Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0616-2010

for

GeNUGate Firewall 6.3

from

GeNUA mbH

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0616-2010

Firewall

GeNUGate Firewall 6.3

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 4 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, 29 September 2010

For the Federal Office for Information Security

Bernd Kowalski L.S.
Abteilungspräsident

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

for components up to EAL4

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.

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp.E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

[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

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and United Kingdom.

In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

2.2 International Recognition of CC - Certificates

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 January 2009 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 web site: 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.

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 6.3 has undergone the certification procedure at BSI.

The evaluation of the product GeNUGate Firewall 6.3 was conducted by Tele-Consulting security | networking | training GmbH. The evaluation was completed on 24 August 2010. 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.

[6] Information Technology Security Evaluation Facility

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

- 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/shall [Anm.: „shall“ verwenden wenn Auflage zur regelmäßigen Neubewertung erfolgt s.u] apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product GeNUGate Firewall 6.3 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
Domagkstraße 7
85551 Kirchheim

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) GeNUGate Firewall 6.3 is part of a larger product, the firewall GeNUGate 6.3 Z (Patchlevel 007), which consists of hardware and software. The TOE GeNUGate Firewall 6.3 itself is part of the shipped software. The operating system is a modified OpenBSD.

GeNUGate 6.3 Z is a combination of an application level gateway (ALG) and a packet filter (PFL), which are implemented on two different systems. It is thus a two-tiered firewall. The network connection between ALG and PFL is a cross cable.

Besides the network interface to the PFL, the ALG has (at least) three more interfaces to connect to the external network, the administration network and the secure server network. For the high availability option, the ALG needs another network interface for the HA network. The PFL has a second interface which is connected to the internal network.

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

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

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Function	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 Functions

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 Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.3, 3.4 and 3.5.

This certification covers the following configurations of the TOE:

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

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 6.3

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	GeNUGate Firewall	6.3	CD-ROM
2	DOC	GeNUGate Installations- und Konfigurationshandbuch, Version 6.3 Z	63.D043, August 2010	Manual and CD-ROM

Table 2: Deliverables of the TOE

To make sure the GeNUGate CD-ROM originates from GeNUA and has not been manipulated during delivery process, an identification of the installationpackages can be done. Therefore MD5, SHA-1 and RIPEMD-160 checksums are provided on the GeNUA-server under the following URL:

http://www.genua.de/customer/gg_support/checksums/cs_630z.html

The valid checksums of the TOE are:

