Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1154-2021

for

genugate 10.0 Firewall Software

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-1154-2021 (*)

Firewall

genugate 10.0 Firewall Software

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 ASE_TSS.2, ALC_FLR.2,
ALC_PAM.1, AVA_VAN.5

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, 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), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

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

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

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

Bonn, 22 June 2021

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

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

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

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

- Common Criteria for IT Security Evaluation (CC), Version 3.1[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_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.

[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 genugate 10.0 Firewall Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1039-2017. Specific results from the evaluation process BSI-DSZ-CC-1039-2017 were re-used.

The evaluation of the product genugate 10.0 Firewall Software was conducted by secuvera. The evaluation was completed on 14 June 2021. secuvera 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 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 22 June 2021 is valid until 21 June 2026. 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 genugate 10.0 Firewall Software 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] 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) is the genugate 10.0 Firewall Software which is part of a larger product, the firewall genugate 10.0 Z, which consists of hardware and software. The TOE genugate 10.0 Firewall Software itself is part of the shipped software. The operating system is a modified OpenBSD.

The firewall genugate 10.0 Z is a combination of an application level gateway (ALG) and a packet filter (PFL), which are implemented on two different systems. It is thus a two-tiered firewall. The network connection between ALG and PFL is a cross cable.

Besides the network interface to the PFL, the ALG has (at least) three more interfaces to connect to the external network, the administration network and the demilitarized zone network (a 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.

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

To mitigate hardware failures the genugate has a high availability option where two or more genugate systems are operating in parallel and take over a failing system.

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 on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details) and one of them is newly defined. The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ASE_TSS.2, ALC_FLR.2, ALC_PAM.1, AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], 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_SA	Security audit
SF_DF	Data flow control
SF_IA	Identification and Authentication
SF_SM	Security management
SF_PT	Protection of the TSF
SF_PI	Patch installation

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6], 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 [6], 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 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:

genugate 10.0 Firewall Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	genugate firewall	10.0	Install image
2	SW	genugate platform	10.0 Z	Install image
3	DOC	genugate 10.0 Z Installationshandbuch, Version 10.0 Z Patch 000, Ausgabe März 2021, Revision v10.0-RC3, [8] genugate 10.0 Z Administrationshandbuch, Version 10.0 Z Patch 000, Ausgabe März 2021, Revision v10.0-RC3, [9]	10.0 Z	Manual (German version) (also part of the install image)

Table 2: Deliverables of the TOE

Please note that the Hardware components genugate S, Revision 2.0 and 3.0, genugate M, Revision 2.0 and 3.0, genugate L, Revision 2.0 and 3.0 are part of the evaluated and certified configuration of the TOE but they are not part of the TOE. The product genugate 10.0 Z may be shipped with hardware but the TOE is the aforementioned software and documentation only. The evaluated configuration is limited to the above listed latest hardware models and revisions but the commercial product genugate 10.0 Z is designed to run on a wider range of hardware that exceeds the scope of the certification.

The TOE is identified as software that is distributed on an installation image. The Image can either be shipped with the required non-TOE hardware, or can be downloaded from the genua support server. Both an USB install image and an ISO-image are available for installation. The documentation is contained in the install images but can also be downloaded from the genua support server. The TOE is part of the install images for the product genugate 10.0 Z.

The licence information is sent by genua to the customer.

The user is able to verify the authenticity of the delivered TOE. The procedure is described in detail in the guidance documentation [8, 9]. Therefore SHA-256 and SHA-512 checksums are provided on the genua webserver under the following URL:

https://kunde.genua.de/nc/produkte.html?cid=51677&path=Produkte>genugate>Checksummen

The valid checksums of the TOE are:

ISO-Image:

SHA256(G1000_000.iso)=
9911f5f8bcab26e64e585e2faad7e4355a1bb027e066295c2fc949b52e033869

SHA512(G1000_000.iso)=
d6787d17ef311261c13de78ab35d043f101fe045028ddee4e28e2043f473fe268dbf0e7d7e2740874
291a7e812f102f083b650b65280779e4ebe5471f7bc2f97

USB-Image:

SHA256(G1000_000.img)=
271576423004707642604f862e36b3bf8d250534acfec619ae2470b2c07374bf

