Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1194-2023

for

genuscreen 8.0

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-1194-2023 (*)

Firewall

genuscreen 8.0

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, AVA_VAN.4 and ALC_PAM.1

SOGIS
Recognition Agreement
for components up to
EAL 4

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 Scheme Interpretations and 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 5.

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
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 6 April 2023

For the Federal Office for Information Security

Sandro Amendola
Head of Division

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.

Contents

A. Certification

1. 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.

2. 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[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- 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[4] [1] also published as ISO/IEC 15408

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

2 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

3 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- 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]

3. 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.

3.1. European Recognition of 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.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. 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 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.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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.

3.2. 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 current list of signatory nations and approved certification schemes can be seen on the website: https://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 related bodies

[4] Proclamation of the Bundesministerium des Innern und für Heimat of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 and ALC_FLR components.

4. 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 8.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1142-2020. Specific results from the evaluation process BSI-DSZ-CC-1142-2020 were re-used.

The evaluation of the product genuscreen 8.0 was conducted by secuvera. The evaluation was completed on 30 March 2023. secuvera is an evaluation facility (ITSEF)[5] 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.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is 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 components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or 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 would 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 6 April 2023 is valid until 5 April 2028. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

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,
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.

6. Publication

The product genuscreen 8.0 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[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] 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 8.0 is a distributed stateful packet filter firewall system with VPN capabilities and central configuration.

It consists only of software and documentation. It protects networks at the border to the Internet by filtering incoming and outgoing data traffic. It also protects the data flowing between several protected networks against unauthorised inspection and modification. One part of the TOE runs on a number (at least 2) of machines (genuscreen appliances) that work as network filters and IPsec routers. The other part of the TOE runs on the machine to manage the network of genuscreens. This machine, the genucenter management system, is a central component. The genuscreens are installed on a secure network from the genucenter or using an USB install image. The genucenter itself is installed from an USB or optical installation medium. The TOE supports IPv4 and IPv6.

The genuscreen filters 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 genuscreen's operating system, OpenBSD. The genuscreen can work as bridges or routers. The genuscreens can be used in an optional high availability (HA) setup where the genuscreens synchronise their internal states.

The genuscreens 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.

Optionally, a SIP module can be installed on the genuscreen components in order to integrate a Session Border Controller (SBC). The SIP relay is not included in the basic installation image but must be installed as an optional module at the genucenter. The SIP relay software is then installed on all appliances that use the relay.

The genucenter provides administrators with a Graphical User Interface (GUI) to initialise and manage the genuscreens from a central server. The genucenter also allows collecting audit data and monitoring.

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) and some of them are newly defined. The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.2, ASE_TSS.2, AVA_VAN.4 and ALC_PAM.1.

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
SF_NS	Network Separation

TOE Security Functionality	Addressed issue
SF_IPSEC	IPsec Filtering
SF_SIP	SIP Relay
SF_IA	Identification and Authentication
SF_AU	Audit
SF_SSH	SSH Channel
SF_ADM	Administration
SF_GEN	General Management Facilities
SF_PI	Patch installation

Table 1: TOE Security Functionalities

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

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 8.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Two or more genuscreen firewall components Model: genuscreen XS (revision 2), genuscreen S (revision 2 and 3), genuscreen M (revision 2 and 3), genuscreen L (revision 2 and 3), genuscreen XL (revision 2 and 3), cryptOHBguard Management Server genucenter: genucenter S (revision 2 and 3), genucenter M (revision 2 and 3), genucenter L (revision 2 and 3)	N/A	Hardware (not part of the TOE)
2	SW	genuscreen Installationsmedium Version 8.0	8.0p11	CD-ROM / USB image
3	SW	genucenter Installationsmedium Version 8.0	8.0p5	CD-ROM / USB image
4	SW	SIP Module, sip-800_011-amd64.tgz	8.0p11	TAR archive
5	Doc.	genuscreen Installations- und Konfigurationshandbuch Version 8.0, Ausgabe 17. Februar 2023, Revision 3a6fcd2b [8]	8.0	PDF download
6	Doc.	genucenter Installations- und Konfigurationshandbuch Version 8.0, Ausgabe 17. Februar 2023, Revision 3a6fcd2b [9]	8.0	PDF download
7	Doc.	Lizenzschreiben	N/A	Letter

Table 2: Deliverables of the TOE

The hardware of the TOE (not part of the TOE) is composed at the supplier company “Pyramid Computer GmbH” and shipped by a parcel service to the customer site on behalf of genua. This delivery includes the genuscreen software (CD-ROM or USB-Stick). The licence information is sent to the customer by genua. The SIP relay and the documentation has to be downloaded from the genua Kundenportal by a secure connection via TLSv1.2 or TLSv1.3. The software of the genuscreen and genucenter is alternatively also available at the genua Kundenportal, however, this form of delivery is not covered by the evaluation.

