SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-109 MR Maintenance Report

Issue 1.0 12 March 2019

FM1280 V05.1 Dual Interface Smart Card Chip with IC Dedicated Software

1 Introduction

The certified TOE was evaluated according to Common Criteria version 3.1 R4 and Evaluation Assurance Level EAL 5+.

The IT Security Evaluation Facility (ITSEF/EVIT) was Brightsight BV and the sponsor/developer was Shanghai Fudan Microelectronics Groups Co., Ltd. (in short Fudan). The Security Developer Analysts at Fudan for this maintenance process were Shan Weijun and Zhang Weibin.

Fudan submitted an Impact Analysis Report (IAR) [17] to SERTIT. The IAR is intended to satisfy requirements outlined in version 2.1 of the Common Criteria document *Assurance Continuity: CCRA Requirements* [CCDB-2012-06-01]. In accordance with those requirements, the IAR [17] describes the changes made to the TOE.

2 Certified TOE identification

FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software:

- TOE hardware version: V05
- TOE software version: V2.751
  - Boot: V1.001
  - FMSH_CryptoLib: V3.104
  - Driver: V1.000
- Documents:

[1] FM1280 Security Preparatory Guidance, Version 1.0, 10 May 2018

[2] FM1280 Security Programming Guidance, Version 3.0, 10 May 2018

[3] Application Programming Interface for FMSH_CryptoLib, Version 0.4, 25 December 2017

[4] Application Programming Interface for Driver, Version 1.1, 18 January 2018

[5] FM1280 User Manual, Version 1.1, 6 December 2017

[6] FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software Security Target, V0.5, 10 May 2018

[7] FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software Security Target Lite, V2.0, 16 May 2018

[8] SERTIT-109 CR Certificate Report, Issue: 2.0, 2 July 2018

[9] SERTIT-109 C Certificate, Issue: 2.0, 2 July 2018

3 Maintained TOE identification

FM1280 V05.1 Dual Interface Smart Card Chip with IC Dedicated Software:

- TOE hardware version: V05.1
- TOE software version: V2.752
  - Boot: V2.0
  - FMSH_CryptoLib: V3.105
  - Driver: V2.22
- Documents:

[10] FM1280 Security Preparatory Guidance, Version 2.2, 25 November 2018

[11] FM1280 Security Programming Guidance, Version 3.4, 25 November 2018

[12] Application Programming Interface for FMSH_CryptoLib, Version 0.4, 25 December 2017

[13] Application Programming Interface for Driver, Version 1.1, 18 January 2018

[14] FM1280 User Manual, Version 1.1, 6 December 2017

[15] FM1280 V05.1 Dual Interface Smart Card Chip with IC Dedicated Software Security Target, V0.5, 25 November 2018

[16] FM1280 V05.1 Dual Interface Smart Card Chip with IC Dedicated Software Security Target lite, V1.0, 26 November 2018

[17] FM1280 V05.1 Dual Interface Smart Card Chip with IC Dedicated Software Impact Analysis Report, V0.4, 26 November 2018

[18] Impact Assessment for FM1280 V05.1 Dual Interface Smart Card Chip with IC Dedicated Software Impact Analysis Report, V1.0, 26 November 2018

4 Description of Changes

The IAR [17] chapter 2 lists a number of changes to the certified TOE. Each change is identified and clearly and adequately described. This report list the changes relevant to the TOE. The changed TOE parts are described below:

- Modified security-enforcing components:
  - TOE hardware: None.
  - TOE software:
    - The DES-CBC relevant API of the crypto library is updated for the improvement of the performance and the side-channel countermeasure. Additional verification test was performed by the ITSEF [18]. Test result was pass.

  - The ECC implementation is improved by using existing ex-Euclidean hardware. Code review performed by the ITSEF [18] shows there was no vulnerability.
  - TRNG function is moved from patch to ROM. Vulnerability analysis performed by the ITSEF shows this does not have security impact on the TOE.
    - BCA_SetKey(), FMSH_Cmp_BN(), RSA_Public(): the return value generation method is improved. Code review performed by the ITSEF [18] shows there was no vulnerability.
    - The boot component is updated for better coding style or functional bug fix. Code review performed by ITSEF [18] shows there was no vulnerability.
- Modified security-non-interfering components:
  - TOE software
    - The driver component is updated for better coding style and performance. Code review performed by ITSEF [18] shows there was no vulnerability.
  - TOE hardware
    - The hardware logo on top of the chip is update
    - The analog components are updated for better accuracy, performance and stability of the contactless communication and flash memory operation.

Note: There is no change to the chip layout except for the above components.

Due to the above changes, the corresponding TOE documents are updated and described in chapter 5.

5 Affected Developer Evidence

The IAR [17] chapter 3 lists all of the affected items of the developer evidence for each change in to the certified TOE a structured and clear manner. All items of the developer evidence that has been modified in order to address the developer action elements are identified. The developer has described the required modifications to the affected items of the developer evidence. There are no changes to the development environment.

6 Conclusion

The IAR [17] provided by the developer clearly presented the change to the certified TOE scope, and analysed impacts to all the assurance classes following the requirements described in [CCDB-2012-06-01]. The changes to the TOE have either no security impact or minor security impact to the TOE. For the changes with minor security impact, the ITSEF performed vulnerability analysis, code review and a verification test. The results show the changes do not impact the assurance gained and the change is considered as a minor maintenance.

The TOE’s security functionality described by the Security Function Requirements specified in the ST [15] and ST Lite [16] is not affected by this change. Through functional testing of the FM1280 V05.1 Dual Interface Smart Card Chip with IC Dedicated Software, assurance gained in the original TOE certification was maintained. As change to the TOE has been classified as minor, it is the conclusion of SERTIT that the maintained TOE is appropriate for assurance continuity and re-evaluation is not required.

Certificate Maintenance team	Lars Borgos, SERTIT
Date approved	12 March 2019