Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1267-2026

for

genugate firewall 11.0 p0

from

genua 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-1267-2026 (*)

Firewall

genugate firewall 11.0 p0

from	genua GmbH
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 extended EAL 4 augmented by ALC_FLR.2, ASE_TSS.2, AVA_VAN.5 and ALC_PAM.1
valid until:	22 February 2031

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), CEM:2022 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), CC:2022. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

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

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

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

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

Bonn, 23 February 2026

For the Federal Office for Information Security

Fabian Hodouschek
Head of Certification

L.S.

Sandro Amendola
Director-General Directorate General S

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - 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]
- BMI Regulations on Ex-parte Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licensing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), CC:2022 [4] [1] also published as ISO/IEC 15408

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBI. 2025 , no. 301, p. 2

[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 02 December 2025, Bundesgesetzblatt 2025, no. 301

[3] BMI Regulations on Ex-parte Costs – Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) – dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Methodology for IT Security Evaluation (CEM), CC:2022 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

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

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

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

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

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

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

This certificate is recognized 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_PAM.1, 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.

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 Federal Office for Information Security dated 14. April 2023 at https://www.bsi.bund.de.

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 genugate firewall 11.0 p0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1154-2021.

The evaluation of the product genugate firewall 11.0 p0 was conducted by secuvera GmbH. The evaluation was completed on 19 February 2026. secuvera GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: genua GmbH.

The product was developed by: genua 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 evaluated guidance documentation are observed,
- the product is operated in the environment as specified and in the Security Target.

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 23 February 2026 is valid until 22 February 2031. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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

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

6. Publication

The product genugate firewall 11.0 p0 has been included in the BSI list of certified products, which is published regularly in the listing found at the BSI Website https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Further information can be obtained from BSI-Infoline +49 (0)228 9582-111.

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

[6] genua GmbH
Domagkstraße 7
85551 Kirchheim

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) genugate firewall 11.0 p0 is part of a larger product, the firewall genugate 11.0 p0, which consists of hardware and software. The TOE itself is part of the software. The operating system is a modified OpenBSD. The TOE supports IPv4 and IPv6.

The product genugate exists in two variants. The first simply named genugate is a two-tiered application with the physically separated components Application Level Gateway (ALG) and the Packet Filter (PFL) connected in series. They run on dedicated hardware provided by genua and other selected suppliers. The second variant named genugate Virtual is the virtualized ALG without the PFL. In virtualized environments, the serial connection of two virtualized components on one hypervisor does not bring any significant security advantage. The total system can only be as secure as the hypervisor.

Besides the network interface to the PFL (or the internal network in case of the genugate Virtual), the ALG has (at least) three more interfaces in order to connect to the external network, the administration network and the demilitarized zone(s) (DMZ). For the high availability option, the ALG needs another network interface for the HA network. The PFL has a second interface which is connected to the internal network, and optional interfaces for further DMZs.

The aim of the firewall is to control the IP traffic between the different connected networks. Therefore the ALG uses proxies that implement filter policies in order to control all data transmitted between the different networks, while the PFL uses packet filtering as an additional means to control all data that is sent to and from the internal network.

The TOE, genugate firewall 11.0 p0, consists of the software that implements the IP traffic control and related functionality of the firewall on the ALG. This includes the proxies, the hardened OpenBSD kernel IP stack, packet filter, but also other supportive functionality as logging of security events (see the next section for a more detailed definition of the TOE scope and boundary).

The PFL software, although the PFL is present in the architecture of the hardware variant genugate, is not part of the TOE.

The Security Target [5] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details), and some (ALC_PAM.1) are newly defined by [11]. The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.2, ASE_TSS.2, AVA_VAN.5 and ALC_PAM.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [5], chapter 6.1. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue,
SF.SecurityAudit	see ST [5], chapter 7.1.1
SF.DataFlowControl	see ST [5], chapter 7.1.2

TOE Security Functionality	Addressed issue,
SF.IdentificationAuthentication	see ST [5], chapter 7.1.3
SF.SecurityManagement	see ST [5], chapter 7.1.4
SF.SelfProtection	see ST [5], chapter 7.1.5
SF.PatchInstallation	see ST [5], chapter 7.1.6
SF.TrustedCommunication	see ST [5], chapter 7.1.7
SF.CryptographicSupport	see ST [5], chapter 7.1.8

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [5], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [5], chapter 3.2 . Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [5], chapter 3.3, 3.4 and 3.5.

