FM1280 07.1 Dual Interface Smart Card Chip with IC Dedicated Software 2.771

Security Target Lite

Nov. 2025

Version 1.2

Shanghai Fudan Microelectronics Group Co., Ltd.

Change History

No	Version	Date	Chapter	Change	By
1	1.0	2025/7	All chapters	Created the initial version	Shan Weijun
2	1.1	2025/11	6.2.3	Update application note	Shan Weijun
3	1.2	2025/11	6.2.3	Remove application note	Shan Weijun

Contents

1 ST Introduction

This Security Target (ST) is built upon the Security IC Platform Protection Profile with Augmentation Packages [1]. Registered and Certified by Bundesamtfür Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014.

This chapter presents the ST reference, the reference for the Target Of Evaluation (TOE), a TOE overview description and a description of the logical and physical scope of the TOE.

1.1. ST and TOE identifiers

ST reference:	FM1280 07.1 Dual Interface Smart Card Chip with IC Dedicated Software 2.771 Security Target Lite V1.2
TOE reference:	FM1280 07.1 Dual Interface Smart Card Chip with IC Dedicated Software 2.771

1.2. TOE overview

The TOE is FM1280 07.1 Dual Interface Smart Card Chip with IC Dedicated Software 2.771, in short of FM1280, developed by Shanghai Fudan Microelectronics. It can be widely and easily applied in various security fields such as banking and finance market, social security card, transport card, small-amount payment and security identification, etc.

The FM1280 consists of the IC Hardware, the IC Dedicated Software and the supporting documents.

The hardware is based on a CPU, memories of ROM, NVM and RAMs, and cryptographic coprocessors for execution and acceleration of symmetric and asymmetric cryptographic algorithms, security components and several communication interfaces.

The CPU is a microprocessor that supports a 32-bit instruction set and security features. The on-chip memories consist of ROM, NVM, and RAM. The NVM is a non-volatile memory that can be used to store not only data but also code. The data stored in the ROM, NVM, RAM is protected on its integrity and confidentiality.

The FM1280 supports the following communication interfaces:

- ISO/IEC 14443 contactless interface
- ISO/IEC 7816 contact interface.

The FM1280 has been designed to provide a platform for Security IC Embedded Software which ensures that the critical user data of the Composite TOE are stored and processed in a secure way. To this end the FM1280 has the following security features:

- Hardware coprocessor for TDES
- Hardware coprocessor for AES
- True Random Number Generator
- Hardware for RSA support
- Protection against power and electronic magnetic analysis
- Protection against physical attacks

- Protection against perturbation attacks
- Memory access control
- Memory encryption
- Data and critical register protection
- Active shielding
- Security sensors
- Software library with cryptographic services

Some of these features can be controlled by the Security IC embedded software. The software library in the IC Dedicated Software has been designed to provide easy access to the hardware functions and to complement these.

The Driver is a part of the IC Dedicated Software. It provides API functions of NVM operations, IO operations and CRC calculation.

The documents include a FM1280 Security Preparatory Guidance, a FM1280 Security Programming Guidance, an Application Programming Interface for FMSH_CryptoLib, an Application Programming Interface for Driver, and a FM1280 User Manual.

There is no non-TOE hardware, firmware and software required by TOE.

1.3. TOE description

1.3.1. Physical scope

The block diagram of the TOE hardware and software is depicted below.

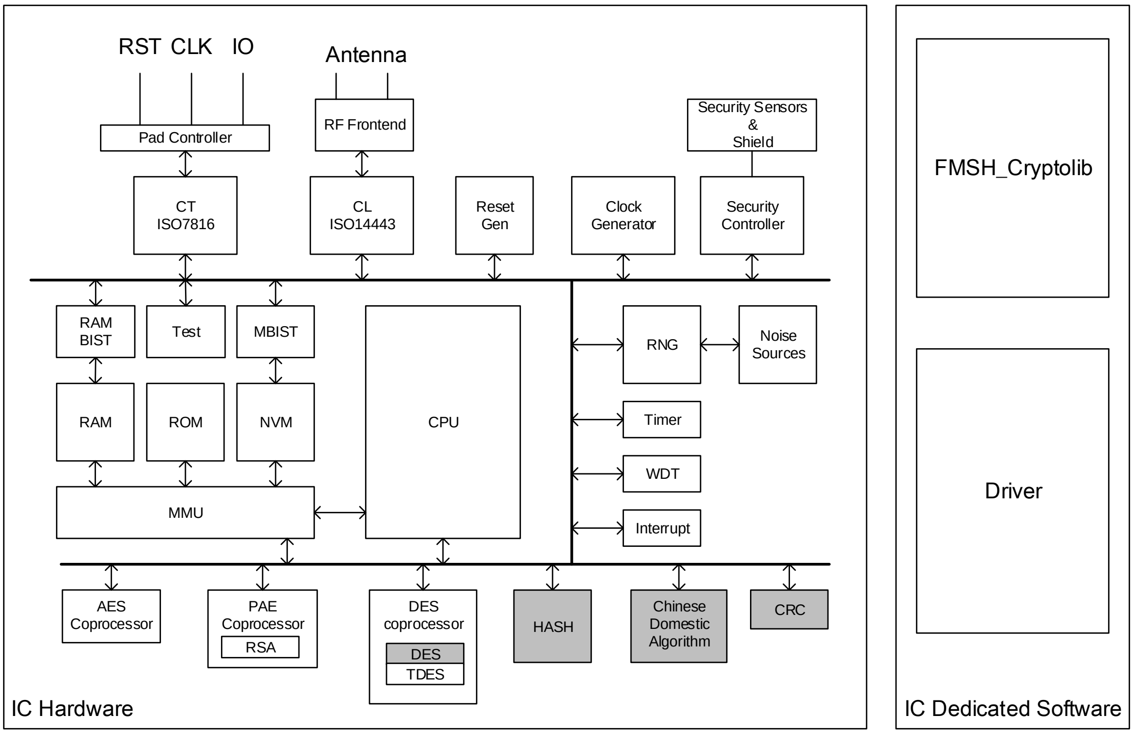

Figure 1 Block Diagram of FM1280 07.1 Dual Interface Smart Card Chip with Software

