Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1142-2020

for

genuscreen 7.0

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-1142-2020 (*)

Firewall

genuscreen 7.0

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 IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

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 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, 18 August 2020

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

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

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]
- BSI Schedule of Costs, BMI Regulations on Ex-parte Costs [3]
- 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]

[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 Criteria for IT Security Evaluation (CC), Version 3.1[4] [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]

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.

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

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 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+ 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 7.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1085-2019. Specific results from the evaluation process BSI-DSZ-CC-1085-2019 were re-used.

The evaluation of the product genuscreen 7.0 was conducted by secuvera GmbH. The evaluation was completed on 7 August 2020. secuvera GmbH 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

[5] Information Technology Security Evaluation Facility

maximum validity of the certificate has been limited. The certificate issued on 18 August 2020 is valid until 17 August 2025. 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,
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 7.0 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 7.0 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. The TOE provides IPv4 and basic IPv6 support. 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 be used in an optional high availability (HA) setup where the firewall components synchronize their internal states.

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.

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 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 communication server between the genuscreen appliances and the genucenter management system avoids exposing the genucenter to the Internet. The connection between the genucenter and genuscreens is encrypted with SSH.

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
SF_NS	Network Separation
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

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 7.0

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), infodas SDoT Server V3 Management Server genucenter Model: genucenter S (revision 2), genucenter M (revision 2 and 3), genucenter L (revision 2 and 3)	N/A	Hardware (not part of the TOE)
2	SW	Firewall Komponenten Installation CD genuscreen Version 7.0	7.0 Patchlevel 11	CD-ROM / USB image
3	SW	Management Server Installation CD genucenter Version 7.0	7.0 Patchlevel 6	CD-ROM / USB image
4	SW	SIP Module sip-700_011-amd64.tgz	7.0 Patchlevel 11	TAR archive
5	Doc.	genucenter Installations- und Konfigurationshandbuch, Version 7.0, 25. März 2020 Revision: cbb982ec [8]	7.0	CD-ROM / USB image
6	Doc.	genuscreen Installations- und Konfigurationshandbuch, Version 7.0, 25. März 2020 Revision: cbb982ec [9]	7.0	CD-ROM / USB image
7	Doc.	Lizenzschreiben	N/A	Letter

Table 2: Deliverables of the TOE

All listed parts on the CD-ROM /USB-Image are delivered together on the corresponding CD-ROM /USB-image (genucenter respectively genuscreen). The SIP-relay has to be downloaded securely from the genua website by registered users.

The hardware of the TOE (not part of the TOE) is composed at the supplier company “pyramid computers” and shipped by DHL 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 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- and SHA512-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 are:

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

8d2169d2e16b3df8101b39b58328b1083f470b97d8388682db8da28a13a0d31a
appsoft.tgz

5e6b51e65f0d8c6114ee6c8768128c11529f885442596815a05b7376e01241cc base.tgz

7f46bc2fefc5f67a1911ffcd317d747eb30f833e678f4217a5235a580d36a83f center.tgz

d99dfc06135c7f17655594fd5eee3ae649a4a042b2153a18cbd1dec11fb7353e comp.tgz

04a65acb07f88b9d838359e0e9d76b5c4492e1386565ab0183a5eeca3fde5897 etc.tgz

4631334301cbc9f40d51dda833fb35b69de310a28d5e6b1f7bb33169f2ce8891 gems.tgz

b5e80ef040e8009bb297ee2e36ffb885327f1d95080c6ddd93aea736751c7964 metrics.tgz

0d4d550feaf36e9741f0214fbbd912fe1de663fd39e384a29dcc96b5eb08e1f6 ports.tgz

74802e73585d2f7d816a73d2f31eab46229c5e4ac9cdd7f381ca10417591adcc vstop.tgz

12377b47099a7dbc69ecdb9b19d0a5e3553abd04377cdc4b6307fa8662a54ab4
handbuch_de.pdf

genucenter, CD/ROM, checksum of the tgz-archives and the manual (SHA512):

d50309f71f30781dfe6d6046457916eeffedf7cb3c7e11db13a56bf4744cff5eb8ed08a7dfaed
20d0268ff7f6f30eb4e52839457bebfe1c615cfabbba717a8c5 appsoft.tgz

c8c766b135288e1a7225eae69817be4e764212af62d0bea020bb31e7a83b76edc58bc71f6
c33d9763e2bc86990fa800bcb99504d85150215814df98e725fc8cb base.tgz

