TÜV Rheinland Nederland B.V.

TÜVRheinland®
Precisely Right.

Assurance Continuity Maintenance Report

Crypto Library V3.1.x on P6021y VB

Sponsor and developer:	**NXP Semiconductors Germany GmbH,** **Business Unit Security and Connectivity** **Stresemannallee 101** **D-22529 Hamburg** **Germany**
Evaluation facility:	**Brightsight** **Delftechpark 1** **2628 XJ Delft** **The Netherlands**
Reportnumber:	**NSCIB-CC-15-66030-MA1**
Report version:	1
Projectnumber:	**NSCIB-CC-15-66030**
Authors(s):	**Wouter Slegers**
Date:	**12 December 2016**
Number of pages:	6
Number of appendices:	0

SOGIS
IT SECURITY CERTIFIED

TÜV Rheinland Nederland B.V.

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

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

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 evaluator's IAR Analysis *[IA]*. The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the NSCIB under NSCIB-CC-15-66030 in *[CR]*.

The changes to the certified product are related to additional usage in combination with updated firmware of the underlying hardware platform without change of the software. The identification procedure of the maintained product is by reference modified to include updated firmware.

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-15-66030-CR and reproduction is authorized provided the report is reproduced in its entirety.

TÜVRheinland®
Precisely Right.

1 Assessment

1.1 Introduction

The IT product identified in this report was assessed according to the Assurance Continuity: CCRA Requirements *[AC]* and the provided 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 *[NSCIB]* under NSCIB-CC-15-66030 as outlined in *[CR]*.

The developer that submitted a request for assurance maintenance for the TOE is NXP Semiconductors Germany GmbH,

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 IAR Analysis *[IA]*.

1.2 Description of Changes

The TOE is a crypto library composed on the underlying hardware platform. The original evaluation of the TOE was conducted as a composite evaluation and used the results of the CC evaluation of the underlying hardware certified under the German CC Scheme as described in *[HW-CERT]*.

The changes to the certified product as described in the *[IAR]* are only related to additional usage in combination with the updated firmware of the hardware that has been certified by the German CC Scheme in a maintenance procedure of the hardware *[HW-MA]*. The update to the hardware was classified by the German CC Scheme as minor changes with no impact on security. This update to the software was classified by developer *[IAR]* and original evaluator *[IA]* as minor changes with no impact on security.

There are no changes in the software component of the TOE.

The updated firmware of the hardware was addressed in the underlying hardware certificate *[HW-MA]* and referred Security Target *[HW-ST]*. An update of the guidance documentation is not needed.

TÜVRheinland®
Precisely Right.

2 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.

TÜVRheinland®
Precisely Right.

3 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 Crypto Library V3.1.x on P6021y VB, NSCIB-CC-15-66030-CR, June 2nd 2016.

[IA]   Brightsight Evaluation report on the Impact Analysis Report (IAR), Crypto Library V3.1.x on P6021y/P6022y VB EAL6+/5+, document reference 16-RPT-413 v2.0, dated 31 October 2016

[IAR]   NXP Secure Smart Card Controller P602xy VB. Description of FW 0C.60/0C.70 Changes. Impact Analysis Report, Rev.0.1, 26 April 2016 (confidential document)

[HW-CERT]   Certification report. NXP Secure Smart Card Controller P6021y VB including IC Dedicated Software, BSI-DSZ-CC-0955-2016, 17 March 2016.

[HW-MA]   Assurance Continuity Maintenance Report BSI-DSZ-CC-0955-2016-MA-01 NXP Smart Card Controller P6021y VB with IC Dedicated Software, document reference BSI_DSZ-CC-0955-2016-MA-01, dated 13 June 2016

[HW-ST]   NXP Secure Smart Card Controller P6021y VB Security Target, Revision 1.5, 19 July 2016.

[NSCIB]   Netherlands Scheme for Certification in the Area of IT Security, Version 2.2, August 10th, 2015.

[ST]   Crypto Library V3.1.x on P6021y VB Security Target, Rev. 1.4, March 18, 2016.

(This is the end of this report).