

Assurance Continuity Maintenance Report

nShield Solo XC Hardware Security Module v12.60.15

Sponsor and developer: **Entrust**
One Station Square
Cambridge CB1 2GA
UK

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

Report number: **NSCIB-CC-0368256-MA**

Report version: **1**

Project number: **0368256**

Author(s): **Denise Cater**

Date: **22 July 2021**

Number of pages: **5**

Number of appendices: **0**



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 [EAR]. 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-21-0368256.

The changes to the certified product are related to a minor change in the guidance not impacting the security functionality of the certified product. The identification of the maintained product is modified to nShield Solo XC Hardware Security Module v12.60.15.

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-0368256-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 Impact Analysis Report [IAR] and evaluator's IAR Analysis [EAR]. 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-21-0368256.

On 08 July 2021 Entrust submitted a request for assurance maintenance for the nShield Solo XC Hardware Security Module v12.60.15.

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 [EAR].

2.2 Description of Changes

The TOE can be used as a general purpose Cryptographic Module in a wide range of use cases, including, but not limited to, Trust Service Providers to provide a QSCD for Remote Server Signing.

It is a general purpose Cryptographic Module which comes in a PCI express board form factor protected by a tamper resistant enclosure. It performs encryption, digital signing, and key management on behalf of an extensive range of commercial and custom-built applications including public key infrastructures (PKIs), identity management systems, application-level encryption and tokenization, SSL/TLS, and code signing.

The changes to the certified product as described in the [IAR] are related to a minor update the guidance, [CCECG]. This update to the guidance was classified by developer [IAR] and original evaluator [EAR] as minor changes with no impact on security.

There are no changes in the software/firmware/hardware components of the TOE.

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
- [CCECG] nShield Solo XC Common Criteria Evaluated Configuration Guide, v1.1.1, June 11 2021
- [CR] Certification Report nShield Solo XC Hardware Security Module v12.60.15, NSCIB-CC-0368256-CR, v1.0, 17 March 2021
- [EAR] Evaluator Assessment of Changes Report (EAR) nShield Solo XC Hardware Security Module v12.60.15– Partial ETR, 21-RPT-706, version 2.0, 22 July 2021
- [IAR] Impact Analysis Report (IAR) nShield Solo XC Hardware Security Module v12.60.15, v1.1, 28 June 2021 (confidential document)
- [NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
- [ST] nShield Solo XC HSM Security Target, v1.1.1, Friday June 11 2021.

(This is the end of this report).