*The TSF shall only accept exactly one CMAC key to be used by the Voice Traffic Filtering SFP.*

Subject to change without notice

**7.1.3 [TFM]FDP\_IFC.1 Subset information flow control [iteration for Trusted Filter Management (TFM)]**

Hierarchical to: No other components.


Dependencies: FDP\_IFF.1 Simple security attributes

Tailoring (assignment, selection, refinement operations on SFR elements):

[1] assignment	information flow control SFP	<i>Management Traffic Filtering SFP</i>
[2] assignment	list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP	<i>the list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects as defined in Table 6</i>

**[TFM]FDP\_IFC.1.1** The TSF shall enforce the <sup>[1]</sup>*Management Traffic Filtering SFP* on <sup>[2]</sup>*the list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects as defined in Table 6.*

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 30 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

Subjects	Information	Operations
high resp. low network interface (an active entity in a network segment of high classification level resp. in a network segment of any lower classification level) with security attributes: - direction (outgoing, incoming)	IPv4 packet with security attributes: - protocol type - source IP address - destination IP address - format (header/body fields)	forward drop

Table 6: List of subjects, information, and operations covered by Management Traffic Filtering SFP

### 7.1.4 [TFM]FDP\_IFF.1 Simple security attributes [iteration for Trusted Filter Management (TFM)]

Hierarchical to: No other components.

Dependencies: FDP\_IFC.1 Subset information flow control  
FMT\_MSA.3 Static attribute initialisation

Subject to  
change  
without notice

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	information flow control SFP	<i>Management Traffic Filtering SFP</i>
[2]	assignment	list of subjects and information controlled under the indicated SFP, and for each, the security attributes	<i>stated in Table 6</i>
[3]	assignment	for each operation, the security attribute-based relationship that must hold between subject and information security attributes	<i>stated in Table 7</i>
[4]	refinement (editorial)	the [assignment: additional information flow control SFP rules]	[assignment: additional information flow control SFP rules]
[5]	assignment	additional information flow control SFP rules	<i>no additional information flow control SFP rules</i>
[6]	assignment	rules, based on security attributes, that explicitly authorise information flows	<i>none</i>
[7]	assignment	rules, based on security attributes, that explicitly deny information flows	<i>each IPv4 packet is dropped, i.e. not permitted to forward, if the TSF is not in operational mode, i.e. the rules of the Management Traffic Filtering SFP as stated in Table 6 and Table 7 are out of order and the TSF is unable to check the relationship between subject and information security attributes</i>

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 31 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

<sup>[TFM]</sup>**FDP\_ IFF.1.1** The TSF shall enforce the <sup>[1]</sup>*Management Traffic Filtering SFP* based on the following types of subject and information security attributes: <sup>[2]</sup>*stated in Table 6.*

<sup>[TFM]</sup>**FDP\_ IFF.1.2** The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: <sup>[3]</sup>*stated in Table 7.*

<sup>[TFM]</sup>**FDP\_ IFF.1.3** The TSF shall enforce <sup>[4][5]</sup>*no additional information flow control SFP rules.*

<sup>[TFM]</sup>**FDP\_ IFF.1.4** The TSF shall explicitly authorise an information flow based on the following rules: <sup>[6]</sup>*none.*

<sup>[TFM]</sup>**FDP\_ IFF.1.5** The TSF shall explicitly deny an information flow based on the following rules: <sup>[7]</sup>*each IPv4 packet is dropped, i.e. not permitted to forward, if the TSF is not in operational mode, i.e. the rules of the Management Traffic Filtering SFP as defined in Table 6 and Table 7 are out of order and the TSF is unable to check the relationship between subject and information security attributes.*

Subject to  
change  
without notice

Operation	Relationship between subject and information security attributes
Forward	An IPv4 packet is permitted to forward in either direction of the network interfaces, if it is not dropped according to any other rule of the Management Traffic Filtering SFP.
drop [transport]	An IPv4 packet is dropped, i.e. not permitted to forward, if its transport protocol type is not TCP.
drop [protocol]	An IPv4 packet is dropped, i.e. not permitted to forward, if a set of packet inspection rules corresponding to the protocol type of the packet is not configured.
drop [relationship]	An IPv4 packet is dropped, i.e. not permitted to forward, if the source and destination IP addresses are not configured as authorised communication partners.
drop [format]	An IPv4 packet is dropped, i.e. not permitted to forward, if it fails a stateless deep packet inspection based on the configured set of packet inspection rules corresponding to the protocol type of the packet.

