Federal Office
for Information Security

Assurance Continuity Maintenance Report

with partial re-evaluation applying ALC_PAM for patch management

BSI-DSZ-CC-1154-2023-MA-01

genugate 10.0 p14 Firewall Software

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-1154-2021.

The assurance statement as outlined in the Certification Report BSI-DSZ-CC-1154-2021 dated 22 June 2021 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-1154-2021. The validity of the certificate will not change.

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, 25 September 2023

The Federal Office for Information Security

Identification of the TOE

The Target of Evaluation (TOE) is called:

genugate 10.0 p14 Firewall Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	genugate firewall	10.0 p14	Install image
2	SW	genugate platform	10.0 p14 Z	Install image
3	DOC	genugate 10.0 Z, Installationshandbuch, Version 10.0 Z Patch 014, Ausgabe Mai 2023, Revision v10.0p14-RC1, [8] genugate 10.0 Z, Administrationshandbuch, Version 10.0 Z Patch 014, Ausgabe Mai 2023, Revision v10.0p14-RC1, [9]	10.0 Z Patch 14	Manual (German version)

Table 1: Deliverables of the TOE

Please note that the TOE genugate 10.0 p14 Firewall Software is part of a larger product, the firewall genugate 10.0 p14 Z, which consists of hardware and software.

The Hardware components genugate S, the genugate M, the genugate L, revisions 2.0, 3.0 and 4.0 as well as the infodas hardware SDoT Server V3B are part of the evaluated and certified configuration of the TOE but they are not part of the TOE.

The valid checksums of the TOE are:

ISO-Image:

SHA256(G1000_014.iso) =
bc56ffd6164dc50ff94e9aa07a18c2e6e361dc089e81f0af95e4233697789d20

SHA512(G1000_014.iso)=
43dd87ecbc1619d996f6648a60fa098efd1446b3d5887cc4f3b4c266a60af125072f0a725023de7d
7dc53a486dd5da27ef75ce536dcb751cdba7b5461dee7863

USB-Image:

SHA256(G1000_014.img) =
47218699d28880555ed6235e421c4999db75570f8869fbf4ea0d06f67597d7a8

SHA512(G1000_014.img)=
21c7b75f94bc8c12cfb8f2162b9a1e6adb9875be40afe68858c194f22c9a93bb347d1bc683ed7ed6
84aaadc8b6c174541315379eaf14d349ad642901df116da4

Installation packages in folder /6.6/amd64/:

SHA256(CKSUM) = 417052e8d4bf9ec7d0c7f8e43ffee7758fcc9917b725297971ecd2bc1faa82fc

SHA256(INSTALL.amd64) =
4058fdd5e7b568083cd8e3f53ed920000a119c5f353ea4da5e91de8e20bdfb88

SHA256(RMD160) = 804fec608443ff19ffdfe8b2a48b5882160aad0dba60eca64f7fa8902cbbecac

SHA256(SHA1) = a31cf47938105da45418e4557d4649f9413d9f168e9c64b57ec2e0a1f80812a6

SHA256(SHA256) =
6786daa2971f8b9f3bae201c69ecc30fba0b63b144d51012cec4c86499776c33

SHA256(SHA512) =
3630d39a23434b1481370e29364eb7ecb9de65a57609de946515df747de454a1

SHA256(base66.tgz) =
c3cfc79ac7df12d5568c3735a36ae6f53fd506d8c1a8d3e42ec544d2542dcf93

SHA256(boot.catalog)=
ecaa855c8a90194dab2bd91dacda98a708cb5aca53d5112db3d7937dbaf45d1d

SHA256(cd66.iso) =
b0ed49498badc96dd8b13ccaa7f83897989315861575 61af482828aa51556141

SHA256(cdboot) =
4e1a424559d9ecab37ec416d93a0a1cfecb87b0f3d5af3d576575e5f16860172

SHA256(cdbr) = 4e6948cb3fb8a10ba98d1033648b32ca22b7011f44c4f11d95bd9e63be444261

SHA256(comp66.tgz) =
ff040ca845f44f0ed60003281ec20b891fcd3a5a8e7676f516a21256b80a8fec

