Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0966-2015

for

genuscreen 5.0

from

genua gmbh

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-0966-2015 (*)

Firewall

genuscreen 5.0

from	genua gmbh
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 extended EAL 4 augmented by ALC_FLR.2, ASE_TSS.2 and AVA_VAN.4

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 4

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.

Common Criteria
Recognition Arrangement
for components up to
EAL 2

Bonn, 3 December 2015

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

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

1. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- 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 SOGIS Technical Domains only.

---

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 Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogisportal.eu.

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

This certificate is recognized according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the components ALC_FLR.2, ASE_TSS.2 and AVA_VAN.4 that are not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL 4 components of these assurance families are relevant.

2.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

As this certificate is a re-certification of a certificate issued according to CCRA-2000 this certificate is recognized according to the rules of CCRA-2000, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained components above EAL 4 that are not mutually recognised in accordance with the provisions of the CCRA-2000, for mutual recognition the EAL 4 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 genuscreen 5.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0823-2014. Specific results from the evaluation process BSI-DSZ-CC-0823-2014 were re-used.

The evaluation of the product genuscreen 5.0 was conducted by secuvera GmbH. The evaluation was completed on 4 November 2015. secuvera GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

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

The product was developed by: genua gmbh.

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, as specified in the following report and in the Security Target.

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

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 3 December 2015 is valid until 2 December 2020. Its validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[6] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

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 5.0, has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] genua gmbh
Domagkstrasse 7
85551 Kirchheim

B. Certification Results

The following results represent a summary of

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

1. Executive Summary

The TOE genuscreen 5.0 is a distributed stateful packet filter firewall system with VPN capabilities and central configuration. It provides basic IPv6 support and protects networks at the border to the Internet by filtering incoming and outgoing data traffic. It protects data flow between several protected networks against unauthorised inspection and modification. It consists of software on a number of machines (genuscreen appliances) that work as network filters, hereafter called firewall components, and the management system (genucenter management system), a central component to manage this network of firewall components.

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.

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. Alternatively, an encrypted tunnel not using the transport layer but the application layer can be build up with SSH connections.

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. The management system also allows collecting audit data and monitoring.

The TOE contains cryptographic functionality. The cryptographic algorithms are part of the TOE. This includes the random number generator which is of class DRG.3 (see AIS20 [4]). The physical scope of TOE consists only of software and documentation. The TOE does not include any hardware or firmware. The genucenter must be operated on real hardware. Running the genucenter in a virtual machine is out of scope for this 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 EAL 4 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. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
SF_PF	Packet Filter

TOE Security Functionality	Addressed issue
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 Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and 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 5.0,

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Management Server Model: gz200, gz400, gz600 and gz800 Two or more Firewall Components Model: gs100b, gs100c, gs300, gs400, gs500, gs600, gs700 and gs800	N/A	Hardware (not part of the TOE)
2	SW	Firewall Component Installation CD genuscreen Version 5.0 Z	5.0 Z Patchlevel 4	CD-ROM

No	Type	Identifier	Release	Form of Delivery
3	SW	Management Server Installation CD genucenter Version 5.0 Z	5.0 Z Patchlevel 4	CD-ROM
4	Doc.	genucenter Installationsund Konfigurationshandbuch, Version 5.0, Ausgabe 26. Mai 2015, Revision genucenter Version 5.0 004 (76532b81d2df286a67319a327d44f90fff5dd9bd) [8]	5.0 Z	Manual and CD-ROM
5	Doc.	genuscreen Installations- und Konfigurationshandbuch, Version: 5.0 Z; Stand 13. Mai 2015, Revision: 50.D047 [9]	5.0 Z	Manual and CD-ROM
6	Doc.	Lizenzschreiben	N/A	Letter

Table 2: Deliverables of the TOE

All listed parts on the CD-ROM are delivered on the corresponding CD-ROM (genucenter and genuscreen).

The user is able to verify the authenticity of the delivered TOE. The procedure is described in detail in the guidance documentation [8] and [9]. The valid checksums are published on the genua website. The valid checksums of the TOE are:

For genucenter (SHA256):

BASE55.TGZ:

c0aefa341427159c79043f5a69e1254177100603cf9c2a08840dd5d1d59912b5

CENTER55.TGZ:

90d00b3d58b376fe412deed6a72308559a7ba2c4d9e66a269e7ac75881058fb9

COMP55.TGZ:

470df2fd33e4488bfa339c19b2bfe05e1840944573a04830771516e31cb6e8d7

ETC55.TGZ:

d71645518abd84d25f897effde9f307397ab9b79f81564ccc91bf2aa6afd4987

GEMS55.TGZ:

a86aa51cbf740353ad695db88bb9ad5c122d451b62997b1a028d90f65e585a12

PORTS55.TGZ:

f07f6e04f9b6b39c34e273cae15fe93a9551fca33e9059d53a53b0ed33a95877

GENUCENTER_500_004_HANDBUCH.PDF:

ff43d41b859dbdf83b2ccd300f56cc7b239631d28747089a51aa699e157089a1

For genuscreen (SHA256):

BSD:

f4441cb6d777bd7e48e9332e261a403cc45228fd9f8fcc31790e41db49dd6286

GENUSCREEN_500_HANDBUCH_DE.PDF:

6d5af00fb4cfa52d7eb28d058255ff28f25b3db4afaf24a21ddd5085d1351e3f

Note:

The TOE (Software, Documentation) is delivered with the OpenBSD-platform and the necessary hardware.