The user shall verify the authenticity of the delivered TOE. The procedure is described in detail in the guidance documentation. The integrity verification of the SIP module by SHA256-checksums is done equivalent to the checks of the genuscreen and genucenter. The valid checksums are published on the genua website. The valid checksums of the TOE components, which are also published on the genua “Kundenportal,” are:

genucenter, CD/ROM, checksum of the tgz-archives and the manual (SHA256):

ef49e32a001a1736bf83217bcbaa0fb3e1b224e9775e4836ec4ec3f409ed8fbe
appsoft.tgz

d088e07185e64556c7aa63773fcaa75b7dd944ce2360c0952e2cb66d067fd86f
base.tgz

43ff8b3d7cbc3433f0caa690b11a318437c90ecbd8ea8dbc9f8fff30b4705259
center_assets.tgz

b20c6d7581da4baf546907f3fedb51b73c2c1ab15d36de06504d5008e3bb6d0d
center.tgz

0aa014627fbf330d44ebe906ceee7a5045089c05560af0627841d42f20330b93
comp.tgz

0ba25778198704851cc6415d1c0349fbeeba48620c144e624db183cc179879c5
etc.tgz

d1d15120852219ce895e40547e5588fcf1665b87b1b6cc07a0c66f82b941ad85
firmware.tgz

f281f5539d1be73e97654ee2f7e2d83aa2a5e3b6b1963a91822f188be66a51f9
gems.tgz

3229a6c37c72db7d4a123e6d34c8b5c9e70fcb91c737a02cdefa0e8e7c40a097
genuos_center.tgz
e704e4eeb3b3baac08c41af23b089a685556e89f68e5da81d4cfa02de0111a50
ports.tgz

48793f2d09bbd1fdadc6b0aa64b21e8b3ec42b173bd1b56eede6394b0b0d6a71
Z800_000.manual-zert.de.pdf

genucenter USB- and CD-Image (SHA256):

846eb4cf4930b6477834c804bf057baea780e7b3e8e0ba5ce52342b6c8b4926e
Z800_005.img

fbf311597b97e64b59569b041d9879d35156355236de98d1899139488da33df3
Z800_005.iso

genuscreen, CD/ROM, Checksum of all binaries and the manual (SHA256):

a5798184dafbe2e44408b8f0adc9df9d02af25ea13d54f96329cce7546295851
bsd.amd64

40e01a2a5d312436e56ba33b485d61d080cbb983ef99c739b91f96ac79a22d79
bsd.i386

05270cfb075cb1d01421de75f920b9da4e262f97a9fad6fcb832825265674619
genuscreen-800-handbuch-zert-de.pdf

genuscreen USB- and CD-Image (SHA256):

7f63a6411a26b9d73cc372616a22a31bd162a411ec53949a50b9ed0266f8b732
S800_011.img

5f2ae4a44c8be3f15342023444619ab76412ac41f824e6b321127b95cdbf7656
S800_011.iso

SIP Relay module sip-700_011-amd64.tgz (SHA256):

06a2f4feb0b1f859f03d03516da7d197418c3e742995f26264ea05186f59619e
sip-800_011-amd64.tgz

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. The following security policies are defined for the TOE.

The following policies are defined by the ST [6]:

- Firewall SFP: creation, modification, deletion and application of firewall security policy rules.
- Network Separation SFP: network separation using routing domains.
- IPSEC: flow control functions in relation to the VPN connections between the firewall components.
- 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.
- SIP Relay: access control by the SIP relay.
- Administration: administration of the TOE.
- Identification and Authentication: identification and authentication of administrators, service users and revisors.
- Audit: audit capabilities of the TOE.
- General Management Facilities: general management of the TOE.
- Random Number Generation: generation of random numbers.
- Patch Installation: patch installation process.

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 environment of the TOE. The topics as depicted in the ST [6], chapter 4.2 are of relevance.

