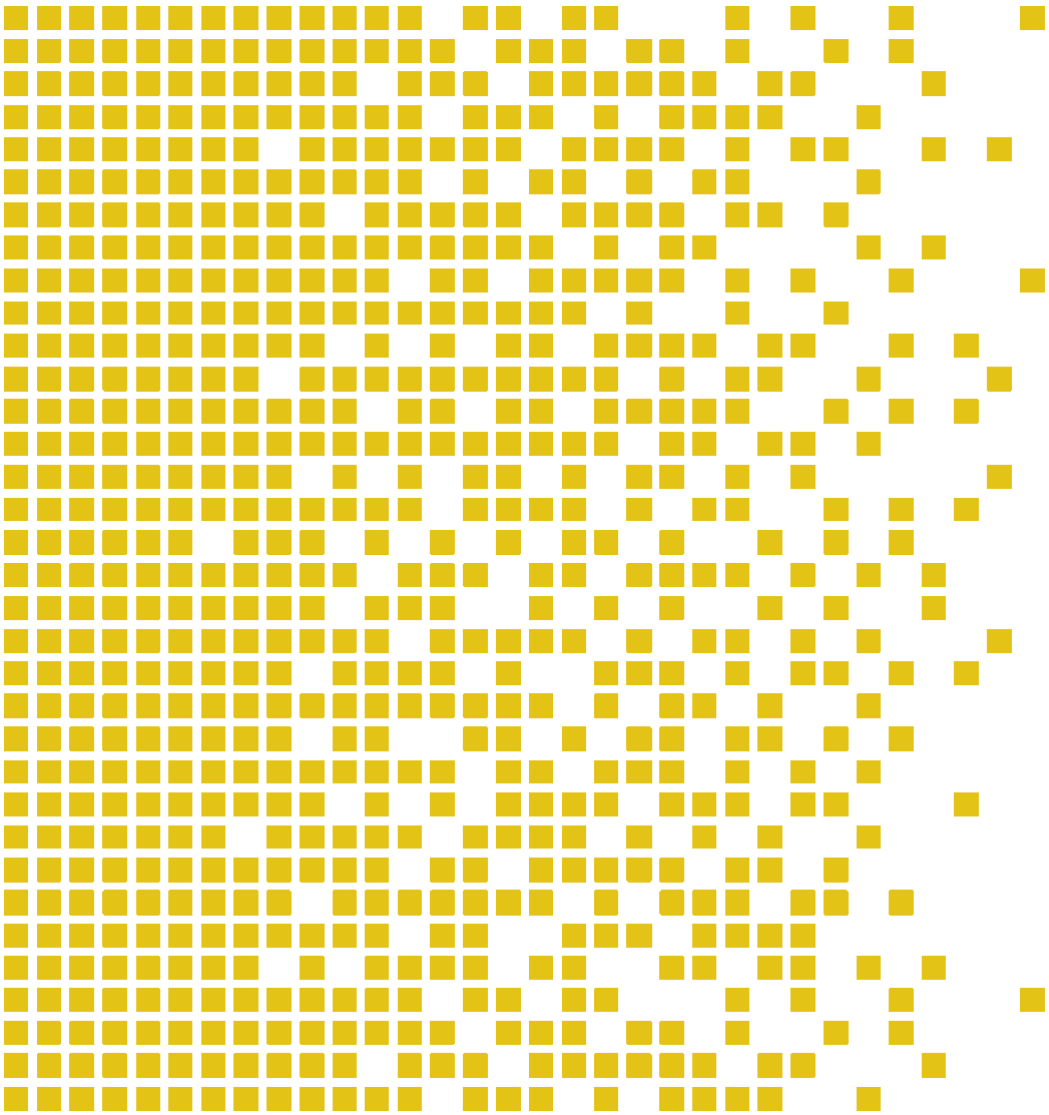
SERTIT-099 CR Certification Report

Issue 1.0 9 February 2018

FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software



SERTIT, Postboks 814, 1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Dutch evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The recognition under CCRA is limited to cPP related assurance packages or EAL2 and ALC_FLR CC part 3 components

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Dutch evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL4.

Contents

1 Certification Statement

Shanghai Fudan Microelectronics Group Co., Ltd FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software is a high-end dual-interface secure smart card integrated circuit suitable for ID cards, Banking cards, e-Passport applications and the like.

FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 4+ augmented with AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality in the specified environment when running on the platforms specified in Annex A. It has also met the requirements of Protection Profile BSI-CC-PP-0084-2014 V1.0.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Arne Høye Rage Quality Assurance
Approved	Jørn Arnesen Head of SERTIT
Date approved	9 February 2018

2 Abbreviations

API	Application Programming Interface
CC	Common Criteria for Information Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CMS	Chip Management System
DEMA	Differential Electro Magnetic Analysis
DES	Data Encryption Standard
DPA	Differential Fault Analysis
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
EMFI	Electro-Magnetic Fault Injection
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
FBBI	Forward-Body Bias Injection
IC	Integrated Circuit
OSP	Organizational Security Policy
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman Public Key Encryption
SERTIT	Norwegian Certification Authority for IT Security
SEMA	Simple Electro Magnetic Analysis
SFR	Security Functional Requirements
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

TSP	TOE Security Policy
VM	Voltage Manipulation

3 References

[1] FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software Security Target, Shanghai Fudan Microelectronics Group Co., Ltd, Version 1.8, December 2017.

[2] FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software Security Target Lite, Shanghai Fudan Microelectronics Group Co., Ltd, Version 1.8, December 2017

[3] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[4] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[5] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[6] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[7] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[8] JIL Attack Methods for Smartcards and Similar Devices, Version 2.2, January 2013.

[9] JIL Application of Application Attack Potential to Smart Cards, Version 2.9, May 2013.

[10] AIS20/31 A proposal for Functionality classes for random number generators, Version 2.0, 18 September 2011.

[11] The Application of CC to Integrated Circuits, Version 3.0, Revision 1, March 2009

[12] Requirements to perform Integrated Circuit Evaluation, Version 1.1, May 2013

[13] Security Architecture requirements (ADV_ARC) for smart cards and similar devices, Version 2.1, April, 2014

[14] Evaluation Technical Report (ETR) Common Criteria EAL4+ Evaluation of the Fudan FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software 17-RPT-670 Version 2.0, 12 December, 2017 (Brightsight).

[15] FM1280 Security Preparatory Guidance, Version 1.1, 06 December 2017

[16] FM1280 Security Programming Guidance, Version 2.1, 10 November 2017

[17] Application Programming Interface for FMSH_CryptoLib, Version 0.3, 15 September 2017

[18] Application Programming Interface for Driver, Version 1.0, 11 August 2017

[19] FM1280 User Manual, Version1.1, 06 December 2017

[20] Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, Version 1.0, January 2014.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software to the Sponsor, Shanghai Fudan Microelectronics Group Co., Ltd, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target [1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Shanghai Fudan Microelectronics Groups Co., Ltd.

The TOE is a secure smart card integrated circuit with dedicated software mainly for banking and finance market, electronic commerce or governmental applications. The scope of the TOE includes a dual-interface IC hardware and IC dedicated software for DES and RSA. The IC has a DES coprocessor, a RSA coprocessor and a True Random Number Generator (AIS20/31 [10] PTG.2 class.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the Security Target [1], chapter 1.3.

4.4 Protection Profile Conformance

The Security Target [1] claimed conformance to the following protection profile:

BSI-CC-PP-0084-2014 V1.0

4.5 Assurance Level

The Security Target [1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 4+, augmented by AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2. Common Criteria Part 3 [5] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [3].

4.6 Security Policy

The TOE security policies are detailed in Security Target [1], chapter 3.3.

4.7 Security Claims

The Security Target [1] fully specifies the TOE's security objectives, the threats and OSP's which these objectives counter or meet and security functional requirements and security functions to meet the objectives. Most of the SFR's are taken from CC Part 2 [4]. Others come from extended component definitions copied from the claimed PP [20]. Use of the standard and the standardized PP [20] facilitates comparison with other evaluated products

The following SFR's are defined in the Protection Profile [20]: FCS_RNG.1, FMT_LIM.1, FMT_LIM.2, FAU_SAS.1, FDP_SDC.1.

4.8 Threats Countered

All threats that are countered are described in the Security Target [1], chapter 3.2.

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks are described that are not countered.

4.11 Environmental Assumptions and Dependencies

The assumptions that apply to this TOE are described in the Security Target [1], chapter 3.4.

4.12 IT Security Objectives

The security objectives that apply to this TOE are described in the Security Target [1], chapter 4.1.