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 52, 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:

genugate firewall 11.0 p0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW/ HW	genugate firewall	11.0 p0	Install image and hardware with no software pre-installed.

No	Type	Identifier	Release	Form of Delivery
2	DOC	English and German manuals (only German versions are part of TOE): • administrator and user guidance (genugate Administration and Configuration Manual, genugate Administrations- und Konfigurationshandbuch); • installation manual (for hardware variant: genugate Installation Manual, genugate Installationshandbuch; for virtual variant: genugate Virtual Installation Manual, genugate Virtual Installationshandbuch); • certification guidance (genugate Certification: General Information, genugate Erläuterungen zur Zertifizierung)	11.0 p0	Manuals, downloaded separately from genua customer support server

Table 2: Deliverables of the TOE

The server hardware is genugate S, genugate M, or genugate L, with hardware revision 3.0 or 4.0; or SDoT Server V3B. The SDoT Server V3B hardware is an Infodas product and is supplied and delivered by Infodas. If the genugate hardware variant with Infodas hardware SDoT Server V3B shall be used, the end customer must order and purchase the hardware SDoT Server V3B separately from company Infodas.

Otherwise, the hardware of the TOE is composed at Pyramid Computer GmbH, Schubert System Elektronik GmbH and Arrow Central Europe GmbH and shipped together with the installation image to the customer.

The TOE is located as software distributed within installation images. The installation images (ISO image, USB image or QCOW2 image format) can either be shipped with the required non-TOE hardware on a separate USB flash drive, or can be downloaded from the genua support server, whereby the download is the only one possible for customers buying the genugate Virtual product variant.

The documentation can be downloaded from the genua support server. The TOE is contained in the installation images for the product genugate 11.0. The licence information is sent to the customer by genua.

For the genugate Virtual the end user has to check the hardware if the needed virtualization features (VT-x for Intel CPUs and AMD-V for AMD CPUs) are supported, see chapter 1.3.1 of the ST [5] for the requirements on hardware and hypervisor in the scope of the evaluation. In both cases, for the physical as well as for the virtual variant of the genugate, the hardware is not part of the TOE.

The user is able to verify the authenticity of the delivered TOE. The procedure is described in detail in the guidance documentation. The valid SHA256 checksums to verify the authenticity of the delivered TOE and manuals are published on the developers' web page

protected via TLS1.2 and TLS1.3 at *https://kunde.genua.de/support/genugate-110-checksummen*.

These SHA256 checksums are as follows:

ISO-Image:

G1100_000.iso

31119bc24e978acf629f84938d9f20e9b08842678b23c0c331d3ca4b7a5e9315

IMG-Image:

G1100_000.img:

379701857a064d4c255f55df660d6be878b019d9796f3c8c954ed19f6ed240aa

qcow2-Image:

G1100_000-stage1-128G.qcow2:

ee5d1a8b8e62cb49a316016632766e4c63aeebf59025a908041181466ed59ad3

Handbücher:

genugate-1100-admin-de.pdf:

1303ded7139bed3fa19f5b0efb176fcad572dd84f8bf29479d93a914039a7d02

genugate-1100-install-de.pdf:

e6465e767bba08dd4f19e1a69580d584b01d5f30c272794aa9c9fa2449ae8e41

genugate-1100-virtual-install-de.pdf:

e671ee1b28a9ab26b141b6a79f19fd7a3297f1f68ec6c211ab629bfb11b25875

genugate-1100-zertifizierung-de.pdf:

38b16b6dfb2712118ce6cf0d52b687aaacafe8b112aff9a99229aff0c7403220

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers Security audit, Data flow control, Identification and Authentication, Security management, Protection of the TSF, and patch installation, as detailed in the ST [5] in chapter 7.

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. Details can be found in the Security Target [5], chapter 4.2.

5. Architectural Information

The TOE genugate firewall 11.0 p0 is used to control the connections and data transfer between different networks, where each network has different security needs and different threat levels for the other networks.

The TOE can be configured in such a way that the security needs for each network are optimally met. A standard configuration consists of the following networks connected to the TOE:

internal network: This is the network that has to be protected against attacks from the external network. Usually only a few services from the internal network are accessible from the external network, secured by user authentication. The internal network is secured by the TOE, using filtering mechanisms at different levels of the IP stack. This network is usually controlled by a defined security policy.

external network: This is the most insecure network, e. g. the internet. In general, no security policy exists, and all kind of attacks can occur in this network.

administrative network: This network is used to allow a secure administration of the TOE. This network is isolated from all other networks and only administrators have access. The usual access is through the HTTPS web interface, but an SSH access for debugging and maintenance operation is also available.

demilitarized zones: These networks allow access to common services from the external network, without the need to open the internal network. Usually, Web servers and FTP servers are installed in this network. This network is usually controlled by a defined security policy.

