

Assurance Continuity Maintenance Report

Crypto Library V3.1.x on P6021y VB

Sponsor and developer: **NXP Semiconductors GmbH**
Business Unit Security & Connectivity
Troplowitzstrasse 20
22529 Hamburg, Germany

Evaluation facility: **Brightsight**
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-66030-MA**

Report version: **1**

Project number: **66030**

Author(s): **Wouter Slegers**

Date: **29 July 2019**

Number of pages: **5**

Number of appendices: **0**



C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

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

CONTENTS:

1 Summary	3
2 Assessment	4
2.1 Introduction	4
2.2 Description of Changes	4
3 Conclusion	5
4 Bibliography	5

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 evaluator's IAR Analysis [IA]. 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-18-66030.

The changes to the certified product are related to maintenance of the underlying hardware guidance without change of the hardware and software. The identification of the maintained product is not modified and remains Crypto Library V3.1.x on P6021y VB.

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-66030-CR3 [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 Impact Analysis Report [IAR] and evaluator's IAR Analysis [IA]. 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-18-66030.

On 4 March 2019 NXP Semiconductors GmbH submitted a request for assurance maintenance for the Crypto Library V3.1.x on P6021y VB.

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 (only guidance), (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 composite TOE, consisting of a library which provides cryptographic functions, and an underlying platform, which is a secure micro controller. 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 as described in [HW CERT].

The changes to the certified product as described in the [IAR] are only related to underlying hardware guidance. The update to the hardware guidance was classified as minor changes with no impact on security. This update to the hardware guidance required no changes in the software components of the TOE.

Except for the referred underlying hardware guidance, no update of the guidance documentation is needed.

Users of the TOE are advised to review the changes of the underlying hardware guidance to determine if the specific case addressed by the changed hardware guidance applies to their specific use case.

The configuration list for the TOE has been updated as a result of the changes to include 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 Crypto Library V3.1.x on P6021y VB, NSCIB-CC-66030-CR3, version 3, dated 30 August 2018
- [IA] Evaluation Report on Impact Assessment, 19-RPT-453 v3.0, dated 12 June 2019
- [IAR] Crypto Library v3.1.2 on P6021yVB Impact Analysis Report, Rev 0.1, 18.02.2019 (confidential document)
- [HW-CERT] Certification Report. NXP Secure Smart Card Controller P6021y VB including UC Dedicated Software, BSI-DSZ-CC-1072-V2-2019, 27 June 2019
- [NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September 2017
- [ST] Crypto Library V3.1.x on P6021y Security Target, Rev. 1.9, 22 March 2018

(This is the end of this report).