The hardware of the product (not part of the TOE) is composed at Pyramid Computers and and shipped by DHL to the customer site on behalf of genua. The delivery includes the genuscreen software (CD-ROM).

The licence information is sent to the customer by genua.

All systems without integrated CD-Drive, i.e. genuscreen 100 series, are fully composed at genua including software installation. These systems are shipped to the customer by UPS.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. The following securtiy policies are 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).
- Random Number Generation (implemented by FCS_RNG).

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: OE.PHYSEC, OE.INIT, OE.NOEVIL, OE.SINGEN, OE.TIMESTMP, OE.ADMIN, and OE.HANET. Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The TOE is the software part of the firewall system genuscreen 5.0 developed by genua gmbh.

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 and SSH-based encryption and authentication to protect data flows between the subnets assigned to them by the authorised administrators.

The firewall components can be used in an optional high availability (HA) setup (for genuscreen) where the firewall components synchronize their internal states. In case of one system breaks down the function of this component is resumed by the other.

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 the data flow 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 optionally. Traffic sent to or received from interfaces with classification is not transported in clear text. Cryptographic operations are part of the TOE. This includes the random number generator which is of class DRG.3 (see AIS20 [4]). The TOE provides basic IPv6 support.

The GUI of the management server supports three types of user roles, i.e. Administrator, Revisor and Service. The Management Server allows to collect audit data and monitoring. All components are initialised in a secure network.

The communication server (represented by an additional genuscreen appliance) between the genuscreen appliances and the genucenter management system avoids exposing the genucenter to the Internet.

The firewall components have a local GUI, too, which can be activated (i.e. when the connectivity to the management system got lost). The GUI of the firewall components

supports two types of roles, i.e. Administrator and Revisor. 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
- Subsystem HA-Betrieb
- Subsystem Krypto

The Management Server consist of the following subsystems:

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

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 five systems installed with the TOE. Two of these systems are used as IPsec-Gateways. Two of theses systems are used as data source and data sink, therefore they need open filter rules. The fifth system takes over the routing functions, but is also used to test filter rules. The tests itself are running on the developer server which is also used for configuration functions.

The Security Target specifies seven assumptions about the environment of the TOE: A.PHYSEC, A.INIT, A.NOEVIL, A.SINGEN A.TIMESTMP, A.ADMIN and A.HANET. A.PHYSEC and A.NOEVIL are not applicable to the test environment. A.ADMIN, A.INIT, A.SINGEN and A.HANET are given in the test environment. A.TIMESTMP is given in all TOE configurations because of the properties of the underlying operation system. All configurations were loaded by CD. The evaluator accepts this procedure. It makes it easier to repeat testing without impacting the behaviour of the security functions.

For the most part the tests are automatically running under control of the tool aegis and further testing framework of the development and QS testing lab. The tools also provides automatically the test results. The test procedures are executable scripts (Ruby, Perl or Shell). The developer uses two kinds of tests: Local Tests and Live tests. Local Tests need the developer environment and were executed inside the developer systems. The tests itself are running on development servers, which also provide configuration functions. Live tests are performed on virtual machines as well as on real physical systems.

Integrated in their program code all scripts compare the real result with the expected results. The output is the status value OK (if the real result is equal to the expected one) or FAIL (if the real result is not equal the expected one). Using the test scripts the developer automatically ensures that the entrance conditions and the dependencies between tests are considered. Therefore the responsibility for the correct testing is transferred to the developer.

The specified tests cover all security functions and the testing is performed against the TOE design. All real test results are equal with the expected test results.

Independent Evaluator Tests

The test equipment provided by the developer consists of several different firewall components of different Hardware models, a CommServer (Hardware model 100b) and two instances of the TOE.

According to the Security Target 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 configuration is consistent with the configuration in the Security Target.

To observe the behaviour of the firewall appliances on each a console access was activated.

According to the assumptions identified in the Security Target the following is stated: A.PHYSEC and A.NOEVIL are not applicable to the test environment. A.ADMIN, A.SINGEN, A.INIT und A.HANET is given in the test environment. A.TIMESTMP is given in all TOE configurations because of the properties of the underlying operation system.

Testing covers the complex installation and all security functions. The main focus was the SSH protocol, the management, cryptographic functions and random number generator (RNG) and its entropy source (part of OpenBSD kernel) functions.

The repetition of the developer testing was also done in the ITSEF laboratory. In this evaluation the evaluator chose a sample of developer test. In some cases the evaluator interpreted the test with respect to the ITSEF laboratories test environment.