Table 7: Rules of the Management Traffic Filtering SFP for permitting an information flow

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 32 of 45



<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

**7.1.5 [TFV]FDP\_IFC.1 Subset information flow control  
[iteration for Trusted Filter Voice (TFV)]**

Hierarchical to: No other components.

Dependencies: FDP\_IFF.1 Simple security attributes

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	information flow control SFP	<i>Voice Traffic Filtering SFP</i>
[2]	assignment	list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP	<i>the list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects as defined in Table 8</i>

[TFV]FDP\_IFC.1.1 The TSF shall enforce the [1]*Voice Traffic Filtering SFP* on [2]*the list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects as defined in Table 8.*

Subject to change without notice

Subjects	Information	Operations
high resp. low network interface (an active entity in a network segment of high classification level resp. in a network segment of any lower classification level) with security attributes: - direction (outgoing, incoming)	IPv4 packet with security attributes: - protocol type - source IP address - destination IP address - format (header/body fields) - cryptographic authorisation tag	forward drop


Table 8: List of subjects, information, and operations covered by Voice Traffic Filtering SFP

**7.1.6 [TFV]FDP\_IFF.1 Simple security attributes  
[iteration for Trusted Filter Voice (TFV)]**

Hierarchical to: No other components.

Dependencies: FDP\_IFC.1 Subset information flow control  
FMT\_MSA.3 Static attribute initialisation

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 33 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	information flow control SFP	<i>Voice Traffic Filtering SFP</i>
[2]	assignment	list of subjects and information controlled under the indicated SFP, and for each, the security attributes	<i>stated in Table 8</i>
[3]	assignment	for each operation, the security attribute-based relationship that must hold between subject and information security attributes	<i>stated in Table 9</i>
[4]	assignment	additional information flow control SFP rules	<i>additional information flow control SFP rules stated in Table 9</i>
[5]	assignment	rules, based on security attributes, that explicitly authorise information flows	<i>none</i>
[6]	assignment	rules, based on security attributes, that explicitly deny information flows	<i>Each IPv4 packet is dropped, i.e. not permitted to forward, if the TSF is not in operational mode, i.e. the rules of the Voice Traffic Filtering SFP as stated in Table 8 and Table 9 are out of order and the TSF is unable to check the relationship between subject and information security attributes</i>

Subject to change without notice

<sup>[1]</sup>TFVIFDP\_IFF.1.1 The TSF shall enforce the <sup>[1]</sup>*Voice Traffic Filtering SFP* based on the following types of subject and information security attributes: <sup>[2]</sup>*stated in Table 8*.


<sup>[3]</sup>TFVIFDP\_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: <sup>[3]</sup>*stated in Table 9*.

<sup>[4]</sup>TFVIFDP\_IFF.1.3 The TSF shall enforce the <sup>[4]</sup>*additional information flow control SFP rules stated in Table 9*.

<sup>[5]</sup>TFVIFDP\_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: <sup>[5]</sup>*none*.

<sup>[6]</sup>TFVIFDP\_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: <sup>[6]</sup>*Each IPv4 packet is dropped, i.e. not permitted to forward, if the TSF is not in operational mode, i.e. the rules of the Voice Traffic Filtering SFP as stated in Table 8 and Table 9 are out of order and the TSF is unable to check the relationship between subject and information security attributes*.

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 34 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

Operation	Relationship between subject and information security attributes
Forward	An IPv4 packet is permitted to forward in either direction of the network interfaces if it is not dropped according to any other rule of the Voice Traffic Filtering SFP. Additional rule [RTP authorisation]: When transmitting an IPv4 packet of protocol type RTP in outgoing direction to the low network interface, its cryptographic authorisation tag is detached and the packet length field in the RTP header is updated accordingly.
drop [transport]	An IPv4 packet is dropped, i.e. not permitted to forward, if its transport protocol type is not UDP.
drop [protocol]	An IPv4 packet is dropped, i.e. not permitted to forward, if its protocol type is not SIP, RTSP or RTP.
drop [relationship]	An IPv4 packet is dropped, i.e. not permitted to forward, if the source and destination IP addresses are not configured as authorised communication partners.
drop [format]	An IPv4 packet is dropped, i.e. not permitted to forward, if it fails a stateless deep packet inspection based on a configured set of SIP, RTSP or RTP packet inspection rules.
drop [RTP authorisation]	An IPv4 packet of protocol type RTP is dropped, i.e. not permitted to forward, if it is received in outgoing direction from the high network interface with an incorrect, w.r.t. a single cryptographic key, or missing cryptographic authorisation tag.

