Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0890-2013

for

genugate firewall 8.0

from

genua mbh

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-0890-2013

Firewall

genugate firewall 8.0

from	genua mbh
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

Common Criteria
Recognition
Arrangement
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 advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

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, 17 December 2013

For the Federal Office for Information Security

SOGIS
IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

Bernd Kowalski
Head of Department

L.S.

SOGIS Recognition
Agreement
for components up
to EAL 4

This page is intentionally left blank.

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.

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

Contents

A Certification....................7

1 Specifications of the Certification Procedure....................7
2 Recognition Agreements....................7
3 Performance of Evaluation and Certification....................8
4 Validity of the Certification Result....................9
5 Publication....................9

B Certification Results....................11

1 Executive Summary....................12
2 Identification of the TOE....................13
3 Security Policy....................16
4 Assumptions and Clarification of Scope....................16
5 Architectural Information....................17
6 Documentation....................18
7 IT Product Testing....................18
8 Evaluated Configuration....................21
9 Results of the Evaluation....................21
10 Obligations and Notes for the Usage of the TOE....................22
11 Security Target....................22
12 Definitions....................23
13 Bibliography....................25

C Excerpts from the Criteria....................27

CC Part 1:....................27
CC Part 3:....................28

D Annexes....................37

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 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.

2.1 European Recognition of ITSEC/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 technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

[4] 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

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

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

This evaluation contains the components ALC_FLR.2, ASE_TSS.2 and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL4 components of these assurance families are relevant.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. 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 nations listed above.

This evaluation contains the components ALC_FLR.2, ASE_TSS.2 and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

3 Performance of Evaluation and Certification

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

The product genugate firewall 8.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0718-2012. Specific results from the evaluation process BSI-DSZ-CC-0718-2012 were re-used.

The evaluation of the product genugate firewall 8.0 was conducted by secuvera GmbH. The evaluation was completed on 10 December 2013. secuvera GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

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

The product was developed by: genua mbh.

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

[6] Information Technology Security Evaluation Facility

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only 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 levels please refer to the excerpts from the criteria at the end of the Certification 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-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 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.

5 Publication

The product genugate firewall 8.0 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[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] genua mbh
Domagkstr. 7
85551 Kirchheim
Deutschland

This page is intentionally left blank.

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 Firewall 8.0 which is part of a larger product, the firewall genugate 8.0 Z (Patchlevel 0), which consists of hardware and software. The TOE genugate Firewall 8.0 itself is part of the shipped software. The operating system is a modified OpenBSD.

genugate 8.0 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. 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. They are selected from Common Criteria Part 2 and some of them are newly defined. 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 Functionality

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 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 firewall 8.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	genugate 400 revision 6 and 7, genugate 600 revision 6 and 7, genugate 800 revision 6 and 7, genugate 200 revision 6 and 7, with a fourth network interface, Infodas Server Typ II	N/A	Hardware
2	SW	genugate Firewall	8.0	CD-ROM
3	SW	genugate Platform	8.0 Z Patchlevel 0	CD-ROM
4	DOC	genugate Installationshandbuch, Version 8.0 Z, Oktober 2013 [8] genugate Administrationshandbuch, Version 8.0 Z, Oktober 2013 [9] GUI Referenz, Version 8.0 Z, Oktober 2013 [10]	8.0 Z Patchlevel 0	Manual and CD-ROM
5	HW	USB Stick	N/A	

Table 2: Deliverables of the TOE

To make sure the genugate CD-ROM 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 and below in this report:

http://www.genua.de/customer/gg_support/checksums/cs_800z.html

The valid checksums of the TOE are:

SHA256 (5.2/i386/CKSUM) = 396c93de5023a4224069c8aa924b28323a5fd8dce85d1bf6eec39b64fd3fc4f1

SHA256 (5.2/i386/INSTALL.i386) = d80c590da61551c2d60c809468729b531a3f92e797a850bf798299cf9ef22ab6

SHA256 (5.2/i386/INSTALL.linux) =
93f69dd249b06b35a42ad3aee71483091403dcd324e256c12c955da2a64c5097

SHA256 (5.2/i386/MD5) = e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

SHA256 (5.2/i386/RMD160) =
a6de6a8edbd10c423f5350f3e0d5d65a9895e50a844301a51865237aaa3e3e2b

SHA256 (5.2/i386/SHA1) = da33959c2ea99d96ce9d22a8c622005ce365b3a05bfbe465245668c4466f65e6

