Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0300-2006

for

GeNUGate Firewall 6.0

from

GeNUA
Gesellschaft für Netzwerk- und
UNIX-Administration mbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5455, Infoline +49 (0)3018 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom
Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0300-2006

GeNUGate Firewall 6.0

from

GeNUA
Gesellschaft für Netzwerk- und UNIX-Administration mbH

Common Criteria Arrangement
for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Version 2.3* (ISO/IEC 15408:2005) extended by advice of the Certification Body for components beyond EAL4 for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

Functionality:	**product specific Security Target** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL 4 augmented by** **AVA_VLA.4 and ALC_FLR.2**

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 12. September 2006

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT
Security
Certified

SOGIS - MRA

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.

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

This evaluation contains the component AVA_VLA.4 that is not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4-component 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 6.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-ITSEC-0226-2004. For this evaluation specific results from the evaluation process based on BSI-DSZ-ITSEC-0155 and BSI-DSZ-ITSEC-0226-2004 (the first re-evaluation) were re-used.

The evaluation of the product GeNUGate Firewall 6.0 was conducted by Tele-Consulting GmbH. The Tele-Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

GeNUA
Gesellschaft für Netzwerk- und
UNIX-Administration mbH
Domagkstrasse 7
85551 Kirchheim

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 12. September 2006.

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, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-18.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] GeNUA
Gesellschaft für Netzwerk- und
UNIX-Administration mbH
Domagkstrasse 7
85551 Heimstetten

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.

Contents of the certification results

1 Executive Summary

The TOE GeNUGate Firewall 6.0 is part of a larger product, the firewall GeNUGate 6.0 Z (Patchlevel 11), which consists of hardware and software. The TOE GeNUGate Firewall 6.0 itself is part of the shipped software. The operating system is a modified OpenBSD.

GeNUGate 6.0 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. Both systems are shipped in one case. 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. 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.

The TOE, GeNUGate Firewall 6.0, 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.

The IT product GeNUGate Firewall 6.0 was evaluated by Tele-Consulting GmbH. The evaluation was completed on 24. August 2006. The Tele-Consulting GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

GeNUA
Gesellschaft für Netzwerk- und
UNIX-Administration mbH
Domagkstrasse 7
85551 Heimstetten

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part

[8] Information Technology Security Evaluation Facility

3 for details). The TOE meets the assurance requirements of assurance level EAL 4 (methodically designed, tested, and reviewed) augmented by AVA_VLA.4 and ALC_FLR.2. Table 6 in section 9 of this report shows the assurance components and the evaluation results.The following table shows the augmented assurance components.

Requirement	**Identifier**
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+: AVA_VLA.4	Highly resistant
+: ALC_FLR.2	Flaw reporting procedures

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	**Addressed issue**
FAU	**Security audit**
FAU_ARP.1	Security alarms
FAU_SAA.1	Potential violation analysis
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_STG.2	Guarantees of audit data availability
FAU_STG.4	Prevention of audit data loss
FDP	**User data protection**
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FIA	**Identification and authentication**
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action
FIA_UAU.6	Re-authenticating
FIA_UID.2	User identification before any action
FMT	**Security management**
FMT_MOF.1	Management of security functions behaviour

Security Functional Requirement	Addressed issue
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on security roles
FMT_SMR.3	Assuming roles
FPT	**Protection of the TSF**
FPT_RCV.2	Automated recovery

Table 2: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Addressed issue
FAU	**Security audit**
FAU_GEN.1EX	Audit data generation
FIA	**Identification and authentication**
FIA_UAU.5EX	External authentication mechanisms
FPT	**Protection of the TSF**
FPT_SST.1	TOE testing
FPT_RTE.1	Restricted Runtime Environment

Table 3: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.1.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Addressed issue
FPT	Protection of the TSF
FPT_STM.1	Reliable time stamps

Table 4: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.4.

These Security Functional Requirements are implemented by the TOE Security Functions:

TOE Security Function	Addressed issue
SF_SA	Security audit

TOE Security Function	Addressed issue
SF_DF	Data flow control
SF_IA	Identification and Authentication
SF_SM	Security management
SF_PT	Protection of the TSF

Table 5: Security Functions of the TOE

For more details please refer to the Security Target [6], chapter 6.1.

1.3 Strength of Function

The TOE's strength of functions is claimed high (SOF-high) for specific functions as indicated in the Security Target [6, chapter 8.4].

