Federal Office
for Information Security

Assurance Continuity Maintenance Report

with partial re-evaluation applying ALC_PAM for patch management

BSI-DSZ-CC-1194-2023-MA-01

genuscreen 8.0 as part of genuscreen8.0p15/genucenter 8.0p7/SIP Relay module 8.0p15

from

genua GmbH

SOGIS
Recognition Agreement
for components up to
EAL 4

The IT product identified in this report underwent a fast track ALC_PAM assurance continuity process derived from the procedures on Patch Management Extension [1] and on the base of the developer's Impact Analysis Report (IAR) and Security Relevance Report (SRR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under the certification ID BSI-DSZ-CC-1194-2023.

The assurance statement as outlined in the Certification Report BSI-DSZ-CC-1194-2023 dated 06. April 2023 is of relevance and has to be considered when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-1194-2023.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Common Criteria

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

Bonn, 17 November 2023

The Federal Office for Information Security

Identification of the TOE

The Target of Evaluation (TOE) is called:

genuscreen 8.0 as part of genuscreen8.0p15/genucenter 8.0p7/SIP Relay module 8.0p15

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, 3 and 4), genuscreen M (revision 2, 3 and 4), genuscreen L (revision 2, 3 and 4), genuscreen XL (revision 2, 3 and 4), cryptOHBguard, infodas SDoT Server V3B Management Server genucenter: genucenter S (revision 2, 3 and 4), genucenter M (revision 2, 3 and 4), genucenter L (revision 2, 3 and 4)	N/A	Hardware (not part of the TOE)
2	SW	genuscreen Installationsmedium Version 8.0	8.0p15	CD-ROM / USB image
3	SW	genucenter Installationsmedium Version 8.0	8.0p7	CD-ROM / USB image
4	SW	SIP Module, sip-800_011-amd64.tgz	8.0p15	TGZ archive
5	Doc.	genuscreen Installations- und Konfigurationshandbuch Version 8.0, Ausgabe 10. Oktober 2023, Revision: 19f041c4 [8]	8.0	Secure PDF download
6	Doc.	genucenter Installations- und Konfigurationshandbuch Version 8.0, Ausgabe Ausgabe 10. Oktober 2023, Revision: 19f041c4 [9]	8.0	Secure PDF download
7	Doc.	Lizenzschreiben	N/A	Letter

Table 1: Deliverables of the TOE

The hardware of the TOE (not part of the TOE) is mainly composed at the supplier company “Pyramid Computer GmbH” and “Embedded Brains” 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 SHA-256 checksums are provided on the genua-webserver after a login.

The valid checksums of the TOE are:

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

```
8c21dd31825f2649ea5dcb5cb52644974669e7418a383c86b2bd90b2245622ba appsoft.tgz
f75ce7cc2954ec982c62b6d617c4223301a69f8c956e0ea26f250735dcdb1321 base.tgz
63140e73b3d08a8477686f472310bd8284e03fde082bba7b014f544edacf386e center_assets.tgz
92b8bdd4a697ac7f7621786268176eb99121203b4764e8b01a72de24010873e0 center.tgz
2338bbfa9c692d39ffe0039a571e85575f641739f3850083af4439281bfc8171 comp.tgz
dc8d4a842a479fbc7160bfb111e6ccebf135fcebd278f1688cdbee392b9803fc etc.tgz
e3828c3c458ba15e3236f4d856e765a411015cd82462fb29828cfbc340e71b3a firmware.tgz
18f976ab35ef678bb26220fead6fdc774554c939226bf155ae9f91a962e3e3f9 gems.tgz
1144666c4e753ceb19e381ad1c1a6ff47275b9b04b8d2b51470ecdd07566f4c8 genuos_center.tgz
ec1cac9124e67e9e399160a5b5359ca6a56eb089dcc3f70a1345718c7d667913 ports.tgz
fa1a60ed3501fa88f2b98b9d239b86d3ca5e926c22c790de7781e58445f70d9b Z800_007.manual-
zert.de.pdf
```

genucenter USB- and CD-Image (SHA256):

```
09c1e99130ff63fd0a72a02e8bcad0573a808b39b289874736804becb7739fdb Z800_007.img
8e02824f955053df28d1d8a2e6b2cb399c0244a0e75063430c7756ca216cca91 Z800_007.iso
```

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

```
ee38a36d797ea228ab78f06bb0478f5e30eed0a7deb37b2c75653ed4b2fbcecc bsd
0adc49fbd117b308db127e5ab37c3f138a87242329db5421b47574606425e186 bsd.i386
9e19f82645613b10ade0659c7772d037cf0a43e7a171e8598e45e03fb2048775 genuscreen-800_015-
handbuch-zert-de.pdf
```

genuscreen USB- and CD-Image (SHA256):

```
33f27b5de286911c24ce57f261ccdbba6326c9ccf8457abfa03a102a5b12a4ca S800_015.img
b2ed8e40884cc2524b52b14f29b9746261a264114b451f148f66223281ab2f94 S800_015.iso
```