SHA256(efi.img) = c4754731839f73f3c182634e89cf8871ff00b8f536d7011f8c798c0df9f58d99

SHA256(etc66.tgz) =
08dcda5af9b1f3f57e10b72e4b413eb5e14bc4c099f5252f5ce2b721d196cbb0

SHA256(game66.tgz) =
8c839ddfb0ca9ec99a2b1f78a1a441305ac3202ea2cade54c595de43d7346929

SHA256(index.txt) =
8d8cea529491d502b19f331533a3d4dfc769001436ed42518b616c4e5dbcfef1

SHA256(kernel66.tgz) =
68000b4349c794713f7a68dcce4f6a1d44611f2b963f599e25865e7f3d6c846a

SHA256(man66.tgz) =
43a6fbf7555f9312a7a8a2228c077631a1802ecb514b4a2e07ef855002f3de8f

SHA256(pxeboot) =
18ede940f9bab1cd50ab1a6093b061bf3e342ec57de0c17a2d7f1898d1fc7c26

SHA256(xbase66.tgz) =
d08656ecdd99273e7d56048b86043b60c919d215dd643809fed48396211b589e

SHA256(xetc66.tgz) =
f4ad5ed9301c619930e4b31cbc328218762b53a28e4a1d00d300858184c812c6

SHA256(xfont66.tgz) =
96a2b8cf159c7c634d3b788213d95cae2bbde0505a106b281f7ec9e3d5b9ab5c

SHA256(xshare66.tgz) =
8b082a1370d9d2602fdd3f1f729eaf26f86b85bb8702fdd71bf91fed9bd413f3

SHA512(CKSUM)=
0d7601604ac5ef0ea6f046f10f492e3f06c537cf2de8e08bb50788f5bf6e8c5cabf10cd265fb5f7913e
b1b6264fdb5b638e10b8f56d508e56b1a2a636068ac29

*SHA512(INSTALL.amd64)=
62026c6ec29279def7d7b2a11c29ff5cd28873747c2efe9a3561aef09e97aff7c0ed6a5d20c380f55
820fade1420c72e398b2569d4599b070f89de5d4fcbdde1*

*SHA512(RMD160)=
5d5ca2c2ebee4111bfa5e8520e87f09cfe6ce0c35c738e2ca72b23fb6ec4a3779f27b45e18e1e225
a09968cf81901ca61258035124d804ec94c45d0d81540d1c*

*SHA512(SHA1)=
e59c4ad9d79acf4ba98e6460412e73ef8a508911ee9ee58efe953afef82a25888d6d4e89a2ba6a6
21091464b6cdf2fc054453dca6642ce284cb488fa4fc4a632*

*SHA512(SHA256)=
40402bf27fc6aea424c5a5471ef98b5bab56329ec77232b6b4b52f243eebb8d95e7c25ac98d300f
556874fc3566579f213b7c4fe606e69ec9e5cdb929f7336fa*

*SHA512(SHA512)=
54c9858e50ebf7c124acf2e65da89a9026a53c15036fbb4a7a0ffeffb08effd85e69627e5f2cc7e270
4f4b0d0e767b01f8490496970eca6cceaeb6eb7d060946*

*SHA512(base66.tgz)=
eef40f0f69fd182433bc950ce7d93948b58292887863fd05a863c90b8994db3f712415511119a9a4
0b8722ad91bb2935aa2858b28991d469b2aa4352717de1dd*

*SHA512(boot.catalog)=
5824f2529aef42aca6743d5ef4307e5da2dc6829251a94027e00346be0894cb8361b4a52d1708e
1cf9d242a71243e500ea063a649300f8512d9a54316b240e6f*

*SHA512(cd66.iso)=
f91c50cd61ae1822048dd62c07fbafd61e1a5c4277188255afba29e3a220f9ae6780f61b542ca51f
87ff275399d640a65690ea921b37bd91c94bc711bb1e3874*

*SHA512(cdboot)=
cce59f3c9a8cb8df6561622358bf7b897cc5014c0c68bdfb0f1a94f62ab4975781951a888be76fce5
cd0d276507beb7a098aaa4461655e201193c6101cf8bba7*

