Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1089-2020

for

secunet SBC Container Version 4.2.10-7

from

secunet Security Networks AG

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1089-2020 (*)

Netzwerk- und Kommunikationsprodukte

secunet SBC Container, Version 4.2.10-7

from	secunet Security Networks AG
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ASE_TSS.2, ALC_FLR.2 and AVA_VAN.5.

SOGIS
Recognition Agreement
for components up to
EAL 4

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, 8 July 2020
For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG1 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 (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

[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 components ASE_TSS.2, ALC_FLR.2 and AVA_VAN.5. that are not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL 4 components of these assurance families are relevant.

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ 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 secunet SBC Container, Version 4.2.10-7 has undergone the certification procedure at BSI.

The evaluation of the product secunet SBC Container, Version 4.2.10-7 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 24 June 2020. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: secunet Security Networks AG.

The product was developed by: secunet Security Networks AG.

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

5. Validity of the Certification Result

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

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

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the

[5] Information Technology Security Evaluation Facility

maximum validity of the certificate has been limited. The certificate issued on 8 July 2020 is valid until 07. July 2025. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security 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 secunet SBC Container, Version 4.2.10-7 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] secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen

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

Target of evaluation (TOE) is the product secunet SBC Container Version 4.2.10-7 provided by Frafos GmbH.

TOE Type: Session Border Controller

The secunet SBC Container is a Session Border Controller Container, a Linux systemd-nspawn container which can be deployed on a Linux operating system. The main purpose of the secunet SBC Container is a secure bridging between an SIP caller and the SIP callee. Concretely, the SBC supports a safeguarded initiation of SIP sessions (also called signaling) and bridging of media communication streams such as RTP or SRTP. A Session Border Controller (SBC) is a device which is deployed in Voice-over-IP (VoIP) networks to manage the signaling and media streams of audio and video communication. The used hardware is under full control of the operating system. However, the connected networks have to be separated physically, especially the management network, to allow the secunet SBC container to perform the intended operation in a secure manner.

The TOE is integrated in a Linux operating system platform, where the Back-to-Back User Agent module (abbreviated B2BUA with the functionality being referred to as Packet Filtering) is placed.

The associated guidance is considered part of the TOE:

- Secunet SBC Container Handbook 4.2 documentation [9]

There exists only one configuration of the TOE, referenced as indicated above. The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ASE_TSS.2, ALC_FLR.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functionality	Addressed issue
SF.Packet Filtering	The TOE performs an inspection and filtering on several levels: SIP method filtering: the TOE performs filtering based on the SIP method, e.g.: “INVITE”, “SUBSCRIBE”, “REGISTER”, to allow e.g. only to register devices from the inside network. The TOE administrator must configure a limit of invite messages per time interval from outside to protect the components in the inner network from Denial-of-Service (DoS) attacks. Another filtering method is the manipulation of SIP headers. This serves two purposes: for topology hiding SIP header information originating from the inside network is stripped to hide any information which potentially discloses inside network information, e.g. the user-agent field. Also the headers of SIP messages from the external net-work to the internal network are stripped in order to prevent exploitation of the internal

TOE Security Functionality	Addressed issue
	components with e.g. malformed SIP packets or media containers. The administrator can also configure filters on the content type defined in the body of the SIP message, e.g. “application-sdp”. Also the filter can restrict media types e.g. audio, video or application. Finally, the filter can be configured to allow only specific codecs, e.g. G.711 or Opus. To hide the topology of the internal network the TOE implements a strict Back-to-Back user agent to establish two completely separated calls originating from the SBC. If configured according to guidance, at the external network no internal dialog IDs (Call-ID header field, ’tag’ attribute in From and To header fields) and IP addresses are disclosed to the external network. Media streams such as (S)RTP shall only be allowed if a session was initiated before using SIP. Malformed SIP packets and media stream containers shall always be re-fused or dropped.
SF.Management	The initial deployment as well as updates of the TOE are performed by changing the whole container using appropriate tools. This is out of the TOE scope and part of the TOE environment. The TOE is configured by JSON configuration files deployed directly through the SSH interface. The TOE only maintains the role TOE Administrator. This role however is assigned to every user who is in the Linux group “sudoers” which allows these users to update TOE configuration. The TOE allows to define complex filtering and protocol management rules. This includes: • create, modify and delete the signaling (SIP) and media stream endpoints on the SBC, • create, modify and delete the routing of SIP calls, SIP registrations and other SIP messages between the realms and elements in the network, • create, modify and delete the rules for filtering and manipulation options of SIP calls, SIP registrations and other SIP messages, • create, modify and delete the rules for filtering of media containers (transcoding of media streams must be deactivated in the certified use) and • manage all SIP Information Flow SFP security attributes.
SF.Authentication	Users can log in at the management interface with username and password from the management network. The Authentication is performed either locally or by using an external LDAP server if configured. The TOE enforces a password policy with a minimum size of 8 characters on changing of passwords. After three wrong authentication attempts the user account is disabled for a configurable time period to prevent brute force attacks against the management interface. When external authentication is used the authentication of the user is performed by the LDAP server. Then after a successful authentication at the LDAP server the TOE as-signs the access conditions of this user based on the roles received from the LDAP server.
SF.Logging	The TOE provides several interfaces for logging and analyzing of the VoIP network. A syslog daemon is running on the TOE which writes log files to a configured remote syslog server located in the management network.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 6.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