813eafd26cbf59adc429e33a09b5b623964d767175a000d0337d0f3600086d6875e0ce8ce6
b3c81eb18cc456adf46921dc3b6c6eb1065f57c6905858c3bb6843 center.tgz

9135138d4b3153ae0d78713302cc9621141bff6cd4706f38d999d7328c0cbf9bce1d372c5fe
58f7969c26b1a42169f9d2f706c4c3cc9fac0869c2365b500b8fe comp.tgz

e40452ec62678d1a7c770730e8ac267d1b63ff663f1b12c40db97980e82442a81be1e943b0
6d866b9b45b4d8e0325ff24e9773827526ddd1bfbae058ba5781ba etc.tgz

b51fc171b31525861e347832777dcba330e2f51c91f0ba0dd341d195e82986171c166d33e5
aa00e85500aa9452f6f8ee52d63bf3d940d04efc53042fe61fb367 gems.tgz

3962a53e991eb1b7f805f603f734f27d45ae9c023d7012f5345cee76cdcb8b85570cd31e4f4f
95d86fbb375e147fb5bd3aeb857fc1349a186b1ee19c13da3dc0 metrics.tgz

a4a7ff815d75636e100e6817809085ce37c5b475cbd8d60b6df6d89b77cb84aba456ac3d4b
d35f6f42637a3c8166bdeeb460599ef7c9de6471c988164f6fc302 ports.tgz

f794abf94d81cc3a6fdddd873cf8033acd1eab2f6286048efa0cba55a28202a89f30337b7c42
43c910da26011c0636a2257621dddcf01ea4fb5c5afd11917703 vstop.tgz

a474be8f919d5661a34286200eb87468dacf22b094eb90f19a08784ef72b550bf637166cad
8dee254007d7d2a0395c813714c9eaf2a6d5f418953d1658f7fc38 handbuch_de.pdf

genucenter USB- and CD-Image (SHA256):

3d30bf983adcd127ab932d4adfa8d61d341f89467da9bbe7cf74b533c051ec1b
Z700_006.img

cf2f62cbbd5dfd5d9dfae6acd9814ac020b3cad72e9b0e6ce9bf5c8228876022
Z700_006.iso

genucenter USB- and CD-Image (SHA512):

e103c44e3e74418ffaf95470008ca578b3425f19cefc4e4634ad8eba909f1337e3b0f081fb0d
3c75cde2173c46f6216e4190ac721f09410dbce9f45372f96f8a Z700_006.img

8817ca978b1ecbeb797b72b280eed3ebc2972563fcb6a4cb32ca5b264ce6a45bdbba25481
870845e8c631403f0796f53ad67e641758a797118efd7f164770fbf Z700_006.iso

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

9e6b0d0587a68470185152153e3a01e7517223b6a900586daa729d4566052dd7 bsd

9e6b0d0587a68470185152153e3a01e7517223b6a900586daa729d4566052dd7
bsd.amd64

c57c286a7a90d04b31f09337ad4599062a05ebcb3bf16275e629027a7cc1feca bsd.i386

96dbb1b622063a7e22ddaf3e69a0ae39b796fcd7b3addc548bebb8a03f4c6539
genuscreen_700-handbuch-de.pdf

genuscreen, CD/ROM, Checksum of all binaries and the manual (SHA512):

