Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0718-2012

for

GeNUGate Firewall 7.0

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-0718-2012

Firewall

GeNUGate Firewall 7.0

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 January 2012
For the Federal Office for Information Security

Joachim Weber
Head of Division

L.S.

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL 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

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.

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.

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 7.0 has undergone the certification procedure at BSI.

The evaluation of the product GeNUGate Firewall 7.0 was conducted by Tele-Consulting security | networking | training GmbH. The evaluation was completed on 16.12.2011. The Tele-Consulting security | networking | training GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the 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.

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

[6] Information Technology Security Evaluation Facility

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

5 Publication

The product GeNUGate Firewall 7.0 has been included in the BSI list of the 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

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 TOE GeNUGate Firewall 7.0 is part of a larger product, the firewall GeNUGate 7.0 Z (Patchlevel 007), which consists of hardware and software. The TOE GeNUGate Firewall 7.0 itself is part of the shipped software. The operating system is a modified OpenBSD.

GeNUGate 7.0 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 high availability (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 Functionalities:

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.

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

- Internal network: This is the network that has to be secured against attacks form the external network. Usually only a few services from the internal network are accessible from the external network, secured by user authentication. This is the network that is secured by both the ALG and the PFL, using filtering mechanisms at two different levels of the IP stack. This network is usually controlled by a defined security policy.
- External network: This is the most insecure network, e. g. the internet. In general, no security policy exists, and all kind of attacks can occur in this network.
- Administration network: This network is used to allow a secure administration of the TOE. This network is isolated from all other networks and only administrators have access. The usual access is through the HTTPS web interface, but an SSH and TELNET access for debugging and maintenance operation is also available.
- Secure server network: This network allows access to common services for the external network, without the need to open the internal network. Usually, Web- and FTP-servers are installed in this network. This network is usually controlled by a defined security policy.
- HA network: This network is necessary for the high availability option. It is used to synchronize the configuration between the systems.

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 Firewall 7.0

The TOE (software, guidance) is shipped as part of a larger product, the firewall GeNUGate 7.0 Z (Patchlevel 007), together with the OpenBSD platform and the required hardware. The following table outlines the deliverables of the GeNUGate 7.0 Z (Patchlevel 007):

No	Type	Identifier	Release	Form of Delivery
1	HW	GeNUGate 400, 600, 800 or 200 with four network interfaces	N/A	Hardware
2	SW	GeNUGate Firewall	7.0	CD-ROM
3	SW	GeNUGate Platform	7.0 Z Patchlevel 7[8]	CD-ROM

No	Type	Identifier	Release	Form of Delivery
4	DOC	DK GeNUGate Installations- und Konfigurationshandbuch, Version 7.0 Z, Revision build. gg.70.D039, November 2011	70.D039	Manual and CD-ROM
5	HW	USB Stick	N/A	

Table 2: Deliverables of the GeNUGate 7.0 Z (Patchlevel 007)

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-1, SHA-256 and SHA-512 checksums are provided on the GeNUA-server under the following URL:

http://www.genua.de/customer/gg_support/checksums/cs_700z.html

The valid checksums of the TOE are:

Installationspakete in dem Verzeichnis 4.6/i386

```
SHA1 (INSTALL.i386) = 3c9864aaff075d794cda3fa85d25e9c80ef78ef6
SHA1 (INSTALL.linux) = e967fe03cc4f2e30cf8702313e2eb2652cc0442d
SHA1 (MD5) = da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA1 (base46.tgz) = 27ca3ae79912bd07839f9158209fe99a054a8883
SHA1 (cd46.iso) = 5966f16c149dc3c561edf9679bd642ffdd680c73
SHA1 (cdboot) = 1d30b388ddc676046205b617f71cb2a6df3fa710
SHA1 (cdbr) = 95a33103112e839ec7db20e1293a65b7f5863ae0
SHA1 (comp46.tgz) = 66df506a999aff9a3067962547279952f6c32b31
SHA1 (etc46.tgz) = e473677b915a747144fe4f59a0464d90c1bd4ff0
SHA1 (game46.tgz) = a7eb0ab21974ea9a9f796a610d92bebe82656172
SHA1 (man46.tgz) = 3797594bbd7b1c8c02ca5484f61b86132e2abde9
SHA1 (misc46.tgz) = d5b4a26b131a3a6af9f65cdbd2790617e613dab9
SHA1 (pxeboot) = 81bd352a8c26cb9bcbf56a50eeee094f6ac749c0
SHA1 (xbase46.tgz) = bd04b87995c9c20e745349c5d32ba2f21fade7ab
SHA1 (xetc46.tgz) = 5419f6d230168995f7ac98f3839afa2b54d93010
SHA1 (xshare46.tgz) = 3628c89c7e2bf83fea172650c49e0f25e0732aad
```

```
SHA256 (INSTALL.i386) =
168dbca270ebae1f36949c0c9ed42cda3c26f9d437640e22939bf2b2a7e9c0ca
SHA256 (INSTALL.linux) =
a2c3f50602b04127f87efcf395370504a58ab132ca4e0201b0d65fca3157ff27
SHA256 (MD5) =
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA256 (base46.tgz) =
009f4eef78a3ca97d05cd6cb6e52d7ee89b0d8c9b78393d3aa3b1865a27f6704
SHA256 (cd46.iso) =
e7ccc77b260fdeed4e04bed40527b005369d39dcd71eb76a5ad512383ec90ec4
SHA256 (cdboot) =
4ce5c25b55e334fab43bead90c3698ead636d90fafce2b2c0958d5693df25817
SHA256 (cdbr) =
49a542b18e88a729b6e361da0d92a7784e4f6fcad87bf03540befd2d583e1081
```

[8] The ALG displays the version GeNUGate Version 7.0 Z 007 (70.D037), the PFL the version GeNUGate Version 7.0 Z 006 (70.D036)

```
SHA256 (comp46.tgz) =
48ea6f41cbd79afc22eeb50dd3755bd20086c8111cc4dbc5b1951729cc4e1b80
SHA256 (etc46.tgz) =
12e05e95628c35bf733c21bf8122f8ad6d8f0cd91877e2f24110e38e65014455
SHA256 (game46.tgz) =
d4241aff249557a9a7d13357142f32bf75ad4ba31d90d76050e712c3ba27480e
SHA256 (man46.tgz) =
383c028b5fd78c25f95f3cfbdb7b46fe17fce1ad7e302b8ee55879a263202ef3
SHA256 (misc46.tgz) =
a732cb77b0c039cdad31613d8cdf0a29231e25b8542921c11ec27b036de31792
SHA256 (pxeboot) =
61fa41a40a1376ebf4a5fa4fbe1574c48ec20bb7e5eab7477020aa1fdf948e89
SHA256 (xbase46.tgz) =
d165cda7db4d60febee9947ff3d5a63a93a2970353e9f309086ae1e74b15080b
SHA256 (xetc46.tgz) =
f3c30942eb56b23e9f2b5a6edd5931782b8f15a2f9b922b1bf4280873813e1ea
SHA256 (xshare46.tgz) =
8fe72ddc8c3130238d6ca24d973791293ff8e94305c90876d3e93bfb83358450

SHA512 (INSTALL.i386) =
eee6f5cc575947c6dfa3614459ba1db5af6361669593cc89b8e06dbd53056762dd21c1a3cb
e98350d0a8b4c73fda459d61ab6394ffec5866e608e06f60d443be
SHA512 (INSTALL.linux) =
b5fce93b01787509d0d0e6c1331a008988e7a8ff5ca00c0bbe1e5d4fef42ac2093ef5b88200
0a2f4e9a5d66a0855e746361b80ea235815cb5a807cd5e464699a
SHA512 (MD5) =
cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d
85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e
SHA512 (base46.tgz) =
7767019a1acfde6039f59d58f3e5eda5382ab34ebe02d9a49e38bd346a598e653c04cc86cc
fad2d9fb31e314daef0b1f9fea79b108da877ad17b2c0eea065e3e
SHA512 (cd46.iso) =
f20b2a958b5df56ec1fb8e97b389ad0a8e28ec5fa6c24b60f26dc554dc15a12b5e9ad21a6e2
a53ffbd0c29f1fbf93d44e2acaf3b0870ea4f9699f90c28289e26
SHA512 (cdboot) =
2d106732d58397a00a5d948d535e642ed73751b866f7c6bea1eadbc3534da2f92707daa03
21b2424ad870264887004665db2d6184e310d281f1859526cdcbde3
SHA512 (cdbr) =
56c3c8ed44ecc5e66c973c9ea6487bf734b656df9241a84712b41ab943448c2e4a5766beac
7b50ac4bd4e138e1e5a23d09b2f4e2285a5ad961848559e213533a
SHA512 (comp46.tgz) =
f4bcc939d53fa1142e0a16dd2825fa8cd26e35fc24cb3c4a5d5ffeff314f1f193e66446d83b421
aaed3d5a454cc5ecc367e464dc6411be51219c2f3d8e6e4dfe
SHA512 (etc46.tgz) =
5c70562d34758f61b906bf0538eab4f094ba3b14ee0a88b683d4db7118283985fecb0abc8a
3b9aad5c4075a1012279031f7536bead2fa5f9c32a4efa101364ac
SHA512 (game46.tgz) =
e5f0726ce8dbab29cf77116c15f470a0c1611f2a830064c7b7a144217eec85a06569e65f0c1
2ebb693798b8677c1159eb90b9dc160c73907be265f617f48d2d8
SHA512 (man46.tgz) =
6a424918aaeb0a303171e3caf605bf763f19b362c2ac012f0cdff5a153d05e3ba771b2aeb8f3
```