HA network: This internal network is necessary for the high availability option. It is used to synchronize the configuration between the systems.

The internal HA network must use IPv4 addresses. For all other networks IPv4 and IPv6 is supported (with the exception that the proxy mcastudprelay, which is needed for multicast UDP packets, only supports IPv4).

For the physical genugate, the internal network is moreover protected by a two-tiered security architecture that filters on different levels of the network stack (ALG and PFL, running physically separated on different hardware). ALG and PFL must be separately configured. The filter rules of the PFL cannot be modified during normal operation. All this provides an additional layer of security hardening.

The genugate Virtual consists of the virtualized ALG and implements equivalent filter tasks on IP level as the PFL does, which suits a virtualized environment.

The PFL software, although the PFL is present in the architecture of the hardware variant genugate, is not part of the TOE.

6. Documentation

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

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

7. IT Product Testing

The developer testing concept is based on periodically running automatic tests in the product specific test environment that contains physical as well as virtual test systems. These are supplemented by unit tests that are executed directly on a test server and some

manual tests. Additionally to these developer tests there are separate tests of the quality assurance department.

The developer testing environment includes genugate hardware of different hardware revisions. The regular tests are not necessarily performed on hardware that is in scope of the certification. This is because the product is assumed to run on a wider range of hardware than that in scope of the certification. To ensure this the developer performs hardware tests in preparation of every major product version which includes changes to a newer version of the included OpenBSD operating system. Based on these tests of the operating system for all relevant hardware the further testing is assumed to be independent of the hardware. Nevertheless for the certification relevant test results it is ensured that the hardware dependent tests run on hardware revisions in scope of the certification and also virtualized.

Using the test scripts the developer automatically ensures for the most part that the entrance conditions and the dependencies between tests are considered. Therefore the responsibility for the correct testing is transferred to the developer.

Additionally the developer runs tests in the quality assurance (QA) lab. The QA lab is an independent test department inside the company. The QA lab is involved prior to every release and has to approve by its positive testing result and is completely separated from the developer test environment. The lab consists of physical and virtual genugate systems. These tests are divided in automatically and manual tests. The automatically tests are run on a regular base.

Complete coverage was achieved for all the TOE security functions as described in the functional specification. The overall test depth of the developer tests comprises the TOE design subsystems and the internal interfaces of those subsystems as required for the assurance level of the evaluation.

All real test results are equal with the expected test results.

The Independent Evaluator Tests were performed in a logically and physically separated network within the laboratory of the ITSEF. The TOE in this network was accessible via the connected test devices. The test environment was built-up according to comply with the security objectives of the TOE environment. For each physical genugate also a PFL was used. Further an OSPF router and test clients were used in the test network.

A sample of developer tests has been retested with the developer as part of the ITSEF tests. Testing in the own premises covers among the complex installation all security functions.

The test results have not shown any deviations between the expected test results and the actual test results during the installation or operation. Also no deviations during the performed verification of the TOE and manuals were identified.

The penetration testing was performed in the ITSEF using the TOE in version 11.0 p0 in a logically and physically separated network within the laboratory of the ITSEF. The TOE in this network was accessible via the connected test devices.

During the penetration testing not all tests were performed on each TOE hardware and not on the genugate virtual. As the functionalities of the TOE are independent of the underlying platform, a sampling was performed in which the platforms for each test procedure were chosen randomly.

The tests addressed threat by physical access, threat by logical access, external attackers, and internal attackers. Additionally, as part of ADV_IMP a source code analysis was performed.

If all operational measures required by the developer are applied, no attack scenario with high attack potential was actually successful in the TOE's operational environment as defined in the ST.