The FM1280 includes the IC Hardware, the IC Dedicated Software and supporting documents for developers. The grey coloured blocks in IC hardware are the algorithm modules whose security is not claimed in this TOE. The IC Dedicated Software comprises of FMSH_Cryptolib and Driver. The Dedicated Test Software is only used to support testing of the TOE and downloading IC Embedded Software at manufacturer sites. The code of download function is stored in ROM, and is disabled before TOE Delivery. The code of test function is downloaded into the NVM, and is completely removed from the memory after testing. Hence it is not a part of the TOE. The IC Embedded Software is provided by developers. It is not a part of the TOE neither.

1.3.1.1. TOE components

The TOE consists of the following components that are delivered to the composite product manufacturer:

Table 1 TOE components table

Type	Name	Version	Delivery form
IC Hardware	FM1280	07.1	Wafer, module in package with security labels
IC Dedicated Software	Firmware 2.771 including the following:		
	FMSH_CryptoLib	3.111	On-chip ROM and NVM
	FM_CryptoLib.h FM_CryptoLib_struct.h FM_Firmware_staticLib_Crypto.lib	1.14	PGP encrypted SDK package
	Driver	1.001	On-chip ROM
	FM_DriverAPI.h FM_Firmware_staticLib_Driver.lib	1.121	PGP encrypted SDK package
	AU library	02	Pre-installed in NVM
Document	FM1280 07.1 Security Preparatory Guidance	0.5	PGP encrypted PDF file
	FM1280 07.1 Security Programming Guidance	0.9	PGP encrypted PDF file
	FM1280 07.1 Application Programming Interface for FMSH_CryptoLib	0.5	PGP encrypted PDF file
	FM1280 07.1 Application Programming Interface for Driver	0.3	PGP encrypted PDF file
	FM1280 07.1 User Manual	1.6	PGP encrypted PDF file

Application notes:
The TOE version is defined by the versions of IC hardware and IC dedicated software together. The IC hardware version is 07.1, and the IC Dedicated Software version, also named Firmware, is 2.771.
The head files and the link library are provided for the user to help them to their product. The head files include FM_CryptoLib.h, FM_CryptoLib_struct.h, FM_DriverLib.h and FM_DriverDef.h. The link libraries are FM_Firmware_staticLib_Crypto.lib and FM_Firmware_staticLib_Driver.lib.
The PGP encrypted files are delivered by e-mail or storage media, such as USB flash disk or DVD.

1.3.2. Logical scope

1.3.2.1. Hardware description

The hardware of the FM1280 has the following components:

- low power 32-bit secure CPU
- Memories:
    - NVM
    - ROM
    - RAM
- Physical Interfaces:
    - ISO/IEC 14443 contactless interface
    - ISO/IEC 7816 contact interface
- CRC Coprocessor
- True Random Number Generator
- DES/TDES Coprocessor
- AES Coprocessor
- PAE Coprocessor for RSA support
- Chinese Domestic Algorithm Coprocessor
- HASH
- Memory Management Unit (MMU)
- Timers
- Watch Dog Timer (WDT)
- Clock and Reset management
- Security Controller and Environmental Detector Circuits
- Test component

The low power 32-bit secure CPU is designed specifically for the high volume memory smart card and embedded security application with the proven security features.

Memories consist of NVM, ROM, RAM.

The two physical communication interfaces consist of a contactless interface to support ISO/IEC 14443 protocol and a contact interface to support ISO/IEC 7816 protocol. Two interfaces are able to work concurrently or independently.

The CRC coprocessor supports CRC16 on ISO14443, CRC16 on CCITT and CRC32 on ISO3309. The security of the CRC is not claimed in this TOE.

True Random Number Generator provides true random numbers with high quality satisfied with AIS31.

DES/TDES Coprocessor is a hardware module for DES/TDES calculation with security features. The Security IC embedded software needs to use these APIs in secure ways according to the application’s security need.

AES Coprocessor is a hardware module for AES calculation with security features. The Security IC embedded software needs to use these APIs in secure ways according to the application's security need.

PAE Coprocessor provides hardware acceleration for RSA calculation with security features.

The TOE contains crypto support for Chinese Domestic Algorithms. The security of these algorithms is not claimed in the TOE.

HASH is a function to map data of arbitrary size to data of fixed size. Its security is not claimed in this TOE.

The MMU provides the access service to memories. In the aspect of security, MMU provides memory access control, memory encryption, data integrity check and data bus masking.

The timer is a specialized type of clock for measuring time intervals. The TOE contains two 32-bit timers whose driver is able to be select from system clock and external clocks. Each of them is capable to work as two 16-bit timers.

The watchdog is used to detect and recover from CPU malfunctions. The CPU regularly resets the watchdog timer to prevent it from 'time out'.

Clock and reset management provides the management of the power and the clock of the TOE.

The sensors are provided to ensure that the TOE only works in a safe environment. The active shield covers the chip's surface to resist physical attacks. The data and code stored in the NVM, ROM and RAM are encrypted and come with check bits.