Installationspakete in dem Verzeichnis 4.4/i386

MD5 (INSTALL.i386) = 506da8fd2ab79095a5c0824909e9864c

MD5 (INSTALL.linux) = 34ab7e52e8b1ed96682349a2f0addcce

MD5 (base44.tgz) = 7ef86235809ad7bf7e458e14c03f01c8

MD5 (cd44.iso) = cce2a234907f83e3a5f925d6cee0c1aa

MD5 (cdboot) = 4a70ab74371088bff958ecda8a98af9c

MD5 (cdbr) = f609db1eeaf4dc7dc6a280a6c99eea0f

MD5 (cdemu44.iso) = d063d1da57015b2e6b7c8eab6b1ca347

MD5 (comp44.tgz) = 509e442afafcfb74c3a879d4bff423c2

MD5 (etc44.tgz) = ef1efebaa4d650af6d1d6ecbab313c78

MD5 (game44.tgz) = a1b38b380b28ea3e516b06bc8fd73155

MD5 (man44.tgz) = 9b00241c9ef1ee8fdd24af4e14e31ebd

MD5 (misc44.tgz) = 7e44c8c1f61f7b040428940632b4eb4e

MD5 (pxeboot) = 938b1ed43dcdbab09b7add8147b6e43f

MD5 (xbase44.tgz) = 03ff7b5b14cb7c71ba35d86c1dff9087

MD5 (xetc44.tgz) = 9faf8c287e2561c2a26fb927cd57f4ba

MD5 (xshare44.tgz) = 963d39520f9de0f6a1a5649a5c1bf975

SHA1 (INSTALL.i386) = b402b9b40c35df66c670f85a05ea0a90e6a8f4ba

SHA1 (INSTALL.linux) = 238f5edc8c3a9bd9a6cad9cef08ab9997d66134e

SHA1 (base44.tgz) = 73c6ac00d21338a2a20975bed9d2831ee1b6ebb4

SHA1 (cd44.iso) = 92939aaff4eb210438e37baf13182e3cf4c5ec14

SHA1 (cdboot) = 5950bc5c1e72c661582a47a2345d275fec81904e

SHA1 (cdbr) = 2780c318e455723980eb67a11aba8111cf2330c6

SHA1 (cdemu44.iso) = 417c85bd9180e6e8d41d8a912cc7258f29f34afb

SHA1 (comp44.tgz) = 8445fc7a6f5e50c9734e73ec45dee2df90f172dc

SHA1 (etc44.tgz) = bc8af210963a21910d738dc19e58cfc2063cb42c

SHA1 (game44.tgz) = 3d980afe4159118bcc8f017fd23c8a5a8cb950aa

SHA1 (man44.tgz) = a0f1fae015faf68520acaba4089f2518b65c644d

SHA1 (misc44.tgz) = aeb19df78eb9037b6e5085e7fc32e789a3e8365e

SHA1 (pxeboot) = 152b0b3799c8e5dee6790bb2e6332abc4aafd709

SHA1 (xbase44.tgz) = 52afa60460a8e4d08d6f2eb619b63e8a9a677851

SHA1 (xetc44.tgz) = a785df11d200b6ffeebb3f6acb590ad94f5a92c3

SHA1 (xshare44.tgz) = 13bb8259873e241ef52dd60356bc105f05ee057d

RMD160 (INSTALL.i386) = 8ad60900127b80d45df25f4d27389234544a8f5f

RMD160 (INSTALL.linux) = fd302d99871329572bff0a7c580d29b3123b7963

RMD160 (base44.tgz) = a39dcd9b7f2a77aa7e28a151cc607183a647b27b

RMD160 (cd44.iso) = 53d7984742fed5e0760e9799f5b1b74ac464672b

RMD160 (cdboot) = f75d8e355a38d1048b6c16f7f11e168a99794891

RMD160 (cdbr) = 680f1e206016ae8aafc37d57dabd680a2f3d2fa7

RMD160 (cdemu44.iso) = 5f999a5f00bb455a2d407f41e2529c9b80a62fcd

RMD160 (comp44.tgz) = 2a273022236f33376290b41d9c8bfb3874cc7c09

RMD160 (etc44.tgz) = 2ffe052ee5b7fff60b04809702fd1b2bca6282f5

RMD160 (game44.tgz) = a4e06c4180e06867d9efee665816e65e1606999b

RMD160 (man44.tgz) = f9636940b743a9eb9dfe90c16dd4a663bf186dfd

RMD160 (misc44.tgz) = a38b36cfaf9d0e0afc47651d19b021c28cbaefe5

RMD160 (pxeboot) = 9008afe55fc0adf4e69a4852ae9f3f1ebedcd461

RMD160 (xbase44.tgz) = 5e69e581861c94232291968db3494bf47adbaae9

RMD160 (xetc44.tgz) = d6eed602133b85e3707d0fc4db216e07df5c94ef

RMD160 (xshare44.tgz) = 926de72c24e1c76fa50acd9686572ff762bb5abe

Handbuch:

MD5(manual-de.pdf)= b3c3ba08f8839a6592513cdb2f81474b

SHA1(manual-de.pdf)= 320f9e327a5b387062735a9a950f1b6fa89050ca

RMD160(manual-de.pdf)= 3088eda6f282fa2eb8b64ae1bf74775cd1e65591

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. All relays generate log data when the connection state changes. All administration through the administration web generates log data. 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: 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. 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 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 timestamps for the TOE.
- 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.

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

5 Architectural Information

The TOE GeNUGate Firewall 6.3 is part of a larger product, the firewall GeNUGate 6.3 Z (Patchlevel 7), which consists of hardware and software. The TOE GeNUGate Firewall 6.3 itself is part of the shipped software. The operating system is a modified OpenBSD.

GeNUGate 6.3 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 6.3, 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 6.3 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 on 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 ALG does not perform IP forwarding.
- 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.
- 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.
- The log files are analysed online.
- The administrators are notified about security relevant events.
- File system flags prohibit the deletion of 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 GeNUGate Version 800, GeNUGate Version 400, GeNUGate Version 600 and GeNUGate Version 200. For those tests which need a DMZ (Secure Server Network) the DMZ is located as an alias on a consisting interface card. They are tested on single systems as well as HA-configurations.

