Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0565-2009

for

GeNUScreen 2.0

from

GeNUA mbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0565-2009

Firewall

GeNUScreen 2.0

from	GeNUA mbH
PP Conformance:	None
Functionality:	product specific Security Target; Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2, ASE_TSS.2 and AVA_VAN.4

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 EAL4 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,12 October 2009

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

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

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

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

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

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

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

Contents

A Certification....7
1 Specifications of the Certification Procedure....7
2 Recognition Agreements....7
2.1 European Recognition of ITSEC/CC - Certificates....7
2.2 International Recognition of CC - Certificates....8
3 Performance of Evaluation and Certification....8
4 Validity of the certification result....8
5 Publication....9
B Certification Results....11
1 Executive Summary....12
2 Identification of the TOE....14
3 Security Policy....15
4 Assumptions and Clarification of Scope....16
5 Architectural Information....16
6 Documentation....17
7 IT Product Testing....17
8 Evaluated Configuration....18
9 Results of the Evaluation....18
9.1 CC specific results....18
9.2 Results of cryptographic assessment....19
10 Obligations and notes for the usage of the TOE....19
11 Security Target....19
12 Definitions....20
12.1 Acronyms....20
12.2 Glossary....21
13 Bibliography....23
C Excerpts from the Criteria....25
D Annexes....35

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

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

---

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

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

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

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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

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 component AVA_VAN.4 that is not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 component of this assurance family is 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 GeNUScreen 2.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0382-2007. Specific results from the evaluation process BSI-DSZ-CC-0382-2007 were re-used.

The evaluation of the product GeNUScreen 2.0 was conducted by

Tele-Consulting
security | networking | training GmbH.

The evaluation was completed on 06 October 2009.

The Tele-Consulting
security | networking | training GmbH

is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: GeNUA mbH

The product was developed by: GeNUA mbH

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

4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

[6] Information Technology Security Evaluation Facility

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

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular 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 GeNUScreen 2.0 has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] GeNUA mbH
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) is a distributed stateful packet filter firewall system with VPN capabilities and central configuration. It provides basic IPv6 support.

The TOE GeNUScreen 2.0 protects networks at the border to the Internet by filtering incoming and outgoing data traffic. It protects the data flowing between several protected networks against unauthorised inspection and modification. It consists of software on a number (at least 2) of machines (GeNUScreen appliances) that work as network filters, hereafter called firewall components, and another machine to manage this network of firewall components. This machine, the management system (GeNUCenter management system), is a central component. The firewall components are initialised on a secure network from the management system.

After initialisation, the firewall components can be distributed to the locations of the networks they are protecting.

The GeNUScreen firewall components filter incoming and outgoing traffic for multiple networks and can thus enforce a given security policy on the data flow. The filter is implemented in the kernel of the firewall components' operating system, OpenBSD. The firewall components can work as bridges or routers.

At the same time the firewall components can provide confidentiality and integrity for data traffic passing between the networks. This Virtual Private Network function is achieved by IPsec encryption and authentication mechanisms using up-to-date ciphers and key sizes. The IPsec transforms are implemented in the kernel. The key agreement for IPsec follows the ISAKMP Internet standard [RFC2409], and is implemented in user space by OpenBSD's isakmpd.

Alternatively, an encrypted tunnel not using the transport layer but the application layer can be build up with SSH connections. This scenario is useful if the full IP connectivity provided by IPsec is unwanted. This composition is referred to as the SSH launch daemon.

Interfaces of the firewall components can be classified at level high or low. Traffic on interfaces with a low classification is not transferred as cleartext.

The management system component provides administrators with a Graphical User Interface (GUI) to initialise and manage the firewall components from a central server.

While cryptographic operations are part of the TOE, the actual random generator, needed by the cryptographic operations, is not part of the TOE.

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 EAL4 augmented by ALC_FLR.2, ASE_TSS.2 and AVA_VAN.4.

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_PF	Packet Filter
SF_RS	Classification
SF_IPSEC	IPsec Filtering
SF_SSHLD	SSH Launch Daemon
SF_IA	Identification and Authentication
SF_AU	Audit
SF_SSH	SSH Channel
SF_ADM	Administration
SF_GEN	General Management Facilities

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. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats. This is outlined in the Security Target [6], chapter 3.

To guarantee that all firewall components are set up correctly and know each other's and the management system's public keys, the following procedure is required:

1. A secure network is set up with only the management system and the firewall components on it.
2. The management system must be installed from CD. During installation, public/private key pairs are generated which are used later to identify and authorise the administrators.
3. The administrators initialise his/her account with a non-guessable password.
4. The administrators use the GUI to create configurations for all the firewall components. The configuration includes the creation of public/private key pairs for the firewall components for later authentication by the Internet Key Exchange (IKE) and Secure Shell (SSH) protocols.
5. The firewall components are installed by PXE boot from the management system. Among other things, the process installs on each firewall component
   - the management system's public key,
   - the individual firewall component's public/private key pair,
   - all the public keys of all the firewall components with which the individual firewall component is configured to communicate directly,
   - a seed value for the random number generator.