The test component is used for test purposes by the manufacturer. Its test functions are disabled before TOE delivery.

The TOE works in these three operation modes below,

- Org Mode
- Prog Mode
- User Mode

The Org Mode and Prog Mode are only for manufacturer to carry out production testing and initializing the TOE's configuration. The operation mode is changed into User Mode before the TOE delivery to the developers and it cannot return to other two operation modes. The access of the testing functions is disabled in User Mode.

1.3.2.2. Software description

The TOE provides the following cryptographic services to the Security IC embedded software which are claimed as security functions:

- TRNG
- TDES
- AES
- RSA

The TOE provides the following cryptographic services to the Security IC embedded software which are not claimed as security functions:

- DRNG
- DES
- SHA1/SHA256 by HASH
- Chinese Domestic Algorithms

A remark must be made that the TOE only provides the functions of DRNG, DES, SHA1/SHA256 and Chinese Domestic Algorithms which are not claimed as security functions.

The TOE provides high entropy random numbers to the Security IC embedded software from a true random number generator.

The TOE provides the following driver services to the Security IC embedded software:

- NVM operation, such as read, write, erase and data check
- Interface communications
- CRC

A remark must be made that the driver services have not been made to be resistant against attacks. When they are used in secure code sections additional security must be added.

1.4 Life cycle and delivery

The end-consumer environment of the TOE is phase 7 of the Security IC product life-cycle as defined in the PP [1]. In this phase the FM1280 is in usage by the end-consumer. Its method of use now depends on the Security IC Embedded Software. Examples of use cases are ID cards or Bank cards.

The scope of the assurance referring to the TOE's life cycle is limited to phases 2, 3 and 4. These phases are under the control of the TOE manufacturer. At the end of phase 4 the TOE components described in 1.3.1.1 are delivered to the Composite Manufacturer.

The embedded software is loaded on the NVM in Phase 3 and the load feature is disabled before the TOE is delivered to the users.

2. Conformance claim

This chapter presents conformance claim and the conformance claim rationale.

2.1. CC Conformance

This Security Target claims to be conformant to the Common Criteria version 3.1:

- Part 1 revision 5 [2].
- Part 2 revision 5 [3]
- Part 3 revision 5 [4]

For the evaluation will be used the methodology in Common Criteria Evaluation Methodology version 3.1 CEM revision 5 [5]

This security Target claims to be CC Part 2 extended and CC Part 3 conformant.

2.2. PP Claim

This Security Target claims **strict** conformance to the Security IC Platform Protection Profile, [1].

The TOE also provides additional functionality, which is not covered in [1].

2.3. Package claim

This Security Target claims conformance to the assurance package **EAL6** augmented with ASE_TSS.2. This assurance level is in line with the Security IC Platform Protection Profile [1].

2.4. Conformance claim rationale

This TOE is equivalent to the conformance claim stated in a Security IC Platform Protection Profile [1].

3. Security problem definition

This chapter presents the threats, organisational security policies and assumptions for the TOE.

The Assets, Assumptions, Threats and Organisational Security Policies are completely taken from the Security IC Platform Protection Profile [1].

3.1. Description of Assets

Since this Security Target claims conformance to the Security IC Platform Protection Profile [1], the assets defined in section 3.1 of the Protection Profile are applied.

3.2. Threats

This Security Target claims conformance to the Security IC Platform Protection Profile [1]. The Threats that apply to this Security Target are defined in section 3.2 of the Protection Profile. The following table lists the threats of the Protection Profile.

Table 2 Threats defined in the Protection Profile

Threat	Title
T.Leak-Inherent	Inherent Information Leakage
T.Phys-Probing	Physical Probing
T.Malfunction	Malfunction due to Environmental Stress
T.Phys-Manipulation	Physical Manipulation
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

3.3. Organisational security policies

This Security Target claims conformance to the Security IC Platform Protection Profile [1]. The Organisational Security Policies that apply to this Security Target are defined in section 3.3 of the Protection Profile, they are:

P.Process-TOE Protection during TOE Development and Production

The following Organisational Security Policy is also taken from the PP [1] to facilitate the TOE crypto services:

P.Crypto-Service Cryptographic services of the TOE

The TOE provides additional functionality, which is not covered in [1]. In accordance with Application Note 5 of [1] this functionality is added using the policy P.Add-Sec-Fun

P.Add-Sec-Fun Additional Specific Security Functionality
The TOE shall provide the following security functionality to the security IC embedded software:

- Memory access control

3.4. Assumptions

This Security Target claims conformance to the Security IC Platform Protection Profile [1]. The assumptions claimed in this Security Target defined in section 3.4 of the Protection Profile. They are specified below.

Table 3 Assumptions defined in the Protection Profile

Assumption	Title
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
A.Resp-Appl	Treatment of User Data

4. Security objectives

This chapter provides the statement of security objectives and the security objective rationale. For this chapter the Security IC Platform Protection Profile [1] can be applied completely. Only a short overview is given in the following.

4.1. Security objectives for the TOE

All objectives described in the section 4.1 of the Security IC Platform Protection Profile [1] are claimed for the TOE, these are:

Table 4 Security objectives for the TOE defined in the Protection Profile

Security Objective	Title
O.Phys-Manipulation	Protection against Physical Manipulation
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunctions
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality
O.Identification	TOE Identification
O.RND	Random Numbers

The following additional security objectives are taken from the PP [1] for the provision of hardware based Cryptographic services:

Security Objective	Title
O.TDES	Cryptographic service Triple-DES
O.AES	Cryptographic service AES

In addition the TOE defines the following objectives:

O.RSA RSA functionality

The TOE shall provide secure cryptographic services implementing the RSA cryptographic algorithm for encryption and decryption.

