**STMicroelectronics**

# ST33J2M0 D03 including optional cryptographic library NESLIB, and optional technology MIFARE4Mobile® Security Target for composition

# Common Criteria for IT security evaluation

**SMD_ST33J2M0_ST_19_004 Rev D03.0**

**July 2022**

BLANK

# ST33J2M0 D03 platform
# Security Target for composition

## Common Criteria for IT security evaluation

# 1 Introduction (ASE_INT)

## 1.1 Security Target reference

1   Document identification: ST33J2M0 D03 including optional cryptographic library NesLib, and optional technology MIFARE4Mobile® SECURITY TARGET FOR COMPOSITION.

2   Version number: Rev D03.0, issued in July 2022.

3   Registration:   registered at ST Microelectronics under number SMD_ST33J2M0_ST_19_004.

## 1.2 TOE reference

4   This document presents **the Security Target (ST)** of the **ST33J2M0 D03** Security Integrated Circuit (IC), designed on the **ST33 platform of STMicroelectronics**, with firmware version 3.2.5 and 3.3.0, optional cryptographic library **NesLib 6.3.4,** and optional technology **MIFARE4Mobile® rev 2.2.9 and 2.2.10**.

5   The precise reference of the Target of Evaluation (TOE) is given in *Section 1.4: TOE identification* and the security IC features are given in *Section 1.6: TOE description*.

6   A glossary of terms and abbreviations used in this document is given in *Appendix A: Glossary*.

# Contents

# List of tables

# List of figures

## 1.3 Context

7    The Target of Evaluation (TOE) referred to in *Section 1.4: TOE identification*, is evaluated under the French IT Security Evaluation and Certification Scheme and is developed by the Secure Microcontrollers Division of STMicroelectronics (ST).

8    The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL5 augmented by ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ASE_TSS.2, ATE_COV.3, ATE_FUN.2 and AVA_VAN.5.

9    The intent of this Security Target is to specify the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) applicable to the TOE security ICs, and to summarise their chosen TSF services and assurance measures.

10   This ST claims to be an instantiation of the "*Eurosmart - Security IC Platform Protection Profile with Augmentation Packages*" (PP) registered and certified under the reference *BSI-CC-PP-0084-2014* in the German IT Security Evaluation and Certification Scheme, **with the following augmentations**:

   •    Addition #1:    "Support of Cipher Schemes"              from *AUG*

   •    Addition #4:    "Area based Memory Access Control"       from *AUG*

   •    Additions specific to this Security Target, some of which in compliance with *JIL SRFPDCL* and *ANSSI-CC-CER/F/06.003*.

   The original text of this PP is typeset as indicated here, its augmentations from *AUG* as indicated here, and text originating in *JIL SRFPDCL* and *ANSSI-CC-CER/F/06.003* as indicated here, when they are reproduced in this document.

   This ST instantiates the following packages from the above mentioned PP:

   •    Authentication of the Security IC

   •    Loader dedicated for usage in secured environment only

   •    Loader dedicated for usage by authorized users only.

11   Extensions introduced in this ST to the SFRs of the Protection Profile (PP) are **exclusively** drawn from the Common Criteria part 2 standard SFRs.

12   This ST makes various refinements to the above mentioned PP and *AUG*. They are all properly identified in the text typeset as ***indicated here*** or ~~here~~. The original text of the PP is repeated as scarcely as possible in this document for reading convenience. All PP identifiers have been however prefixed by their respective origin label: **BSI** for *BSI-CC-PP-0084-2014*, **AUG1** for Addition #1 of *AUG*, **AUG4** for Addition #4 of *AUG*., and **ANSSI** for *JIL SRFPDCL* and *ANSSI-CC-CER/F/06.003*.

## 1.4 TOE identification

13   The Target of Evaluation (TOE) is the ST33J2M0 D03 platform.

14   "ST33J2M0 D03" completely identifies the TOE including its components listed in *Table 1: TOE components*, its guidance documentation detailed in *Table 15: Guidance documentation*, and its development and production sites indicated in *Table 16: Sites list*.