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:

secunet SBC Container Version 4.2.10-7

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	SHA-256 hash sum
1	SW	secunet SBC container version 4.2.10-7	Labelling “secunet-sbc-container-4-2-10-7.tgz “	5ea9f74f894f40372c1f735063e910c90a4b428067160d0d9247e9e906b440d7
2	detached signature file	secunet SBC container signature	Labelling “secunet-sbc-container-4-2-10-7.tgz.sig”	–
3	DOC	Secunet SBC Container Handbook 4.2 documentation	secunet-sbc-container-handbook-4.2-v1.11.tgz Version 1.11	3a4ca42004d219e3783ce96884e50eb27a456cdcf8c30c7ff0818e2943c1e6b5
4	detached signature file	Documentation signature	secunet-sbc-con-tainer-handbook-4.2-v1.11.tgz.sig	–

Table 2: Deliverables of the TOE

The TOE is delivered via secure communication channel (SFTP server) as described in [7], section 2.

The whole files for secunet SBC Container and Handbook are enclosed in an openPGP block that are signed with the Frafos private release key. This signature can be verified with the public key that is exchanged via secure communication channel.

The TOE can be uniquely identified by the SHA-256 checksums listed above.

3. Security Policy

The security policy enforced by the TOE is defined by the selected set of Security Functional Requirements and implemented by the TOE functionality. The TOE implements logical security functionality in order to perform data inspection and protect user data by filtering SIP headers and media stream containers. Hence the TOE maintains integrity and confidentiality of code and data stored in its memories by the correct operation of the security functionality provided by the TOE. Therefore the TOE' s policy is to protect against malfunction, leakage and manipulation. Besides, the TOE' s life cycle is supported as well as the user Identification whereas the abuse of functionality is prevented. Specific details concerning the above mentioned security policies can be found in sec. 3 of [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:

Security Objectives for the operational environment defined in Security Target	Description according to ST
OE. SecurePlatform	The TOE software shall be deployed on a hardened Linux Operating System such as a secunet wall. The container functionality systemd-nspawn has to be provided. It shall also ensure that the integrity of the TOE is protected against malicious manipulation. The operating system platform shall ensure that only packets from the internal and external networks with a destination port number that correspond to a signaling or media interface con-figured in the Secunet SBC Container are directed to the Secunet SBC Container. The signaling ports are the SIP and SIP/TLS ports defined in the signaling interface; The media ports are the port number corresponding to the port range defined in the media interface starting at 10000 minimum, as no other services are bound to any port equal or above 10000. Other packets received on these interfaces shall be dropped. The operating system platform shall ensure that from the internal and external network all SIP and media stream packets and no other packets are directed to the TOE. Other connections are only allowed from the secured management network over a dedicated and physically separated network interface. This includes SSH access for management purpose, LDAP authentication as well as monitoring (SNMP and monitoring access). The operating system platform shall further ensure that outgoing DNS requests are only directed to the internal or to the secured administrative network. The operating system Administrator has to make sure that the operating system is installed and operated in a secure way. The platform must also ensure that