O.MEM_ACCESS Memory Access Control

The TOE shall control access of CPU instructions to memory partitions based on logical address of the code. For different memory partitions, the access of CPU instructions could be none, readable, writable, executable or their combination.

4.2. Security objectives for the security IC embedded software

All security objectives for the Security IC Embedded Software environment described in section 4.2 of the Security IC Platform Protection Profile [1] are claimed for the TOE, these are:

Table 5 Security Objectives for the security IC embedded software environment defined in the Protection Profile

Security Objective	Title
OE.Resp-Appl	Treatment of User Data of the composite TOE

4.3. Security objectives for the operational environment

The security objectives for the operational environment that are claimed in this Security Target are the security objectives described in section 4.3 of the "Security IC Platform Protection Profile" [1], which are:

Table 6 Security Objectives for the operational environment defined in the Protection Profile

Security Objective	Title
OE.Process-Sec-IC	Protection during composite product manufacturing

4.4. Security objectives rationale

Section 4.4 in the Protection Profile provides a rationale how the assumptions, threats and organisational security policies are addressed by the objectives. The table below shows this relationship.

Assumption, Threat or Organisational Security Policy	Security Objective
A.Resp-Appl	OE.Resp-Appl
P.Process-TOE	O.Identification
A.Process-Sec-IC	OE.Process-Sec-IC
T.Leak-Inherent	O.Leak-Inherent
T.Phys-Probing	O.Phys-Probing
T.Malfunction	O.Malfunction
T.Phys-Manipulation	O.Phys-Manipulation
T.Leak-Forced	O.Leak-Forced
T.Abuse-Func	O.Abuse-Func
T.RND	O.RND

For the justification of the above mapping please refer to the Protection Profile.

The table below shows how the additional organisational security policies are addressed by objectives for the TOE.

Assumption, Threat or Organisational Security Policy	Security Objective
P.Add-Sec-Fun	O.MEM_ACCESS
P.Crypto-Service	O.TDES O.AES O.RSA

Note that O.TDES and O.AES have been taken from the PP [1]. The others have been added.

The objective O.MEM_ACCESS implements specific security functionality as required by P.Add-Sec-Fun.

The objective O.RSA implement specific crypto services as required by P.Crypto-Service.

5. Extended Components Definitions

This Security Target uses the extended security functional requirements defined in chapter 5 of the Security IC Platform Protection Profile [1].

This Security Target does not define extended components in addition to the Protection Profile.

6. Security requirements

This chapter presents the statement of security requirements for the TOE and the security requirements rationale. This chapter applies the Security IC Platform Protection Profile [1].

6.1. Definitions

In the next sections the following notation is used:

- The iteration operation is used when a component is claimed with varying operations, it is denoted by adding “[XXX]” to the component name.
- Refinement, selection or assignment operations are used to add details or assign specific values to components, they are indicated by italic text and explained in footnotes.

6.2. Security Functional Requirements (SFR)

To support a better understanding of the combination Security IC Platform Protection Profile vs. Security Target, the TOE Security Functional Requirements are presented in the following several different sections.

6.2.1. SFRs derived from the Security IC Platform Protection Profile

The table below lists the Security Functional Requirements that are directly taken from the Security IC Platform Protection Profile.

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”

Application note: FCS_COP.1 and FCS_CKM.4 are also from PP0084 and described in section 6.2.2.

Application note: For FPT_FLS.1 there are 2 secure states, CPU halt and chip reset. When the external voltage is below the voltage safe range but above the power-down voltage level and when instruction fault is detected, the secure state is CPU halt. For the rest malfunctions, the secure state is chip reset.

Application note: For FPT_FLS.1 there are 2 automatic responses, CPU halt and chip reset. When the external voltage is below the voltage safe range but above the power-down voltage level and when instruction fault is detected, the automatic response is CPU halt. For the rest malfunctions, the automatic response is chip reset.

Except for FAU_SAS.1, FDP_SDC.1, FDP_SDI.2 and FCS_RNG.1 all assignment and selection operations are defined in the Protection Profile.

- In FAU_SAS.1 the left open assignment is the type of persistent memory;
- In FDP_SDC.1 the left open assignment is the memory area;
- In FDP_SDI.2 the left open assignments are the user data attributes and the action to be taken;
- In the FCS_RNG.1 the left open definition is the quality metric for the random numbers.

The following statements define these completed SFRs.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

FAU_SAS.1.1 The TSF shall provide *the test process before TOE Delivery*[1] with the capability to store *the Initialisation Data and/or Pre-personalisation Data* [2]in the *OTP*[3].

Dependencies: No dependencies.

FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.

FDP_SDC.1.1 The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *ROM, NVM and part of the RAMs*[4].

Dependencies: No dependencies.

Application note: The confidentiality of user data stored in the NVM, System RAM and Coprocessor RAM is provided. The confidentiality of user data stored in CLA RAM is not claimed.

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for *parity errors or error correction errors or inconsistency between stored data and complementary bits or copy bits* [5] on all objects, based on the following attributes: *parity bits, error correction bits, complementary bits, or copy bits*[6].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall *reset*[7].

---

[1][assignment: list of subjects]
[2][assignment: list of audit information]
[3][assignment: type of persistent memory]
[4][assignment: memory area]
[5][assignment: integrity errors]
[6][assignment: user data attributes]
[7][assignment: action to be taken]

Dependencies: No dependencies.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

FCS_RNG.1.1 The TSF shall provide a *physical*[8] random number generator that Implements:

- *(PTG.2.1)A total failure test of the entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.*
- *(PTG.2.2)If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source*[9].
- *(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.*
- *(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.*
- *(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered externally*[10]*. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time*[11]

FCS_RNG.1.2 The TSF shall provide *octets of bits*[12] that meet:

- *(PTG.2.6) Test procedure A[6] and no other test suites*[13] *does not distinguish the internal random numbers from output sequences of an ideal RNG.*
- *(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.*

Dependencies: No dependencies.