Table 9: Rules of the Voice Traffic Filtering SFP for permitting an information flow

Subject to  
change  
without notice

### 7.1.7 <sup>[VT]</sup>FDP\_IFC.1 Subset information flow control [iteration for Voice Terminal Security Module (VTSM)]

Hierarchical to: No other components.


Dependencies: FDP\_IFF.1 Simple security attributes

Tailoring (assignment, selection, refinement operations on SFR elements):

[1] assignment	information flow control SFP	<i>Voice Traffic Authorisation SFP</i>
[2] assignment	list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP	<i>the list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects as defined in Table 10</i>

<sup>[VT]</sup>FDP\_IFC.1.1 The TSF shall enforce the <sup>[1]</sup>*Voice Traffic Authorisation SFP* on <sup>[2]</sup>*the list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects as defined in Table 10.*

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 35 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

Subjects	Information	Operations
unique trusted VoIP agent resp. several other remote VoIP agents (active entities participating in an ongoing VoIP session) with security attributes: <ul style="list-style-type: none"> <li>- direction (outgoing, incoming)</li> <li>- network segment</li> <li>- network classification level</li> </ul>	audio frames with security attributes: <ul style="list-style-type: none"> <li>- cryptographic authorisation tag</li> </ul>	forward drop

Table 10: List of subjects, information, and operations covered by Voice Traffic Authorisation SFP

### 7.1.8 [VT]FDP\_ IFF.1 Simple security attributes [iteration for Voice Terminal Security Module (VTSM)]

Hierarchical to: No other components.


Dependencies: FDP\_IFC.1 Subset information flow control  
FMT\_MSA.3 Static attribute initialisation

Subject to  
change  
without notice

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	information flow control SFP	<i>Voice Traffic Authorisation SFP</i>
[2]	assignment	list of subjects and information controlled under the indicated SFP, and for each, the security attributes	<i>stated in Table 10</i>
[3]	assignment	for each operation, the security attribute-based relationship that must hold between subject and information security attributes	<i>stated in Table 11</i>
[4]	assignment	additional information flow control SFP rules	<i>additional information flow control SFP rules stated in Table 11</i>
[5]	assignment	rules, based on security attributes, that explicitly authorise information flows	<i>none</i>
[6]	assignment	rules, based on security attributes, that explicitly deny information flows	<i>Each audio frame is dropped, i.e. not permitted to forward, if the TSF is not in operational mode, i.e. the rules of the Voice Traffic Authorisation SFP as stated in Table 10 and Table 11 are out of order and the TSF is unable to check the relationship between subject and information security attributes</i>

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 36 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---


- <sup>[1]</sup>FDP\_IFF.1.1 The TSF shall enforce the <sup>[1]</sup>*Voice Traffic Authorisation SFP* based on the following types of subject and information security attributes: <sup>[2]</sup>*stated in Table 10.*
- <sup>[1]</sup>FDP\_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: <sup>[3]</sup>*stated in Table 11.*
- <sup>[1]</sup>FDP\_IFF.1.3 The TSF shall enforce the <sup>[4]</sup>*additional information flow control SFP rules stated in Table 11.*
- <sup>[1]</sup>FDP\_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: <sup>[5]</sup>*none.*
- <sup>[1]</sup>FDP\_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: <sup>[6]</sup>*Each audio frame is dropped, i.e. not permitted to forward, if the TSF is not in operational mode, i.e. the rules of the Voice Traffic Authorisation SFP as stated in Table 10 and Table 11 are out of order and the TSF is unable to check the relationship between subject and information security attributes.*

Subject to  
change  
without notice

Operation	Relationship between subject and information security attributes
forward [in]	Any audio frame is permitted to forward if it is received in incoming direction from a remote VoIP agent.
forward [out]	Any audio frame is permitted to forward if it is transmitted in outgoing direction from the unique trusted VoIP agent. Additional rule [authorisation]: When transmitting an audio frame in outgoing direction to a remote VoIP agent in a network segment of any lower classification level, a cryptographic authorisation tag using a specific cryptographic key is attached. Additional rule [indication]: While transmitting audio frames in outgoing direction to a remote VoIP agent in a network segment of high classification level, an indicator LED is switched on.
drop	An audio frame is never dropped according to any relationship between subject and information security attributes