dc414f35acabed9f078e7ec242762508c7c234aa406c9cb8eb74
SHA512 (misc46.tgz) =
817e4fd84cd56d5948d1a520bbb30e99d1352e10f5d9ae14fa7ab37b78e6346a6a2626f277
b8e6741fac4c26dc6c200f061d124eb2e0520e65a3bec8fe17f78d
SHA512 (pxeboot) =
79f6cd3ac1ca62fb1a1a59bfa5f76fb41b8d5e1bc0e111f748ecb5fabedfab20b47a28e063ffc5
c049836b0a17870d2c78e2143818624aae2985a56d32ac25a6
SHA512 (xbase46.tgz) =
b5501cee840c275631356af7b3e2c226e807deecef496927c0ee3642525b6024e59900bd1
b6317b1c400ce32a48cc69aa449831f2c7282987d0bdab68ba66836
SHA512 (xetc46.tgz) =
84bde67618a50f204e04e83d043c20f0c1cefe53aad9256f65f67f1092f366606ab329429bea
1292e663f438d97a8e5658171513c8600825b816e07260b01907
SHA512 (xshare46.tgz) =
de6f1d1fe42fa7ab4dc840ddcfbcb51822f2806209e8767c67a2fd01e8d9eaf7e4abcda1d920
dc6b3504ce24c4d43f73897f8134c66bcd8697e2e60ecacad9dc

SHA1 (manual-de.pdf) = b84c1937e23d45db2cf55a0f0cf386ba540cbebf

SHA256 (manual-de.pdf) =
aae30a6692057569476826e050a2ef7271f1fa53d15f722d682583429d7c6372

SHA512 (manual-de.pdf) =
803c3e0aee72e7f4e9a221eab1a902a38a05f0f9eac025e882ef11bcad9a411d51b5f13d5ac
65eb163915e8a57b9196e18f8d506f98c1dbf0832d17504b4eeda

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Security audit: The TOE generates log data whenever important events occur. The log data is analysed by automated tools that look for pattern in the log data. The log data can be transformed into a human readable form and can be searched by all administrators and auditors
- Data flow control: The packet filter at the ALG and PFL implement the flow control at the network layer (IP) and transport layer (TCP/UDP). The filter rules take the information from the IP and TCP/UDP Header (where applicable) in order to apply the filter rules.
- Identification and Authentication:
  - All IP packets are identified at the network layer by their source and destination IP addresses (and ports if applicable).
  - For the TELNET-, FTP-relays a compulsory user authentication at the TOE can be configured by the administrator. For the SMTP-relay an optional user authentication at the TOE can be configured by the administrator.
  - The side channel authentication allows users to activate configurable TCP-relays after a successful authentication at the side channel web site.
  - Administration is only possible after successful authentication at the administration web server. Auditors (administrators with read-only rights) can view the configuration after successful authentication at the administration web server. Connections to the administration webserver are only accepted from the administration network.