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:

GeNUScreen 2.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Management Server Model: 200, 400, 600 or 800	N/A	Hardware
2	HW	Two or more Firewall Components Model: 100C, 300S, 500S, 200, 400, 600 or 800	N/A	Hardware
3	SW	Managemet Server Installation CD GeNUCenter Version 2.0 Z	2.0 Z, Patchlevel 0	CD-ROM
4	SW	Firewall Component Installation CD GeNUScreen Version 2.0 Z	2.0 Z, Patchlevel 0	CD-ROM
5	Doc	GeNUCenter Installations- und Konfigurationshandbuch, Version 2.0 Z, Patchlevel 0, Revision build.4.D073, 25.09.2009	4.D073	Manual and CD-ROM
6	Doc	GeNUScreen Installations- und Konfigurationshandbuch, Version 2.0 Z, Patchlevel 0, Revision build.4.D073, 25.09.2009	4.D073	Manual and CD-ROM
7	Doc	Licence letter	N/A	Letter

Table 2: Deliverables of the TOE

All listed parts on the CD-ROM were delivered together on the corresponding CD-ROM (GeNUCenter respectively GeNUScreen).

The user is able to verify the authenticity of the delivered TOE. The procedure is described in detail in the guidance documentation. The valid checksums are published on the GeNUA website. The valid checksums of the TOE are:

GeNUCenter:
Installation packets in directory /cdrom/
MD5
MD5(4.4/i386/base44.tgz) = 721071389a6c8b6a3a4dc4257f334139
MD5(4.4/i386/center44.tgz) = d6bf7012484f40e07a8662b6e1a93fd0
MD5(4.4/i386/comp44.tgz) = a45733caf696272213ee4ed85d34a3bd
MD5(4.4/i386/etc44.tgz) = 2606b2c0cf313bef6b4aabd679639f9a

MD5(4.4/i386/ports44.tgz) = d129590d7a46925ef5f494c2868ec166
MD5(handbuch.pdf) = ad0ff975c3f9178a85a7917df5f5b651

SHA1
SHA1(4.4/i386/base44.tgz) = 87acc8331c320214e95c720f9afe62f6dbc8e51b
SHA1(4.4/i386/center44.tgz) = c928662816df1217bffd6d121d4f55c0514a98f8
SHA1(4.4/i386/comp44.tgz) = b1d052e7ae22531205bef43ebb62711a02f464a5
SHA1(4.4/i386/etc44.tgz) = 9cb4888c58efbeb57abaaa81fe00ecff6ae75f6e
SHA1(4.4/i386/ports44.tgz) = 44928296e9ffd37a78f73f17d4e549f1203fffce
SHA1(handbuch.pdf) = 41122039c87da61f383b33238e1792623ac84f58

RIPEMD160
RIPEMD160(4.4/i386/base44.tgz) = 86b942609c45eadf421911d0306cbc2b32ed18f8
RIPEMD160(4.4/i386/center44.tgz) = 150e6a145e019d6fb231810726e26bc484577651
RIPEMD160(4.4/i386/comp44.tgz) = ad629fc9e58e385667aafdc2238f00210884129f
RIPEMD160(4.4/i386/etc44.tgz) = 4b648b465e84c923c58c047d44c1ca6e371f9cb4
RIPEMD160(4.4/i386/ports44.tgz) = 8563e327d09465a0f5eb52461df2bb98da8b933a
RIPEMD160(handbuch.pdf) = c21795e6cef0cc8a56ae601e1c011affa7b5498a

GeNUScreen:

MD5
MD5(bsd) = d97185bbf25b3367418753a7c3330492
MD5(handbuch.pdf) = db99b4c088c3faac6b46492a7bceebd5

SHA1
SHA1(bsd) = 7375c47b31a652497f58a119d37847177b3243d4
SHA1(handbuch.pdf) = 565297eca8fea6e50c16212790c958cf6562f58b

RIPEMD160
RIPEMD160(bsd) = 773d8fad04696438b1dd4f13455952515d0d2eff
RIPEMD160(handbuch.pdf) = 36c12457c1263e5d68fe10d58619ee77f40afc28

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. There are ten securtiy policies defined for the TOE.