Table 11: Rules of the Voice Traffic Authorisation SFP for permitting an information flow

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 37 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

**7.1.9 FDP\_ITT.2 Transmission separation by attribute**

Hierarchical to: FDP\_ITT.1 Basic internal transfer protection

Dependencies: [FDP\_ACC.1 Subset access control, or  
FDP\_IFC.1 Subset information flow control]

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	access control SFP(s) and/or information flow control SFP(s)	<i>Voice Traffic Filtering SFP and Voice Traffic Authorisation SFP</i>
[2]	selection	disclosure, modification, loss of use	<i>modification</i>
[3]	assignment	security attributes that require separation	<i>cryptographic authorisation tag</i>

**FDP\_ITT.2.1** The TSF shall enforce the <sup>[1]</sup>*Voice Traffic Filtering SFP and Voice Traffic Authorisation SFP* to prevent the <sup>[2]</sup>*modification* of user data when it is transmitted between physically-separated parts of the TOE.

**FDP\_ITT.2.2** The TSF shall separate data controlled by the SFP(s) when transmitted between physically-separated parts of the TOE, based on the values of the following:  
<sup>[3]</sup>*cryptographic authorisation tag*.

Subject to  
change  
without notice

**7.1.10 FMT\_SMF.1 Specification of Management Functions**


Hierarchical to: No other components.

Dependencies: No dependencies.

Tailoring (assignment, selection, refinement operations on SFR elements):

[1]	assignment	list of management functions to be provided by the TSF	<ul style="list-style-type: none"> <li>- <i>modification, i.e. reception and persistent storage, and removal of the protocol filter configuration for Management Traffic Filtering SFP and Voice Traffic Filtering SFP</i></li> <li>- <i>modification, i.e. reception and persistent storage, and removal of authorised communication partners for Management Traffic Filtering SFP and Voice Traffic Filtering SFP</i></li> <li>- <i>modification, i.e. reception and persistent storage, and removal of CMAC keys for Voice Traffic Filtering SFP and Voice Traffic Authorisation SFP</i></li> </ul>
-----	------------	--	--

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 38 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

---

[2] refinement	The TSF shall be capable of performing the following management functions: ... removal ....	The TSF shall be capable of performing the following management functions: ... removal ... <i>and, when leaving the operational mode caused by a declassification event or emergency clear event, the TSF shall remove protocol filter configuration and authorised communication partners (Management/Voice Traffic Filtering SFPs), and all CMAC keys (Voice Traffic Filtering/Authorisation SFPs).</i>
----------------	--	---

---

**FMT\_SMF.1.1** The TSF shall be capable of performing the following management functions: <sup>[1]</sup>

- *modification, i.e. reception and persistent storage, and removal of the protocol filter configuration for Management Traffic Filtering SFP and Voice Traffic Filtering SFP*
- *modification, i.e. reception and persistent storage, and removal of authorised communication partners for Management Traffic Filtering SFP and Voice Traffic Filtering SFP*
- *modification, i.e. reception and persistent storage, and removal of CMAC keys for Voice Traffic Filtering SFP and Voice Traffic Authorisation SFP*

<sup>[2]</sup>*and, when leaving the operational mode caused by a declassification event or emergency clear event, the TSF shall remove protocol filter configuration and authorised communication partners (Management/Voice Traffic Filtering SFPs), and all CMAC keys (Voice Traffic Filtering/Authorisation SFPs).*

Subject to  
change  
without notice

**7.1.11 FPT\_RCV.1 Manual recovery**

Hierarchical to: No other components.

Dependencies: AGD\_OPE.1 Operational user guidance

Tailoring (assignment, selection, refinement operations on SFR elements):

---


[1] assignment	list of failures/service discontinuities	<i>leaving the operational mode, caused by a declassification event or emergency clear event,</i>
----------------	--	---

---

**FPT\_RCV.1.1** After <sup>[1]</sup>*leaving the operational mode, caused by a declassification event or emergency clear event*, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 39 of 45



<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

## 7.2 Security Assurance Requirements (SARs)

The SAR components are taken from CC Part 3 and referenced in Table 12. They correspond to EAL4 augmented with AVA\_VAN.4 (replacing AVA\_VAN.3).


