TÜV Rheinland Nederland B.V.

TÜVRheinland®
Precisely Right.

Assurance Continuity Maintenance Report

CryptoServer CP5 Se12 5.1.0.0, CryptoServer CP5 Se52 5.1.0.0, CryptoServer CP5 Se500 5.1.0.0, CryptoServer CP5 Se1500 5.1.0.0

Sponsor and developer:	**Utimaco IS GmbH** **Germanusstr. 4** **52080 Aachen** **Germany**
Evaluation facility:	**Brightsight** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-222073-MA**
Report version:	**1**
Project number:	**222073**
Author(s):	**Wouter Slegers**
Date:	**21 April 2020**
Number of pages:	**5**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

CONTENTS:

TÜVRheinland®
Precisely Right.

1 Summary

The IT product identified in this report was assessed according to the Assurance Continuity: CCRA Requirements *[AC],* the developer's updated guidance documents and evaluator's change impact in the form of updated evaluation evidence. The baseline for this assessment was the Certification Report *[CR]*, the Security Target and the Evaluation Technical Report of the product certified by the NSCIB under NSCIB-CC-19-222073.

The changes to the certified product are related to additionally allowing use of three existing interfaces in the guidance. The identification of the maintained product is maintained, but the guidance has been updated.

Consideration of the nature of the changes leads to the conclusion that they can be classified as minor changes 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 as outlined in the Certification Report *[CR]* is maintained for the new version of the product.

This report is an addendum to the Certification Report NSCIB-CC-222073-CR *[CR]* and reproduction is authorised provided the report is reproduced in its entirety.

2 Assessment

2.1 Introduction

The IT product identified in this report was assessed according to the Assurance Continuity: CCRA Requirements *[AC]*, the developer's updated guidance documents and evaluator's change impact in the form of updated evaluation evidence. The baseline for this assessment was the Certification Report *[CR]*, the Security Target and the Evaluation Technical Report of the product certified by the NSCIB under NSCIB-CC-19-222073.

On 2020-03-31 Utimaco IS GmbH submitted a request for assurance maintenance for the CryptoServer CP5 Se12 5.1.0.0, CryptoServer CP5 Se52 5.1.0.0, CryptoServer CP5 Se500 5.1.0.0, CryptoServer CP5 Se1500 5.1.0.0.

NSCIB has assessed the updated guidance according to the requirements outlined in the document Assurance Continuity: CCRA Requirements *[AC]*.

In accordance with those requirements, the updated guidance 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.

This is supported by the evaluator's IAR Analysis *[IA]*.

2.2 Description of Changes

The TOE is a hardware security module whose primary purpose is to provide secure cryptographic services. The original evaluation of the TOE was conducted as a stand-alone evaluation.

The changes to the certified product as described in the updated guidance are only related to additionally allowed usage of three existing interfaces. The update to the guidance was classified as minor changes with no impact on security.

There are no changes in the hardware and software of the TOE, only to the guidance.

The guidance list for the TOE has been updated in the updated Security Target *[ST]*.

3   Conclusion

Consideration of the nature of the changes leads to the conclusion that they can be classified as minor changes 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 as outlined in the Certification Report *[CR]* is maintained for this version of the product.

4   Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[AC]   Assurance Continuity: CCRA Requirements, 2012-06-01, Version 2.1, June 2012.

[CR]   Certification Report CryptoServer CP5 Se12 5.1.0.0, CryptoServer CP5 Se52 5.1.0.0, CryptoServer CP5 Se500 5.1.0.0, CryptoServer CP5 Se1500 5.1.0.0, NSCIB-CC-222073-CR, version 1.1, 14 March 2019.

[ETRfC]   ETR for Composition of CryptoServer Se-Series Gen2 CP5 EAL4+, 18-RPT-622, version 6.0, 21 April 2020.

[IA]   Evaluation Technical Report CryptoServer Se-Series Gen2 CP EAL4+, 18-RPT-621, version 5.0, 21 April 2020.

[NSCIB]   Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[ST]   CryptoServer Security Target for CryptoServer Se-Series Gen2 CP5, document reference 2016-0002, version 2.0.2, dated 1st April 2020.

[ST-Lite]   CryptoServer Security Target Lite for CryptoServer Se-Series Gen2 CP5, document reference 2018-0014, version 2.0.2, dated 1st April 2020.

(This is the end of this report).