4.13 Security Objectives for the TOE's Environment

The security objectives for the environment are described in the Security Target [1], chapter 4.2 and chapter 4.3.

4.14 Security Functional Requirements

The following Security Functional Requirements are directly taken from the Protection Profile [20].

Security Functional Requirement	Title
FRU_FLT.2	“Limited fault tolerance“
FPT_FLS.1	“Failure with preservation of secure state”
FMT_LIM.1	“Limited capabilities”
FMT_LIM.2	“Limited availability”
FAU_SAS.1	“Audit storage”
FPT_PHP.3	“Resistance to physical attack”
FDP_ITT.1	“Basic internal transfer protection”
FDP_IFC.1	“Subset information flow control”
FPT_ITT.1	“Basic internal TSF data transfer protection”
FDP_SDC.1	“Stored data confidentiality”
FDP_SDI.2	“Stored data integrity monitoring and action”
FCS_RNG.1	“Quality metric for random numbers”
FCS_COP.1[TDES]	“Cryptographic operation - Triple-DES”

Except for FAU_SAS.1, FDP_SDC.1, FDP_SDI.2, FCS_RNG.1 and FCS_COP.1[TDES], all assignments and selections are completely defined in the Protection Profile [20]. The operations for FAU_SAS.1, FDP_SDC.1, FDP_SDI.2, FCS_RNG.1 and FCS_COP.1[TDES] are completed in the Security Target [1].

The following additional Security Functional Requirements are claimed in the Security Target [1]:

Security Functional Requirement	Title
FDP_ACC.1	“Subset access control”
FDP_ACF.1	“Security attribute based access control”
FCS_COP.1[RSA]	“Cryptographic operation – RSA”

4.15 Security Function Policy

The TOE is a secure microcontroller with with IC dedicated support software.

The TOE consists of IC Hardware, the IC dedicated software and the supporting documents. The hardware is based on a CPU, memories of ROM, EEPROM, RAMs, cryptographic coprocessors for execution and acceleration of TDES and RSA cryptographic algorithms, security components and several communication interfaces.

The IC dedicated software consists of driver, boot and a cryptographic library.

The TOE supports the following communication interfaces:

- ISO/IEC 14443 TYPE A contactless interface
- ISO/IEC 7816 contact interface.
- GPIO
- SPI and High Speed SPI
- I2C
- UART

The TOE is delivered to a composite product manufacturer. The IC embedded software is developed by the composite product manufacturer. The IC embedded software is sent to Fudan Company to be loaded in EEPROM and delivered back to the composite product manufacturer together with the TOE. The firmware loading feature is disabled after TOE delivery. The security IC embedded software is not part of the TOE.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E [6]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [1], which prospective consumers are advised to read. To ensure that the Security Target [1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [5] and the Common Evaluation Methodology (CEM) [7]. Interpretations [8], [9], [10] and CC mandatory documents [11], [12], [13] are used.

SERTIT monitored the evaluation, which was carried out by Brightsight B.V. as Commercial Evaluation Facility (ITSEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR) [14] to SERTIT on 2 Nobember 2016. As a result SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target [1] with reference to the assumed operating environment specified by the Security Target [1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3 [5]. These classes comprise the EAL5 assurance package augmented with AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Architectural design
	ADV_FSP.4	Functional specification
	ADV_IMP.1	Implementation representation
	ADV_TDS.3	TOE design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative user guidance
Life-cycle support	ALC_CMC.4	CM capabilities
	ALC_CMS.4	CM scope
	ALC_DEL.1	Delivery
	ALC_DVS.2	Development security
	ALC_LCD.1	Life-cycle definition
	ALC_TAT.1	Tools and techniques
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Coverage
	ATE_DPT.2	Depth
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing
Vulnerability assessment	AVA_VAN.5	Vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall “pass” verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target [1]. The results of this work were reported in the ETR [14] under the CC Part 3 [5] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated versions of its constituent components have been supplied, and to check that the security of the TOE has not been compromised in delivery.

The delivery and acceptance procedures are described in the supporting document [15].