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The following users are described in the Security Target to give a better understanding of the threats and organisational security policies:

user Any person or software agent sending IP packets to or receiving from the TOE. The assumed attack potential is high. The general term user is used when it does not matter whether the user did authenticate at the TOE or not.

unauthenticated user Any person or software agent sending IP packets to or receiving from the TOE that did not authenticate at the TOE. The assumed attack potential is high. This term is used for users that did not (yet) authenticate at the TOE.

authenticated user Any person or software agent sending IP packets to or receiving from the TOE that authenticated at the TOE. The assumed attack potential is high.

administrator These are authenticated users that have the role of an administrator. This role authorises them to change the TOE configuration. Their assumed attack potential is undefined.

auditor These are authenticated users that have the role of an auditor. This role authorises them to view the TOE configuration. Their assumed attack potential is undefined.

Assets for the TOE are defined as resources in the connected networks and security sensitive data on the TOE.

The Security Target describes four threats for the TOE:

T.NOAUTH An unauthenticated user may attempt to bypass the security functions of the TOE and gain unauthenticated access to resources in other connected networks or read, modify or destroy security sensitive data on the TOE. The attack method is exploiting authentication protocol weaknesses.

T.SPOOF A user may attempt to send spoofed IP packets to the TOE in order to gain unauthorised access to resources in other connected networks. Without spoofing checks the TOE would route a response to the spoofed IP packet into a connected network that the user is not authorised to access.

T.MEDIAT A user may send non-permissible data through the TOE that result in gaining access to resources in other connected networks.

T.SELPRO A user may gain access to the TOE and read, modify or destroy security sensitive data on the TOE, by sending IP packets to the TOE and exploiting a weakness of the protocol used.

Only one Organisational Security Policy is described:

P.AUDIT All users must be accountable for their actions.

1.5 Special configuration requirements

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

- internal network: This is the network that has to be secured against attacks from the external network. Usually only a few services from the internal network are accessible from the external network, secured by user authentication. 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.
- secure server network: This network allows access to common services from 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.

1.6 Assumptions about the operating environment

The following assumptions for the environment are stated in the ST [6, chapter 3.2]:

A.PHYSEC The TOE is physically secure. Only authorised persons have physical access to the TOE.

A.NOEVIL Administrators are non-hostile and follow all administrator guidance; however, they are capable of error. They use passwords that are not easily guessable.

A.ADMIN All administration is done only in the administration network.

A.SINGEN Information can not flow among the internal, external, or secure server network, unless it passes through the TOE.

A.POLICY The security policy of the internal network allows only the administrators access to the network components and the network configuration.

A.TIMESTMP The environment provides reliable timestamps.

1.7 Disclaimers

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 TOE, GeNUGate Firewall 6.0, 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 Target of Evaluation (TOE) is called:

GeNUGate Firewall 6.0

The TOE (software, guidance) is shipped as part of a larger product, the firewall GeNUGate 6.0 Z (Patchlevel 11), together with the OpenBSD platform and the required hardware. The following table outlines the deliverables of the GeNUGate 6.0 Z:

No	Type	Identifier	Release	Form of Delivery
1	HW	GeNUGate 400, 600, 800 or 200 with fourth network interface	N/A	
2	SW	GeNUGate Firewall	6.0	CD-ROM

No	Type	Identifier	Release	Form of Delivery
3	SW	GeNUGate Platform	6.0 Z Patchlevel 11	CD-ROM
4	DOC	Administrator and user guidance manual	6.0 Z	Manual and CD-ROM
5	HW	PFL floppy/USB stick	N/A	

Table 5: Deliverables of the firewall GeNUGate 6.0 Z

To make sure the GeNUGate CD-ROM originates from GeNUA and has not been manipulatet during delivery process, an identification of the installationpackages can be done. Therefore SHA-1 and RIPEMD-160 checksums are provided in chapter 10 of this report and on the GeNUA-server under the following URL:

http://www.genua.de/customer/gg_support/checksums/cs_600z.html

3 Security Policy

The TOE controls the connections and data transfer between different networks, where each network has different security needs and different threat levels for the other networks.

4 Assumptions and Clarification of Scope

For detailed description of the assumptions see chapter 1.5 of this report.

4.1 Usage assumptions

The assumptions A.PHYSEC, A.NOEVIL and A.ADMIN describe the assumed usage of the TOE.

4.2 Environmental assumptions

A.SINGEN, A.POLICY and A.TIMESTMP describe the assumptions about the TOE environment.