The developer has developed an amount of regression tests for ipsecctl, openssh and isakmpd. All those tests have been repeated independently by the ITSEF laboratory.

The test results have not shown any deviations between the expected test results and the actual test results.

Penetration Tests

The evaluator has done an independent vulnerability analysis. As a result additionally vulnerability tests have been designed. Penetration testing was performed as part of the

independent evaluator tests described in the previous chapter. Additionally a source code analysis was done.

No attack scenario with moderate attack potential was actually successful in the TOE's operational environment as defined in the ST, if all measures required by the developer are applied.

8. Evaluated Configuration

The TOE configuration consists of software on at least two firewall components (genuscreen appliances) that work as network filters. Another machine to manage this network of firewall components is called management system (genucenter management system) which 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 firewall components can work as bridges or routers. The firewall components can be used in an optional high availability (HA) setup (please note that the high availability option of genucenter is not part of the TOE.) where the firewall components synchronize their internal states.

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 or SSH connections.

The connection between the genucenter and genuscreens is encrypted with SSH.

All HW and the platform OpenBSD Version 5.5, kernel and user space programs, HTTP/S server, DHCP server, TFTP server are not part of the TOE and belong to the environment. The TOE contains cryptographic functionality. The cryptographic algorithms are part of the TOE. This includes the random number generator which is of class DRG.3 (see AIS20 [4]).

Please note that, as detailed in the Security Target [6] chapter 1.4.8, the functions CryptoCard, USB update, FTP and SIP Relays, VPN to Other Appliances or Mobile Clients, L2TP VPN, LDAP Authentication, Dynamic Routing, and virtual genucenter are out of scope of the evaluated configuration.

In general, all information contained in the Security Target [6] and the guidance documentation ([8] and [9]) 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 EAL 5 extended by advice of the Certification Body for components beyond EAL 5.

For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.2, ASE_TSS.2 and AVA_VAN.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-0823-2014, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on some design-, configuration- and functional changes of the TOE.

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 extended
  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 strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

For details of the cryptographic algorithms that are used by the TOE to enforce its security policy please refer to table 8.1 of the Security Target [6]. Any Cryptographic Functionality that is marked in column 'Security Level above 100 Bits' of that table with 'no' achieves a security level of lower than 100 Bits (in general context).

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a

re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

For a secure operation it is necessary to follow all recommendations of the "Installations- und Konfigurationshandbuch genuscreen" [9] and "genucenter Installations- und Konfigurationshandbuch" [8] and to follow all requirements to the environment described in the Security Target [6]. Especially all recommendations regarding configuration of packetfilter in combination of SSH-based VPN-tunnels should be read carefully. In case of a lost appliance (e.g. theft) the procedures in the manual should be followed, see [9] genuscreen manual chapter 8.1 “Verlust einer genuscreen” and [8] genucenter manual chapter 3.8 “Vorgehen bei Verlust einer Appliance”.

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 (A.PHYSEC). Comparable protection mechanisms must be implemented to logically and physically protect backups files of the genucenter management system.

Administration and revision of the TOE should only be performed by personnel with solid knowledge about networking (especially IP and TCP/UDP), packet filter firewalls and secure use of public key procedures.

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

After installation of firewall component by using the management system on each component PXE boot must be disabled (system hardening).

In addition, all further aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

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

AIS Application Notes and Interpretations of the Scheme

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
ipsecctl	a utility foe Control Flow in IPsec, to determine which packets are to be processed by IPsec.
ISAKMP	Internet Security Association Key Management Protocol
ISAKMPD	The name of the OpenBSD ISAKMP daemon implementation.
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

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

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

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

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

Informal - Expressed in natural language.

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

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

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 - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-0966-2015, genuscreen 5.0, Version 2, 14 August 2015, genua gmbh

[7] Evaluation Technical Report, Version 2, 03 November 2015, Evaluation Technical Report BSI-DSZ-CC-0966 for genuscreen 5.0 from genua gmbh of secuvera GmbH (confidential document)

[8] Guidance documentation for the TOE, genucenter Installations- und Konfigurationshandbuch, Version 5.0, Ausgabe 26. May 2015, Revision genucenter Version 5.0 004 (76532b81d2df286a67319a327d44f90fff5dd9bd), genua gmbh

[9] Guidance documentation for the TOE, Installations- und Konfigurationshandbuch genuscreen, Version: 5.0 Z; Stand 13 May 2015, Revision: 50.D047, genua gmbhThis page is intentionally left blank.

[8] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 38, Version 2, Reuse of evaluation results

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

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

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

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

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

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

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

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

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

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

The following table shows the assurance class decomposition.

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

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

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

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

Evaluation assurance level (EAL) overview (chapter 8.1)

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

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

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

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

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

“Objectives

EAL 1 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.

EAL 1 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.

EAL 1 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 EAL 1 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 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 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.

EAL 2 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 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 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 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 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. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 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 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 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 EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 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 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 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.

EAL 6 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 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 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 EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
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”

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.”

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.