SHA256 (5.2/i386/SHA256) = 86fe657b602237e61d68f0c02ffffb888ce8614f36e9b45ed2c48ee4b1b26e90

SHA256 (5.2/i386/SHA512) = 7b83f6276f93c1eb049b56757106f92b7b77174d5cfbbeb15814f026e8ab60f0

SHA256 (5.2/i386/base52.tgz) =
250bf41c817c325255dafa36fa72aad83604620a412dd212e99dfd6e095465a7

SHA256 (5.2/i386/cd52.iso) = e552b88af8c58f0c6bdb60c31817216b7c43ae5531f6f1212a12462c6a345489

SHA256 (5.2/i386/cdboot) = 7f73237a1429e1269af573edff70f70a6369fe53aec340f363f0f6f3de230036

SHA256 (5.2/i386/cdbr) = ec0001636bde74ffd5ffda3bf7eebb9a0d8e2e07772dff73faf9849bf2d3837b

SHA256 (5.2/i386/comp52.tgz) =
0c7080d340b70665564bee14f047b76771f844202160b681455c65483e1a40f1

SHA256 (5.2/i386/etc52.tgz) = c5c4bddcf7e1ec3bffc8b2d1e23c80ef426e18d4c1c62bcc11933c1218956d99

SHA256 (5.2/i386/game52.tgz) =
4d85234b3211a2e72e45728187569b33549d9850436a9a8e541dd75ea7967cb3

SHA256 (5.2/i386/index.txt) = f3110d6d28c08fbdb6797cd1ff9a35d0deb4296b43c0aabf206dd8e59cd5ac48

SHA256 (5.2/i386/man52.tgz) =
4351dadaab419083e1a7cfbd99d9acd26b80a3231701074fb5c7275abcf8f646

SHA256 (5.2/i386/pxeboot) = 1d153c5af96a5430fd1d39a930cde3ca8b356b2eb284847ad8d2dc8787b24588

SHA256 (5.2/i386/xbase52.tgz) =
4db83a5af2d9aca7b321e2642bc10e52a56ffa8364a139ad8e4f931f3821f0ad

SHA256 (5.2/i386/xetc52.tgz) =
58eaa9cd470a1ace2349d50e34e6b6153743a54a7b1fbcd2881a605ed7a3261d

SHA256 (5.2/i386/xfont52.tgz) =
0b9b47b925c14a9a4d5f3f4ce37dbfa2121c02410ab43fcd89beb454b1c57644

SHA256 (5.2/i386/xshare52.tgz) =
a0a543c84e398f652185a2c73a436968b6151efe663f78890fd4510f528bd6bb

SHA512 (5.2/i386/CKSUM) =
d6532dfd392dfe29571ea5a9b8995b7e5403a9eeca1b5c33d6f07a294f563ce3a22371d97f7b11eafc9fd315d3
1f34f7f51965b634379c63d0a5cb84b7f2a896

SHA512 (5.2/i386/INSTALL.i386) =
d6ddd53026959f27ff52f4043beba7d07ae7348b33888374dc1652490534208bc8dcc74e87809e54a53933f33
e25082c72a123df2a8c0cd70b9b2098ba7c4adf

SHA512 (5.2/i386/INSTALL.linux) =
f18c8305551717d056133c4fce2ffa4ea9f3ad6dfc9bfa57216bc081a05b7ea543e14cae9cc80bdf9b2d9b5647f1
fac2b56252a210c61dfc0a005f7698df2e73

SHA512 (5.2/i386/MD5) =
cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d287
7eec2f63b931bd47417a81a538327af927da3e

SHA512 (5.2/i386/RMD160) =
3e1dacdfc5f03ba1cb707460b1d5e43ee264dbd5ef7cf5a149743942d436267e25e27c7f01c89fce18fdb26ed2
aea07ea8c21871ba6a8c340222bb9dcc10022d

SHA512 (5.2/i386/SHA1) =
8fd51b4c1d3401008d8c618b3f1ee609b70942bd222dcccaaaabc422f85ecf375997bfc619d37242a9ae759403
f924e1da7a54c8f96694cee34e8bc48814f729

SHA512 (5.2/i386/SHA256) =
0a50f848d107c3add5a424583af58ce57551d8ad570d7b49ceae5d157058b907b224014705bbf493a862141ef
682f32214193712e07ef38860417d84f6802c83

SHA512 (5.2/i386/SHA512) =
2c9f62f1b712d71c85c8deff0584edf7341066876005ddfd8b32627c595b46e771a66d0c4e059036cbe7008bad
41414a67257421d591b45047e6d1ad5030a144