SHA512(G1000_000.img)=
8a042144def37211a477c94688243fd10dbd75e0d9907fe683843fb47aaeaabae9de324eeb42709af
5e773dd00ddbcf7ee82aaa560fb924432a9e2d05520fcbd

Installation packages in folder 6.6/amd64/:

SHA256(6.6/amd64/CKSUM)=
ba7e85162b461e1ae55f4ace29844df35d33523aada692acc4d0cd82cc41e2f2

SHA256(6.6/amd64/INSTALL.amd64)=
4058fdd5e7b568083cd8e3f53ed920000a119c5f353ea4da5e91de8e20bdfb88

SHA256(6.6/amd64/RMD160)=
dbce170155a44b4ac72c133d8d359de27dec24c942a7bef43b20ad2694639ddb

SHA256(6.6/amd64/SHA1)=
65bd02df6bc3efef7a741b58cbb48686c910ced39299495aa9c878f9a375e493

SHA256(6.6/amd64/SHA256)=
1674d9c70b8cc2a6fb8381ca418d418f616b512b63624477fdb8219e6e8eee81

SHA256(6.6/amd64/SHA512)=
1838f16a7e7855e8549f2138ef91c4f59e39cbc9ce5f95bcb49b7c72489ae023

SHA256(6.6/amd64/base66.tgz)=
231e5fa744f854e32131dee9f2f119aeb2e1f8a27e811718fe171c7b78d72181

SHA256(6.6/amd64/boot.catalog)=
26cbdc495f8661f5befd99892ba798502c78bcab90dc1cf5cdc52d0300fbd3ad

SHA256(6.6/amd64/cd66.iso)=
990c119b75d822a6f57fdf64dcc1b39218397716057c160820314e95cd6166a1

SHA256(6.6/amd64/cdboot)=
fefdb3bdbbf6512ad813f8be0b8193d3e898e6b8f9bad7ae418873c3e901f468

SHA256(6.6/amd64/cdbr)=
4e6948cb3fb8a10ba98d1033648b32ca22b7011f44c4f11d95bd9e63be444261

SHA256(6.6/amd64/comp66.tgz)=
2fb513f3033de92f58446e0ed3fafd4084f4352ccc13a6d2cabf4dc5609d9a25

SHA256(6.6/amd64/efi.img)=
11b88c47d9592d42cecc7b5310263c73620329ab6acd319c135b6eab95ca2e02

SHA256(6.6/amd64/etc66.tgz)=
329d5ec5fc149b404b3baaabddd3ad64bbe3d288482c9bd9d37a13207cd14f51

SHA256(6.6/amd64/game66.tgz)=
40d74031baf4922ff46bd4b14b719d89c61853a8ac7f1e79dd399dd046ee38b8

SHA256(6.6/amd64/index.txt)=
8d8cea529491d502b19f331533a3d4dfc769001436ed42518b616c4e5dbcfef1

SHA256(6.6/amd64/kernel66.tgz)=
75ce8cb54faf0f955be9966d66e09febe37b6f4da48cb5ef47712311123e4db4

SHA256(6.6/amd64/man66.tgz)=
be240f257496dd6e7e7822c58c7a0dcc467b3e034057ebc5921901eec4f970ec

SHA256(6.6/amd64/pxeboot)=
58326cc8219ed8059a47fa00211ee4b302f43f15a8cfd1e74d73320cab12d51a

SHA256(6.6/amd64/xbase66.tgz)=
d2e2398c6653f3c16d1d1a967f3fa0031d72a301457f26cccf0b49411d37bd64

SHA256(6.6/amd64/xetc66.tgz)=
9efdfeb7e2254b9bbc3e8c56c34bd3a346a7ab362d813a8a989a91ef58825967

SHA256(6.6/amd64/xfont66.tgz)=
a245d0d6e76c47a5c3403d1701ac821d92527b3dea0ac3fd39c987ccc97fc570

SHA256(6.6/amd64/xshare66.tgz)=
6e0b85d1233f7e79aad7097e41eabe20c7e7bbabed78b84aea02d251a12dead8