5. Architectural Information

The TOE is the firewall system genuscreen 8.0 developed by genua GmbH.

The TOE consists of

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

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

After installation, all communication between the genucenter and the genuscreens is protected by Secure Shell (SSH).

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

The genuscreens can be used in an optional high availability (HA) setup where the genuscreens synchronize their internal states. In case 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 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 genuscreens, which filter incoming and outgoing traffic for multiple networks. The genuscreens provide confidentiality and integrity for data traffic passing between the networks by using IPsec encryption/authentication functionality. The genuscreens can work as bridges and routers. Cryptographic operations are part of the TOE. The TOE provides IPv4 and basic IPv6 support.

The TOE includes an optional SIP relay to allow the usage of a Session Border Controller (SBC). The SIP relay is not included in the basic installation image but can be installed as an optional module at the genucenter. The SIP relay software is then installed on all appliances that use the relay.

Administrators can initialise and manage the genuscreens using a graphical user interface (GUI) of the genucenter. That GUI supports different types of user roles. The genucenter allows to collect audit data and monitoring.

The genuscreens have a local GUI which can be activated (i.e. when the connectivity to the genucenter got lost). The GUI of the genuscreens also supports different types of roles. The genuscreens can locally store log files.

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

Tests are done by the developer and quality assurance (QAU) teams.

Tests of the developer team and QAU run in a virtualised test environment. In that environment the Open Source Cloud Computing Infrastructure OpenStack is used.

The test environment includes six machines installed with the TOE. Three of these machines are used as IPsec-Gateways. Two are used as data source and data sink, therefore they need wide open filter rules. The sixth machine takes over the routing

functions, but is also used to test filter rules. All machines are using IPv4 and IPv6 addresses.

The tests itself are running on the developer server, which is also used for configuration functions. Tests are performed on virtual machines as well as on real ones. When virtual tests are performed first a set of different clients is build up in the test environment.

Quality assurance tests are used to test different aspects of the TOE. QAU is using proprietary test clients and a proprietary git repository to store test scripts. Initially the tested software components and tests are loaded from the corresponding repositories and are installed in the test environment.

The Security Target specifies ten assumptions about the environment of the TOE: A.PHYSEC, A.NOEVIL, A.REMOTE_AUTH and A.REST are not applicable to the test environment, A.INIT, A.SINGEN, A.ADMIN, A.HANET and A.LOCAL are given in the test environment, A.TIMESTMP is given in all TOE configurations because of the properties of the underlying operation system.

Integrated scripts compare the actual result with the expected one. The output is the status value OK respectively pass (if the real result is equal 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.

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 the following hardware: genucenter L, Revision 3.0, genuscreen S, Revision 3.0, genuscreen M, Revision 3.0, genuscreen L, Revision 3.0, cryptOHBguard 10scs, genuscreen XS, Revision 3, genuscreen XS, Revision 2.0 (used at genua onsite testing), genucenter S, Revision 2.0 (used at genua onsite testing).

According to the Security Target the evaluator has installed the genuscreens and genucenter in a separate administrator network. All components were installed on physical hardware, the installation of the TOE on virtual machines is out of scope of the evaluated configuration. For the operational configuration the genuscreens and the genucenter were integrated over the communication server in one network. The test configuration was enhanced with internal networks for each genuscreen.

The configuration is therefore consistent with the configuration given in the Security Target.

To observe the behaviour of the genuscreens the behaviour of the systems was monitored with the Webshell in the WebGUI of the genucenter and with the serial console of the genuscreens.

According to the assumptions identified in the Security Target the following is stated: A.ADMIN, A.INIT und A.SINGEN are given in the test environment, A.PHYSEC, A.NOEVIL, A.LOCAL and A.REST are not applicable to the test environment, A.TIMESTMP is given in all TOE configurations because of the properties of the underlying operation system, A.HANET and A.REMOTE_AUTH are not considered as these were not required while testing.

A sample of developer tests have been retested as part of the ITSEF tests. Testing in the own premises covers among the complex installation all security functions.

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 divided in the parts along the threat paths manipulation of the installation, manipulation of the boot process, exploiting over a network (internet, internal interfaces), and special operation modes. All penetration testing was performed with the test equipment provided by the developer.

Additionally, a source code analysis was done.

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

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 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 connections.

The TOE includes an optional SIP relay to allow the usage of a Session Border Controller (SBC). The SIP relay is not included in the basic installation image but must be installed as an optional module at the genucenter. The SIP relay software is then installed on all appliances that use the relay.