	the configuration data which contains the filtering policy is kept integrity protected. Additionally the platform must provide reliable time stamps to the TOE in order to allow the TOE to provide reliable audit records.
OE.PhysicalAccess	The TOE shall be used in a controlled environment. The environment shall ensure that only authorized personnel can access the TOE physically. This also holds for the Management net-work including all servers and the machine from where the user connects to the TOE.
OE.ManagementNetwork	Access to the SSH interface shall only be possible from a distinct and secure management network which shall be physically separated from both the internal and external network and only accessible by administrators. Also the machine used by the TOE Administrator to connect to the SSH inter-face, the optional ABC Monitor and the server(-s) which receive and store the audit logs from the TOE shall be located in this management network. If LDAP authentication is configured, no data transferred during the authentication shall leave the secured management network.
OE.Administrators	The administrators of the TOE and the underlying Linux operating system shall be well skilled and trustworthy and shall configure as well as operate TOE and operating system platform in a secure way. The TOE Administrator shall be an expert in the field of VoIP technology and the setup and management of a Session Border Controller.
OE.NetworkFlow	The hardware machine running the TOE and the Linux operating system platform shall be deployed so that it provides the only connection between the internal and the external network. The operating system platform shall be configured that signaling and media traffic from internal and external net-work handed is over to the Secunet SBC Container and other packets received on these interface are dropped. Additionally, the internal and external networks must be connected to physically separated network interfaces (no VLANs or similar mechanisms).
OE.LDAP	If user authentication is performed by a remote LDAP server the LDAP server shall be located in the secure management network. The LDAP server shall ensure that no data transferred during authentication leaves the management network. The LDAP server also needs to provide a mechanism to limit the authentication attempts, when using LDAP authentication. This server also needs to implement the LDAP protocol correctly.
OE.Syslog	Syslog messages are generated by the TOE and sent to the

	syslog server in the management network. This syslog server shall provide a secure storing mechanism to ensure that the integrity of the received syslog messages is protected after the syslog server receives the message.

Table 3: Security Objectives for the TOE-Environment

Details can be found in the Security Target [6], chapter 4.2 and [9].

5. Architectural Information

The TOE is executed as a systemd-spawn container on a hardened Linux operating system platform, such as a secunet wall. This operating system platform protects the integrity of the TOE. The integrity check of container is the first step of initialization. The main purpose of the secunet SBC Container is the initiation of a secure SIP session (also called signaling) and media communication streams such as RTP or SRTP. To protect the internal network the TOE perform data inspection and filtering on several protocol levels.

The security functions of the TOE are:

- SF.PacketFiltering
- SF.Management
- SF.Authentication
- SF.Logging

According to the TOE design specification these security functions are enforced by the following subsystems:

- Signaling and processing (SF.PacketFiltering)
- Configuration (SF.Management)
- User management and authentication (SF.Management, SF.Authentication)
- Logging (SF.Logging)

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

7.1. Developer Testing

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

For the tests of the TOE the developer used the test environment with two virtual machines. This test environment consists of an executable shell script that starts up the virtual machines and initializes the complete test setup. The automated test cases are developed in C++. The test configuration takes place using file “config.txt” and includes the topology and IP addresses to be applied for the test scenario. A description of the test cases and the single steps which are done in the test execution is given in “index.html” and supplementary data in the “result tarball” as test reports.

Testing Results

The results of the developer tests are documented and prove the correct implementation. All test cases were executed successfully and ended up with the expected test results.

7.2. Independent Testing

The independent testing approach contains repetition of the developer test. Additionally the evaluators considered results from the RFC analysis. The TOE has four TSFI from which three TSFI are thoroughly tested. The other, interface 2 (configuration interface) is only accessible (OE.ManagementNetwork) from trusted personal (OE.Administrators) and well covered by developer tests. The coverage of developer tests was listed in the testplan to enrich the independent testing strategy.

The TOE configuration is identic for operations on a generic Linux resp. on a secunet wall. Only one configuration exists for the TOE, which was subject to the independent testing.

The evaluators covered 33 test aspects that were not included in the developer test set earlier. The interfaces have been selected by their exposition to third parties. The evaluators also included interfaces where the interface could be offended by misconfiguration in the TOE environment. The tests span over all four TSFI. The other SBC interfaces have been implicitly used in administrating the TOE. Also these are only accessible to trusted personnel.

The evaluators decided to repeat all tests cases provided by the developer.

Testing Result

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

7.3. Vulnerability Analysis

For the penetration tests assessment of ‘Common Vulnerability Entries’, code review, fuzzing and load tests were used. The evaluators retrieved the applied versions of reused libraries and retrieved known vulnerabilities. During code review and fuzzing the penetration testers identified interfaces at the attack surface and send patterns that could trigger implementation flaws. During overload scenario applicability of TOE reconfigurations and SFP enforcement have been checked. No vulnerabilities have been identified during these activities.