The Security Target specifies ten 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 and A.TRUSTU. A.PHYSEC, A.NOEVIL and A.POLICY are not applicable to the test environment. A.ADMIN, A.HANET and A.SINGEN 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 (see [10], [11]). 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 rich 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 real result with the expected one. The output is the status value PASS (if the real result is equal the expected one), FAIL (if the real result is not equal the expected one) or NORESULT (problems occur during runtime e.g. cable break). The volume of the script protocol is influenced through the AET_DEBUGLEVEL option. Tests of the type manual need 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 two GeNUGates (model 600 R4, model 200 R2), a GeNUScreen 100 C (OSPF-Router) and 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 PF 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 crossover cable.

The needed 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 ten 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 and A.TRUSTU. A.PHYSEC, A.NOEVIL and A.POLICY are not applicable to the test environment. A.ADMIN, A.HANET and A.SINGEN 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 (03. and 04.11.09).

Phase 2: The testing was performed with several versions of the TOE. The main phase of testing was performed in December 2009 and January 2010, March 2010, May 2010 and in June 2010 (terminating tests in August with the TOE "build.63.D043”).

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

The analysis of the vulnerability does show that none of the identified vulnerabilities in the intended environment of the TOE is exploitable. For all identified vulnerabilities no attack has been identified, the evaluator has to renounce to specify and perform penetration testing.

In early phases of the evaluation the evaluator has worked towards to identify vulnerabilities and to let them eliminate.

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

To outline further penetration tests, there were analysed starting points, coming off the “onion skins model” of the security and self protection functions of the TOE. Therefore the ITSEF has provided tests with high communication load to activate self protection functions. Furthermore testing was provided using the system console of the ALG –this interface usually is not available to an attacker. This 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 belongs a lot of self protection functions.

Penetration tests of the evaluators have shown that there are no exploitable vulnerabilities in the assumed environment.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

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

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] 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 EAL4 extended by advice of the Certification Body for components beyond EAL 4 [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
  AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended

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

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

9.2 Results of cryptographic assessment

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

10 Obligations and Notes for the Usage of the TOE

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

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

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

The assumptions to the IT environment in the Security Target suppose that the TOE operates in a physically secure environment which prevents access from unauthorised users (OE.PHYSEC). This assumption includes the protection of the boot disc and the USB stick with the PFL configuration. Boot disc and 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 boot diskette respectively 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 performed by personnel which dispose about solid knowledge about networking, packet filter firewalls and secure use of public key procedures.

There should 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 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

12.1 Acronyms

ALG	Application Level Gateway
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
CASE	Computer Aided Software Engineering
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
CPAN	Comprehensive Perl Archive Network
DMZ	Demiliarised Zone
DNS	Domain Name Service
EAL	Evaluation Assurance Level
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
LDA	Lightweight Directory Access Protocol
MD	Message Digest
MIME	Multipurpose Internet Mail Extensions
MSSQL	Microsoft SQL Server relational Database Management System
MTA	Message Transfer Agent, Mail Transfer Agent
MX	Mail Exchanger
MySQL	a relational Database Management System
NFS	Network File System
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
OS	Operating System
OSI	Open Systems Interconnection
PDF	Portable Data Format
Perl	Practical Extraction and Reporting Language
PF	Packet Filter (Komponente von OpenBSD)
PFL	Packet Filter (Komponente des GeNUGate)
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure SHell
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
UDP	User Datagram Protocol
URI	Universal Resource Identifiers

URL	Uniform Resource Locator
VPN	Virtual Private Network
WWW	World Wide Web

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

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

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

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, Revision 3, July 2009

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

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

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0616, Version 9, 17.08.2010, GeNUGate 6.3, GeNUA mbH

[7] Evaluation Technical Report, Version 3, 24.08.2010, Evaluation Technical Report BSI-DSZ-CC-0616 for GeNUGate Firewall 6.3 from GeNUA mbH of Tele-Consulting GmbH, (confidential document)

[8] Configuration list for the TOE:
A4A2083, configuration list „cc.5“ GeNUGate 6.3, 13.08.2010 (confidential document)
A4A2097, configuration list gg63 (Baseline), 13.08.2010 (confidential document)

[9] Guidance documentation for the TOE, Installations- und Konfigurationshandbuch, Version 6.3 Z, August 2010, Revision: gg.63.D043

[10] Peter Miller, Aegis - A Project Change Supervisor - Reference Manual, Version 4.16, October 2004

[11] Peter Miller, Aegis - A Project Change Supervisor - User Guide, Version 4.16, October 2004

[8] 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)

This page is intentionally left blank.

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-

Assurance Class	Assurance Components
	level design presentation
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_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	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.