SHA512(6.6/amd64/CKSUM)=
20f1f545e9c6c76a3c91f8ef9ee56eed9b69be02f9dbe74085d352fcefa0d5e6047e74cfb5acf4e48d4
83cea12b321951a077796107cdbdd4314c389d8e19a1b

SHA512(6.6/amd64/INSTALL.amd64)=
62026c6ec29279def7d7b2a11c29ff5cd28873747c2efe9a3561aef09e97aff7c0ed6a5d20c380f5582
0fade1420c72e398b2569d4599b070f89de5d4fcbdde1

SHA512(6.6/amd64/RMD160)=
c630d35bda5387230c6f80c54f987756551d3545d141fad41a5e2aabe495ec2eef4902d25479bc8dc
39a5ebda76c9f23e0ea772106b62e2405d45c854c51f4d7

SHA512(6.6/amd64/SHA1)=
0c7cc78b182123de784241b0ba87e8c723041d6240f57f7b69bc24e21ec48b8f22fa2dab07ba66b90
033bfdca64f5bf15d2b9d7b1d4e29ca6455c092430ffccb

SHA512(6.6/amd64/SHA256)=
dd1139762d1fb67bedddf48e49b8169235f36f995bcecfc0369dc321ba475a5b6d9ff484d780808f813
60c7b2e8430ca5031676084eee78068ca6c8f4947bfce

SHA512(6.6/amd64/SHA512)=
c60eb0f5b9bb5037acf357495fb5d92f7356c97a50a5bf4aeeb88a89935100760bf7df75d401f67b05
ed7f00e46c86437abd4484725c6a327896522cb4c50eda

SHA512(6.6/amd64/base66.tgz)=
3d14e65698e63112fb3e97e0f04cd2c20283f5b2309aa1415fdda20e82efdc383adb7011d173575bb
b5878d01cf8e859e12675ce1418991afdc2223699515a2f

SHA512(6.6/amd64/boot.catalog)=
451e55459ad91589c595f06de8fe523878c6ea9b07a75e2a78e0ca50776581615c4fa3e7da73a076f
5b1a38b0e6b029d1498117586f2ba36e605ed13c3eac013

SHA512(6.6/amd64/cd66.iso)=
f90cb477d486ea2ffacc58c0fb9c1e024b8a9838879734d6d60e4da43fb748406e3dbca9511b0088a
a4c1c01815841d50ae988c25731d951dfd1c44f1f1c151d

SHA512(6.6/amd64/cdboot)=
0c3132ba697b724dc3bd3a7dd5590e180c41a016f02b6542efc82f731ae5008eee46500aeaf42235470d30cf1afe86e046f5f30b868e8cc537d3c8e64d515759

SHA512(6.6/amd64/cdbr)=
7a1c20a96abcdad54bdcddd315949907bb7de36f8f09c041cfe78c23dd0f9d9e2498b570cbcaf3d6703a67dfbe2a4fbfa486a754078da93d6b691de11213498d

SHA512(6.6/amd64/comp66.tgz)=
9cfe3cd05cb34e6070edb02d87d3ff28b920f9bca52f438e0074b94b8d1b07af01310c0fe28b5a1d40596f93338993aa67cc9c16d746bb5c1ab15675f70b9be9

SHA512(6.6/amd64/efi.img)=
ac7b55410b147021b0299594bed54af3119a39bb55e4a33b9c33abad871c707569e9e5106f4310b233ea5347e93d672d5c2633aeb8841933852a92021b4cdd85

SHA512(6.6/amd64/etc66.tgz)=
e56c26ebf848dbd51f3aa21c8c29c94a98dffc7a9af90c46d3d4f0d18506c81dd14be490e443299ce7acc0634f48081f512b5ea60caf7fdda1b3b7cece823216

SHA512(6.6/amd64/game66.tgz)=
3c96916b4e6496ebd94529f533b5edafbfaee3c9b107e4c5fcbe9f85385e55f957b5f5d38643e6d6d7c57468e512f3efd73f5532d4c7293a890f5bb1d2d744a0

SHA512(6.6/amd64/index.txt)=
3bdf719553754ef402e973c6c36a214abd79ddf524319e5ff5e8c490eab93ac565278628343e1a4d1026a3f84e2b98da198e543481fbc51693fac3480dd4f4f0

