Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1145-2021-MA-01

CryptoServer CSPLight, Version 1.0.2

from

Utimaco IS GmbH

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 2.1, June 2012 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-1145-2021.

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

Consideration of 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-1145-2021 dated 01.04.2021 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-1145-2021.

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

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

Bonn, 5 November 2021

The Federal Office for Information Security

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 *Assurance Continuity: CCRA Requirements* [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 CryptoServer CSPLight, Version 1.0.2, Utimaco IS GmbH, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements outlined in the document *Assurance Continuity: CCRA Requirements* [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 CryptoServer CSPLight, Version 1.0.2 was changed due to requirements from TR certification and recently discovered non-security related bugs. Configuration Management procedures required a change in the product identifier. Therefore the version number changed from 1.0.0 to 1.0.2.

TR certification related changes
The previously certified TOE is currently undergoing TR certification which required changes to the product. The vendor has since implemented these changes to comply with TR requirements. BSI supported by the ITSEF classified the changes as minor. The user guidance has been updated to reflect these changes.

Bug fixes
The TOE received bug fixes related to the Core and UI Logic Subsystems. BSI supported by the ITSEF classified the changes as minor.

The Security Target was editorially updated.

Conclusion

The maintained change is at the level of implementation representation. The change has no effect on product assurance.

Consideration of 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-1145-2021 dated 01.04.2021 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 [7] 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 9, Para. 4, Clause 2).

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

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

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

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] Impact Analysis Report CryptoServer CSPLight, version 1.0.3, 18 June 2021, Utimaco IS GmbH (confidential document)

[3] Certification Report BSI-DSZ-CC-1145-2021 for CryptoServer CSPLightVersion 1.0.0, Bundesamt für Sicherheit in der Informationstechnik, 01 April 2021

[4] Security Target BSI-DSZ-CC-1145-2021, Version 1.0.2, 18 March 2021, Security Target Lite for CryptoServer CSPLight, Utimaco IS GmbH (sanitised public document)

[5] CryptoServer CSPLight Configuration Management 1.0.3, 21 June 2021 (Confidential document)

[6] CryptoServer CSPLight Administration Manual, version 1.0.1, Utimaco IS GmbH, 27 May 2021

[7] Security Target, Version 1.0.4, 21 June 2021, Security Target Lite for CryptoServer CSPLight, Utimaco IS GmbH (sanitised public document)

[8] Evaluation Technical Report, Version 1.5, 2021-03-26, Evaluation Technical Report(ETR) – Summary, SRC Security Research & Consulting GmbH (confidential document)