Five policies are explictly defined:

- FW-SFP: creation, modification, deletion and application of firewall security policy rules
- RS-SFP: interface classification
- IKE-SFP: cryptographic functions in relation to the key management of the VPN connections between the firewall components
- SSH-SFP: flow control functions in relation to the communication between the management system and the firewall components
- SSHLD-SFP: flow control functions in relation to the SSH launch daemon communication between the firewall components

All other policies are implictly defined and cover the following areas:

- IPSEC: flow control functions in relation to the VPN connections between the firewall components

- Administration Policy (implemented by SF_ADM)
- Identification and Authentication Policy (implemented by SF_IA)
- Audit Policy (implemented by SF_AU)
- General Management Facilities Policy (implemented by SF_GEN)

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats 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: OE.PHYSEC, OE.INIT, OE.NOEVIL, OE.SINGEN, OE.TIMESTMP, OE.ADMIN and OE.RANDOM.

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

5 Architectural Information

The TOE is the firewall system GeNUScreen 2.0 developed by GeNUA Gesellschaft für Netzwerk- und UNIX-Administration mbH.

The TOE consists of

- several firewall components that work as network filters and encrypting gateways,
- a central Management Server that is used to configure, administrate and monitor the firewall components.

The Management Server allows authorised administrators to configure filter rules and protection policies on the firewall components by use of a web-based graphical user interface (GUI) at the Management Server. It also enables authorised administrators to update the software on the firewall components. The GUI must be used from a trusted machine connected to the management Server through a trusted network.

After installation, all communication between the Management Server and the firewall components is protected by Secure Shell (SSH) transforms against eavesdropping and modification.

The firewall components employ IPsec encryption and authentication to protect data flows between the subnets assigned to them by the authorised administrators.

Management consists of definition/modification and transmission of firewall policies and security policies for network traffic. The GUI also allows transfer of audit data from the firewall components.

The TOE provides VPN and firewall functionality and is easy to manage. It protects networks at the border of the Internet by filtering data. It also protects data flowing between several protected networks against unauthorised inspection and modification. It consists of software on at least two machines (GeNUScreen appliances), which filter incoming and outgoing traffic for multiple networks. The firewall components (GeNUScreen appliances) provide confidentiality and integrity for data traffic passing between the networks by using IPsec encryption/authentication functionality. Alternatively, an encrypted tunnel using the application layer can be build up from SSH connections. This composition is referred to as the SSH launch daemon. The firewall components can work as bridges and routers. Interfaces of the firewall components can be classified at level high or low.

Traffic sent to or received from interfaces with a low classification is not transported in clear text. Cryptographic operations are part of the TOE. The TOE provides basic IPv6 support.

The TOE also includes a central component, the Management Server, to manage the firewall components. Administrators can initialise and manage the firewall components using a graphical user interface (GUI) to the Management Server. The Management Server allows to collect audit data and monitoring. All components are initialised in a secure network.

The firewall components have a local GUI which can be activated (i.e. when the connectivity to the management system got lost). The firewall components can locally store log files.

The Firewall Components consist of the following subsystems:

- Subsystem Netzwerk (pf)
- Subsystem IPsec Code
- Subsystem IKE Daemon
- Subsystem Service Programms
- Subsystem SSH Client
- Subsystem SSH Daemon
- Subsystem Standalone GUI

The Management Server consist of the following subsystems:

- Subsystem Web GUI
- Subsystem Backend Daemon
- Subsystem SSH Client
- Subsystem SSH Daemon

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

The 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 test configuration in the GeNUA laboratory includes five systems installed with the TOE. Two of these systems (VPN N, VPN S) are used as IPsec-Gateways. Two of theses systems (Client N, Client S) are used as data source and data sink, therefore they need wide open filter rules. The fifth system (router) takes over the routing functions, but is also used to test filter rules. The tests itself are running on the developer server (z200), which is also used for configuration functions. Live-Tests are performed on virtual machines as well

as on real ones. The following HW models are used: Model 100C (Client N, VPN S,), Model 500 (Router), Modell 500 (VPN-N), Model 300 (Client S) Model, and Model 500 (Management-Center).

The developer test scripts 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 subsystems as described in the TOE design and as required for the assurance level of the evaluation.

For the evaluator tests, the test equipment provided by the developer consists of three firewall components (model 100C rev2, model 200 rev3, model 300 S), a Management Server (model 400 rev3) and several versions of the TOE.

According to the Security Target [6] the evaluator has installed the firewall components in a separate administrator network. For the operational configuration the firewall appliances and the management server were integrated over a switch in one network. The test configuration was enhanced with internal networks for each firewall component.

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 by the evaluation facility, without being able to compromise the TOE in the intended environment.

8 Evaluated Configuration

This certification covers the following configurations of the TOE: The Target of Evaluation (TOE) is called: GeNUScreen 2.0. It consists of the deliverables as outlined in chapter 2 of this report.

For installing the TOE a special procedure has to be followed. It is described in the user guidance documentation ([9] and [10]) of the TOE and summarised in chapter 1 of this report.

Please note that all information contained in the Security Target [6] and the guidance documentation ([9] and [10]) have to be followed in order to set-up, configure and use the TOE in a secure manner conformant to the evaluated configuration.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL4 extended by advice of the Certification Body for components beyond EAL4 [4].

