Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1123-2023

for

NAVICS MLS Boundary Protection System Operational Software V01.00

from

ROHDE & SCHWARZ SIT GmbH

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1123-2023 (*)

Boundary Protection System

NAVICS MLS Boundary Protection System Operational Software
V01.00

from	ROHDE & SCHWARZ SIT GmbH
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.4

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

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

Bonn, 13 March 2023

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

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

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

3 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 3 March 2005, Bundesgesetzblatt I, p. 519

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

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

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

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

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

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

3.2. International Recognition of CC – Certificates (CCRA)

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

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies

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

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

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

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product NAVICS MLS Boundary Protection System Operational Software V01.00 has undergone the certification procedure at BSI.

The evaluation of the product NAVICS MLS Boundary Protection System Operational Software V01.00 was conducted by Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI). The evaluation was completed on 3 February 2023. DFKI is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: ROHDE & SCHWARZ SIT GmbH.

The product was developed by: ROHDE & SCHWARZ SIT GmbH.

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

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the product’s resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 13 March 2023 is valid until 12. March 2028. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

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

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

6. Publication

The product NAVICS MLS Boundary Protection System Operational Software V01.00 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] ROHDE & SCHWARZ SIT GmbH
Hemminger Str. 41
70499 Stuttgart/Weilimdorf

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) NAVICS MLS Boundary Protection System Operational Software V01.00 is operating 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, i.e.

- 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;
- 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 Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by AVA_VAN.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 7. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functionality	Addressed issue
Management Traffic Filtering	IPv4 packets are only forwarded if they contain valid management data and match the configured communication rules.
Voice Traffic Filtering	IPv4 packets are only forwarded if they contain valid audio data and match the configured communication rules. If going from a higher to a lower classification level, the proper CMAC tag is also checked for and removed before forwarding.
Voice Traffic Authorisation	Secure communication is indicated by a status LED. Furthermore, a CMAC tag is attached to audio frames sent from a higher to a lower classification level.
Internal TOE Transfer Protection	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 a CMAC tag, enabling voice traffic separation and preventing data modification or corruption.
Secure State	Only one state corresponds 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 and the system enters a maintenance mode.

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6], chapter 4. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], sections 4.3, 4.1 and 4.2 respectively.

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

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

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

NAVICS MLS Boundary Protection System Operational Software, V01.00

The following table outlines the TOE deliverables:

No	Type	Identifier	Version	Form of Delivery
1	SW	R&S TFSM Operational Software	10.04.10	Embedded in No. 2
2	SW	R&S Trusted Filter IP Operational Software (Non-TOE) Part Number 5414.8679.02 SHA-256 (shipped separately): F0DDBE11 6657FCD9 514C94BF 07495DE4 63C6AABF EBD2D739 9484DD3A D8CFEB4E	10.04.10	Internal electronic delivery to manufacturer's final assembly
3	SW	R&S VTSM Operational Software Part Number 5414.8685.02 SHA-256 (shipped separately): 269BD3D9 97C866F9 8A8DC084 DB2FE380 1C6DBA63 4EABE0AA 151A5A42 F1AFDB8D	10.02.04	Internal electronic delivery to manufacturer's final assembly
4	DOC	Test Description Trusted Filter IP Part Number 5416.2490.01 T SHA-256: ADFEA893 13753E6E 71C1E47F C6646C49 5489FC7E B7EC25CF 8D2C59E7 E68557B9	03.01	Internal electronic delivery to manufacturer's final assembly
5	DOC	R&S TF5900M Trusted Filter IP User Manual Part Number 6190.3078.02 SHA-256: A4A4327D 09F4FC4C F89EC574 36363DDE 6EF9832D B2523AA2 4A380C98 43098AF8	06	Electronic delivery to the end user (operator)

No	Type	Identifier	Version	Form of Delivery
6	DOC	Test Instruction Voice Terminal MLS Part Number 6157.0415.01 T SHA-256: EB8AE9FC A769CD67 8D64BE80 34832B15 6346B288 49957B3A 398AEEA8 5E071A38	01.12	Internal electronic delivery to manufacturer's final assembly
7	DOC	R&S GB5900SM Voice Terminal Softkey User Manual Part Number 6202.7625.02 SHA-256: 8C86E2EE 3F804B77 029D2920 1EEC6BA9 CFBE46E8 362A2389 55D1F447 156DF5DE	03	Electronic delivery to the end user (operator)

Table 2: Deliverables of the TOE

The evaluated TOE is a SW only TOE that is installed on non-TOE HW at the HW production facility by the manufacturer.
Therefor the delivery process evaluated for this certification process is the delivery of the TOE's software components from the SW development facility to the production facility of the manufacturer.
The TOE's software components are transmitted electronically to the user with their integrity protected by SHA-256 checksums.