Assurance class	Assurance components	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability assessment	<b>AVA_VAN.4</b>	<b>Methodical vulnerability analysis</b>

Subject to  
change  
without notice

Table 12: Security Assurance Requirements (EAL4 augmented with AVA\_VAN.4)

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 40 of 45



<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

## 7.3 Security Requirements Rationale

### 7.3.1 Justification of SFR/SAR dependencies


All dependencies of the SAR components are satisfied.

All dependencies of the SFR components are satisfied, not applicable or addressed by security objectives for the operational environment (see Table 13).

SFR component	Dependencies	Justification
FCS_COP.1	FDP_ITC.1/.2 or FCK_CKM.1 FCS_CKM.4	satisfied by FDP_ITC.1 addressed by OE.SECURERULES: key destruction is not necessary because a) CMAC tags have a very short life-cycle according to voice traffic authorisation/filtering SFPs, i.e. there are no persistent data that depend on active CMAC keys; and b) misuse of residual CMAC keys is prevented by decommissioning all active CMAC keys (OE.SECURERULES)
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1 FMT_MSA.3	not applicable due to assignment (no SFPs) not applicable since there are no attributes
[TFM]FDP_IFC.1	FDP_IFF.1	satisfied by [TFM]FDP_IFF.1
[TFM]FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	satisfied by [TFM]FDP_IFC.1 not applicable since the attributes are not initialized
[TFV]FDP_IFC.1	FDP_IFF.1	satisfied by [TFV]FDP_IFF.1
[TFV]FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	satisfied by [TFV]FDP_IFC.1 not applicable since the attributes are not initialized
[VT]FDP_IFC.1	FDP_IFF.1	satisfied by [VT]FDP_IFF.1
[VT]FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	satisfied by [VT]FDP_IFC.1 not applicable since the attributes are not initialized
FDP_ITT.2	FDP_ACC.1 or FDP_IFC.1	satisfied by [TFV]FDP_IFC.1 and [VT]FDP_IFC.1
FMT_SMF.1	—	—
FPT_RCV.1	AGD_OPE.1	satisfied

Table 13: SFR dependencies justification

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 41 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---


**7.3.2 SFRs trace to and meet all security objectives for the TOE**

	OT.TRUSTEDFILTERMANAGEMENT	OT.TRUSTEDFILTERVOICE	OT.VOICETERMINAL	OT.SECURESTATE
<b>FCS_COP.1</b>		x	x	
<b>FDP_ITC.1</b>		x	x	
<b>[TFM]FDP_IFC.1</b>	x			x
<b>[TFM]FDP_IFF.1</b>	x			x
<b>[TFV]FDP_IFC.1</b>		x		x
<b>[TFV]FDP_IFF.1</b>		x		x
<b>[VT]FDP_IFC.1</b>			x	x
<b>[VT]FDP_IFF.1</b>			x	x
<b>FDP_ITT.2</b>		x	x	
<b>FMT_SMF.1</b>	x	x	x	x
<b>FPT_RCV.1</b>				x

Table 14: Tracing of SFRs to TOE Security Objectives

Subject to  
change  
without notice

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 42 of 45

<b>NAVICS MLS</b>	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
-------------------	--	---

OT.TRUSTEDFILTERMANAGEMENT The rules of the *Management Traffic Filtering SFP* (<sup>[TFM]</sup>FDP\_IFC.1, <sup>[TFM]</sup>FDP\_IFF.1 and FMT\_SMF.1) comprehensively meet all the conditions for filtering (forward/drop) of IPv4 packets across the boundary between the network segment of high classification level and a network segment of any lower classification level.

OT.TRUSTEDFILTERVOICE The rules of the *Voice Traffic Filtering SFP* (<sup>[TFV]</sup>FDP\_IFC.1, <sup>[TFV]</sup>FDP\_IFF.1 and FMT\_SMF.1) comprehensively meet all the conditions for filtering (forward/drop) of IPv4 packets across the boundary between the network segment of high classification level and a network segment of any lower classification level. The CMAC as cryptographic authorisation tag is verified using a single authorisation key (FCS\_COP.1, FDP\_ITC.1) and used to separate differently tagged voice traffic (FDP\_ITT.2).