Application note: Online testing is triggered by an API invocation.

6.2.2. SFRs regarding cryptographic functionality

FCS_COP.1[TDES] Cryptographic operation - Triple-DES

Hierarchical to: No other components.

FCS_COP.1.1[TDES] The TSF shall perform *encryption and decryption*[14] in accordance with a specified cryptographic algorithm *TDES in ECB and CBC mode*[15]and

---

[8][selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*]

[9][selection: prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy].

[10] [selection: externally, at regular intervals, continuously, applied upon specified internal events].

[11] [assignment: list of security capabilities].

[12][selection: bits, octets of bits, numbers [assignment: format of the numbers]]

[13][assignment: additional standard test suites]

[14][assignment: list of cryptographic operations]

[15][assignment: cryptographic algorithm]

cryptographic key sizes of *112 bit and 168 bit*[16] that meet the following *NIST SP800-67[7], NIST SP800-38A*[17]*[8]*.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Application note: The TOE also supports single DES. However, the security of the single DES algorithm is not resistant against attacks with a high attack potential. Therefore, the application of single DES shall not be used in parts of the Security Embedded Software that require high security.

FCS_CKM.4[TDES] Cryptographic key destruction - TDES

Hierarchical to: No other components.

Dependencies: FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1[TDES] The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting the internally stored key*[18] that meets the following: *none*[19].

FCS_COP.1[AES] Cryptographic operation - AES

Hierarchical to: No other components.

FCS_COP.1.1[AES] The TSF shall perform *encryption and decryption*[20] in accordance with a specified cryptographic algorithm *AES in ECB and CBC mode*[21]and cryptographic key sizes of *128 bit, 192 bit and 256 bit*[22] that meet the following *FIPS 197[10], NIST SP800-38A*[23]*[8]*.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4[AES] Cryptographic key destruction - AES

Hierarchical to: No other components.

Dependencies: FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1[AES] The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting the internally stored key*[24] that meets the following: *none*[25].

---

[16][assignment: cryptographic key sizes]
[17][assignment: list of standards]
[18][assignment: cryptographic key destruction method]
[19][assignment: list of standards]
[20][assignment: list of cryptographic operations]
[21][assignment: cryptographic algorithm]
[22][assignment: cryptographic key sizes]
[23][assignment: list of standards]
[24][assignment: cryptographic key destruction method]
[25][assignment: list of standards]

FCS_COP.1[RSA] Cryptographic operation - RSA

Hierarchical to: No other components.

FCS_COP.1.1[RSA] The TSF shall perform *signature generation and decryption*[26] in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes from 256 to 2048 bit (step 64 bits) that meet PKCS#1 V2.2.[9]

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4[RSA] Cryptographic key destruction - RSA

Hierarchical to: No other components.

Dependencies: FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1[RSA] The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting the internally stored key*[27] that meets the following: *none*[28].

6.2.3. SFRs regarding access control

The hardware of the TOE shall provide different permissions to the Security IC embedded software to enable the management of access to code and data. The Security Function Policy (SFP) *Memory Access Control Policy* uses the following definitions.

The **Subjects** are:

- The *Software* in the memories (including Security IC Embedded software) of the TOE accessing memory as part of their software execution. There are two *Software* Subjects: *API service Code and User Code.*
  The *API service Code* consists of FMSH_CryptoLib and the Driver services for IC Embedded software.

The **Objects** are:

- *Memory Data (*including code) stored in memory. It includes *API service Code, User Code, User Data, User Sensitive Data, CFG Section Data, System RAM Data, Coprocessor RAM Data, and CLA RAM Data*.

The memory **Operations** are:

- *Read/write* data from and to memory,
- *Execute* code from memory

The **Security Attributes** are:

- *Data Area* (location of the data in memory)

[26][assignment: list of cryptographic operations]
[27][assignment: cryptographic key destruction method]
[28][assignment: list of standards]

- *Code Area* (location of the code in memory)
- *Operation mode, these can be Org Mode, Prog Mode and User Mode.*
- *Access permission rights (*these can be "No access", combination of "Executable", "Read" or "Write")

The TOE shall meet the requirements "Subset access control (FDP_ACC.1)" as specified below.

FDP_ACC.1	**Subset access control**
Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the *Access Control Policy*[29] on (1) *the subjects: API service Code and User Code,* (2) *the objects: Memory Data,* (3) *the operation: read, write and execute*[30]
Dependencies:	FDP_ACF.1 Security attribute based access control.

Application Note: The Access Control Policy shall be enforced by implementing a Memory Management Unit. Before a respective memory address is accessed, the Memory Management Unit checks if the memory operation is allowed.

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below.

FDP_ACF.1	**Security attribute based access control**
Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the *Access Control Policy* [31] to objects based on the following: all subjects and objects and the attributes *Code Area, Data Area and Access Permission Rights*[32].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *The operation is allowed if the Code Area and the Data Area match an entry in the current set of Access Permission Rights*[33]
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*[34]
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none*[35].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute

[29] [assignment: access control SFP]
[30] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[31] [assignment: access control SFP]
[32] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
[33] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[34] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[35] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

6.3. Security Assurance Requirements (SAR)

The Security Assurance Requirements claimed for the TOE are the SARs claimed in section 6.2 of the Security IC Protection Profile [1].