15   D03 is the version of the evaluated platform. Any change in the TOE components, the guidance documentation and the list of sites leads to a new version of the evaluated platform, thus a new TOE.

**Table 1.     TOE components**

| IC Maskset name | Master identification number [1] | IC version | Firmware version | Optional NesLib crypto library version | Optional MIFARE4Mobile version |
|---|---|---|---|---|---|
| K500A | 0137h | H | 3.2.5 and 3.3.0 | 6.3.4 | 2.2.9 and 2.2.10 |
| | | I | 3.3.0 | | |

1.   Part of the product information.

16    The IC maskset name is the product hardware identification.
The IC version is updated for any change in hardware (i.e. part of the layers of the maskset) or in the OST software.

17    All along the product life, the marking on the die, a set of accessible registers and a set of specific instructions allow the customer to check the product information, providing the identification elements, as listed in *Table 1: TOE components*, and the configuration elements as detailed in the Data Sheet, referenced in *Table 15: Guidance documentation*.

## 1.5     TOE overview

18    The ST33J2M0 is a serial access microcontroller designed for secure mobile applications that incorporates the most recent generation of ARM processors for embedded secure systems. Its SecurCore® SC300™ 32-bit RISC core is built on the Cortex® M3 core with additional security features to help to protect against advanced forms of attacks.

19    Cadenced at 70 MHz, the SC300™ core brings great performance and excellent code density thanks to the Thumb®-2 instruction set.

20    Strong and multiple fault protection mechanisms ensure a guaranteed high-detection coverage that facilitates the development of highly secure software. This is achieved by using two CPUs in locked-step mode, error codes in sensitive memories and hardware logic.

21    The high-speed embedded Flash memory introduces flexibility to the system.

22    Different derivative devices may be configured depending on the customer needs:

   •    either by ST during the manufacturing or packaging process,

   •    or by the customer during the packaging, composite product integration, or personnalisation process.

23    The derivative devices all share the same hardware design and the same maskset (denoted by the Master identification number). The Master identification number is unique for all product configurations.

24    The configuration of the derivative devices is realized in Admin configuration, by ST or by the customer. It can impact the available NVM size, IOs, the availability of Nescrypt, AES accelerator, EDES+ accelerator, Crypto1, and the availability of the LPU, as detailed here below:

Table 2.    Derivative devices configuration possibilities

| Features | Possible values |
|---|---|
| NVM size | Selectable by 128 Kbytes granularity from 2048 Kbytes to 512 Kbytes |
| I2C | Active, Inactive |
| IART | Active, Inactive |
| SWP | Active, Inactive |
| SPI | Active, Inactive |
| Nescrypt | Active, Inactive |
| AES accelerator (HW_AES) | Active, Inactive |
| EDES+ accelerator | Active, Inactive |
| Library Protection Unit (LPU) | Active, Inactive |
| Crypto1 | Active, Inactive |

25    All combinations of different features values are possible and covered by this certification. All possible configurations can vary under a unique IC, and without impact on security.

26    The Master identification number is unique for all product configurations.
Each derivative device has a specific Child product identification number, also part of the product information, and specified in the Data Sheet and in the Firmware User Manual, referenced in *Table 15*.

27    The rest of this document applies to all possible configuration of the TOE, with or without NesLib or MIFARE4Mobile libraries, except when a restriction is mentioned. For easier reading, the restrictions are typeset as indicated here.

28    Note that the IC version I with Firmware version 3.2.5 is not in the scope of this evaluation.

29    In a few words, the ST33J2M0 D03 offers a unique combination of high performances and very powerful features for high level security:

•    Two instances of the SecurCore® SC300™ CPU connected in Lockstep mode,

•    Die integrity,

•    Monitoring of environmental parameters,

•    Protection mechanisms against faults,

•    AIS20/AIS31 class PTG.2 compliant True Random Number Generator,

•    Memory Management Unit,

•    CRC calculation block,

•    optional Hardware Security Enhanced DES accelerator,

•    optional Hardware Security AES accelerator,

•    optional NExt Step CRYPTography accelerator (NESCRYPT),

•    optional cryptographic library,

•    optional secure MIFARE4Mobile® library.