c96df2ea9ba7158163e41f27cdeb31e3344e52e59c95b88b054353e0d3492706c9915b24d
e1f3e45553aac2a974af1bd859309092b14ac0186f97edc6bfde609 bsd

c96df2ea9ba7158163e41f27cdeb31e3344e52e59c95b88b054353e0d3492706c9915b24d
e1f3e45553aac2a974af1bd859309092b14ac0186f97edc6bfde609 bsd.amd64

ca365d2e49f4b659076158a0cadfcd26dc10a0f095b866b43f9f0ca4c77936072cad53a21b6
a7128ee4f093f54747b46b4ea731a740417c2663f2044c741d64c bsd.i386

d089bacaf8c017904f3a55fbbb7d2ee0adde98836c95571970b78db237e917f4ac26c38c00
1e238e81df833112c9aa29718d498d77e9be8c869c67affabf90b0 genuscreen_700-handbuch-de.pdf

genuscreen USB- and CD-Image (SHA256):

667ef7d839eb495ed40031c295e22fc3831e876c9e81aad43270846df430faeb
S700_011.img

de8a8e3e8e5c850b87c20bfad094e0953c564e6ea2dcd9bd315b2b57d1b6089b
S700_011.iso

genuscreen USB- and CD-Image (SHA512):

5d45a3223c274219f0722629025c531d5d48e9c9df1f47c575f6e8a53c0cb15f10f15eb0c6b
4b1eccbb1d7e607c8a3316658127b47428983910532ae5b609c26 S700_011.img

9e3064dd1b171475453026ccc63db149091a419fffd6421556e91ea638d95afab5044bd8c2f
167568a46af1d76c2d935aa7576fbf8bdb1f17a7e6786d65d4617 S700_011.iso

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

127f3757d2fced8e36a8ce9299898d2fca643ff700fbe3b03921e1fe03f58d38

SIP Relay module sip-700_011-amd64.tgz (SHA512):

1d01fb6947f4e08b5f87984d2889e5fa1e7e444eb03f659865fa47cc0d502f733f6049383902
23e4441fcd9eedd0857206723e71bb3e95897e041f8ee5749e1b

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.

These 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.

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

5. Architectural Information

The TOE is the firewall system genuscreen 7.0 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 only 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 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 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 data flowing between several protected networks against unauthorised inspection and modification. It consists of software on at least two machines (genuscreen appliances) that 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. The firewall components 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. 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 TOE also includes a central component, the Management Server, to manage the firewall components (genucenter). Administrators can initialise and manage the firewall components using a graphical user interface (GUI) for the Management Server. The GUI of the management server supports three types of user roles, i.e. Administrator, Revisor and Service User. 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 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.

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 and evaluator tests combined, all configurations of the TOE being intended by the current evaluation were tested or a rational for the validity of test results were provided.

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 these systems are used as data source and data sink, therefore they need wide 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. For testing a set of physical and virtual machines is used.

The Security Target specifies eight assumptions about the environment of the TOE: Assumptions A.PHYSEC, A.INIT, A.NOEVIL, A.SINGEN A.TIMESTMP, A.ADMIN, A.HANET and A.REMOTE_AUTH. A.PHYSEC, A.NOEVIL, and A.REMOTE_AUTH are not applicable to the test environment. A.ADMIN, A.INIT, A.SINGEN and 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. All configurations were loaded from CD respectively from USB.

For the most part the tests are automatically running under control of the configuration tool and further testing framework of the development and QS testing lab. The tools also provide the test results automatically. 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 provides configuration functions. Live tests are able to be performed on virtual machines as well as on real physical systems.

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

For the initial certification BSI-DSZ-CC-1085-2019:

The test equipment provided by the developer consists of several different firewall components of different Hardware models, a CommServer (genuscreen XS) and two instances of the TOE (genucenter L as well as genuscreen S; genuscreen M; genuscreen L; infodas SDoT Server V3).

According to the Security Target, the evaluator installed the firewall components 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 firewall appliances and the management server were integrated via 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, a console access was activated on each appliance.