SHA512(6.6/amd64/kernel66.tgz)=
d738584447235a91a658f5e2ace404379875dec0bbae5472ccbd41f4eb356a3ba3fd39b12ab64c68b0058a0f79fee3d63754a4e0f7425ff5a79ea7580ba5ef3f

SHA512(6.6/amd64/man66.tgz)=
eae4c4b6c0fea1e9f68094aea4fd39b417c3ad4a35ae8d34e03de1c7f8afdf991693225e9ffb291f588762daa0b820e39227e33fceabd6c2106eeb747089ef01

SHA512(6.6/amd64/pxeboot)=
238c60836ca008646154bb2f140a4a9b9f98af811554ed4ef42d82252c41d2e197212aa828bafb96ea6dc5f4680aa0101883ba49a9d17c4b913b29779c01c34f

SHA512(6.6/amd64/xbase66.tgz)=
9d02a094a2f5fd82f7512615aa92000681aee8866aa558dfbc83e909b669247bcccab9416683080ecad046c1ac491b0a2900c18c2f7e6c7e06f6056a987d8450

SHA512(6.6/amd64/xetc66.tgz)=
05594c62f21728748d4ddffd1513efe50b1e05800b4c6b0ac556f145b403c9ed7ac39ec6a18c111e0d57c0e5a69abb7b10d57dd5df7914f521866165c722f50c

SHA512(6.6/amd64/xfont66.tgz)=
4b27a457e182ad3315f8e2e1c17f88763fc788552e67f14ead920e3b152a700cdd0bab63694fde0a7f2fe2dda6af755f47ee885fcc6c04bbb20641245039f185

SHA512(6.6/amd64/xshare66.tgz)=
de573240d84d23d9df75070c220f8c09f5891cad488183fe54e91fc82ed83e4e9c15b1c9d66ff9c005c3dfb633370c12635963fe9b9abd1e4c1b3763e71b1d57

Documentation:

SHA256(docs/genugate-1000-admin-de.pdf)=
617c1907b5de31a02c22c8ffc29cacc1ea2559507795d8b163728bb2d23ea0a0

SHA256(docs/genugate-1000-admin-en.pdf)=
cec987e38d102a1c10414647c2d17bfdbf31a8081aedae88a12f28bf9b2fdb54

SHA256(docs/genugate-1000-elk_guide-de.pdf)=
813c20853aafda9ac2c0b5da30bf7f30741e0206a88980d14cc051ff6926f833

SHA256(docs/genugate-1000-elk_guide-en.pdf)=
6510d45b3595fed96796d7582c97b9df048ba15f6e0993dc8fd79b2ccdad128b

SHA256(docs/genugate-1000-install-de.pdf)=
e497ab88a5eee0cc58678449e75a32476b6837773593124dae3def11dc97b1b8

SHA256(docs/genugate-1000-install-en.pdf)=
e61c7faf67086ffa8f41aa4b94ec37bf015d0041546fec9e8608fe4e15de1fdd

SHA256(docs/genugate-1000-relnote-de.pdf)=
3d53d3dcde9306b6bee39e4761aefdb19f6faf74f9b386d76a79c77290aa7d61

SHA256(docs/genugate-1000-relnote-en.pdf)=
31d292ead4a009781d63f0e7a50703a96b5204c839dd8c68c0c4804807a5b2bf

SHA256(docs/genugate-1000-vs-diode-de.pdf)=
234b76ca00b5a34851399b7a9ceb429ece04539e0a0b47bd446463a0f2559848

SHA256(docs/openbsd.tgz)=
fba601195844e3bdbb1908a5e2f5061ede5367e0d4b709d288cc6d689509f4c7

SHA256(docs/openbsd.zip)=
49bec7b47be88441e3cd123478285bc7eff999b9bb7a794a9fdbaf268860409d

SHA512(docs/genugate-1000-admin-de.pdf)=
69a18472cef6e446a6c87eafcee812f01ff55a3cbab2a0b66c771f4280b2cb6141ab25f8efb1b142bdd
faa38bc839acaab56985e271a9a362aebfb81b098eaa8