## 1.6     TOE description

### 1.6.1     TOE hardware description

30     The TOE features hardware accelerators for advanced cryptographic functions, with built-in countermeasures against side channel and fault attacks.

31     If AES is active, the AES (Advanced Encryption Standard) accelerator provides a high-performance implementation of AES-128, AES-192 and AES-256 algorithms. It can operate in ECB (Electronic Code Book) and CBC (Cipher Block Chaining) mode.

32     If EDES+ is active, the 3-key triple DES accelerator (EDES+) supports efficiently the Data Encryption Standard (TDES [2]), enabling DES computation. It can operate in ECB (Electronic Code Book) and CBC (Cipher Block Chaining) mode.
       Note that a triple DES can be performed by a triple DES computation or by 3 single DES computations.

33     If Nescrypt is active, the NESCRYPT crypto-processor allows fast and secure implementation of the most popular public key cryptosystems with a high level of performance ([7], [12], [15],[16], [17], [18]).

34     The TOE offers 50 Kbytes of User RAM and up to 2048 Kbytes of secure User high-density Flash memory (NVM). A memory management unit (MMU) allows to use virtual addressing on these memories, and enables the user to define its own region organization with specific protection and access permissions.

35     As randomness is a key stone in many applications, the ST33J2M0 D03 features a highly reliable True Random Number Generator (TRNG), compliant with PTG.2 Class of AIS20/AIS31 [1] and directly accessible thru dedicated registers.

36     The TOE also provides a 16- and 32-bit ISO 3309 CRC calculation block (compliant to ISO13239, IEEE 802.3, etc.).

37     The ST33J2M0 D03 offers a serial communication interface fully compatible with the ISO/IEC 7816-3 standard (T=0, T=1) and a single-wire protocol (SWP) interface for communication with a near field communication (NFC) router in Secure Element applications.
       Two I2C Master/Slave interfaces are available as well as an SPI Master/Slave interface for communication in non-SIM applications.
       Three general-purpose 16-bit timers as well as a watchdog timer are available.
       All these IOs are configurable as detailed in Table 2: Derivative devices configuration possibilities.

38     The detailed features of this TOE are described in the Data Sheet and in the Cortex SC300 Technical Reference Manual, referenced in Table 15.