- To gain interactive access (shell access) to the console, the administrator has to authenticate.

  All of the different authentication methods disable a user/administrator account after a configurable number of unsuccessful attempts.

- Security management: The security management can be divided into three different roles: normal users do not have any rights, auditors (administrators with read-only rights) can view the configuration, and (normal) administrators can change the configuration.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- Those responsible for the TOE must assure that the TOE is placed at a secured place where only authorised people have access.
- Those responsible for the TOE must assure that all administrators and auditors are competent, regularly trained and execute the administration in a responsible way.
- Those responsible for the TOE must assure that administration is only done in the physically secured administration network during normal operation mode.
- Those responsible for the TOE must assure that the TOE is the only connection between the different networks.
- Those responsible for the TOE must assure that the security policy for the internal network allows only administrators access to the network components and the network configuration. They must assure that the policy is maintained.
- The IT-environment must supply reliable time stamps for the TOE.
- The IT-environment must supply a real-time clock.
- The IT-environment must supply a physical network for transfer of TSF data between nodes for the optional high availability setup.
- Those responsible for the TOE must assure that the users follow the user guidance, especially that they choose not easily guessable passwords and that they keep them secret.
- The IT-environment must assure that the non-TOE parts of the kernel space do not interfere with the security functions of the TOE.
- The IT-environment must assure that the non-TOE parts of the user space do not interfere with the security functions of the TOE.
- The IT-environment must provide a sufficiently secure environment for the legacy TELNET and FTP protocols (and SMTP if authentication is used).
- The IT-environment must assure that the server for external authentication (RADIUS, LDAP) are located in secure networks.
- The files imported for password file authentication contain good passwords.
- The IT-environment must provide OSPF and OSPFv6 routers that are secured against attacks from the internal network.

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

5 Architectural Information

The TOE GeNUGate Firewall 7.0 is part of a larger product, the firewall GeNUGate 7.0 Z (Patchlevel 7), which consists of hardware and software. The TOE GeNUGate Firewall 7.0 itself is part of the shipped software. The operating system is a modified OpenBSD.

GeNUGate 7.0 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 7.0, 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 7.0 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 configuration option ´Authorize IP´ 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.

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 ggdXXX (GeNUGate model 800), ggdXXY (GeNUGate model 400), ggdXYY (GeNUGate model 600) and ggdYYY (GeNUGate model 200). For those tests which need a DMZ (Secure Server Network) the DMZ is located as an alias on a consisting interface card. They 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 and A.POLICY 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 automatically the test results. The test procedures are executable scripts (Perl or Shell).

The developer provides his tests respectively the scripts in a directory. The scripts relevant for the certification are included in the subdirectory zert. Beside zert there exists 38 additional subdirectories which also contain test scripts. Tests in zert usually contain several single tests. These are independent tests which are put into the context of the execution of other tests. Thus dependencies among tests are demonstrated. More than 640 single tests are provided in zert.

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 result. 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) or NORESULT (problems occur during runtime e.g. cable break). The volume of the script protocol is influenced through the AET_DEBUGLEVEL option. 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 part that the entrance conditions and the dependencies between tests are considered. Therefore the responsibility for the correct testing is transferred to the developer.

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

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

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

Independent Evaluator Tests

The test equipment provided by the developer consists of three GeNUGates (model 400), a GeNUScreen 100 C (OSPF-Router), several switches and several versions of the TOE.

According to the Security Target the evaluator has installed the GeNUGates in a separate administrator network. The evaluator has configured the ALG with 5 interfaces (external network, admin network, HA network, DMZ, internal network to the PFL) and the PFL with 2 interfaces (internal network to the ALG, internal network).