5.3 Installation and Guidance Documentation

According to the Security Target [1] Section 1.4, the installation procedure is not applicable because the embedded software is loaded on the EEPROM in Phase 3 and the load feature is disabled before the TOE is delivered to the user. No additional installation is required.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Security IC Embedded Software shall follow the guidance documentation [15], [16], [17], [18], [19] for the TOE in order to ensure that the TOE is operated in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

An independent vulnerability analysis was done, consisting of the following steps:

- A design and implementation review on the TOE was done to identify weaknesses in the TOE that could potentially be exploited by attackers. A code review of the crypto library and boot code was also executed.
- Validation tests of security features performed in the ATE class are taken into account for the following vulnerability analysis.
- A vulnerability analysis based on the design and implementation review results and the validation test results of security features, was performed

considering the well-known attacks from the "JIL Attack Methods for Smartcards and Similar Devices" [8]. User guidance is also taken into consideration while analysing potential vulnerabilities.

- A penetration test plan is established based on the results of the vulnerability analysis.
- Practical penetration tests are performed according the penetration test plan.

5.6 Developer's Tests

The developer tests consist of four parts; 1) testing on engineering samples, 2) testing on wafers and 3) testing on simulation tools.

- Testing on engineering samples:

  Developer tests performed on engineering samples (cards or Dual-In-Line-Package ICs)

- Testing on wafers:

  Developer tests performed on wafers

- Testing on simulation tools:

  Developer tests were done on simulation tools in the chip development environment, which were used to verify the logical functions.

5.7 Evaluators' Tests

The evaluator's responsibility for performing independent testing is required by the ATE_IND class. Since developer's testing procedures have been found to be extensive and thorough, and developer's hardware testing tools are not generally available to allow reproduction of developer test cases in the test lab, the choice was made to perform the evaluator independent testing by witnessing of the developer's test cases, using the developer's tools, at the premises, Fudan Shanghai, of the developer. The evaluator employed a sampling strategy to select developer tests to validate the developer's test results. The sampling strategy is as follows:

- Tests on TSFI's are sampled
- Tests on Interfaces of SFR-enforcing modules are sample.
- Tests on Security Mechanisms are sampled.
- All the testing methods (Wafer/Sample/Simulation) will be sampled

In addition to this, the evaluator has defined additional test cases, prompted by study of the developer documentation. The test strategy is as shown below:

- Augmentation of developer testing for interfaces by varying parameters to more rigorously test the interface
- Supplementation of developer testing strategy, for example by applying the tests performed on engineering samples to wafer samples.

The considerations that are taken during the selection of the interfaces to be tested are:

- Observation and understanding during the performance of the work units in ATE_COV, DPT and FUN.
- Significance of the interfaces with respect to security

These tests are also performed using the developer's tools at the premises of the developer. The evaluator witnessed the whole process of the tests.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR [14], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that the FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4+ augmented with AVA_VAN.5, ATE_DPT.2 and ALC_DVS.2 for the specified Common Criteria Part 2 extended functionality and Protection Profile BSI-CC-PP-0084-2014 V1.0, in the specified environment.

6.2 Recommendations

Prospective consumers of FM1280 V05 Dual Interface Smart Card Chip with IC Dedicated Software should understand the specific scope of the certification by reading this report in conjunction with the Security Target [1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation [15], [16], [17], [18], [19] included in the evaluated configuration.

The above “Evaluation Findings” include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Type	Name	Version	Delivery form
IC Hardware	FM1280	V05	Wafer, module
IC Dedicated Software	Firmware V2.75 including the following:		
	Boot	V1.001	On-chip ROM
	FMSH_CryptoLib	V3.103	On-chip ROM Header file: FM_CryptoLib.h FM_CryptoLib_struct.h
	Driver	V1.000	On-chip ROM Header file: FM_DriverLib.h FM_DriverDef.h
Document	FM1280 Security Preparatory Guidance[15]	V1.1	document
	FM1280 Security Programming Guidance[16]	V2.1	document
	Application Programming Interface for FMSH_CryptoLib[17]	V0.3	document
	Application Programming Interface for Driver[18]	V1.0	document
	FM1280 User Manual[19]	V1.1	document

TOE Documentation

The supporting guidance documents evaluated were:

[a] FM1280 Security Preparatory Guidance[15]

[b] FM1280 Security Programming Guidance[16]

[c] Application Programming Interface for FMSH_CryptoLib[17]

[d] Application Programming Interface for Driver[18]

[e] FM1280 User Manual[19]

Further discussion of the supporting guidance material is given in Section 5.3 “Installation and Guidance Documentation”.

TOE Configuration

The TOE configuration used for testing was the same used for developer tests. This is described in chapter 5.6 of this report.