SHA512 (5.2/i386/base52.tgz) =
9f2deb79d4f635a3f3c3c7bf3cacde26f8a78d73fdd3ae03cfe50481c648f9ffafdd231fbb4f921dcb9767b757097
8003a3ac664ca401fd041884458c5360c4c

SHA512 (5.2/i386/cd52.iso) =
38f8b3ee7bc9c91565b81b0db67fcf8a722597ecac143f40387b898bb131f4ceab1ba83390cf45fb0a075289d0
67af4fe31708b99f3dabdf4044c6c3ff89bc51

SHA512 (5.2/i386/cdboot) =
3eae6b56fb653f2a107b775589776de5c6d219559e09bed51f4ed84f018bdd47af02f2757c66ad6c5a0f175640
b698a9c1413ef676b180a53aa95fd21d8f0fc7

SHA512 (5.2/i386/cdbr) =
43b0dd7da99846b582c11871f21d2991a8b8717f8a983495e82ac40141c542a59d11fb43749bf9558046d59c5
6f1794b393240b2102874ec89839d5bdccd42b3

SHA512 (5.2/i386/comp52.tgz) =
f436b7b3669cfd771cc850008d569ca886b9f431e4e4b20317f19b0b25ae8a8c9d073bd1105963a908869764e
79ff6cad67653ca76de1e70a3b85808b09f9fbf

SHA512 (5.2/i386/etc52.tgz) =
e5d894aef3cd0bba7b7c0e3adef4054ca4264f8c654413fc0c31dce56a20b1ef020f7aec3e9964e7e64160c600
ea5494ef8150759dde9f336df7ea1ac4feca79

SHA512 (5.2/i386/game52.tgz) =
fc7d6a1b380b8e6f994eadc3b62037b75cc818f7722574ffe1297e046754764d29697bfd08b1d444dc5f47a3cc
885f4f3b07d0487998eae0cc4370d926521129

SHA512 (5.2/i386/index.txt) =
8b6f08787a05d38dadb4711a2b30b6cef86f7612d60b113f88a1480c603d6df661ce028a908682c303c6cb43f9
9343e627c8f7f938e8fa881e0f0a60a6f17149

SHA512 (5.2/i386/man52.tgz) =
776528d90bba7cce7e9b04a386e7117c05cdc9e99731faeea2580b431aa1ac780794533cc1837b0468f3ede9
d7eb5187802478a2caa4c9b92b096e085143e8ec

SHA512 (5.2/i386/pxeboot) =
caf7cfc75245cccc14dff8692ef23ce225c3117b62185be5534f333100999c3a4ba3cf18976d32a80c15bb51726f
60a94bd6df91cba41760c6102ff0f6f0e2dc

SHA512 (5.2/i386/xbase52.tgz) =
4c566114a531d44fc47b9aa29c8020688de16741eb32ca2297ed243c65626f43a8ef125f4ccd0337ab7ca599a
a47e673035c39f6e98b2f64e18978866a846b28

SHA512 (5.2/i386/xetc52.tgz) =
f299f76c68f154a2dbad064c3a6ba39dc3f9c60af3137716c18c4aef061429ddca0aaf8778f74f6357323f72fabe
2ecfb55c06539227ff37dec59b15f4f6a327

SHA512 (5.2/i386/xfont52.tgz) =
a855520c914a12892a0e08b0936ed89cee6462dda5b7ede69c10db2a4b3c774843d5f07bf0e5bf15da508189
c1a412b4fd858eaa2dcd4a741617d133c7b489de

SHA512 (5.2/i386/xshare52.tgz) =
ed79488de031ab0684bc25e5640a8f39e9605eedcfed428246975a27869145b658eaf8a217deb88b3d588694
129c317ce70886922e7b84c56c6b228751d7a449

SHA256 (docs/genugate-800-admin-de.pdf) =
232c3ee6417593c25a4bbab3edad5836e8619e6268a6458eb03db2a8d162548f

SHA256 (docs/genugate-800-admin-en.pdf) =
0b5f2080db235aa0a00466e64ffb87b6aaebd445ecfe743ae98c477579857a55

SHA256 (docs/genugate-800-guiref-de.pdf) =
526310283d9f32d8106be1ba78e481e51b464931169e663b5be45c659fc1ccf1

SHA256 (docs/genugate-800-guiref-en.pdf) =
311e10cd36c3184b51dcddfb39e08b4020bed3c2f7dbeabb667d551e9ec31052

