Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1039-2017

for

genugate 9.0 Firewall Software

from

genua gmbh

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1039-2017 (*)

Firewall

genugate 9.0 Firewall Software

from genua gmbh

PP Conformance: None

Functionality: Product specific Security Target
Common Criteria Part 2 extended

Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by ALC_FLR.2, ASE_TSS.2 and AVA_VAN.5

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, 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 4

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, 29 December 2017

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

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

This page is intentionally left blank.

Contents

This page is intentionally left blank.

A. Certification

1. Preliminary Remarks

Under the BSIG1 Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

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

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

[3] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- 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.sogisportal.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 components above EAL 4 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: http://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 of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

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 9.0 Firewall Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0890-2013. Specific results from the evaluation process BSI-DSZ-CC-0890-2013 were re-used.

The evaluation of the product genugate 9.0 Firewall Software was conducted by secuvera GmbH. The evaluation was completed on 21 December 2017. 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 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 maximum validity of the certificate has been limited. The certificate issued on 29 December 2017 is valid until 28 December 2022. 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 9.0 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 9.0 Firewall Software which is part of a larger product, the firewall genugate 9.0 Z patch level 2, which consists of hardware and software. The TOE genugate 9.0 Firewall Software itself is part of the shipped software. The operating system is a modified OpenBSD.

genugate 9.0 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 secure server 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 entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.2, ASE_TSS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. 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

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 9.0 Firewall Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	genugate S, Revision 1.0 and 2.0 genugate M, Revision 1.0 and 2.0 genugate L, Revision 1.0 and 2.0 K130 infodas server, Revision 1.0	N/A	Hardware
2	SW	genugate firewall	9.0	Install image (CD-ROM and USB Install Stick)
3	SW	genugate platform	9.0 Z patch level 2 (Release Date 21.11.2017)	Install image (CD-ROM and USB Install Stick)
4	DOC	genugate Installationshandbuch, Version 9.0 Z, Ausgabe November 2017, Revision gg.90.D021 genugate 9.0 Z, genugate Administrations-handbuch, Ausgabe November 2017, Revision gg.90.D022	9.0 Z patch level 2 (Release Date 21.11.2017)	Manual (German version) (also delivered on CD-ROM and USB Install Stick)
5	HW	PFL USB Stick	N/A	Hardware

Table 2: Deliverables of the TOE

To make sure the genugate CD-ROM or USB Install Stick originates from genua and has not been manipulated during delivery process, an identification of the installation packages can be done. Therefore SHA-256 and SHA-512 checksums are provided on the genua-webserver under the following URL:

https://www.genua.de/support/downloads/checksummen/genugate/90-z.html

SHA256

d8964c01bb3ca96eb489b639d2b0b805eb8ba9b82487ca0e8df416a2b8aee096 /5.9/amd64/base59.tgz

73f8bc42b9f42f8c0d1893fc74ae915cd4463aa71bea05ca741d2aa2273b1c09 /5.9/amd64/boot.catalog

7431f312c2aaa06115f58e971aea5f77d6c0832722b9792b32663ea7c4f60edd /5.9/amd64/cd59.iso

93f3ea2ea935cbf55ed7f34500e50bc1ac65d1d8c26c18d7d66e5df41e5d92ab /5.9/amd64/cdboot

14a35f24acdacf78947eeee576683cce3e28647adc1c59d94491690f3d344e53 /5.9/amd64/cdbr

7c13c68b535cd9edb5da15948ac62c24bba68775e2aa5b861bbbb16e73537a4e /5.9/amd64/CKSUM

4f10f3dc0f97d270b8e32ad41023458a2cb2f79f7cc83a4123b3ff15d981be5d /5.9/amd64/comp59.tgz

cb8ff3b95df7e8a5b5d3b660a0099c81712c23a80d1c657e63c509af3f9ce3cc /5.9/amd64/etc59.tgz

f9bc8b9276b9dd4832649c1bf3769f00854d5a3b96aea0f3cd221faacc3dbd3a /5.9/amd64/game59.tgz

03885d79c6b5ebada12d3f1155cbc38afe6f005412cfe355eb203ad88504d14d /5.9/amd64/index.txt

87f05764ad0f411f6f85ff471ef9f72a5a9050c29e0bdfda5ec334eb06380005 /5.9/amd64/INSTALL.amd64

622a751e873ba0a032e79c4a4f2368a37ba876a1777e8889830fe07cc75c8aa7 /5.9/amd64/man59.tgz

aa111081ef7f33c14954935e23decf3020291457ffd2f91c900cd85bab8a351a /5.9/amd64/pxeboot

c2b9eab711a20b2778fa47d51cfb52131d5ab3dc7af11e824103caaa8116d257 /5.9/amd64/RMD160

