Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1216-V2-2026-MA-01

secunet eID PKI Suite Certified CA Kernel SC Version 4.1.0

from

secunet Security Networks AG

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the procedures on Assurance Continuity [1] and the developer's Impact Analysis Report (IAR). 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 BSI-DSZ-CC-1216-V2-2026.

The change to the certified product is at the level of minor changes. The identification of the maintained product is indicated by a new version number compared to the certified product.

Considering the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-1216-V2-2026 dated 11 February 2026 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-1216-V2-2026.

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

Bonn, 25 June 2026

The Federal Office for Information Security

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 99 9582-0 - Fax +49 228 9582-5477 - Infoline +49 228 99 9582-111

Assessment

The IT product identified in this report was assessed according to the procedures on Assurance Continuity [1] and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [3], its Security Target and the Evaluation Technical Report as outlined in [3].

The vendor for the secunet eID PKI Suite Certified CA Kernel SC Version 4.1.0, secunet Security Networks AG, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements according to the procedures on Assurance Continuity [1]. In accordance with those requirements, the IAR describes (i) the changes made to the certified TOE, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The secunet eID PKI Suite Certified CA Kernel SC Version 4.1.0 was changed in the following details:

- Adapt XMSS key generation to new Utimaco version
- Integration of new SmartCard-Stack
- Block CMP requests which contain the badger OID in the ExtraCert
- PreGen Tool for hybrid hsm handler

Configuration Management procedures required a change in the product identifier. Therefore the version number changed from Version 4.0.0 to Version 4.1.0.

The Security Target [4] was editorially updated [7].

Some TOE deliverables in table 2 of the original Report [3] have been updated.

The following table outlines the changed TOE deliverables:

No	Type	Identifier	Release
1	SW	Certified CA Kernel (zip file) Secunet_eID_PKI_Suite_CertifiedCAKernel-x_y_z.zip that contains the following items:	4.1.0
2	SW	JAR archive with the Certified CA Kernel functionality, CertifiedCAKernel.jar SHA256: dbadd119336315ac9be334b5cfd6a8f3d551d6fc29be627fd818079d347fceb7	4.1.0
3	SW	JAR archive with the SinacardHandler functionality HSMHandlerSinacard.jar SHA256: 473110623b32db35d5c67123ecb6bfc8270b8e000c3b822737339d5c1bd441f4	4.1.0
4	SW	JAR archive with the HybridHandler functionality HSMHandlerHybrid.jar SHA256: 811ca718d55a3bb1808ab57b30a6f5df840e8c54cd277696db335a2589254fc6	4.1.0

No	Type	Identifier	Release
5	SW	Batch file with bootstrapping functionality for Windows bootstrap.bat SHA256: 4BDB1533A2377405F86C4A5A1EDBCCECF303E2B35EAAFF273F3DD9132D450E2F	4.1.0
6	SW	Shell file with bootstrapping functionality for Linux bootstrap.sh SHA256: 0CD8097E5CCE64D15B1F50AD22E1A9C481BA81D4BB89EFADC00E512876563B49	4.1.0
7	SW	Shell file with the key pregeneration tool for Linux PreKeyGenerationTool.sh SHA256: 1DEF4A65E413F1F5CA485007BECD945440A0BED629E056EF779ADCAF4AB0EB4B	4.1.0
8	SW	Batch file with the key pregeneration tool for Windows PreKeyGenerationTool.bat SHA256: B9F369EDC3DEE81C33C8ED2B9D9E2DBDC1D50BE0611D5F4A716F743FEF9685E1	4.1.0
9	DOC	Manual including API documentation: Manual Certified CA Kernel.pdf [6] SHA256: 88adb41863239bf82847a9fa9036d73922ee6e9b47c0e02160516b00938a82a9 Javadoc-api: javadoc-api.zip [8] SHA256: 0bc7a213e9ae7325f75421b3bd2003efe8e1d138e17f40243eb3ad87a5727340	4.5.2
10	DOC	Release Notes (information about TOE changes, bugfixes etc.): ReleaseNotes.pdf [9] SHA256: 4815988b03cebd10135c70de0206355843e9a54b5e7ac6be1ad64d0f617b4544	4.1.0
11	DOC	Security Target: secunet eID PKI Suite Certified CA Kernel Security Target [7] SHA256: 270adfee7d79a8d6f2faa591844d3c467e3988b9d0c4c4f0bf024996b0d523b5	3.7.2

Table 1: Deliverables of the TOE

Conclusion

The maintained change is at the level of implementation. The change has no effect on product assurance, but the updated guidance documentation [6] has to be followed. [5], [8] and [9] have been updated as well.

Considering the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-1216-V2-2026 dated dated 11 February 2026 is of relevance and has to be considered when using the product.

Obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies 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 for the TOE is required and thus requested from the sponsor of the certificate.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG[1] Section 52, Para. 4, Clause 2).

For details on results of the evaluation of cryptographic aspects refer to the Certification Report [3] chapter 9.2.

This report is an addendum to the Certification Report [3].

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBl. 2025 , no. 301, p. 2

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 3.1, 29 February 2024

Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.2, March 2024

[2] Auswirkungsanalyse Certified CA Kernel Version 4.1.0, Version 1.9, 02.06.2026, , secunet Security Networks AG (confidential document)

[3] Certification Report BSI-DSZ-CC-1216-V2-2026 for secunet eID PKI Suite Certified CA Kernel,Version 4.0.0, Bundesamt für Sicherheit in der Informationstechnik, 11 February 2026

[4] Security Target BSI-DSZ-CC-1216-V2-2026, Version 3.6.10, 21.12.2025, secunet eID PKI Suite Certified CA Kernel SC Security Target, secunet Security Networks AG

[5] Configuration list for the TOE, Version 1.9.7, 22.06.2026, Konfigurationsliste ALC_CMS.4, cms_secunet+eID+PKI+Suite_V.1.9.7.pdf, secunet Security Networks AG (Confidential document)

[6] Guidance documentation for the TOE, Version 4.5.2, 21.05.2025, Handbuch (AGD_PRE.1 und AGD_OPE.1), agd_secunet+eID+PKI+Suite_v4.5.2.pdf, secunet Security Networks AG

[7] Security Target BSI-DSZ-CC-1216-V2-2026-MA01, Version 3.7.2, 22.06.2026 , secunet eID PKI Suite Certified CA Kernel SC Security Target, secunet Security Networks AG

[8] API Documentation (JavaDoc), Version 4.1.0, Mai 2026, javadoc-api-4.1.0-473a00.zip, secunet Security Networks AG

[9] Release Notes, Version 4.1.0, 27.05.2026, ReleaseNotes.pdf, secunet Security Networks AG