SHA256 (docs/genugate-800-install-de.pdf) =
0964a41990832768b5a999724be21656953404d20d6aaa1b2a1a6afd08b6af46

SHA256 (docs/genugate-800-install-en.pdf) =
e3f8ca21d5b1fc6dfac839a82317613e6fcd10ec901a2b93c8260ebf8b1b19c2

SHA256 (docs/genugate-800-relnote-de.pdf) =
2b9ad3c636686308d4afdd64b307e61ca473c373d23cc18ec9ef5fd355229f52

SHA256 (docs/genugate-800-relnote-en.pdf) =
e5c20e0523e3e60f499db923650c9d7c8eb9c5846b4e51db36f1ddcd8e85c153

SHA512 (docs/genugate-800-admin-de.pdf) =
be570513635e89e605cf4b3d84bb5443084ade3d9f21ef9487047f67531c41a86a0c66b74270ae3aa71a85315
c5523a8e696d317588247b9bf2bd571a69720f2

SHA512 (docs/genugate-800-admin-en.pdf) =
62f1c17cd6b16eae2105130f08d51cc030469ac74cc9a80a01e705e24492fb83937891f6c2b5bef1e76c59cd52
e8bbbf9012ca29e0695808a9da83f763ba0844

SHA512 (docs/genugate-800-guiref-de.pdf) =
36465d1f132bfe0379463f8a5f0f54a6bd716cd98bae6f1e2ac02c7c300dec4b6f2d4b8969cb64ad60fd8009f92
d985756e001c73b5bae6362e680c3e3aa8860

SHA512 (docs/genugate-800-guiref-en.pdf) =
5a1e362f832cda3a0f288452350004d42bc57878ede7c6777520406693e27ab95a1868ab856f67081f9715215
fd7a1601b4dc4e7b7e9af623420c582cd5bb5d4

SHA512 (docs/genugate-800-install-de.pdf) =
d8df729d46d26007ee571d9db376302b59cf5eba88cb6d43271c9f497012c03d2994acd0bb406b4bc434436f3
13116fc4fc9f29801a65fed0e4b341e8d5ffe9d

SHA512 (docs/genugate-800-install-en.pdf) =
1b7b2591cfa073aff91fa01b6113b18890a0bda52f5382a951bc7ff1da237a1f20e9d60e0a296b0a5fb94926ca5f
5972f5d5b375bb94c6c1ce5bb54a35ce1fe0

SHA512 (docs/genugate-800-relnote-de.pdf) =
2e4a60070f4902a422310106a6fdcfafa7810f11c5723451404ef16d4aec81119c84250fb350d3b2975d6dc1a01
d9cd93b01052ba9318d277bef6b9823c0cc0d

SHA512 (docs/genugate-800-relnote-en.pdf) =
782cf10e69c52e930468dee993140b104c91bd0421227194fec4db6565159262e1a0cb98d6ce2a1629265f09
d7d16f243b8f685f611d3a040c0e7af8d54ff99c

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 Firewall 8.0 is part of a larger product, the firewall genugate 8.0 Z (Patchlevel 0), which consists of hardware and software. The TOE genugate Firewall 8.0 itself is part of the shipped software. The operating system is a modified OpenBSD.

genugate 8.0 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. 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 Firewall 8.0, 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 8.0 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 the CD-ROM.

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.

genugate product family includes the following security features:

- The TOE supports IPv4 and IPv6 However, the relay sip-pair (not part of the TOE) supports only IPv4. The HA network must use IPv4 addresses. The HTTP relay can only be used with 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.
- 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 rotated 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

Developer Tests

The test configuration in the genua laboratory includes four systems installed with the TOE. These are the systems genugate Version 800, genugate Version 400, genugate Version 600 and genugate Version 200. For those tests which need a DMZ (Secure Server Network) the DMZ is located as an alias on a consisting interface card. These are tested on single systems as well as HA-configurations.

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.SERVER 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.

For the most part the tests are automatically running under control of the tool aegis. The tool also provides automatic test results. The test procedures are executable scripts (Perl or Shell).

The developer provides his tests, i.e. the scripts in a directory. They are independent tests which are put into the context of the execution of other tests. Thus dependencies among tests are demonstrated.

Every tests includes comments. Tests of the type auto (most of the tests) are started with an aegis-test driver. Integrated in their program code, all scripts compare the real result with the expected one. The output is the status value PASS (if the real result is equal the expected one), FAIL (if the real result is not equal the expected one), NORESULT (problems occur during runtime e.g. cable break) or ABORT. The detail of the script protocol can be adjusted. Test of the type manual needs manual interventions, which is documented in the description of the script.