SHA512(docs/genugate-1000-admin-en.pdf)=
7310b608a760bc67600f4306b77ff489fb3efdd9f0548a2f4a14aba5593a9cb418ff7704865a27d0949
b9a0a576292f09a8236aee992fd2407221044b7b76233

SHA512(docs/genugate-1000-elk_guide-de.pdf)=
c0f6566dc06f25ec5fafb433f32f2778d3da5a43bc03ba1481c10ac3cb524dd77ba623461cc5470c4a
2b2b4a4ebcf60739791e4edb05541e454d13e9f71140f9

SHA512(docs/genugate-1000-elk_guide-en.pdf)=
134b2945c786fc904c887453b3bbf5b350e57bc09c0bfb1e43e68193b5994b85d31f72f1d2187c43d
bb20f7740e8be115a81b2f419a2347b2fdb0f9693a4e2f3

SHA512(docs/genugate-1000-install-de.pdf)=
b6980ad247b6c3f1a39bd33e93d805fcff462e7092e74e4fd3aa7d4e7e23d9e7610cb51499016eaf5
6238f1a1a47bc8eecd5b18da3806897bfb659669a7a7ccb

SHA512(docs/genugate-1000-install-en.pdf)=
926a56c8fd5ccd63dc6bb630aecd9765dcf51e5250a0e73d2730870b1ef2133dc68eea7ddc1d1d38
84de99a318d97bfa42bebbef7e56f7473ec81838a832aa7d

SHA512(docs/genugate-1000-relnote-de.pdf)=
c98b275e431dd06928c9c7127e4c558f07b75098b4ea3aed8d9e6fb056f100dd05e3e7cbb368641a
a46f69affb4cda6a37ce1e34017e8fac62779d187e55199b

SHA512(docs/genugate-1000-relnote-en.pdf)=
e1faa522e315cdfeb312948fcf9b80b1fb0a829ec777483ec0f4cb046f147b299e1c865fc7795b471ee
6b60f183aa65782acbb40ec5260ea611a7e31a4165e50

SHA512(docs/genugate-1000-vs-diode-de.pdf)=
ec5ff16b64e5f78922546e4ace694c9fa93a83bea5a73eb914767a84caf43341bf328460a159bddeef
1396fced8bb5d06a33e06647149d718ff3db657d0bc604

SHA512(docs/openbsd.tgz)=
4e0cc6260d68ec88d7bf8fede0f8b59411eba8fc2c1c67dee04a3c735ae6fc17cde240a60b1f370ad6
8f25afc54cfb39b90e9259d0459553c5ee380a8eba2cc6

SHA512(docs/openbsd.zip)=
c55b43bce261ee1131f0397dc7c7c36804318ce0cf74ad882eb675ed0a42cc91e40b881e506c8acd
4f1572a927803692f5c57b96695d1c8e666b8b1ecceb13e0

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 [6] 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 [6], chapter 4.2.

5. Architectural Information

The TOE genugate 10.0 Firewall Software is part of a larger product, the firewall genugate 10.0 Z which consists of hardware and software. The TOE genugate 10.0 Firewall Software itself is part of the shipped software. The operating system is a modified OpenBSD.

genugate 10.0 Z is a combination of an application level gateway (ALG) and a packet filter (PFL), which are implemented on two different systems. It is thus a two-tiered firewall. The network connection between ALG and PFL is a cross cable.

Besides the network interface to the PFL, the ALG has (at least) three more interfaces to connect to the external network, the administration network and the demilitarized zone network (a 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.

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

To mitigate hardware failures the genugate has a high availability option where two or more genugate systems are operating in parallel and take over a failing system.

The TOE, genugate 10.0 Firewall Software, consists of the software that implements the IP traffic control and related functionality of the firewall. This includes the proxies, the modified OpenBSD kernel modules IP-stack, packet filter, but also other supportive functionality as logging of security events.

The TOE has a special maintenance mode. During normal operation IP packets are handled as usual and the file system is secured by the BSD flags. In maintenance mode, however, the BSD flags can be altered. In this mode all IP packets are dropped for security reasons.