According to the assumptions identified in the Security Target the following is stated: A.PHYSEC, A.NOEVIL, and A.REMOTE_AUTH 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 of all security functions. The main focus was the implemented SIP Relay, the management system, cryptographic functions, random number generator (RNG) and its entropy source (part of OpenBSD kernel) functions.

The repetition of the developer testing was performed in the developer laboratory.

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

For this re-certification:

Independent testing was performed at the developers site. Because of the slight adaptions of the TOE compared to the last certified version, only a sampling of relevant tests were performed.

The sampling of the tests was performed on revision 3 of a genuscreen S and a genucenter L. Revision 2 was tested in the last certification in BSI-DSZ-CC-1085-2019.

The main focus of testing was the verification, installation and configuration of the updated SIP relay, and the installation and verification of the genucenter and genuscreen software.

Furthermore a sampling of developers tests were repeated in this test meeting for genuscreen S and genucenter L. By repeating the tests, the proceeding and results of the provided developers tests could be checked. The developer tested all hardware revisions in his developer testing.

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

Penetration Tests

For the initial certification BSI-DSZ-CC-1085-2019:

The evaluator has done an independent vulnerability analysis. As a result, additional 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, with all measures required by the developer applied.

For this re-certification:

A rational was provided to show that the full vulnerability analysis of the initial certification remains valid. Vulnerability tests have been performed as well. The focus of these vulnerability tests were the updated SIP relay, thereby the SIP relay tests of the last evaluation were repeated.

No attack scenario 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 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). An SBC is another network device and is not a part of the TOE. The SIP relay is not included in the basic installation image but must be installed as an optional module at the genucenter and deployed on the genuscreens.

The connection between genucenter and genuscreen is encrypted with SSH.

All HW and the platform OpenBSD Version 6.1 (in case of genucenter Management System) resp. Version 6.2 (in case of genuscreen Firewall Components), 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 1.4.10, several functions (such as CryptoCard, VPN to Other Appliances or Mobile Clients, L2TP VPN, IKEv2/MOBIKE VPN, Dynamic Routing, genucenter HA, Remote Maintenance, genucenter REST API) 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]).

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.

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 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.

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, too.

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 genuscreen Installations- und Konfigurationshandbuch [9] and genucenter Installations- und Konfigurationshandbuch [8] and to follow all requirements for the environment described in the Security Target. Especially all recommendations regarding configuration of packet filter in combination of 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 D “Vorgehen bei Verlust einer Appliance”. Using SNMP, the recommendations in chapter 6.4.2 “SNMP-Trap” should be followed. Before installation the checksums of the software has to be verified, see genucenter manual chapter 2.1.4 “Verifizierung der Software” respectively genuscreen manual chapter 2.9 “Verifizierung der Software”. This integrity verification includes the optional SIP module.

The assumptions to the IT environment in the Security Target state 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 backup 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 with solid knowledge about networking (especially IP and TCP/UDP), packet filter firewalls and secure use of public key procedures.

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

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

genucenter backups have to be stored in a secure place. Recommendations are addressed in chapter 2.5 of the genucenter manual.

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
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
USB	Universal Serial Bus

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-1142-2020, genuscreen 7.0, Version 7.0.15(8ef848c), Date: 2020-07-17, genua GmbH

[7] Evaluation Technical Report BSI-DSZ-CC-1142-2020 for genuscreen 7.0 from genua GmbH, Version 2, Date: 05.08.2020, secuvera GmbH (confidential document)

[8] Guidance documentation for the TOE, genucenter Installations- und Konfigurationshandbuch; Version 7.0, 25. März 2020, Revision: cbb982ec, genua GmbH

[9] Guidance documentation for the TOE, genuscreen Installations- und Konfigurationshandbuch; Version 7.0, 25. März 2020, Revision: cbb982ec, 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

C. Excerpts from the Criteria

CC3.1 R5

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 detailled 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