39     Figure 1 provides an overview of the ST33J2M0 D03 platform.

**Figure 1.     ST33J2M0 D03 platform block diagram**
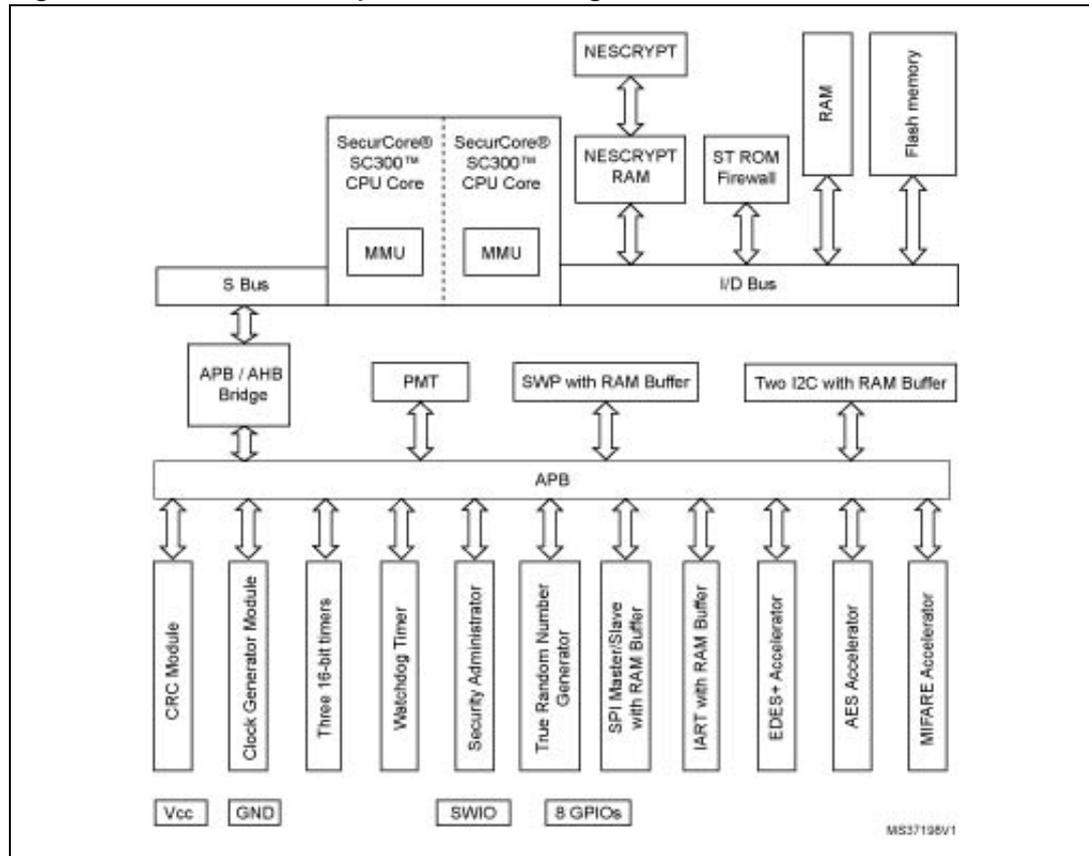


## 1.6.2     TOE software description

40       The OST ROM contains a Dedicated Software which provides full test capabilities (operating system for test, called "OST"), not accessible by the Security IC Embedded Software (ES), after TOE delivery.

41       The System ROM and ST NVM of the TOE contain a Dedicated Software (Firmware) which provides:

- a Secure Flash Loader, enabling to securely and efficiently download the Security IC Embedded Software (ES) into the NVM. It also allows the evaluator to load software into the TOE for test purpose. The Secure Flash Loader is available in Admin configuration. The customer can choose to activate it in any phase of the product life-cycle under highly secured conditions, or to deactivate it definitely at a certain step.

- low-level functions called Flash Drivers, enabling the Security IC Embedded Software (ES) to modify and manage the NVM contents. The Flash Drivers are available in User configuration.

- a set of protected commands for device testing and product profiling, not intended for the Security IC Embedded Software (ES) usage, and not available in User configuration.

- a very reduced set of uncritical commands for basic diagnostic purpose (field return analysis), only reserved to STMicroelectronics.

- a set of highly protected commands for secure diagnostic purpose (advanced quality investigations), that can only be activated by the customer and be operated by

STMicroelectronics on its own audited sites. This feature is protected by specific strong access control, completed by environmental measures which prevent access to customer assets. Furthermore, it can be permanently deactivated by the customer.

42      The Security IC Embedded Software (ES) is in User NVM.

The TOE optionally comprises a specific application in User NVM: this applicative Embedded Software is a cryptographic library called NesLib. NesLib is a cutting edge cryptographic library in terms of security and performance.

NesLib is embedded by the ES developer in his applicative code.
Note that the NesLib RSA, ECC and Diffie-Hellman functions can only be used if Nescrypt is active, the NesLib AES functions can only be used if the AES accelerator is active and the NesLib EDES functions can only be used if the EDES+ accelerator is active.

NesLib is a cryptographic toolbox supporting the most common standards and protocols:

- an asymmetric key cryptographic support module, supporting secure modular arithmetic with large integers, with specialized functions for Rivest, Shamir & Adleman Standard cryptographic algorithm (RSA *[17]*), and Diffie-Hellman *[23]*,

- an asymmetric key cryptographic support module that provides very efficient basic functions to build up protocols using Elliptic Curves Cryptography on prime fields GF(p) with elliptic curves in short Weierstrass form *[15]*, and provides support for ECDH key agreement *[21]* and ECDSA generation and verification *[5]*.