411a4482ed041950aad5ed9bb22b84ffa6ebbf96c6fa24fdfaf4145dc132824a /5.9/amd64/SHA1

5247aa5ab4f3997c1ea57e93f48fe47c6c3663fe0924d68662aaa33b5d50c5ea /5.9/amd64/SHA256

dd9edeb3b81e3c622aa9922e494500b103d7ac62d55cc9ab10f13a1e3fe82cc6 /5.9/amd64/SHA512

6fe040d99d3d65b650d1d3b47e03210ed7bb08f474c94eca7c6bedf5f3679f46 /5.9/amd64/xbase59.tgz

2dcda5988aa3f4ee2347d6197991db798dcf7cef78eecea48c09704692386e82 /5.9/amd64/xetc59.tgz

a603ac60a089b37f3d2162a96e3644d42666fdbfc187d2877daaab8306b124ca /5.9/amd64/xfont59.tgz

7401f88cc391a01ff903c089d768c59e56a2cf71f5144c778d64aec4f2aa59f9 /5.9/amd64/xshare59.tgz

e70e2f08a14eeea25c647bef84fab87448b9898d8d565c60376b21b074408fe6 /docs/genugate-900-admin-de.pdf

2ba43eef72d7588364d2f58b5ed08af208a7a684e48ced6bcb03a7a7cbb41e64 /docs/genugate-900-admin-en.pdf

5546eb16a2f2f3e08a248ecb11d98d160bd827f94f79166d0029267516457751 /docs/genugate-900-install-de.pdf

9f5356a6d7fe4892582d77a1534132149948b0aa325ec4cf5bdafa8cc751e5ef /docs/genugate-900-install-en.pdf

SHA512

57d45b88c053cf9dc6e606f436d343469ab767947e267ba8833a2b4e832aa58c938a8456c229073b494a342ef089cd5659e7084d7af4ec5a7ac95bf2287dddf4 /5.9/amd64/base59.tgz

934003acd5158e48db0c990eb7054a8e0c2aac6d523af5788400a6aaf944c8de972d334797d422514844b91e94525db62edff9c192a0d55f3ee1a1c05b4007f0 /5.9/amd64/boot.catalog

7075e5bb874555be48d9e6f0ad9791f3ea76ea67b17807d4ea623bb8c58813895ac56b9aca106a32341564ddf571203a17e8f496765e6cc3c4536cc9b783c339 /5.9/amd64/cd59.iso

9b7abd0911d571b55fc758af56a343486a817916dd0780d2a97daf4033ee4d5de141142721821f65ca88edc57a99f772c29a6372067fc48ec17d38c6f7475650 /5.9/amd64/cdboot

3c8976b4a6176331b40f931267d971a8603aca097ce1177ec589f8c730911066ea076cf359af827a53a0e674f951e480a38db77b9f0cd50224bd407546091185 /5.9/amd64/cdbr

e006349ac86e9ab29857d5110c9898336583260c1c275d5320269e7e5da84edd3a745f00df9b037a2dbcdf580a3accb395eafa12aebbe0f477a220bd60682710 /5.9/amd64/CKSUM

d7099199a69a139909a5a40f39b63942ebf35e278c364a6b340ccba89b6fdf45b43a9bc72727fbe7e7f992cf37115e878a3854148a76dd83bdf705d29774e5c2 /5.9/amd64/comp59.tgz

228a474757269bce00982376a380f141a79c53d7c034a620e1bba7e84c79a4154b450174ec04ef8925f62ef41686bb93838c027177befe791b7a81739231508a /5.9/amd64/etc59.tgz

8c6e4437dc7be2c7f47e0dabe2263bc652dc49015a350a9d65d61d38a01e14602299b7ef8985976c1add11df8ec81deaae6c693a9ed39b57c9b7cc05cc2481db /5.9/amd64/game59.tgz

55a168d5d1a688b4f7c5ad895326a046eb72048dd52065c143c0b4ba63c9bd4d9c75582eb0b164996dd11e16581e902ea6f2b6c4e7f81c737e95a0a964ea2e0e /5.9/amd64/index.txt

bce86f211a0437e5dc097197f68119a20b95e14d1eff1f7bcb4bc4263d938994749735039c51b3d8eceab94048
25f82a6d2210cac1ae05b893bf37d9baa56836 /5.9/amd64/INSTALL.amd64