SIP Relay module (SHA256):

```
980609017a902b32135f4dff3b5c6a814aa40adfcc30afcb48c658bf1137c419 sip-800_015-amd64.tgz
```

Assessment of Changes

The IT product identified in this report was assessed according to the procedures derived from the procedures on Patch Management Extension [1], the Impact Analysis Report (IAR) [2] and the Security Relevance Report (SRR) [3]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [4], its updated Security Target [6] and the Evaluation Technical Report [5].

Since the document on Patch Management Extension [1] may not be final at this point in time, the actually applied Evaluation Methology for ALC_PAM is documented in the ST [6], annex A.

The vendor for the genuscreen 8.0 as part of genuscreen8.0p15/genucenter 8.0p7/SIP Relay module 8.0p15, genua GmbH, submitted an IAR [2] and SRR [3] to the BSI for approval. The SRR is intended to satisfy the requirements according to the procedures on Patch Management Extension [1] by describing the security relevance of all product changes and patches by their topic, their description, their options for mitigations, their related changes and their security impact.

The genuscreen 8.0 as part of genuscreen8.0p15/genucenter 8.0p7/SIP Relay module 8.0p15 implements the following changes:

- Support of new hardware revisions 4.0, and infodas SDot Server V3B,
- added security patches,
- minor functional changes with no relevance to developer documentation and guidance.

The following documents were changed:

- Security Target [6], only version changes, changes of the hardware revision and some editorial changes were performed.
- In the guidance “genuscreen Installations- und Konfigurationshandbuch” [8], only version changes regarding patch level 14 were updated.
- In the guidance “genucenter Installations- und Konfigurationshandbuch” [9], only references were updated.

The TOE and product versions changed as several patches were published for the TOE:

- genuscreen 8.0p11 to genuscreen 8.0p15,
- genucenter 8.0p5 to genucenter 8.0p7,
- SIP Relay module 8.0p11 to SIP Relay module 8.0p15.

The ITSEF conducted testing. The goal of the testing was to test the basic features of the TOE, to include changed test cases, and to include the new hardware revisions. Therefore a sampling of previous testcases as well as the execution of partially changed test cases was conducted. During that testing all tests passed successfully.

The ITSEF has updated their vulnerability analysis in order to confirm that the initial assurance statement is still valid. This included selected penetration testing as well as an analysis of possible publicly known vulnerabilities.

Obligations and notes for the usage of the product:

The documents as outlined in table 2 of the Certification Report [4] i.e. their updated versions according to this addendum 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 referred to in chapter 9.2 of the Certification Report [4] has to be considered by the user and his system risk management process.

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.

All obligations and notes for the usage of the TOE as given in chapter 10 of the Certification Report [4] remain valid.

Conclusion

The assurance statement as outlined in the Certification Report BSI-DSZ-CC-1194-2023 dated 06. April 2023 remains valid, considering the changes as described in this addendum.

This report is an addendum to the Certification Report [4].

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.2, 30 September 2021

Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.0, November 2019

[2] genuscreen 8.0 Impact Analysis Report, 2023-08-11, Version 8.0.3 (db02639), (confidential document)

[3] SRR: Zertifizierung genuscreen 8.0 Security Impact Analysis Report, 2023-10-11, Version 8.0.5 (1127e72), (confidential document)

[4] Certification Report BSI-DSZ-CC-1194-2023 for genuscreen 8.0 from genua GmbH, Bundesamt für Sicherheit in der Informationstechnik, 6 April 2023

[5] Evaluation Technical Report BSI-DSZ-CC-1194-2023-MA-01 for genuscreen 8.0 from genua GmbH, Version 1, Date 30.10.2023, secuvera GmbH (Confidential document)

[6] genuscreen 8.0 Security Target, 2023-10-10, Version 8.0.10 (7bdd69b)

[7] Archiv von Konfigurationslisten alccms-2023-10-12.tgz, Date 12.10.2023 (confidential document)

[8] Guidance documentation for the TOE, genuscreen Installations- und Konfigurationshandbuch; Version 8.0; Ausgabe 10. Oktober 2023, Revision 19f041c4, genua GmbH

[9] Guidance documentation for the TOE, genucenter Installations- und Konfigurationshandbuch; Version 8.0; Ausgabe 10. Oktober 2023, Revision 19f041c4, genua GmbH