This Security Target will be evaluated according to Security Target evaluation (Class ASE)

The Security Assurance Requirements for the evaluation of the TOE are the components in Assurance Evaluation level EAL6 augmented by the components ASE_TSS.2. The table below shows the details of these assurance requirements.

Table 7 TOE assurance requirements

Security assurance requirements	Titles
Class ADV: Development	
ADV_ARC.1	Architectural design
ADV_FSP.5	Functional specification
ADV_IMP.2	Implementation representation
ADV_INT.3	TSF internals
ADV_SPM.1	Security policy modelling
ADV_TDS.5	TOE design
Class AGD: Guidance documents	
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative user guidance
Class ALC: Life-cycle support	
ALC_CMC.5	CM capabilities
ALC_CMS.5	CM scope
ALC_DEL.1	Delivery
ALC_DVS.2	Development security
ALC_LCD.1	Life-cycle definition
ALC_TAT.3	Tools and techniques
Class ASE: 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.2	TOE summary specification
Class ATE: Tests	
ATE_COV.3	Coverage
ATE_DPT.3	Depth
ATE_FUN.2	Functional testing
ATE_IND.2	Independent testing
Class AVA: Vulnerability analysis	
AVA_VAN.5	Vulnerability analysis

ADV_SPM.1	**Formal TOE security policy model**
Hierarchical to:	No other components.
ADV_SPM.1.1D	The developer shall provide a formal security policy model for the *Memory Access Control Policy (FDP_ACC.1, FDP_ACF.1 with the associated dependencies.)*[36].
ADV_SPM.1.2D	For each policy covered by the formal security policy model, the model shall identify the relevant portions of the statement of SFRs that make up that policy.
ADV_SPM.1.3D	The developer shall provide a formal proof of correspondence between the model and any formal functional specification.
ADV_SPM.1.4D	The developer shall provide a demonstration of correspondence between the model and the functional specification.
Dependencies:	ADV_FSP.4 Complete functional specification

6.4. Security requirements rationale

6.4.1. Security Functional Requirements (SFR)

The table below provides an overview of how the security functional requirements are combined to meet the security objectives.

Security Objectives for the TOE	Security Functional Requirements	Fulfilment of mapping
O.Leak-Inherent	FDP_ITT.1 FDP_IFC.1 FPT_ITT.1	See PP
O.Phys-Probing	FDP_SDC.1 FPT_PHP.3	See PP
O.Malfunction	FRU_FLT.2 FPT_FLS.1	See PP
O.Phys-Manipulation	FPT_PHP.3 FDP_SDI.2	See PP
O.Leak-Forced	FDP_ITT.1 FDP_IFC.1 FPT_ITT.1 FRU_FLT.2 FPT_FLS.1 FPT_PHP.3	See PP
O.Abuse-Func	FMT_LIM.1 FMT_LIM.2 FDP_ITT.1 FDP_IFC.1 FPT_ITT.1 FRU_FLT.2 FPT_FLS.1	See PP

[36] [assignment: list of policies that are formally modelled]

	FPT_PHP.3	
O.Identification	FAU_SAS.1	See PP
O.RND	FCS_RNG.1 FDP_ITT.1 FPT_ITT.1 FDP_IFC.1 FPT_PHP.3 FRU_FLT.2 FPT_FLS.1	See PP
O.TDES	FCS_COP.1[TDES] FCS_CKM.4[TDES]	O.TDES requires the TOE to support Triple-DES encryption and decryption with its specified key lengths. The claim for FCS_COP.1[TDES] is suitable to meet the objective O.TDES.
O.AES	FCS_COP.1[AES] FCS_CKM.4[AES]	O.AES requires the TOE to support AES encryption and decryption with its specified key lengths. The claim for FCS_COP.1[AES] is suitable to meet the objective O.AES.
O.RSA	FCS_COP.1[RSA] FCS_CKM.4[RSA]	O.RSA requires the TOE to support RSA encryption and decryption with its specified key lengths. The claim for FCS_COP.1[RSA] is suitable to meet the objective O. RSA.
O.MEM_ACCESS	FDP_ACC.1 FDP_ACF.1	O.MEM_ACCESS requires the TOE to control access of CPU instructions to memory partitions. The security functional requirement "Security attribute based access control (FDP_ACF.1 with the related Security Function Policy (SFP) "Access Control Policy" FDP_ACC.1) defines the rules to implement a memory region based access control service to the Security IC Embedded Software.
OE.Process-Sec-IC	-	Fulfilled by FM1280 Security Programming Guidance
OE.Plat-Appl	-	Fulfilled by FM1280 Security Programming Guidance
OE.Resp-Appl	-	Fulfilled by FM1280 Security Programming Guidance
Security Objectives for the TOE	Dependencies	Fulfilment of dependencies, see next paragraph

6.4.2. Dependencies of the SFRs

The dependencies for the SFRs claimed according to the Protection Profile are all satisfied in the set of SFRs claimed in the Protection Profile.

In the following table the dependencies of the SFRs claimed in addition to Protection Profile is indicated.