The documentation (No. 5 and 7) is delivered to different end user, typically the operator.

After HW production and software installation, the final product is shipped to the operator. This shipment and further installation is out of scope for this certification.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Information flow control for voice data packets to control the transmission of audio data and packet inspection
- Information flow control for management data packets to control the transmission of management data and packet inspection
- Authorization mechanism of voice data packets via CMAC tags
- Management functionality regarding the rules of information flow control
- Preservation of Secure State

Further details of the TOE security policies are set out in section 7.1 and chapter 8 of the Security Target [6].

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

OE.ProtectedTransmission	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.SecurePlatform	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
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.
OE.SecureRules	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.
OE.TrustedUsers	User data with high classification level is securely processed by authorised external entities, including educated and trained human users.
OE.TrustedAdministrators	The administration of the TOE is performed by authorised administrators who act in the best interest of security.

Details can be found in the Security Target [6], section 5.2.

5. Architectural Information

The TOE consists of two subsystems:

- R&S TFSM Operational Software
  for installation on the Trusted Filter Security Module (TFSM) and
- R&S VTSM Operational Software
  for installation on the Voice Terminal Security Module (VTSM).

The TFSM is embedded in the R&S TF5900M Trusted Filter IP product and the VTSM is embedded in the R&S GB5900SM Voice Terminal Softkey product.

The R&S TFSM Operational Software in the R&S Trusted Filter IP acts as a central gateway for controlling the data flow between high- and low-classified network segments according to defined filter rules and policies. In addition, it is also responsible for the verification and, in the positive case, removal of the cryptographic authorization code (CMAC tag) of corresponding audio packets, which are transmitted from the high-classified network segment to a lower-classified network segment.

The R&S VTSM Operational Software in the R&S Voice Terminal first ensures that audio packets are provided with a cryptographic authorization code (CMAC tag) according to their destination within the network of high- and lower-classified network segments, which can be verified by the R&S TFSM Operational software and thus authorizes the transition to a lower-classified network segment. In addition, it is also responsible for securely displaying the authorization of the transition of audio packets from the high-classified network segment to a lower network segment by a designated LED.

6. Documentation

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

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

7. IT Product Testing

The TOE was installed on the designated hardware (R&S TF5900M Trusted Filter IP, Part Number 5416.2490.02, Version 08.03 and R&S VTSM Operational Software on the R&S RSM-S IP Voice Terminal Security Module, Part Number 5414.0310.05, Version 08.19) and tested in both configurations listed in chapter 8. Checking the LED output was automated via a microcontroller that reports the status to a connected PC via USB for testing purposes. This PC came with an installation of the TOM (Trusted Object Manager – a R&S management application) for TOE configuration and control. The lower and higher classified networks are simulated as two different subnets.

7.1. Developer Testing

The developer mostly focused on the filtering of network traffic which is the main security functionality of the TOE. Both positive and negative tests were performed. The developer used automated tests where possible. The CIK interface as well as the control interface were tested manually. Every security function was covered by at least one test case.

7.2. Independent Testing

For independent testing, all the developer’s automated tests for protocol filtering rules were repeated, including but not limited to TCP, IP, SIP and RTP. A subset of manual tests was also repeated, in which by stimulation of

- the CIK interface
- the management interface
- the control interfaces and
- the emergency-clear button

the configuration and the state of the TOE was changed from the developer's tests.

Furthermore, additional tests were devised to improve test coverage, mostly focusing on negative testing, i.e. operation with invalid or missing configuration, changed network settings or additional CMAC settings.

All tests yielded the expected results. No erroneous behaviour of the TOE and no erroneous result were observed during the course of the tests. The test results show no errors in the implementation of the TOE security functionality.