5 Architectural Information

Both ALG and PFL run on Intel compatible hardware that works with OpenBSD. As the product GeNUGate 6.0 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 and administration networks
- connections for the keyboard, monitor, and serial interfaces at the ALG and PFL
- power supply

Figure 1 gives a schematic overview on the TOE and its environment. It divides the software on ALG and PFL into user and kernel space parts. On both systems, the user and the kernel space contain part of the TOE, and part of the environment. The following table lists the components in each part. The components for the parts A, B, C and D are part of the TOE. The components for E, F, G, and H are part of the environment.

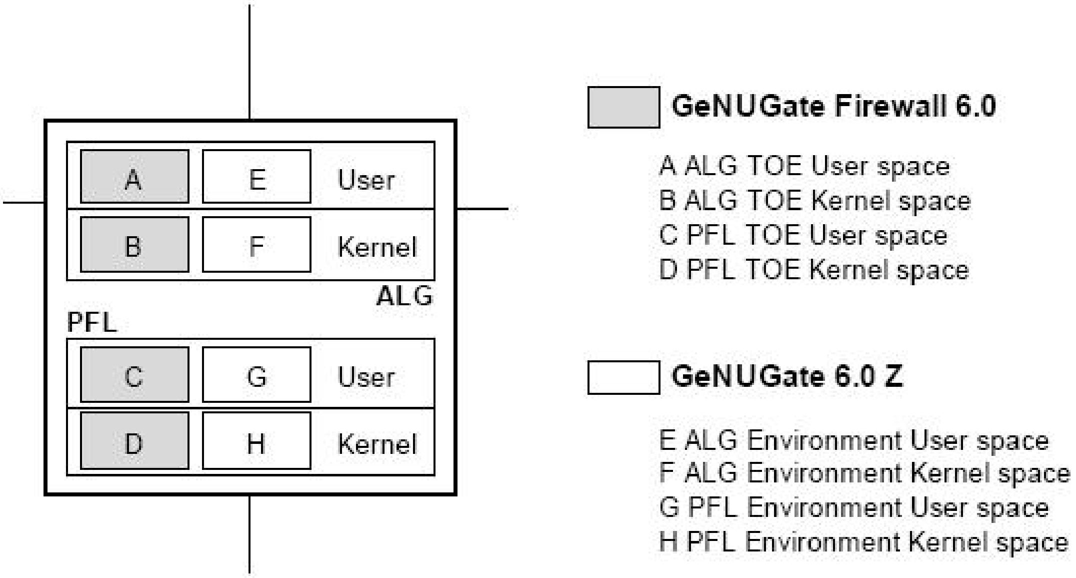

Figure 1: Scope and boundary of the TOE

6 Documentation

Together with the TOE the following documentation is delivered:

“GeNUGate 6.0 Z Installations und Konfigurationshandbuch, August 2006” [8]

This document contains all necessary instructions for correct installation and configuration of the TOE.

7 IT Product Testing

The test platform was set up by the developer according to the ST and all relevant guidance, ensuring that the evaluated configuration as defined in the ST was tested. The developer test scrips (approx. 640 single test scripts, partial automatic, partial manual) were performed successfully on the evaluated configuration of the TOE. 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 high-level 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.

Furthermore, a set of independent penetration tests has been performed successfully by the evaluation facility.

8 Evaluated Configuration

The evaluated configurations were GeNUGate 400, 600, 800 and 200 with fourth network interface as described in the ST.

The developer has tested the TOE software on all available hardware platforms, the evaluator testing was performed on a GeNUGate 400 .

Detailed information about the differences of the single versions of GeNUGate are provided on the GeNUA-server:

http://www.genua.de/dateien/genugate-hardware.pdf

9 Results of the Evaluation

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 identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4, AIS 34]).

The verdicts for the CC, Part 3 assurance components (according to EAL 4 augmented by AVA_VLA.4 and ALC_FLR.2 and the class ASE for the Security Target evaluation) are summarised in the following table:

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS

Assurance classes and components		Verdict
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Subset of the implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Flaw reporting procedures	ALC_FLR.2	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