8. Evaluated Configuration

The TOE has to be configured, and is limited to the restrictions, as stated in the Security Target [5] and Guidance [7 - 10]. The security requirements for a network defined in both documents are to be met. The TOE has to be configured following the TOE guidance. The components of the TOE are defined by the TOE configuration list. The configuration list consists of several archives. Their hash values are listet here:

Configuration list *see* chapter 2 and additionally:

Source Code:

SHA256(gg-502f2027.tgz):

273ab7a414e66b20f277477942c4275e557ff68a53e6267d396cb37db11a4ca7

SHA256(openbsd-7.5.tgz):

36c06a930bc31efc587ecfe288b27f2a8f30a77de7d8f63c2a6511cac478fdd6

SHA256(websocketd-v0.3.1.zip):

6330d15ab1121f2e9423ddc4c039b3398e5066fb6391fde678208f31a63507dc

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [6] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used 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).

For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

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 ALC_FLR.2, ASE_TSS.2, AVA_VAN.5 and ALC_PAM.1 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1154-2021, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on extensions and enhancements of TOE functions and -configurations.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 extended
  EAL 4 augmented by ALC_FLR.2, ASE_TSS.2, AVA_VAN.5 and ALC_PAM.1

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 52, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 120 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 3 (also to be found in the ST [5], chapter 8) 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 120 Bits*' of the following table with '*no*' achieves a security level of lower than 120 Bits (in general context) only.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
Software Patch Verification					
1	Integrity	SHA-512 (default), SHA-384 or SHA-256	FIPS 180-4	N/A	yes
2	Authentication	RSA using RSASSA-PKCS1-v1_5	PKCS #1, v2.2	|k| = 4096	yes
3	Authentication	ECDSA P-256	FIPS 186-5, NIST SP 800-186	|k| = 256	yes
SSH					
1	Trusted channel	SSHv2	RFC 4251, RFC 4252, RFC 4253, RFC 4254	-	-
2	SSH server	ECDSA P-256 with SHA-256	FIPS 186-5,	|k| = 256	yes

	authentication		NIST SP 800-186		
3	SSH user authentication	ECDSA P-256, P-384 or P-521 with SHA-256	FIPS 186-5, NIST SP 800-186	|k| = 256, 384 or 521	yes
4	Key Agreement	ECDH brainpoolP256r1 with SHA-256, brainpoolP384r1 with SHA-384, or brainpoolP512r1 with SHA-512	RFC 5656, RFC 5639	|k| = 256, 384 or 512	yes
5	Key Agreement	ECDH P-256 with SHA-256, P-384 with SHA-384, or P-521 with SHA-512	RFC 5656, SEC 1, NIST SP800-186	|k| = 256, 384 or 512	yes
6	Key Agreement	DH MODP group16 or MODP group18 with SHA-512	RFC 4253, RFC 8268	|k| = 4096 or 8192	yes
7	Confidentiality	AES CTR	FIPS 197, NIST-SP800-38A	|k| = 128, 192 or 256	yes
8	Integrity	HMAC with SHA-256 or SHA-512	RFC 2104, FIPS 180-4	|k| = 256 or 512	yes
TLS					
1	Trusted channel	TLS 1.3	RFC 8446	-	-
2	TLS server authentication	RSA using RSASSA-PSS or RSASSA-PKCS1-v1_5 with SHA-256, SHA-384 or SHA-512 (with RSASSA-PKCS1-v1_5 only in certificate)	PKCS #1, v2.2	|k| = 3072 (default) or bigger	yes
3	TLS server authentication	ECDSA P-256 with SHA-256, P-384 with SHA-384, or P-521 with SHA-512	FIPS 186-5, NIST SP 800-186	|k| = 256, 384 or 512	yes
4	TLS client authentication (for 2FA)	RSA using RSASSA-PSS or RSASSA-PKCS1-v1_5 with SHA-256, SHA-384 or SHA-512 (with RSASSA-PKCS1-v1_5 only for certificate verification)	PKCS #1, v2.2	3072 <= |k|	yes
5	TLS client authentication (for 2FA)	ECDSA P-256 with SHA-256, P-384 with SHA-384, or P-521 with SHA-512	FIPS 186-5, NIST SP 800-186	|k| = 256, 384 or 512	yes
6	Key Agreement	ECDH P-256 or P-384	RFC 5656, SEC 1, NIST SP 800-186	|k| = 256 or 384	yes
7	Key Agreement	ECDH brainpoolP384r1 or brainpoolP512r1	RFC 5656, SEC 1, RFC 5639	|k| = 384 or 512	yes
8	Confidentiality and	AES GCM	FIPS 197,	|k| = 128 or 256	yes