The test environment for penetration tests consist of the TOE, two Linux machines and an asterisk private branch exchange. For the load tests a total of four Linux machines (three sources and one target) have been set up. For the independent tests at the evaluator’s site one laptop running VMware and two virtual machines have been set up.

For penetration tests such as fuzzing relevant parts of the TOE have been compiled into the fuzzer framework of llvm and gasoline. For other tests the SBC container that contains the TOE has been used.

Penetration Test Result

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential high was actually successful in the TOE’ s operational environment as defined in [6]. This shows that all measures required by the developer are applied.

Testing and vulnerability assessment considered both the secunet wall and generic Linux platforms. Other configurations have not been defined by the vendor und thus were not assessed. The results of the evaluation can only be applied on secunet SBC Container Version 4.2.10-7. Without a preceding evaluation, the extension of the results to other versions of the TOE is not possible.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE evaluated configuration is defined by the notation:

- secunet SBC Container
- The documents:
  - Secunet SBC Container Handbook
  - Security Target

To identify the TOE, the document [9] is providing sufficient information about identification mechanisms in chapters 4.1.2.1 and 4.1.2.2.

The description of the required non-TOE hardware, software and firmware is described in Ch. 1.3.4 of [6] and repeated in Ch. 4.1.1 and 4.3 of [9]. The secunet SBC Container as a software-only TOE needs a Linux operating system with the systemd-nspawn container management technology installed. The hardware remains fully controlled by the operating system. The connected networks have to be separated physically. This requirement is especially valid for a management network that is necessary needed for the management and the configuration of the TOE.

9. Results of the Evaluation

9.1. CC specific results

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

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ASE_TSS.2, ALC_FLR.2 and AVA_VAN.5. augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ASE_TSS.2, ALC_FLR.2 and AVA_VAN.5.

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

9.2. Results of cryptographic assessment

The TOE does not include cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

10. Obligations and Notes for the Usage of the TOE

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

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

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

The assessment has a very strict configuration mandated by the security guidance. Violation of guidance instructions to the administrators is prohibited. It enforces especially:

- deactivation of cluster config;
- no modification of daemon and service configurations;
- activation of topology hiding (for the inner SIP clients) by JSON configuration;
- no use of backreferences in regular expressions;
- adequate configuration of an external firewall wrt. to SNMP, DNS, redis;
- careful configuration of rate limiting via CAPS.

The TOE is (principally) unable to protect clients from SIP digest authentication relay attacks. The TOE provides capabilities to limit call rates using CAPS, but finally this does not protect SIP clients against DoS attacks.

11. Security Target

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

12. Definitions

12.1. Acronyms

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
CAPS	
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DNS	Domain Name System
DOS	Denial of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LDAP	Lightweight Directory Access Protocol
openPGP	open Pretty Good Privacy
PP	Protection Profile
RTCP	RealTime Control Protocol
RTP	Real-Time Transport Protocol
SAR	Security Assurance Requirement
SBC	Session Border Controller
SFP	Security Function Policy
SFR	Security Functional Requirement
SIP	Session Initiation Protocol
SNMP	Simple Network Message Protocol
SRTCP	Secure RealTime Control Protocol
SRTP	Secure Real-Time Transport Protocol
ST	Security Target
TOE	Target of Evaluation

TSF	TOE Security Functionality
VoIP	Voice over IP

12.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

13. Bibliography

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

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[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-1089-2020, Version 1.12, 30.04.2020, Security Target for secunet SBC Container, secunet AG

[7] Evaluierungsbericht, Version 1.3, 24.06.2020, Evaluation Technical Report (ETR) – Summary, SRC Security Research & Consulting GmbH (confidential document)

[8] Configuration list for the TOE, Version 2.8, 04.05.2020, Tools and Techniques / Configuration, secunet SBC Container, FRAFOS (confidential document)

[9] Secunet SBC Container Handbook 4.2, Version 1.11, 29.04.2020

[7] specifically

- Anwendungshinweise und Interpretationen zum Schema, AIS1: Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14, 11.10.2017, Bundesamt für Sicherheit in der Informationstechnik
- Anwendungshinweise und Interpretationen zum Schema, AIS14: Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 03.08.2010, Bundesamt für Sicherheit in der Informationstechnik
- Anwendungshinweise und Interpretationen zum Schema, AIS19: Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9, 03.11.2014, Bundesamt für Sicherheit in der Informationstechnik
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 08.06.2011, Bundesamt für Sicherheit in der Informationstechnik
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1), Version 3, 03.09.2009, Bundesamt für Sicherheit in der Informationstechnik

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 detailled 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