*SHA512(cdbr)=
7a1c20a96abcdad54bdcddd315949907bb7de36f8f09c041cfe78c23dd0f9d9e2498b570cbcaf3d6
703a67dfbe2a4fbfa486a754078da93d6b691de11213498d*

*SHA512(comp66.tgz)=
8d375e9f512b5fad9431dad33c21fc59eba034f48b3ded94b6e1fe028016212dcfde96bb01b38bf2
5ee33edc8ca603a72aec592b99c03e8a6233e98d71aae0e6*

*SHA512(efi.img)=
dce685ef520780372d30ff0e5344bb5b8cd30b68b30db97bdd058aa6f102b3df217c1c438f0a68d3
e616d82ca185f7310e4f8c2b414aa44efa3957246db38986*

*SHA512(etc66.tgz)=
ca27249618c12a357c30cf4b5b43910091180f4a563ab5dd12e5fc124055ceac417b8e270c4ca7e
4c709099ff85be545abc191b8803a4f11db5dabbecc464eba*

*SHA512(game66.tgz)=
a05a5744ba65353d5af2b9fc2d51a2ab3f0bc709ca246ea253c3ccc79a5c0701f89ddd6df9498f8af
82ca42e4b8b16759ebeade12a2affababbea9b289f6266a*

*SHA512(index.txt)=
3bdf719553754ef402e973c6c36a214abd79ddf524319e5ff5e8c490eab93ac565278628343e1a4
d1026a3f84e2b98da198e543481fbc51693fac3480dd4f4f0*

SHA512(kernel66.tgz)=
5a66378c4680f392802d7c5315e53432bea8035050190350dae7d065e10fb9bde6981b163f80bb9a689f5e3c519609ecc003f3fdf874ed08e076eb9292b6715a

SHA512(man66.tgz)=
cefb43ced25c75b6e83675ab2887fb196a6515401073d39952f0720cfbf540005e826fa93c79a97e7373430ff8e0a9e2de0277ca45a455938e62269784f0eadf

SHA512(pxeboot)=
573e28152973199d61cbac895c7163383a98f8a9d8dc9947c40b686f3560b1b4aa28f5987c8457813a067ef334d07540e8f6edd80164c4d2da8fc3fa1e26a938

SHA512(xbase66.tgz)=
3432b412b675706efe33e70216906ae9c8f059d617c4d8db4e75d6525f0e8b6b0f32733514a93fcc5c764901e130f2f02524e379143a8b015ebe574fae05ed48

SHA512(xetc66.tgz)=
d6829a3847be70e4ed1287667d8b8b326a3675ce5bb9e7f689d96ae77cf202a0b5b59ddeb0adc19c21972b6511453a2bb8c4c1cf749c43306659b650debcec2b

SHA512(xfont66.tgz)=
fa667f49dbdc1addfa3ebef69e9477ddc3f99e974f5d0e564c40e199e18612d0e907b47c5d1d2b257915a0fb6e794ef8fda67c7f92d25351d4802774aadf40ab

SHA512(xshare66.tgz)=
8617fa967ca5f92db98d3259e1dadff28c0767f2dd64bd941709d6ea0b8317b366fda8f4102a68204b0625170be0deb7a72adfb7f8cd4c4cbd9549357c32acda

Documentation:

SHA256(genugate-1000p14-admin-de.pdf) =
c2c32f0554c5c98b66caabb631436e349c67f82547b0d29d0df3f4621817be61

SHA256(genugate-1000p14-install-de.pdf) =
d41efefe0bec27a862b0c9b00cd971038b1c3c371333e07e2d0a75c20b3a62b2

SHA512(genugate-1000p14-admin-de.pdf)=
1dbf3ff0f6f0fbc7559a22ae742860d6cba52d5ba856a68dd6e7f5dbbbcf85df7e9f3c39c6e091312f45e01d061649b6aa2edbdacd4b4ac93c940c7a5cfcde9e

SHA512(genugate-1000p14-install-de.pdf)=
6df0b1df817205afa43866df143e2fac5948cf09d6f18b7f2e9bc0ebbfce64aaf1e95abdcc0d1598a0bf3efb00dfbd3fda0f36b4db9ed5d7a1556d052e69afcb

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 genugate 10.0 p14 Firewall Software, 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 genugate 10.0 p14 Firewall Software implements the following changes:

- Support of new hardware revisions 4.0, and Infodas SDot Server V3B,
- added security patches,
- minor functional changes,
- renewed Site audit with changes in the development environment.