The connection between genucenter and genuscreen is encrypted with SSH.

All HW and the platform OpenBSD Version 6.8, 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.

Please note that, as detailed in the Security Target [6] chapter 1.4.11, several functions (such as genucard and no deployment server, Smartcard, Secure Boot, IKEv2 X.509 Certificates, VPN to Other Appliances or Mobile Clients, L2TP VPN, MOBIKE VPN, Dynamic Routing, genucenter HA, Remote Maintenance, getimagesfromcpt) are out of scope of the evaluated configuration.

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]).

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.2, ASE_TSS.2, AVA_VAN.4 and ALC_PAM.1 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-1142-2020, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the general product evolution and the addition of ALC_PAM.1.

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, AVA_VAN.4 and ALC_PAM.1

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 the table in chapter 8 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.

For a secure operation it is necessary to follow all recommendations of the “Installations- und Konfigurationshandbuch” of the genuscreen and genucenter and to follow all requirements for the environment described in the Security Target. Especially all recommendations regarding configuration of the packet filter in combination with SSH-based VPN-tunnels should be read carefully, see also genucenter manual chapter 5.7 "Nutzung der Sicherheitseigenschaften” respectively genuscreen manual chapter D.6 "Nutzung der Sicherheitseigenschaften”.

In case of a lost appliance (e.g. theft) the procedures in the manual should be followed, see genuscreen manual chapter C “Vorgehen bei Verlust einer Appliance” and genucenter manual chapter C “Vorgehen bei Verlust einer Appliance”.

Before the installation the checksums of the manuals and software has to be verified. The procedure and checksums to verify the manuals and software, including the SIP-module, are available for logged in users on the genua Kundenportal https://kunde.genua.de

The verification procedure and checksums are available via the following menu entries:

- “Produkte” > “genuscreen” > “Checksummen” > “genuscreen 8.0 Checksummen Zertifiziert“
- “Produkte” > “genucenter” > “Checksummen” > “genucenter 8.0 Checksummen“

The download of the manuals is available via the following menu entries:

- “Produkte” > “genuscreen” > “Handbücher” > “genuscreen 8.0 Handbücher zertifiziert”

The procedure to verify the software is also described in the genucenter manual chapter 2.1.4 “Verifizierung der Software” respectively genuscreen manual chapter 2.9 “Verifizierung der Software”.

The assumptions for 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. See the recommendations given in genucenter-manual, chapter 2.5.

Administration and revision of the TOE should only be performed by personnel who dispose of 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 also be examined.

After installation of a genuscreen by using the genucenter, PXE boot must be disabled (system hardening).

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. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
API	Application Program Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CBC	Cipher Block Chaining
CEM	Common Methodology for Information Technology Security Evaluation
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DRG	Deterministic Random Generator
EAL	Evaluation Assurance Level
eIDAS	Electronic Identification, Authentication and Trust Services
ESP	Encapsulated Security Payload
FTP	File Transfer Protocol
GUI	Graphical User Interface
HA	High Availability

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
L2TP	Layer 2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
MOBIKE	Mobility and Multihoming
NAT	Network address translation
PP	Protection Profile
PXE	Preboot eXecution Environment
QES	Qualified Electronic Signatures
RDR	Redirect rule
REST	Representational State Transfer
RFC	Request for comment
RSA	Rivest Shamir Adleman
SAR	Security Assurance Requirement
SBC	Session Border Controller
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
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions

UDP User Datagram Protocol

VPN Virtual Private Network

13.2. 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.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
https://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[7] 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-1194-2023, genuscreen 8.0, Version 8.0.7 (a57d3b3), Date: 2023-03-09, genua GmbH

[7] Evaluation Technical Report BSI-DSZ-CC-1194-2023 for genuscreen 8.0 from genua GmbH, Version 3, Date: 30.03.2023, secuvera GmbH (confidential document)

[8] Guidance documentation for the TOE, genuscreen Installations- und Konfigurationshandbuch; Version 8.0; Ausgabe 17. Februar 2023, Revision 3a6fcd2b, genua GmbH

[9] Guidance documentation for the TOE, genucenter Installations- und Konfigurationshandbuch; Version 8.0; Ausgabe 17. Februar 2023, Revision 3a6fcd2b, genua GmbH

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- 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
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report