TÜV Rheinland Nederland B.V.

TÜVRheinland®
Precisely Right.

Version 2022-01

Assurance Continuity Maintenance Report

ST33K1M5A and ST33K1M5M B02

Sponsor and developer:	***STMicroelectronics*** **190 avenue Celestin Coq, ZI de Rousset-Peynier** **13106 Rousset** **France**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0428014-2MA1**
Report version:	**1**
Project number:	**0428014_2m1**
Author(s):	**Jordi Mujal**
Date:	**28 July 2023**
Number of pages:	**5**
Number of appendices:	**0**

SOGIS
IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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

CONTENTS:

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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 assessment *[EA]*. 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 CC-22-0428014/2.

The changes to the certified product are related to the updated guidance documentation without change of the hardware and software of the certified product. The identification of the maintained product is modified to ST33K1M5A and ST33K1M5M B02.

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-0428014-CR2 *[CR]* and reproduction is authorised provided the report is reproduced in its entirety.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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 assessment [EA]. 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 CC-22-0428014/2.

On 20 April 2023 STMicroelectronics submitted a request for assurance maintenance for the ST33K1M5A and ST33K1M5M B02.

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 assessment *[EA]*.

2.2 Description of Changes

The TOE is a serial access microcontroller designed for secure mobile applications and compliant with *[PP_0084]*.

The changes to the certified product as described in the *[IAR]* are only related to the update of some guidance documents. The update to the guidance was classified as minor changes with no impact on security. This update to the guidance was classified by developer *[IAR]* and original evaluator *[EA]* as minor changes with no impact on security.

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

Configuration Management procedures required a change in the product identifier. Therefore, the name was modified to ST33K1M5A and ST33K1M5M B02 to include the update of the guidance documentation.

The configuration list for the TOE has been updated as a result of the changes to include the updated Security Target *[ST]* and guidance documents *[DS_A-CB02]*, *[DS_M-CB02]*, *[UM_FW-CB02]*, *[UM_TRNG-CB02]* and *[AN_TRNG-CB02].*

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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 2.2, 3 September 2023.

[DS_A-CB02] Automotive, High-speed secure MCU with 32-bit Arm® Cortex®-M35P CPU with SWP, ISO, SPI and I2C interfaces, and high-density flash memory – ST33K1M5A Datasheet, DS_ST33K1M5A, version 3, May 2023

[DS_M-CB02] High-speed secure MCU with 32-bit Arm® Cortex®-M35P CPU with SWP, ISO, SPI and I2C interfaces, and highdensity flash memory – ST33K1M5M Datasheet, DS_ST33K1M5M, version 3, May 2023.

[UM_FW-CB02] ST33K platform firmware V3 – User manual, UM_ST33K_FW, version 7, March 2023.

[UM_TRNG-CB02] Random number generation V1.4 – User manual, UM_ST_TRNG14, version 7, April 2023.

[AN_TRNG-CB02] ST33K Platform- TRNG Reference implementation: Compliance tests, AN_ST33K_TRNG, version 3, May 2023.

[CR] Certification Report ST33K1M5A and ST33K1M5M B01, version 1, 17 August 2022

[EA] Evaluator Assessment of Changes Report (EAR) ST33K1M5A and ST33K1M5M B02– Partial ETR, 23-RPT-482, version 3.0, 20 July 2023.

[IAR] Security Impact Analysis (SIA) report – ST33K1M5AM B02, SMD_ST33K1M5AM_B02_SIA_23_001, v1.1, April 2023

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

[PP_0084] Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014

[ST] ST33K1M5A and ST33K1M5M B02 SECURITY TARGET, Rev. B02.1, May 2023

[ST-Lite] ST33K1M5A and ST33K1M5M B02 SECURITY TARGET FOR COMPOSITION, Rev. B02.1, May 2023

(This is the end of this report).

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.