Both ALG and PFL run on Intel compatible hardware that works in 64 bit mode (architecture x86_64). As the product genugate 10.0 Z is a combination of hardware and software, the hardware components are selected by genua. The end user has no need to check for compatibility. The TOE is located as software distributed on installation images. The installation images can either be shipped with the hardware, or can be downloaded from the genua support server. Both an USB install image or an ISO-image are available for installation. The documentation is contained in the install images but can also be downloaded from the genua support server. The TOE is contained in the install image for the product genugate 10.0 Z.

The physical connections are:

- the network interfaces to the external, internal, administration networks and the DMZ,
- connections for the keyboard, monitor, and serial interfaces at the ALG and PFL,
- power supply.

The genugate product includes the following security features:

- The TOE supports IPv4 and IPv6. However, the mcastudprelay supports only IPv4. The internal HA synchronisation network must use IPv4 addresses.
- The ALG does not perform IP forwarding but uses socket splicing for TCP connections and UDP datagrams when appropriate. The connection setup is handled in user space, where information flow control policies are enforced. If the TCP-connections/UDP datagrams pass the control checks, the sockets are set to a “fast” mode where no data is copied to user space and back. This mode should not be confused with IP forwarding, where the IP packets are copied between the networks. The socket splicing reconstructs the whole TCP stream/the UDP contents before sending the data.
- The modified OpenBSD kernel performs extra spoofing checks. The source and destination address of the IP packet are checked against the IP address (and netmask) of the receiving interface.
- The modified OpenBSD kernel logs events that occur while checking incoming IP packets and keeps statistic for other events.
- The filter rules of the PFL cannot be modified during normal operation, except the badip list.
- Proxies that accept connections from the connected networks run in a restricted runtime environment.
- All central processes of the ALG are controlled by the process master that monitors the system and keep it running. In case of strange behaviour the process master can take actions.
- The log files are analysed online and the administrators are notified about security relevant events.
- The log files are intelligently rotated so that they avoid filling the available space but the administrator still can see recent log entries and all events of the process master and the online analysis. There are two classes of log files, the rotated and the flagged. The log files are rotated automatically, based on size and time. The flagged log files are only rotated in maintenance mode with the acknowledgement of the administrator.

- File configuration of the system flags prohibit the deletion of the most important log messages.
- The internal network is protected by a two-tiers security architecture that filter on different levels of the network stack (ALG and PFL).
- The SSH relay intercepts SSH connections, can filter selected SSH protocol messages and can authenticate users. The cryptographic operations of the relay are not part of the certification.
- A patch installation mechanism that installs patches signed by genua. The mechanism also checks that the patch is for the appropriate software version and patch level. The public key for the signature verification is contained in the installation images and part of the secure installation process. During operation it is secured by the self-protection measures.

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 overall test concept is based on periodically running automatic tests in the product specific test environment. They are supplemented by unit tests that are executed directly on a test server, and some manual tests. Additionally to these developer tests there were separate tests performed by the QA (quality assurance) lab. The QA lab is an independent test department inside the company. The QS lab is involved prior to every release and has to approve by its positive testing result. The automatic tests are run on a regular base.

The developer testing environment includes genugate hardware of different hardware revisions. The regular tests are not necessarily performed on the hardware that is in scope of the certification because the commercial product is designed to run on a wider range of hardware than than the one in scope of the certification. Therefore, not all test cases are relevant for the scope of this certificate. The evaluator tests however focused on the HW that is included in the certified configuration. For the certification relevant tests it was ensured that the hardware dependent tests run on hardware revisions in scope of the certification.

The automatic developer tests are executable scripts (Perl or Shell). Integrated in their program code all scripts compare their real result with the expected ones.

The Security Target specifies fifteen assumptions about the environment of the TOE: Assumptions A.PHYSEC, A.NOEVIL, A.ADMIN, A.LOCAL, A.REST, A.SINGEN, A.POLICY, A.TIMESTMP, A.HANET, A.USER, A.TRUSTK, A.TRUSTU, A.LEGACY, A.REMOTE_AUTH and A.OSPF. A.PHYSEC, A.POLICY, A.NOEVIL and A.REST are not relevant for the design of the test environment. A.ADMIN, A.USER, A.HANET, A.SINGEN, A.LEGACY, A.REMOTE_AUTH and A.OSPF are reflected in the test environment. A.LOCAL is fulfilled by the knowledge of the developers. A.TIMESTMP, A.TRUSTK and

A.TRUSTU are given in all TOE configurations because of the properties of the environment.