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL4 package including the class ASE as defined in the CC (see also part C of this report)

- The components ALC_FLR.2, ASE_TSS.2 and AVA_VAN.4 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0382-2007, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the changes applied in this version of the TOE.

The evaluation has confirmed:

- for the Functionality: product specific Security Target;
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by
  ALC_FLR.2, ASE_TSS.2 and AVA_VAN.4

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 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). This holds for:

- the TOE Security Functionality SF_IPSEC,
- the TOE Security Functionality SF_SSHLD,
- the TOE Security Functionality SF_SSH and
- for other usage of encryption and decryption within the TOE.

10 Obligations and notes for the usage of the TOE

For a secure operation it is necessary to follow all recommendations of the “Installations- und Konfigurationshandbuch” ([9] and [10]) and to follow all requirements to the environment described in the Security Target [6].

The assumptions about the IT environment in the Security Target suppose that the TOE operates in a physically secure environment which prevents access from unauthorised users (A.PHYSEC).

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

Inspections (revisions) of the TOE configuration should be performed regularly, especially the packet filter rules. During those revisions also the procedures to import public keys should be examined.

11 Security Target

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

12 Definitions

12.1 Acronyms

AES	Advanced Encryption Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Errichtungsgesetz
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CBC	Cipher Block Chaining
CEM	Common Methodology for Information Technology Security Evaluation
DH	Diffie-Hellman
EAL	Evaluation Assurance Level
ESP	Encapsulated Security Payload
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security protocol suite
ISAKMP	Internet Security Association Key Management Protocol
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
LDAP	Lightweight Directory Access Protocol
NAT	Network address translation
PP	Protection Profile
PXE	Preboot eXecution Environment
RDR	Redirect rule
RFC	Request for comment
RSA	Rivest Shamir Adleman
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement

SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
UDP	User Datagram Protocol

12.2 Glossary

Administrator/s - This term is used both as a role and as users possessing that role. The singular administrator is used for the role, and the plural administrators is used for the users (unless a singular form is grammatically needed).

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

Basic-auth - The basic authentication is a simple authentication method defined by the HTTP protocol, see RFC2617. It is used by the GeNUScreen administrative GUI.

Cookie - Cookies are part of the HTTP protocol, see RFC2965. They are used as an authentication method by the GeNUCenter administrative GUI.**Cryptographic (SSH or IPsec) Transform** - A series of protocol steps between two parties consisting of

1. agreement on new encryption and/or authentication keys when necessary
2. application of the keys to a stream of data
3. transmission of encrypted, authenticated data between the parties
4. decryption and check of authentication on the respective endpoints

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.

GeNUCrypt - The IPsec crypto appliance from GeNUA.

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

Informal - Expressed in natural language.

IPsec protocol suite - A set of protocols based on IP/UDP to enable two machines to initiate a key exchange, authenticate each other, negotiate encryption and authentication mechanisms, and subsequently encrypt and/or authenticate selected data passing between them.

Isakmpd - The name of the OpenBSD ISAKMP daemon implementation.

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.

Privilege revocation - A security measure where the process gives up all privileges no longer needed in an irreversible way after startup. Only then the process interacts with external entities. An attacker may only gain low privileges.

Privilege separation - A security measure that separates a task in two processes. One of the processes runs with low privileges and interacts with external entities. The other process runs with higher privileges and performs tasks on behalf of the first process. If the first process is corrupted, an attacker has only gained low privileges.

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

Revisor/s - This term is used both as a role and as users possessing that role. The singular revisor is used for the role, and the plural revisors is used for the users (unless a singular form is grammatically needed).

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 - A set consisting of all hardware, software, and firmware of the 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 1, September 2006
Part 2: Security functional components, Revision 2, September 2007
Part 3: Security assurance components, Revision 2, September 2007

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 2, September 2007

[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 Certifcates (BSI 7148, BSI 7149), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-0565-2009, Version 17, 10 September 2009, GeNUScreen 2.0 Security Target, GeNUA mbH

[7] Evaluation Technical Report, Version 2, 06 October 2009, Evaluation Technical Report BSI-DSZ-CC-0565 for GeNUScreen 2.0 from GeNUA mbH of Tele-Consulting GmbH (confidential document)

[8] Configuration list for the TOE, 28 September 2009 (confidential document)

[9] Guidance documentation for the TOE, GeNUCenter Installations- und Konfigurationshandbuch, Version 2.0Z, Patchlevel 0, Revision build.4.D073, 25 September 2009

[10] Guidance documentation for the TOE, GeNUScreen Installations- und Konfigurationshandbuch, Version 2.0Z, Patchlevel 0, Revision build.4.D073, 25 September 2009

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

„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 A.

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 decompositon.

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	2	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.