Security functional requirement	Dependencies	Fulfilled by security requirements in this Security Target
FCS_COP.1[TDES]	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1,	See explanation below this table
	FCS_CKM.4	FCS_CKM.4[TDES]
FCS_CKM.4[TDES]	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1,	See explanation below this table
FCS_COP.1[AES]	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1,	See explanation below this table
	FCS_CKM.4	FCS_CKM.4[AES]
FCS_CKM.4[AES]	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1,	See explanation below this table
FCS_COP.1[RSA]	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1,	See explanation below this table
	FCS_CKM.4	FCS_CKM.4[RSA]
FCS_CKM.4[RSA]	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1,	See explanation below this table
FDP_ACC.1	FDP_ACF.1	Fulfilled by FDP_ACF.1 in this ST
FDP_ACF.1	FDP_ACC.1	Fulfilled by FDP_ACC.1 in this ST
	FMT_MSA.3	See discussion below

The developer of the Security IC Embedded Software must ensure that the implemented additional security functional requirements FCS_COP.1[TDES], FCS_COP.1[AES] and FCS_COP.1[RSA] are used as specified and that the User Data processed by the related security functionality is protected as defined for the application context.

The dependent requirements for FCS_COP.1[TDES], FCS_COP.1[AES], FCS_COP.1[RSA], FCS_CKM.4[TDES], FCS_CKM.4[AES] and FCS_CKM.4[TDES]address the appropriate management of cryptographic keys used by the specified cryptographic function. All requirements concerning these management functions shall be fulfilled by the environment (Security IC Embedded Software).

The functional requirements [FDP_ITC.1, or FDP_ITC.2 or FCS_CKM.1] are not included in this Security Target since the TOE only provides a pure engine for encryption and decryption without additional features for the handling of cryptographic keys. Therefore, the Security IC Embedded Software must fulfil these requirements related to the needs of the realised application.

The SFR FMT_MSA.3 is not necessary because the security attributes used to enforce the memory access control are fixed by the IC manufacturer.

6.4.3. Security Assurance Requirements (SAR)

The SARs as defined in section 6.3 are in line with the SARs in the Security IC Platform Protection Profile. The context of this ST is equivalent to the context described in the Protection Profile and therefore these SARs are also applicable for this ST.

6.4.4. Dependencies of the SARs

The assurance level EAL6 augmented with ASE_TSS.2 is chosen. The assurance package EAL6 is a well pre-defined level of CC. The assurance components in an EAL package are built in a mutually supportive and systematic way. The requirement chosen for augmentation add one dependency which is between ASE_TSS.2 and ADV_ARC.1. This dependency is also fulfilled. Therefore, the internal dependencies of the SARs are met.

7. TOE summary specification

This chapter provides general information to potential users of the TOE on how the TOE implements the Security Functional Requirements in terms of “Security Functionality”.

7.1. Security architectural design

As required by ASE_TSS.2, TOE summary specification needs to describe how the TOE protects itself against interference, logical tampering and bypass in the level of security architectural design.

7.1.1 Protection against interference and logical tampering

The interference and logical tampering can be taken by external entities that may result in changes to the TSF so that it no longer fulfils the SFRs. The TOE has the ability to protect itself from it by means of following protections.

Attackers may tamper with or probe the internal signals of the chip by means of physical probing, which may lead to the failure of security functions or security mechanisms.

The TOE provides an active shield to sense the physical probing along with the chip operation. The shield covers the entire chip, so the probing into the underneath circuits will will cause a chip reset.

The TOE also provides integrity check for critical registers and memory data. An attacker tampering with these registers or memory data by physical probing will cause an integrity check failure, that will trigger a chip reset or security interrupt.

The TOE provides environmental sensors to detect environmental anomalies, and enters a chip reset or CPU stop when they occur. Moreover, the self-test function of the sensors provides its own protection against manipulation on itself.

In addition, TOE's algorithm service’s hardware and software provide anti-fault injection countermeasures. They check the algorithm results to determine whether they have errors or not, and provide error messages when errors are detected.

Attackers may steal sensitive data by side channel attacks or memory access. The TOE's algorithm service protect the data in operation from disclosure. Moreover, TOE also provides a secure transfer feature and the memory access control to ensure that the sensitive data will not be leaked.

7.1.2 Protection against bypass of security functionality

Non-bypassability is a property expressing that the security functionality of the TSF is always invoked and cannot be circumvented. The TOE’s non-bypassability is guaranteed by the means of software and hardware both.

Preventive measures provided by the software:

The software of the algorithm service provides integrity checks. An error message will be given if errors are found. It prevents the algorithmic service from being bypassed.

Preventive measures provided by the hardware:

The TOE provides a configuration and mode protection function to ensure that the chip's security functions and mechanisms can be effectively implemented.

The TOE's memory access control function prevents the function parameter checking and other security operations from being bypassed.

The TOE's hardware security features and mechanisms are continuously active while the TOE is working. And the algorithm service's security mechanisms are designed to be continuously active while the algorithm is operating. Thus, they cannot be bypassed.

7.2. Protection against malfunction

Malfunctioning relates to the security functional requirements FRU_FLT.2 and FPT_FLS.1. The TOE meets these SFRs by a group of security measures that guarantee correct operation of the TOE.

The TOE ensures its correct operation and prevents any malfunction while the security IC embedded software is executed through an appropriate design of the TOE including environment sensors or detectors. In case that any malfunction occurred, an alarm will be triggered. Any alarm will trigger a system reset except the low voltage alarm that will trigger a CPU Halt.

7.3. Protection against leakage

Leakages relate to the security functional requirements FDP_ITT.1, FDP_IFC.1 and FPT_ITT.1. The TOE meets these SFRs by implementing secure transfer based on data bus masking and SCA countermeasures in the crypto coprocessors and crypto lib that provides logical protection against leakage.

7.4. Protection against physical attacks

Physical manipulation and probing relates to the security functional requirements FPT_PHP.3, FDP_SDC.1 and FDP_SDI.2. The TOE meets this SFR by implementing security measures that provides physical protection against physical probing and manipulation.