The following documents were changed:

- Security Target [6], only version changes, changes of the hardware revision and slight grammar changes were performed.
- In the guidance “Administrationshandbuch” [8], only version changes regarding patch level 14 were updated.
- In the guidance “Installationshandbuch” [9], only references were updated.

The ITSEF conducted testing. The goal of the testing was to test the basic features of the TOE, to include changed or newly designed test cases, and to include the new hardware revisions. Therefore a sampling of previous testcases as well as the execution of changed or new 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 outlined in chapter 9 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.

For the hardware genugate M in revision 4 that was shipped before 6th July 2023, a BIOS update needs to be installed with developer support.

For a secure operation it is necessary to follow all recommendations of the genugate Installationshandbuch [9] and genugate Administrationshandbuch [8] and to follow all requirements to the environment described in the Security Target.

Plausibility of the information about existing bootinstall scripts have to be checked by an administrator each time before booting genugate.

External authentication servers are subject to the same organizational and physical restrictions as the product genugate.

The administrator should activate logging/accounting for services (relays) and regularly check (recommended: daily) these logs for service (relay) abuse (e.g. in case of DoS attack).

The assumptions to the IT environment in the Security Target suppose that the TOE operates in a physically secure environment which prevents access from unauthorised users (OE.PHYSEC). This assumption includes the protection of the hardware and PFL USB stick. USB stick has to be protected against theft, exchange and manipulation and it has to be made sure that the PFL will be only booted with the assigned USB-memory-stick. This aspect has to be considered in a defined security policy (A.POLICY).

Configuration backup files have to be kept logical and physical secure as the TOE including the hardware.

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

The administrator GUI must only be accessed from the administration interface.

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

Finally, please note that the product is designed to run on multiple other hardware versions and revisions to maintain a wide usability, however, the evaluation and certificate concentrated on the latest HW versions and revisions that are mentioned in chapter 2 of the Certification Report [4] and in this addendum on page 2, chapter “Identification of the TOE”.

Conclusion

The assurance statement as outlined in the Certification Report BSI-DSZ-CC-1154-2021 dated 22 June 2021 remains valid, considering the changes as described in this addendum.

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

References

[1] Technical Specification ISO/IEC DTS 9569, Final Draft, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045, Reference number ISO/IEC DTS 9569:2023(E)

[2] genugate firewall 10.0 p14 Impact Analysis Report, 2023-06-02, Version 10.0.4 (47f1694), (confidential document)

[3] SRR: genugate firewall 10.0 p14 Security Impact Analysis Report, 2023-06-02, Version 10.0.3 (8a7fc6b), (confidential document)

[4] Certification Report BSI-DSZ-CC-1154-2021 for genugate 10.0 Firewall Software from genua GmbH, Bundesamt für Sicherheit in der Informationstechnik, 22 June 2021

[5] Evaluation Technical Report BSI-DSZ-CC-1154-2023-PM-01 for for genugate firewall 10.0 p14 from genua GmbH, Version 3, Date 15.09.2023, secuvera GmbH (Confidential document)

[6] genugate firewall 10.0 p14 Security Target, 2023-06-01, Version 10.0.11 (4a78d09)

[7] Archiv von Konfigurationslisten, alccms-20230602.tgz, Date 02.06.2023 (confidential document) (Confidential document)

[8] genugate 10.0 Z Administrationshandbuch, Ausgabe Mai 2023, Revision: v10.0p14-RC1

[9] genugate 10.0 Z Installationshandbuch, Ausgabe Mai 2023, Revision: v10.0p14-RC1