Using the test scripts the developer automatically ensures for the most tests that the pre-conditions and the dependencies between tests are considered.

Additionally the developer run tests in the QA (quality assurance) lab. The QA lab is an independent test department inside the company. The QA lab is completely separated from the developer test environment. The QA lab consists of physical and virtual genugate systems. These tests are divided in automatic and manual tests. The automatic tests run on a regular base. For testing HA and CARP there are two separated 3-machine-HA-clusters. In the QA lab IPv4 and IPv6 is tested.

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

A selected subset of the test scripts provided by the developer have been successfully repeated by the evaluation facility. The achieved test results matched the expected results.

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

Independent Evaluator Tests

These are the systems used in the evaluator tests: genugate Version 200 Revision 6, genugate Version 400 Revision 7, genugate Version 600 Revision 6, genugate Version 800 Revision 7 and Infodas Server Typ II. For those tests which need a DMZ (Secure Server Network) the DMZ is located as an alias on an existing interface card using VLAN.

The systems genugate Version 200 Revision 6, genugate Version 400 Revision 7 and genugate Version 600 Revision 6 were used in HA- and CARP-cluster configurations. kk.gg and ll.gg had been tested in standalone configuration.

Additionally a genuscreen 100 C (OSPF-Router) and several versions 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.

The required ystems of the environment (several servers/clients using Ubuntu Linux, Debian Linux and Windows 7) were connected with the TOE (partly by the OSPF router) 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.SERVER 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: Initial testing and Phase 2: Repeating and completing tests.

Testing in the own premises cover all security functions. The main focus was the data flow control, auditing, the self protection mechanism, IPv6 and vulnerability assessment.

The repeating of the developer testing was done in the evaluation facility. The developer provided a development and test server which was given to the evaluator for the period of evaluation. The evaluator was able to run the tests without the developer.

The analysis of the vulnerabilities show that none of the identified potential vulnerabilities in the intended environment of the TOE is exploitable. For all identified potential vulnerabilities no attack with respect to the given security target can be identified.

The evaluator has continued searching for vulnerabilities especially during the preparation and realisation of his own testing. At the beginning penetration against obvious vulnerabiltities were provided (portscan, vulnerability check etc). This was done with an own tool from secuvera (Tajanas). This tool implements nmap and OpenVAS. This testing was performed directly after installation as well as after activating services.

To outline further penetration tests the evaluator has done a structured vulnerability analysis. Therefore the ITSEF has performed tests with high communication load to exercise self-protection functions and test auditing functions. Furthermore testing was provided using the system console of the ALG (this interface is usually not available to an attacker). This tests invoke negative influence to important components (especially terminate processes), trying to suspend security functions.

For this evaluation the border between functional and penetration testing was merging because the product contains a lot of self protection functions.

Penetration testing of the evaluators has 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, 10]. The security requirements for a network defined in both documents are to be met. The TOE has to be configured following the TOE guidance.

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 EAL5 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-0718-2012, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on minor 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 cryptoalgorithms. 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 for 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.

In addition, the following aspects need to be fulfilled when using the TOE:

For a secure operation it is necessary to follow all recommendations of the "genugate Installationshandbuch" [8], "genugate Administrationshandbuch" [9] and "GUI Referenz" [10] and to follow all requirements to the environment described in the Security Target.

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 USB-stick with the PFL configuration. USB stick has to be protected against theft, exchange and manipulation and it has to be made sure that the PFL will be only booted with the assigned USB-memory-stick. This aspect has to be considered in a defined security policy (A.POLICY).

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

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

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

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).

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

There should be regular 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.

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.

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

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.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

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 - A set of software, firmware and/or hardware possibly accompanied by guidance.

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, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0890-2013, genugate firewall 8.0, Version 5, 09.10.2013, genua mbH

[7] Evaluation Technical Report BSI-DSZ-CC-0890 for genugate firewall 8.0, Version 3, Date 12.11.2013, secuvera Gmbh (formerly Tele-Consulting GmbH), (confidential document)

[8] Guidance documentation: Genugate Installationshandbuch, Version 8.0 Z, Ausgabe Oktober 2013

[9] Guidance documentation: genugate 8.0 Z, genugate Administrationshandbuch, Ausgabe Oktober 2013

[10] Guidance documentation: genugate 8.0 Z, GUI Referenz, Ausgabe Oktober 2013

[8] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	Assurance Components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.