The security measures protect the TOE against manipulation of
(i) the hardware,
(ii) the security IC embedded software in the NVM,

(iii) the application data in the NVM and RAM including the configuration data.

It protects the integrity and confidentiality of User Data or TSF data against disclosure by physical probing when stored or while being processed by the TOE.

The protection of the TOE comprises different features within the design and construction, which make reverse-engineering and tamper attacks more difficult. These features comprise whole chip covered active shield, memory encryption, and data integrity protections for memories and critical registers.

7.5. Identification and prevent abuse of functionality

Abuse of functionality and Identification relates to the security functional requirements FMT_LIM.1, FMT_LIM.2 and FAU_SAS.1. The TOE meets these SFRs by implementation of a configuration and mode protection mechanism that prevents abuse of test functionality delivered as part of the TOE. The Identification data is stored in the OTP.

The test functionality is not available to the user after delivery of the TOE to the Composite Manufacturer.

7.6. Random number generator

Random numbers relate to the security requirement FCS_RNG.1. The TOE meets this SFR by providing a random number generator.

The random number generator is composed of entropy source, total failure test, start-up test, online test and post-processing circuits. The random number generator fulfils the AIS31 PTG.2[6].

7.7. Cryptographic encryption/decryption

The TOE provides the single and Triple-DES algorithm according to the *NIST SP800-67[1] and NIST SP800-38A[8]* Standard to meet the security requirement FCS_COP.1[TDES]. The TOE implements the Triple-DES algorithm as defined by *NIST SP800-67* by means of a hardware coprocessor. It supports the DES algorithm with a single 56-bit key supporting both CBC and ECB mode. It supports the Triple-DES algorithm with three 56-bit keys (168 bit) for the 3-key Triple-DES or two 56-bit keys for 2-key Triple DES supporting both CBC and ECB mode. The keys for the DES algorithms shall be provided by the security IC embedded software.

The single DES algorithm should be used in secure way according to the application's security need.

The TOE provides the AES algorithm according to the *FIPS 197[10] and NIST SP800-38A[8]* Standard to meet the security requirement FCS_COP.1[AES]. The TOE implements the AES algorithm as defined by *FIPS 197* by means of a hardware coprocessor. It supports the AES algorithm with 128-bit, 192-bit or 256-bit key supporting both CBC and ECB mode. The keys for the AES algorithms shall be provided by the security IC embedded software.

The TOE provides the RSA algorithm according to the *PKCS#1 V2.2[9]* Standard to meet the security requirement FCS_COP.1[RSA]. The TOE implements the RSA algorithm as defined by *PKCS#1 V2.2* by means of the combination of a hardware RSA accelerator and the security IC embedded RSA software. It supports RSA encryption and decryption from 256 bits to 2048 bits(step 64 bits). The signature generation and decryption can be performed by either a straightforward method or a CRT (Chinese Remainder Theorem) method. The keys for the RSA algorithm shall be provided by the security IC embedded software.

The TOE provides internal security measures for FCS_CKM.4[TDES], FCS_CKM.4[AES], FCS_CKM.4[RSA] which clear memory areas used by the Crypto Library after usage. These measures ensure that a subsequent process may not gain access to cryptographic assets stored temporarily in memory used by the TOE.

7.8. Memory access control

The TOE provides a Memory Management security function to the Security Embedded IC Software through the Memory Management Unit (MMU) to meet the Security Functional Requirements FDP_ACC.1, FDP_ACF.1.

The memory access is defined by both the fixed logic in MMU and configuration in OTP. Therefore, it cannot be modified from the embedded software.

8. Annexes

8.1. Glossaries

CLA	Contactless interface supporting type A
FMSH_CryptoLib	A part of firmware, providing crypto related APIs for the users' invoking
FA	Fault attack, a kind of attack to retrieve secret data or to bypass security checks by fault injection during Secure IC operation
Org Mode	An operation mode of the TOE. This mode is used for NVM testing and initializing.
Prog Mode	An operation mode of the TOE. This mode is used for initialize the configuration and download program and data after manufacture.
User Mode	An operation mode of the TOE. The TOE is delivered in this mode.

8.2. List of Abbreviations

APDU	Application Protocol Data Unit
API	Application Programming Interface
CT	Contact
CL	Contactless
CPU	Central Processing Unit
DES	Data Encryption Standard
GPIO	General Purpose Input/Output
IC	Integrated Circuit
MMU	Memory Management Unit
NVM	Non-Volatile Memory
PAE	Public-key Algorithm Engine
PP	Protection Profile
RAM	Random Access Memory
ROM	Read Only Memory
ST	Security Target
TRNG	True Random Number Generator
CLA RAM	RAM for contactless type A communication

9. References

Ref	Title	Version	Date
[1]	Security IC Platform Protection Profile, BSI-CC-PP-0084-2014	Version 1.0	13.01.2014
[2]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model CCMB-2017-04-001	Version 3.1 Revision 5	April 2017
[3]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements CCMB-2017-04-002	Version 3.1 Revision 5	April 2017
[4]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements CCMB-2017-04-003	Version 3.1 Revision 5	April 2017
[5]	Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology CCMB-2017-04-004	Version 3.1 Revision 5	April 2017
[6]	[AIS 20/31] Functionality classes and evaluation methodology for deterministic/physical random number generators, version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik	Version 3	May 2013
[7]	NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised January 2012, National Institute of Standards and Technology	Version 1.0	January 2012
[8]	NIST SP 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001	2001 Edition	December 2001
[9]	PKCS #1: RSA Cryptography Standard, RSA Laboratories	Version 2.2	27 October 2012
[10]	Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001		November, 2001