	Integrity (AEAD)		NIST SP 800-38D		
9	Integrity	HMAC with SHA-256 or SHA-384	RFC 2104, FIPS 180-4	|k| = 256 or 384	yes
IPsec					
1	Trusted channel	IPsec and IKEv2	RFC 4301, RFC 7296	-	-
2	Authentication	HMAC with SHA-512, with pre-shared key	RFC 2104, FIPS 180-4	|k| = 512	yes
3	Key Agreement	ECDH brainpoolP512r1	RFC 5656, RFC 5639	|k| = 512	yes
4	Pseudo-random function (PRF)	HMAC with SHA-512	RFC 2104, FIPS 180-4	N/A	yes
5	Confidentiality	AES CBC	FIPS 197, NIST SP 800-38A	|k| = 256	yes
6	Integrity	HMAC with SHA-512	RFC 2104, FIPS 180-4	|k| = 512	yes

Table 3: TOE cryptographic functionality

Reference details for table 3 can be found in the ST [5], chapter 8.

10. Obligations and Notes for the Usage of the TOE

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

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

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

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.

For a secure operation it is necessary to follow all recommendations of the manual of the TOE and to follow all requirements of the environment described in the Security Target.

There should be regularly performed inspections of the TOE configuration. During those inspections also the user, profile and group access rights should be examined.

During operation of the genugate, it is essential to ensure that configuration backups are stored physically and logically secure. This should be done using a protection method similar to the physical and logical security measures used for the genugate.

11. Security Target

For the purpose of publishing, the Security Target [5] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. Acronyms

ACL	Access Control List
AIS	Application Notes and Interpretations of the Scheme
ALG	Application Level Gateway
ANSI	American National Standard Institute
BPF	Berkeley Packet Filter
BSD	Berkeley Software Design
BSDI	Berkeley Software Design, Inc.
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
CARP	Common Address Redundancy Protocol
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CGI	Common Gateway Interface
CLI	Command Line Interface
DMZ	Demilitarised Zone
DNS	Domain Name Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
HA	High Availability
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol

IEC	International Electrotechnical Commission
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISO	International Standardisation Organisation
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
OpenBSD	Open Berkeley Software Distribution, a security focused operating system
OSPF	Open Shortest Path First
Perl	Practical Extraction and Reporting Language
PF	Packet Filter (component of OpenBSD)
PFL	Packet Filter (component of genugate)
PKCS	Public-Key Cryptography Standard
PP	Protection Profile
QA	Quality Assurance
RSA	Rivest, Shamir, and Adleman, a public key encryption algorithm
RSASSA	RSA Signature Scheme with Appendix
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SSH	Secure SHell
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
Telnet	Telecommunication network
TOE	Target of Evaluation
TSF	TOE Security Functionalities
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WWW	World Wide Web

13.2. Glossary

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

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

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

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

Informal – Expressed in natural language.

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

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

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

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

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

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

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

14. Bibliography

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

- Part 5: Pre-defined packages of security requirement
https://www.commoncriteriaportal.org

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

CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.org

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

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

[5] Security Target BSI-DSZ-CC-1267-2026, genugate firewall 11.0 p0, Version: 11.0.12 (141f1f2), Date: 2026-01-27, genua GmbH

[6] Evaluation Technical Report BSI-DSZ-CC-01267 for genugate firewall 11.0 p0, Version 2, Date 09.02.2026, secuvera Gmbh (confidential document)

[7] genugate Administrations- und Konfigurationshandbuch, Version 11.0, Ausgabe 7. Januar 2026, genua GmbH

[8] genugate Installationshandbuch, Version 11.0, Ausgabe 7. Januar 2026, genua GmbH

[9] genugate Virtual, Installationshandbuch Ausgabe 15, Dezember 2025, Revision: 39258e4, genua GmbH

[10] genugate Erläuterungen zur Zertifizierung, Ausgabe: 29. Januar 2026, genua GmbH

[11] Technical Specification ISO/IEC TS 9569, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045, ISO/IEC TS9569, 2023-11

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 38, Version 2, Reuse of evaluation results

C. Excerpts from the Criteria

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

- On conformance claim definitions and descriptions refer to CC:2022 part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC:2022 Part 3 chapter 6.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CCRA CC:2022 Part 5.
- On the assurance class ASE for Security Target evaluation refer to CC:2022 Part 3 chapter 9
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC:2022 Part 3 chapters 7 to 15
- The table 1 in CC:2022 part 5, Chapter 4.2 summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

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

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

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report