6149ccb866564b1bdb5194cc9954909e961a4cd8cf499e2dfcaa167d98996c3f735fa6ea6c711cbe515c9e3da
ad6cb594c3acf73636f9b67980a8b31d2482579 /5.9/amd64/man59.tgz

fea0f7595a56a27a2b004d12cada2ca6a0afc589682068ec07ed7e1d149b890eeb690cd341111462372fa8296
3fff8bbbbed42a5ac48b16f4a63eaf24ea641c6 /5.9/amd64/pxeboot

a50399b9616ccb6019b5507bd0eb1239aa34d4d6c7cc2e203561e2f58737a7d012a1f2ebbfa0471640b26c71
4f51b49c7bb89fc282d4bef15d47ca8ad6dee06d /5.9/amd64/RMD160

28b615f5d30c2900babf040c0b1f920110c36fe1b5f03266183abfdde90246ff46d03a900d9bca61d650f8284d5
cad6e60789fc6fb461192aad9164aac7a749a /5.9/amd64/SHA1

70f856f0e384b424445885a25e50a90fa07045142a5557f08d56932849220e123b9301a9b6fcb4fa38518b3bdf
a3d61b53753d6b813f70acaf112d1628b3c985 /5.9/amd64/SHA256

57e8bc03a1019a67b7dd8f67ce2edc04380e70ec43e3428a5f91dd7cda0ff89b7876c393312bc31de7aa1c2d9
5e2265047c3ac324ec95ecc50d1b31ad9fc9fae /5.9/amd64/SHA512

eb9d83147a7bcb04c98fdd432ba3955833af84449de8a3b4799bb4a26e2e9e78889caa17723548a4add82abd
df65f669bb96a9425242caf47ddf3dc9bf1b8532 /5.9/amd64/xbase59.tgz

7569481affdbc2ac5ce6397603348c160099d08e9e35628726336730f3251763dac67c316100a7e8f6e0339af
d3745eda1ecf82fd8f97720e712596caf983370 /5.9/amd64/xetc59.tgz

1b44b1b295fd651dc66aa204032053a1edc6753a31198e0b290f0fcb35f9f16c7ec0e1a4107336bebe02af0ca6
37a7e537b0fe062d83045c76a7cde546deb551 /5.9/amd64/xfont59.tgz

43ae515e62be502edd7541605c67ad8f6e88511aafe6e255fd290287c78a95cc85f2d681dc1b6a45f1e46fa7be
7ebbfbbef17e99cfe3df1a80ef9c535d7e5c40 /5.9/amd64/xshare59.tgz

7b366b113812e44de89cff8c53c07d518a62ff72b677e3be7d4f7df3c6b01859f6be7370debb2d1ef7fa48ab464
47eb2fd494cdfde25c5acd124f31f2a9226b0 /docs/genugate-900-admin-de.pdf

eadd6d465cafdb61758c6ef71fdabd5631ee2e6b3f8cacaad2c58884eebc717e0c20a3e4416e09a6437f6b034f
6789dbc9128d83b19aab5c33b0ab9afa1d9afb /docs/genugate-900-admin-en.pdf

fa346217ea05bf4872fd78f1ca38b54552c418bf387990aab5c536c8ea1c3b41c0c7ddafd75ebab534d064da18
c01aacbbf1aa37b0f93845dd81c82b8ca70f72 /docs/genugate-900-install-de.pdf

669142a4acfec31ceff6df481bb04be2356682010b3c7d6d7bb7bebf4e265c07413073b915158bf22db7f727a8
499141813ba17e6c55a49845bed17d70d17863 /docs/genugate-900-install-en.pdf

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, 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 9.0 Firewall Software is part of a larger product, the firewall genugate 9.0 Z patch level 2, which consists of hardware and software. The TOE ggenugate 9.0

Firewall Software itself is part of the shipped software. The operating system is a modified OpenBSD.

genugate 9.0 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 secure server 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 9.0 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 for maintenance operation. In this mode all IP packets are dropped for security reasons.

Both ALG and PFL run on Intel compatible hardware that works with OpenBSD. As the product genugate 9.0 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 on CD-ROM or USB Install Stick.

The physical connections are:

- the network interfaces to the external, internal, secure server, administration networks, and high availability network,
- 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 mcastudp relay supports only IPv4. The HA network must use IPv4 addresses.
- The ALG does not perform IP forwarding but uses socket splicing for TCP connections when appropriate. The connection setup is handled in user space, where information flow control policies are enforced. If the TCP-connection passes 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 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 all 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 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 for maintenance operation. In this mode all IP packets are dropped for security reasons.
- 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 different systems synchronize their configuration with one another. The CARP setup can operate in two modes, failover and balancing. A certified setup can only use the failover mode.