Using the test scripts the developer automatically ensured that the entrance conditions and the dependencies between tests were considered.

Complete coverage was achieved for all the TOE security functions. 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.

A selected subset from the test scripts provided by the developer have been successfully repeated by the evaluation facility. The achieved test results matched the expected results as documented by the developer in the developer test documentation.

For the test activities performed by the evaluators, the following systems have been used: genugate S Revision 3.0 and genugate S Revision 2.0, genugate M Revision 3.0 and genugate M Revision 2.0, genugate L Revision 3.0 and genugate L Revision 2.0. Those systems are covered by the certificate.

The systems of revision 3.0 were used in HA- and CARP-cluster configurations. The systems of revision 2.0 were tested in stand-alone configuration. According to the Security Target the evaluator has installed the genugates in a separate network. The evaluator has configured the ALG with four physical interfaces (external network, admin network, HA network, internal network to the PFL) and one virtual interface (DMZ). The PFL was configured with two interfaces (internal network to the ALG, internal network). In HA-configuration (OSPF-HA) the connection to the internal network was realised with an OSPF router. The administrative network, the DMZ and the external network were realised with a switch. The HA network was also realised with a switch. Required systems (several servers/clients using Kali Linux) were connected with the TOE and with the corresponding switches.

The configuration is consistent with the configuration that is described in the Security Target. The coverage of the assumptions is as described above for the developer testing.

The testing of the ITSEF was performed in 2 phases. Phase 1: first iteration with a TOE pre-release, and Phase 2: repeating and completing tests with the final TOE version (TOE Build 606a767ffd v10.0-RC3, the TOE identification is performed as described in chapter 2 of this report). An additional focus of phase 2 was the data flow control, auditing, the self protection mechanism, IPv6 and patch installation.

The repeating of the developer testing was done at the developer site to use the test configuration and tools there.

The evaluator has performed a structured vulnerability analysis. For the vulnerability assessment additional analysis steps were performed. The evaluator performed an identification of possible vulnerabilities and to diminish their exploitation. The analysis showed that none of the identified theoretical vulnerabilities in the intended environment of the TOE and under consideration of the given assumptions is exploitable. For all identified vulnerabilities no attack could be identified. Moreover the evaluator has continued searching for vulnerabilities especially during the preparation and realisation of its own testing, including but not limited to obvious vulnerabilities searches (port scan, vulnerability check, etc). The penetration testing was performed directly after installation as well as after activating services.

The vulnerability analysis including the penetration testing of the evaluators have shown that there are no exploitable vulnerabilities found in the assumed environment and the given attack potential.

8. Evaluated Configuration

The TOE has to be configured, and is limited to the restrictions, as stated in the Security Target [6] and Guidance [8, 9]. 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 [10].

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, ALC_PAM.1, AVA_VAN.5 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-1039-2017, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on extensions and enhancements of TOE functions, on an newly defined assurance requirement, and on a new vulnerability analysis.

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 ASE_TSS.2, ALC_FLR.2, ALC_PAM.1, AVA_VAN.5

ST [6] Annex A “Evaluation Methodology for ALC_PAM” defines the methodology for the extended assurance component ALC_PAM.1. It is not formally bound to an ongoing ISO project of the same intent but an approach that is individual to this certificate in order to provide a certificate without the need to wait for a conclusion of the ISO activities. Action element ALC_PAM.1.1E includes 18 work units regarding 15 content elements. Additionally, there are two implied evaluator actions defined regarding two developer action elements ALC_PAM.1.2D and ALC_PAM.1.3D. They result in seven additional work units for the evaluator.

For the developer action elements ALC_PAM.1.2D and ALC_PAM.1.3D there is additional methodology provided that is to be used to measure the conformance.

Since the two developer action elements ALC_PAM.1.2D and ALC_PAM.1.3D address actions that are to be performed in the future, their fulfilment is not relevant within the scope of this certificate. Nevertheless the related work units ALC_PAM.1-19 – ALC_PAM.1-25 have been used to collect general evidence to show there are appropriate processes in place within the developer's development environment.

