Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1098-2020-MA-02

IDEMIA_HC_Germany_NEO_G2.1_COS, V1

from

IDEMIA Germany GmbH

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the procedures on Assurance Continuity [1]. 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-1098-2020 updated by BSI-DSZ-CC-1098-2020-MA-01.

The certified product itself did not change. The changes are related to supplementary security requirements added to the scope of the certificate concerning the secure usage of the TOE's cryptographic functionality.

Considering the nature of the change leads to the conclusion 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-1098-2020 dated 30 July 2020 and subsequent Maintenance Report BSI-DSZ-CC-1098-2020-MA-01 dated 14 September 2021 in combination with the additional security requirements on the secure usage of the TOE's cryptographic functionality are of relevance and have 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-1098-2020 and subsequent Maintenance Report BSI-DSZ-CC-1098-2020-MA-01 and is compulsory to apply.

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

Bonn, 19 December 2024

The Federal Office for Information Security

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 +49 228 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]. The baseline for this assessment was the Certification Report and Maintenance Report of the certified product (Target of Evaluation, TOE) [2], its Security Target [3] and the Evaluation Technical Report as outlined in [2].

The certified product IDEMIA_HC_Germany_NEO_G2.1_COS, V1 itself did not change.

The changes are related to the following supplementary security requirements regarding the secure usage of the cryptographic functionality provided by the TOE:

- RSA key generation by using the TOE command GENERATE ASYMMETRIC KEY PAIR shall only be performed within trustworthy environments for that side channel analysis is excluded (e.g. secure personalisation environment under control of the personalisation agent).
- ECDSA signature generation by using the TOE commands PSO COMPUTE DIGITAL SIGNATURE and INTERNAL AUTHENTICATE shall not be performed in operational environments, frameworks, systems and/or applications where resistance towards side channel attacks on the private signature key used for such commands is required or such side channel attacks on the private signature key are not excluded by suitable technical or organisational security measures.

Conclusion

The maintained change is at the level of supplementary security requirements added to the scope of the certificate concerning the secure usage of the TOE's cryptographic functionality. The change has effect on product assurance and has therefore to be followed.

Considering the nature of the change leads to the conclusion 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-1098-2020 dated 30 July 2020 and subsequent Maintenance Report BSI-DSZ-CC-1098-2020-MA-01 dated 14 September 2021 in combination with the additional security requirements on the secure usage of the TOE's cryptographic functionality as outlined in section 'Assessment' of this report are of relevance and have 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 [3] not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

Some security measures are partly implemented in this certified TOE, but require additional configuration, control or measures to be implemented by a product layer on

top, e.g. the Application Software using the TOE, or fulfilment of corresponding suitable assumptions to be provided by the TOE's operational environment.

For this reason the TOE includes guidance documentation which contains obligations and guidelines for the developer of the product layer on top how to securely use this certified TOE and which security measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE.

Supplementary security requirements regarding the secure usage of the TOE's cryptographic functionality are specified as follows:

- RSA key generation by using the TOE command GENERATE ASYMMETRIC KEY PAIR shall only be performed within trustworthy environments for that side channel analysis is excluded (e.g. secure personalisation environment under control of the personalisation agent).
- ECDSA signature generation by using the TOE commands PSO COMPUTE DIGITAL SIGNATURE and INTERNAL AUTHENTICATE shall not be performed in operational environments, frameworks, systems and/or applications where resistance towards side channel attacks on the private signature key used for such commands is required or such side channel attacks on the private signature key are not excluded by suitable technical or organisational security measures.

The aforementioned security requirements supplement the security requirements and recommendations for secure use of the TOE as those are already provided by the TOE guidance documentation and in chapter 10 of the Certification Report [2].

In the course of the evaluation of a composite product or system making use of the TOE it must be examined if the required measures have been correctly and effectively implemented by the product layer on top.

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.

For details on results of the evaluation of cryptographic aspects refer to chapter 9.2 of the Certification Report [2]. However, the assessment of the TOE's cryptographic security functionality was partially changed in comparison to the previous certification [2]. For details please refer to the additional security requirements on the secure use of the TOE's cryptographic functionality for RSA key generation via the command GENERATE ASYMMETRIC KEY PAIR and ECDSA signature generation via the commands PSO COMPUTE DIGITAL SIGNATURE and INTERNAL AUTHENTICATE.

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 9, Para 4, Clause 2).

The obligations and recommendations for TOE usage as outlined in the Certification Report and Maintenance Report [2] and the TOE guidance documentation are still valid and have to be considered, but are supplemented by additional mandatory security

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

requirements on the secure use of the TOE's cryptographic functionality as depicted above.

This report is an addendum to the Certification Report and Maintenance Report [2] that is mandatory to be applied.

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] Certification Report BSI-DSZ-CC-1098-2020 for IDEMIA_HC_Germany_NEO_G2.1_COS, V1, 30 July 2020, Bundesamt für Sicherheit in der Informationstechnik

updated by the following Assurance Continuity Maintenance Report:

Maintenance Report BSI-DSZ-CC-1098-2020-MA-01 for IDEMIA_HC_Germany_NEO_G2.1_COS, V1, 14 September 2021, Bundesamt für Sicherheit in der Informationstechnik

[3] Security Target BSI-DSZ-CC-1098-2020, Security Target IDEMIA_HC_Germany_NEO_G2.1_COS, V1, Version 1.18, 3 July 2020, IDEMIA Germany GmbH (confidential document)

Security Target Lite BSI-DSZ-CC-1098-2020, Security Target Lite IDEMIA_HC_Germany_NEO_G2.1_COS, V1, Version 1.05, 2 July 2020, IDEMIA Germany GmbH (sanitised public document)

Note: End of report