OT.VOICETERMINAL The rules of the *Voice Traffic Authorisation SFP* (<sup>[VT]</sup>FDP\_IFC.1 and <sup>[VT]</sup>FDP\_IFF.1) indicate outgoing voice traffic to the user when it is to be transmitted to a remote VoIP agent within the network segment of high classification level. The rules of the *Voice Traffic Authorisation SFP* (<sup>[VT]</sup>FDP\_IFC.1, <sup>[VT]</sup>FDP\_IFF.1 and FMT\_SMF.1) authorise outgoing voice traffic when it is to be transmitted to a remote VoIP agent in a network segment of any lower classification level. The authorisation is performed by attaching each outgoing audio packet with a CMAC (FCS\_COP.1, FDP\_ITC.1) as cryptographic authorisation tag using a specific cryptographic key enabling the separation of differently tagged voice traffic (FDP\_ITT.2).

OT.SECURESTATE When leaving the operational mode, caused by a declassification event or emergency clear event, the TFSF resp. VTSF is ensured to enter a maintenance mode where the ability to return to a secure state is provided (FPT\_RCV.1). When the TFSF resp. VTSF is not in operational mode,


- the rules of the *Management Traffic Filtering SFP* (<sup>[TFM]</sup>FDP\_IFC.1, <sup>[TFM]</sup>FDP\_IFF.1 and FMT\_SMF.1) and the *Voice Traffic Filtering SFP* (<sup>[TFV]</sup>FDP\_IFC.1 and <sup>[TFV]</sup>FDP\_IFF.1 and FMT\_SMF.1) disable filtering and deny the transmission/reception of any IPv4 packets across the boundary between the network segment of high classification level and a network segment of any lower classification level; resp.
- the rules of the *Voice Traffic Authorisation SFP* (<sup>[VT]</sup>FDP\_IFC.1, <sup>[VT]</sup>FDP\_IFF.1 and FMT\_SMF.1) deny the transmission/reception of any audio frames.

Subject to  
change  
without notice

### 7.3.3 Explanation of the chosen SARs

The chosen SAR package EAL4 provides a consistent level of rigour and assurance that is appropriate to the type of the TOE. Additionally, the augmentation with SAR component AVA\_VAN.4 corresponds to the capabilities of the threat agents.

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 43 of 45

NAVICS MLS	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
------------	--	--

## 8 TOE Summary Specification

### 8.1 Management Traffic Filtering SFP (<sup>[TFM]</sup>FDP\_IFC.1, <sup>[TFM]</sup>FDP\_IFF.1, FMT\_SMF.1)

The Management Traffic Filtering SFP is directly implemented for each IPv4 packet (information) while passing between high/low network interfaces (subjects) depending on the subject and information attributes specified in Table 6. The rules for permitting the drop operation (cf. Table 7) are implemented by the following functions:

- SEF.Management.Protocol\_Check implements the transport and protocol rules;
- SEF.Management.Communication\_Matrix implements the relationship rule;
- SEF.Management.Deep\_Packet\_Inspection implements the format rule.

If the IPv4 packet is not dropped by any of the above functions, it is forwarded (SEF.Forward\_Packets).

While in operational mode (see Section 8.5), changing (receiving and persistently storing) the protocol filter configuration and the matrix of authorised communication partners is implemented by SEF.Policy\_Management.

When leaving the operational mode (see Section 8.5), the protocol filter configuration (TFM) and the matrix of authorised communication partners are removed by SEF.Policy\_Management, and all IPv4 packets received at either network interface are ignored, i.e. any information flow according to the Management Traffic Filtering SFP is denied (SEF.Drop\_Packets).

Subject to  
change  
without notice

### 8.2 Voice Traffic Filtering SFP (<sup>[TFV]</sup>FDP\_IFC.1, <sup>[TFV]</sup>FDP\_IFF.1, FMT\_SMF.1)

The Voice Traffic Filtering SFP is directly implemented for each IPv4 packet (information) while passing between high/low network interfaces (subjects) depending on the subject and information attributes specified in Table 8. The rules for permitting the drop operation (cf. Table 9) are implemented by the following functions:

- SEF.Voice.Protocol\_Check implements the transport and protocol rules;
- SEF.Voice.Communication\_Matrix implements the relationship rule;
- SEF.Voice.Deep\_Packet\_Inspection implements the SIP, RTSP and RTP message/format rules;
- SEF.Voice.RTP.CMAC\_Verification implements the RTP authorisation rules.


SEF.Voice.RTP.CMAC\_Verification also implements the additional separation rule for detaching the correctly verified CMAC authorisation tag (see also Section 8.4) before forwarding an IPv4 packet of protocol type RTP.