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 systems used in the evaluator tests are: gg9s (genugate S Revision 1.0 (first iteration) and genugate S Revision 2.0 (second iteration), gg9m (genugate M Revision 1.0 (first iteration) and genugate M Revision 2.0 (second iteration), gg9l (genugate L Revision 1.0 (first iteration) and genugate L Revision 2.0 (second iteration)) and ggk (K130 infodas server, Revision 1.0).

The systems gg9s, gg9m and gg9l were used in HA- and CARP-cluster configurations. ggk was tested in standalone configuration.

Additionally a genucard (OSPF-Router) and two versions (D006 and D022) of the TOE were provided by the developer.

According to the Security Target the evaluator has installed the genugates in a separate network. The evaluator has configured the ALG with 4 physical interfaces (external network, admin network, HA network, internal network to the PFL) and 1 virtual interface (DMZ). The PF was configured with 2 interfaces (internal network to the ALG, internal network).

In HA-configuration (OSFP-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 realised with a switch.

Required systems (several servers/clients using Ubuntu Linux) were connected with the TOE and with the corresponding switches.

The configuration is consistent with the configuration in the Security Target.

The Security Target specifies thirteen assumptions about the environment of the TOE: Assumptions A.PHYSEC, A.NOEVIL, A.ADMIN, 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.NOEVIL, A.POLICY and A.USER are not applicable to the test environment. A.ADMIN, A.HANET, A.SINGEN, A.LEGACY, A.SERVER and A.OSPF are given in the test environment. A.TIMESTMP, A.TRUSTK and A.TRUSTU are given in all TOE configurations because of the properties of the environment.

The testing of the ITSEF was performed in 2 phases. Phase 1: first iteration (TOE Change D006) and Phase 2: Repeating and completing tests, second iteration (TOE Change D022).

Testing in the evaluator's premises covers among the complex installation all security functions. The main focus was the data flow control, auditing, the self protection mechanism and IPv6.

Testing included the repeating of the developer tests in their particular environment and was therefore done at the developer test lab.

The evaluator has done a structured vulnerability analysis based (AVA_VAN). For the vulnerability assessment additional analysis steps were performed. In the evaluation the evaluator has worked towards to identify vulnerabilities and to eliminate them as exploitable. The analysis shows that none of the identified vulnerabilities in the intended environment of the TOE and under consideration of the given assumptions is exploitable. For all identified vulnerabilities no attack with respect to the given security target can 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 vulnerabiltities searches (portscan, vulnerability check, etc). The penetration testing was performed direct after installation as well as after activating services.

For this product the border between functional and penetration testing is overlapping because the product contains a lot of self protection functions.

The vulnerability analysis including the penetration testing of the evaluators have shown that there are none exploitable vulnerabilities in the assumed environment and the given attack potential, i.e. AVA_VAN.5.

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.

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 ALC_FLR.2, ASE_TSS.2 and 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-0890-2013, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on extensions and enhancements of TOE functions 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 conformant
  EAL 4 augmented by ALC_FLR.2, ASE_TSS.2 and AVA_VAN.5

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

9.2. Results of cryptographic assessment

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

10. Obligations and Notes for the Usage of the TOE

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

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

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

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].

During installation administrators have to follow rules for password complexity. For each password change password complexity rules have to be followed. Additionally, the customer is advised to define an organizational password complexity policy (A.POLICY).

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 logical and physical secure as the TOE including the hardware.

Administration of the TOE should only performed by personnel which dispose about 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 also the procedures to import public keys should be examined.

Finally, please note that the TOE may also run on old legacy hardware genugate 200, genugate 400, genugate 600 and genugate 800 but that configuration is not part of the certificate. Relevant are the HW models and revision mentioned in table 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. Definitions

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
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
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
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
OSPF	Open Shortest Path First
Perl	Practical Extraction and Reporting Language
PF	Packet Filter (component of OpenBSD)
PFL	Packet Filter (component of genugate)
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
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
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 4, Sept. 2012
Part 2: Security functional components, Revision 4, Sept. 2012
Part 3: Security assurance components, Revision 4, Sept. 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, Sept. 2012
http://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-1039-2017, genugate firewall 9.0 Security Target, Version 6, 13.12.2017

[7] Evaluation Technical Report BSI-DSZ-CC-01039 for genugate firewall 9.0, Version 1, Date 15.12.2017, secuvera Gmbh (confidential document)

[8] genugate Installationshandbuch, Version 9.0 Z, Ausgabe November 2017, Revision gg.90.D021

[9] genugate 9.0 Z, genugate Administrations-Handbuch, Ausgabe November 2017, Revision gg.90.D022

[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)

This page is intentionally left blank.

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 10.4
- 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 11
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16
- 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 http://www.commoncriteriaportal.org/cc/

This page is intentionally left blank.

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report