Table 6: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by AVA_VLA.4 and ALC_FLR.2.
- The following TOE Security Functions fulfil the claimed Strength of Function:
    - **SF_IA.3**: For the TELNET- and FTP-relays a compulsory user authentication at the TOE can be configured by the administrator. The authentication method can be configured and either be password, radius, LDAP, S/Key, or cryptocard. The password can be changed by the users themselves, but a minimum quality is checked by the TOE. The password must be of minimum length 6, must not only contain uppercase- or lowercase letters, and must not contain the user name. The TELNET- and FTP-relay capture the eventual option-negotiation commands sent before the authentication proceeds, and replay them to the destination, if the authentication completes successfully.
    - **SF_IA.4**: The side channel authentication allows users to activate configurable TCP-relays after a successful authentication at the side channel web site. The authentication method can be configured by the administrators and either be password, radius, LDAP, S/Key, or cryptocard. The password can be changed by the users themselves, but a minimum quality is checked by the TOE. The password must be of minimum length 6, must not only contain uppercase- or lowercase letters, and must not contain the user name.
    - **SF_IA.5**: Administration is only possible after successful authentication at the administration web server. Auditors (administrators with read-only rights) can view the configuration after succesful authentication at the administration web server. Connections to the administration webserver are only accepted from the administration network. The authentication method is password. The password can be changed by the respective administrators themselves, but a minimum quality is checked by the TOE. The password must be of minimum length 6, must not only contain uppercase- or lowercase letters, and must not contain the user name.

The results of the evaluation are only applicable to the TOE GeNUGate 6.0 in the evaluated configuration as described in chapter 2 above.

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The operational documents [6] and [8] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

Additional hints are given by the evaluator:

- 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.
- External authentication servers are subject to the same organizational and physical restrictions as the GeNUGate.
- Plausibility of the information about existing bootinstall scripts have to be checked by an administrator each time before booting GeNUGate.

The following SHA-1 and RIPEMD-160 checksums are provided to check the integrity of the delivered CD:

SHA1 (base37.tgz)	= 04ca449dc3665f7aa81fda94db27a8b2517c4401
SHA1 (comp37.tgz)	= bcdb46ee097146503f2a0e475b98be133a27b561
SHA1 (etc37.tgz)	= 1929dce0a7afcafa5f41bbda939e41e85d037ebd
SHA1 (game37.tgz)	= ddd7b90bfc7a3fdffc22990ded844d54af4f2e26
SHA1 (man37.tgz)	= c1f5388126dcb5d1bcc8bd1643303c5278d72747
SHA1 (misc37.tgz)	= 462612d06fb74ea64e0e132e1b6a4685ec87c55a
SHA1 (xbase37.tgz)	= ae9efd1aed3dbad0ae2b60c42d30065fe6107882
SHA1 (xetc37.tgz)	= f4a916d6e65124a47780efdc373ee51851481504
SHA1 (xshare37.tgz)	= ec5716569fd1f6ba10f1b46ded4c932673d95cbc

RMD160 (base37.tgz)	= 5d2c67d4d3dc317312e624d5544087e956461746
RMD160 (comp37.tgz)	= 9d481ac1fa2bc6849465fd2f2803437b7d822703
RMD160 (etc37.tgz)	= e92b0bba596a59c1f9254b2572181e7c68609661
RMD160 (game37.tgz)	= e6391d75cd2aeb6bc84f162895e0700cd3a25217
RMD160 (man37.tgz)	= f9a2b589fef02ab53047a97d84b08a748b8d6b97
RMD160 (misc37.tgz)	= 9f3fee6f7016a898fc06bf073b7df3d5faeb6bed
RMD160 (xbase37.tgz)	= 5c6ef8583e58f00c39055f66f37a37e54210d799
RMD160 (xetc37.tgz)	= d02fbc7bda09fd85d11c66bcf446821466ef11f2
RMD160 (xshare37.tgz)	= 1d3734ae383686e2e6da5cb45dfd3a467980d374

For the documentation the following checksums are provided:

SHA1 (manual-de.pdf)	= 520120eff457a0f0d54ee36bda4b6e281ef9d7cf
RMD160 (manual-de.pdf)	= ffce57ee8a6cefb107a0dcd37ea8fda0c27764eb

11 Annexes

none.

12 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

ALG	Application Level Gateway
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PFL	Packet Filter
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance 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 - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

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

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

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-CC-0300-2006, Version 242, 22.08.2006, GeNUGate Firewall 6.0 Security Target, GeNUA mbH

[7] Evaluation Technical Report, Version 2, 23.08.2006

[8] GeNUGate 6.0 Z Installations- und Konfigurationshandbuch, August 2006, GeNUA mbH

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

a) **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.

b) **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

a) **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

b) **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

a) **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

b) **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

a) **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	**Assurance Family**
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

"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 11.1)

"Table 6 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 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 extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“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 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, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“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 practice. 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 11.5)

“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 practices.

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 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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 11.8)

“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 11.9)

“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.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”