If the IPv4 packet is not dropped by any of the above functions, it is forwarded (SEF.Forward\_Packets).

While in operational mode (see Section 8.5), changing (receiving and persistently storing) the protocol filter configuration, the matrix of authorised communication partners and the CMAC key is implemented by SEF.Policy\_Management.

When leaving the operational mode (see Section 8.5), the protocol filter configuration (TFV), the matrix of authorised communication partners and the CMAC key are removed by SEF.Policy\_Management, and all IPv4 packets received at either network interface are ignored, i.e. any information flow according to the Voice Traffic Filtering SFP is denied (SEF.Drop\_Packets).

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 44 of 45

NAVICS MLS	Security Target NAVICS MLS Boundary Protection System Operational Software	 <b>ROHDE &amp; SCHWARZ</b>
------------	--	--

### 8.3 Voice Traffic Authorisation SFP (<sup>[VT]</sup>FDP\_IFC.1, <sup>[VT]</sup>FDP\_IFF.1, FMT\_SMF.1)

The Voice Traffic Authorisation SFP is directly implemented for each audio frame (information) while it is received/transmitted from a VoIP agent (subject) depending on the subject and information attributes specified in Table 10. The rules for permitting the forward operation (cf. Table 11) are implemented by SEF.Forward\_Packets: All outgoing/incoming audio frames, transmitted from the unique trusted VoIP agent (Audio FPGA) or received from any other remote VoIP agent (via COM Express), are always forwarded.

The function SEF.Voice.Secure\_LED implements the additional indication rule of the Voice Traffic Authorisation SFP by controlling the indicator LED.

The function SEF.Voice.RTP.CMAC\_Generation implements the additional authorisation rule of the Voice Traffic Authorisation SFP by attaching a CMAC authorisation tag to the audio frame (see also Section 8.4).

While in operational mode (see Section 8.5), changing, i.e. receiving and persistently storing, the CMAC keys is implemented by SEF.Policy\_Management.

When leaving the operational mode (see Section 8.5), the CMAC keys are removed by SEF.Policy\_Management, and all audio frames, transmitted from the unique trusted VoIP agent (Audio FPGA) or received from any other remote VoIP agent (via COM Express), are ignored, i.e. any information flow according to the Voice Traffic Authorisation SFP is denied (SEF.Drop\_Packets).

### 8.4 Internal TOE transfer protection (FDP\_ITT.2, FCS\_COP.1, FDP\_ITC.1)

The internal TOE transfer of voice traffic (Ipv4 packets of protocol type RTP containing audio frames) between the operational software installed on Voice Terminal Security Module (VTSM) and Trusted Filter Voice (TFV) is protected by

- generating the CMAC authorisation tag (cf. SEF.Voice.RTP.CMAC\_Generation in Section 8.3) using a specific CMAC key that enables voice traffic separation; and
- verifying the CMAC authorisation tag (cf. SEF.Voice.RTP.CMAC\_Verification in Section 8.2) using exactly one CMAC key that ensures the separation of differently tagged voice traffic.

The CMAC mechanism prevents any modification of audio frames and separates voice traffic that is differently tagged, e.g. targeted to remote VoIP agents in different network segments of any lower classification level. It also separates voice traffic that is not tagged, i.e. targeted to a remote VoIP agent in the network segment of high classification level.

The generation and verification uses a 256 bit AES key for computing a CMAC-AES256 tag with 128 bit length according to NIST SP 800-38B and FIPS PUB 197.

Import of the AES keys ensures that exactly one key is accepted for SEF.Voice.RTP.CMAC\_Verification.

### 8.5 Secure State (FMT\_SMF.1, FPT\_RCV.1)

The operative life-cycle, implementing the function SEF.Secure\_State, of each part of the operational software on VTSM, TFV and TFM is determined by several states. There is only one state corresponding to the operational mode. In case of a declassification event (TFV/TFM only) or emergency clear event occurring in either part of the system platform, the protocol filter configuration (TFV, TFM), the matrix of authorised communication partners (TFV, TFM) and all CMAC keys (VTSM, TFV) are removed (SEF.Policy\_Management), and the operational mode is left resulting in some maintenance state. Any such state corresponds to the maintenance mode that is maintained until return to operational mode by authorised state changes.

R&S Part Number: 5416.2803.92	Version: 09.00	Date: 2022-11-03
Rohde & Schwarz SIT GmbH		Page 45 of 45