7.3. Vulnerability Testing

After analysing potential vulnerabilities, taking into account the objectives for the operational environment and assuming that the TOE is physically inaccessible to an attacker, no potentially exploitable vulnerabilities remain. Therefore, no penetration tests were performed.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- Operating as Trusted Filter Voice and Voice Terminal
- Operating as Trusted Filter Management

In the first case, both subsystems of the TOE (Trusted Filter Security Module Operational Software and Voice Terminal Security Module Operational Software) are in operation. In the second case, only one subsystem of the TOE (Trusted Filter Security Module Operational Software) is in operation.

Even though the subsystem is the same in both cases, the hardware the TOE is installed on differs in these scenarios. The respective software/firmware in which the TOE is embedded and the respective hardware are not part of the TOE, but are required for the operation of the TOE. Thus, the operation of the two evaluated configurations of the TOE is only permitted if the surrounding software/firmware/hardware corresponds to the delivered components.

For operation as Trusted Filter Management,the following components are required:

- Items 1 and 2 from table 2, installed on
- R&S TF5900M Trusted Filter IP, Part Number 5416.2490.02, Version 08.03

For operation as Trusted Filter Voice and Voice Terminal, the following components are required:

- Items 1 and 2 from table 2, installed on
- R&S TF5900M Trusted Filter IP, Part Number 5416.2490.02, Version 08.03
- Item 3 from table 2, installed on
- R&S GB5900SM Voice Terminal Softkey, Part Number 6157.0180.02, Version 05.00 with integrated R&S RSM-S IP Voice Terminal Security Module, Part Number 5414.0310.05, Version 08.19

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The component AVA_VAN.4 augmented for this TOE evaluation.

The evaluation has confirmed:

- for the Functionality: Product specific Security Target
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by AVA_VAN.4

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

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any cryptographic functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
1	Generation of CMAC tags	CMAC-AES256 (128 bit tag)	NIST SP 800-38B FIPS PUB 197	256	YES
2	Verification of CMAC tags	CMAC-AES256 (128 bit tag)	NIST SP 800-38B FIPS PUB 197	256	YES

Table 3: TOE cryptographic functionality

10. Obligations and Notes for the Usage of the TOE

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

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

11. Security Target

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

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CMAC	Cipher-based Message Authentication Code
CEM	Common Methodology for Information Technology Security Evaluation
CIK	Cryptographic Ignition Key
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IP	Internet Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LED	Light Emitting Diode
MLS	Multi-Level Security
PP	Protection Profile
RTP	Real-Time Transport Protocol

SAR	Security Assurance Requirement
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TCP	Transmission Control Protocol
TFSF	Trusted Filter Security Functionality
TFSM	Trusted Filter Security Module
TFM	Trusted Filter Management
TFV	Trusted Filter Voice
TOE	Target of Evaluation
TOM	Trusted Object Manager
TSF	TOE Security Functionality
VTSM	Voice Terminal Security Model

13.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

14. Bibliography

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

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

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

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

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

[6] Security Target BSI-DSZ-CC-1123-2023, Version 09.00, 03 November 2022, Security Target NAVICS MLS Boundary Protection System Operational Software, Rohde & Schwarz SIT GmbH

[7] Evaluation Technical Report, Version 1.1, 31 January 2023, Evaluation NAVICS MLS Software V01.00 – ETR Summary, Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (confidential document)

[8] Configuration list for the TOE, Version 47.00, 29 November 2022, Configuration List NAVICS MLS Boundary Protection, Part Number 5416.2878.92 (confidential document)

[9] Guidance documentation for the TOE:

- R&S TF5900M Trusted Filter IP User Manual, Version 06, 06 September 2022, Part Number 6190.3078.02, Rohde & Schwarz SIT GmbH
- R&S GB5900SM Voice Terminal Softkey User Manual, Version 03, 06 September 2022, Part Number 6202.7625.02, Rohde & Schwarz SIT GmbH
- Test Description Trusted Filter IP, Version 03.01, 10 December 2020, Part Number 5416.2490.01 T, Rohde & Schwarz SIT GmbH
- Test Instruction Voice Terminal MLS, Version 01.12, 09 December 2020, Part Number 6157.0415.01 T, Rohde & Schwarz SIT GmbH

[7] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

C. Excerpts from the Criteria

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

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

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

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report