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.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
1	Patch Management, Integrity	SHA-512 (default)	[FIPS PUB 180-4]	N/A	N/A
2	Patch Management, Integrity	SHA-384 (alternative)	[FIPS PUB 180-4]	N/A	N/A
3	Patch Management, Integrity	SHA-256 (alternative)	[FIPS PUB 180-4]	N/A	N/A
4	Patch Management, Authentication	RSA using RSASSA-PKCS1-v1_5	[PKCS#1, v2.1]	|k| = 4096	N/A

Table 3: TOE cryptographic functionality

Reference details for table 3:

***[FIPS PUB 180-4]**: NIST. Secure Hash Standard (SHS). Federal Information Processing Standards 180-4, U.S. Department of Commerce / National Institute of Standards and Technology, August 2015. doi:10.6028/NIST.FIPS.180-4*

***[PKCS#1, v2.1]**: J. Jonsson and B. Kaliski. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. RFC 3447, Internet Engineering Task Force, February 2003. http://www.ietf.org/rfc/rfc3447.txt*

For all applicable entries of cryptographic algorithms listed in the table above, the Security Level provided is greater than 100 bit.

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

The Security Target [6] chapter 1.4.5 claims SFRs with cryptographic operations only for the patch management. Excluded from the evaluation are especially the following cryptographic operations of the overall product:

- Although some relays support encryption with TLS, this security target does not contain SFRs for the class FCS (Cryptographic Support). Therefore such cryptographic operations are not part of the TSF.
- The cryptographic operations of the SSH relay. This security target does not contain SFRs for the class FCS (Cryptographic Support). Therefore such cryptographic operations are not part of the TSF.
- The cryptographic operations of the IPsec in the HA network. This security target does not contain SFRs for the class FCS (Cryptographic Support). Therefore such cryptographic operations are not part of the TSF.

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 genugate Installationshandbuch and genugate Administrationshandbuch [8. 9] and to follow all requirements to the environment described in the Security Target [6].

External authentication servers are subject to the same organizational and physical policies as the product genugate.

Plausibility of the information about existing bootinstall scripts have to be checked by an administrator each time before booting genugate.

The administrator should activate logging/accounting for services (relays) and regularly check (recommended: daily) these logs for service (relay) abuse (e.g. in case of DoS attack).

The administrative interface used by administrators and revisors must only be available from the dedicated administrative interface.

The assumptions to the IT environment in the Security Target suppose that the TOE operates in a physically secure environment which prevents access from unauthorised users (OE.PHYSEC). This assumption includes the protection of the hardware and PFL USB stick. USB stick has to be protected against theft, exchange and manipulation and it has to be made sure that the PFL will be only be booted with the assigned USB-memory-stick (A.POLICY).

Configuration backup files have to be kept logically and physically secure, so has the TOE including its hardware.

Administration of the TOE should only be performed by personnel which possesses solid knowledge about networking, packet filter firewalls and secure use of public key procedures.

There should be regularly performed inspections (revisions) of the TOE configuration, especially of the packet filter rules. During those revisions the procedures to import public keys should be examined, too.

Finally, please note that the product is designed to run on multiple other hardware versions and revisions to maintain a wide usability, however, the evaluation and certificate concentrated on the latest HW versions and revisions that are mentioned in chapter 2.

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

12.1. 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

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-1154-2021, genugate firewall 10.0 Security Target, Version 10.0.9(db2b731), 26.03.2021

[7] Evaluation Technical Report BSI-DSZ-CC-01154 for genugate firewall 10.0, Version 2, Date 11.06.2021, secuvera Gmbh (confidential document)

[8] genugate 10.0 Z Installationshandbuch, Version 10.0 Z Patch 000, Ausgabe März 2021, Revision v10.0-RC3

[9] genugate 10.0 Z Administrationshandbuch, Version 10.0 Z Patch 000, Ausgabe März 2021, Revision v10.0-RC3

[10] Archiv von Konfigurationslisten, 1154-ALC_CMS-RC3-20210331.tgz, Date 31.03.2021 (confidential document)

[7] specifically

- 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 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