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 endsystems (several servers/clients under ubuntu, laptop under windows, management station with MS Internet Explorer 6.0) were connected with the TOE with the OSPF router respectively 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 and A.POLICY 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: Repeating developer testing and Phase 2: main phase.

Phase 1: The developer testing was repeated in the developer laboratory (18 and 19 May 2011).

Phase 2: The testing was performed with several versions of the TOE. The main phase of testing was performed in March 2011, May 2011 until July 2011, and in November 2011.

Testing in the own premises covers among the complex installation all security functions. The main focus was the data flow control, the self protection mechanism and IPv6. The aim of testing was to detect failure due to the changed presentation of the GUI and the changed environment (OpenBSD).

The repeating of the developer testing was done in the developer laboratory for two reasons: First the developer tests require the developer environment. Second the evaluator uses the chance to become better acquainted with the test methodology of the developer.

The vulnerability analysis shows that none of the identified vulnerabilities in the intended environment of the TOE is exploitable. For all identified vulnerabilities no attack is identified for attack potential “High”.

The evaluator has continued searching for vulnerabilities especially during the preparation and realisation of its own testing. At the beginning penetration tests against “obvious” vulnerabilities were provided (portscan, vulnerability check etc). These were done with an own tool of the ITSEF (Tajanas). Tajanas implements nessus and nmap. The testing was performed direct after installation as well as after activating services.

To outline further penetration tests, the “onion skins model” and self protection functions of the TOE were analysed as starting points. Therefore the ITSEF has provided tests with high communication load to activate self protection functions. Furthermore the system console of the ALG was tested – this interface is not available to an attacker according to the assumptions. These tests exert a negative influence to important components (especially terminate processes), trying to suspend security functions.

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

Penetration testing of the evaluators have shown that there are none exploitable vulnerabilities in the assumed environment for an attacker with the attack potential “High”.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE can be configured in such a way that the security requirements for a network are met. The TOE has to be configured following the TOE guidance.

9 Results of the Evaluation

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.

The evaluation has confirmed:

- 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.

Results of cryptographic assessment

The TOE does not include crypto algorithms. 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 policies 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:

User related Conclusions and Recommendations

For a secure operation it is necessary to follow all recommendations of the “Installations- und Konfigurationshandbuch” [9] and to follow all requirements to the environment described in the Security Target [6].

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. The 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-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.

Administration and revision of the TOE should only be performed by personnel who have 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.

Sidechannel-Authentication

Depending on the environment of the client systems the usage of the sidechannel authentication incur risks. These will be implemented in network environment where IP-addresses can not be unambiguously assigned to users. Therefore Sidechannel-Authentication should only be used, provided that

- Sidechannel-Authentication is not activated on external interfaces.
- If using Sidechannel-Authentication, a security model has to be established.

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

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
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

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.

GeNUGate - The two-tiered (packet filter/application level gateway) firewall from GeNUA.

Informal - Expressed in natural language.

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

PF - The name of the OpenBSD packet filter.

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 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[9].

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

[6] Security Target BSI-DSZ-CC-0718-2012, Version 7, 24 November 2011, GeNUGate Firewall 7.0, GeNUA mbH

[7] Evaluation Technical Report, Version 2, 15 Dezember 2011, Evaluation Technical Report BSI-DSZ-CC-0718 for GeNUGate Firewall 7.0 from GeNUA mbH of Tele-Consulting GmbH, Tele-Consulting GmbH (confidential document)

[8] Configuration list for the TOE:
Konfigurationsliste gg707 (Baseline), 29 November 2011 (confidential document)
Konfigurationsliste “cc.7“ GeNUGate 7.0, 29 November 2011 (confidential document)

[9] Guidance documentation for the TOE, Installations- und Konfigurationshandbuch, Version 7.0 Z, November 2011, Revision: gg. 70.D0039

[9] specifically

- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, 3 September 2009, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)

C Excerpts from the Criteria

CC Part1:

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.