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-222073-3MA1**

Report version: **1**

Project number: **222073**

Author(s): **Denise Cater**

Date: **20 November 2020**

Number of pages: **5**

Number of appendices: **0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

TÜVRheinland®
Precisely Right.

CONTENTS:

1 Summary

The IT product identified in this report was assessed according to the Assurance Continuity: CCRA Requirements *[AC],* the developer's Impact Analysis Report *[IAR]* and the evaluator's impact assessment in the form of updated evaluation evidence. The baseline for this assessment was the Certification Report *[CR]* together with the first Maintenance Addendum *[MA1]*, 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 and previously maintained product are related to additionally allowing use, through guidance to the SAM developer, of two existing interfaces. The identification of the maintained product is unchanged, 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 revised TOE.

This report is a further addendum to the Certification Report NSCIB-CC-222073-CR *[CR]* and the first Maintenance Addendum *[MA1]*, 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 Impact Analysis Report *[IAR]* and the evaluator's impact assessment 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 together with the first Maintenance Addendum *[MA1]*.

On 7 August 2020 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 *[IAR]* according to the requirements outlined in the document Assurance Continuity: CCRA Requirements *[AC]*.

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.

This is supported by the evaluator's analysis of the *[IAR]* as documented in *[ETR].*

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 *[IAR]* and updated guidance are only related to additionally allowed usage of two 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 components of the TOE; only to the guidance.

The list of guidance document for the TOE has been updated in the 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 1.2, dated 27 May 2020
[ETR]	Evaluation Technical Report CryptoServer Se-Series Gen2 CP5 EAL4+, 18-RPT-621, version 7.0, 19 November 2020.
[ETRfC]	ETR for Composition for CryptoServer Se-Series Gen2 CP5 EAL4+, 18-RPT-622, version 8.0, 19 November 2020.
[IAR]	Impact Analysis Report (IAR) [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], version 1.3, 18 August 2020.
[MA1]	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, NSCIB-CC-222073-MA, version 1, dated 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, Doc number 2016-0002, version 2.0.4, 18 November 2020.
[ST-LITE]	CryptoServer Security Target Lite for CryptoServer Se-Series Gen2 CP5, Doc number 2018-0014, version 2.0.4, 18 November 2020.

(This is the end of this report).