- a module for supporting elliptic curve cryptography on Edwards curve 25519, in particular ed25519 signature generation, verification and point decompression *[26]*.

- a cryptographic support module that provides secure hash functions (SHA-1[a], SHA-2 *[4]*), SHA-3, Keccak and a toolbox for cryptography based on Keccak-p, the permutation underlying SHA-3 *[25]*,

- a symmetric key cryptographic support module whose base algorithm is the Data Encryption Standard cryptographic algorithm (DES) *[2]*,

- a symmetric key cryptographic support module whose base algorithm is the Advanced Encryption Standard cryptographic algorithm (AES) *[6]*,

- support for Deterministic Random Bit Generators *[19]*,

- prime number generation and RSA key pairs generation *[3]*.

43      The TOE optionally comprises a specific application in User NVM: this applicative Embedded Software is MIFARE4Mobile®, a MIFARE technology library *[30]*.
This library is configurable according to the customer's choice. It can include MIFARE Classic®, or MIFARE® DESFire® EV1, or both.
The part of MIFARE4Mobile® featuring MIFARE® DESFire® EV1 is in the scope of this evaluation while the part of MIFARE4Mobile® featuring MIFARE Classic® is not in the scope of this evaluation.
M4M-DESFire features a mutual three pass authentication, a data encryption on RF channel, and a flexible self-securing file system.

Note that:
- MIFARE4Mobile can only be used if the LPU is active.
- M4M-DESFire can only be used if the EDES+ accelerator and the AES accelerator are

---

a.   Note that SHA-1 is no longer recommended as a cryptographic function in the context of smart card applications. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.

active.
- M4M-Classic can only be used if the Crypto1 is active (this hardware cryptographic accelerator is dedicated to MIFARE Classic support, thus not in the scope of this evaluation).

44 In this Security Target, the terms:
- "M4M" means MIFARE4Mobile®[b],
- "M4M-DESFire" denotes the part of MIFARE4Mobile® featuring MIFARE® DESFire® EV1[c],
- "M4M-Classic" denotes the part of MIFARE4Mobile® featuring MIFARE Classic®[d].

**45** **Note: The ES is not part of the TOE and is out of scope of the evaluation, except NesLib and M4M-DESFire, when they are embedded.**

### 1.6.3 TOE documentation

46 The user guidance documentation, part of the TOE, consists of:
- the product Data Sheet and die description,
- the product family Security Guidance,
- the AIS31 user manuals,
- the product family programming manual,
- the ARM SC300 Technical Reference Manual,
- the Firmware user manual,
- optionally the NesLib user manual,
- optionally the MIFARE4Mobile.

47 The complete list of guidance documents is detailed in *Table 15*.

### 1.6.4 Delivery format and method

48 The IC part of the TOE can be delivered in form of wafers, micromodules or packages, as described in the Data Sheet referenced in *Table 15*.
All the possible forms of delivery are equivalent from a security point of view.

49 The firmware is integrated on the IC before delivery, as well as the MIFARE libraries.

50 The NesLib library is delivered in form of a ciphered binary file, so that the ES developer embeds it, linked to his applicative code.

51 All the guidance documents are delivered as ciphered pdf files.

## 1.7 TOE life cycle

52 This Security Target is fully conform to the claimed PP. In the following, just a summary and some useful explanations are given. For complete details on the TOE life cycle, please refer to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), section 1.2.3.

---

b. MIFARE4Mobile is a registered trademark of NXP B.V. and is used under license.

c. MIFARE DESFire are registered trademarks of NXP B.V. and are used under license.

d. MIFARE and MIFARE Classic are registered trademarks of NXP B.V. and are used under license.

53      The composite product life cycle is decomposed into 7 phases. Each of these phases has the very same boundaries as those defined in the claimed protection profile.

**Figure 2.**      **Security IC Life-Cycle if Security IC Embedded Software is loaded by Security IC Dedicated Software into the programmable non-volatile Memory**
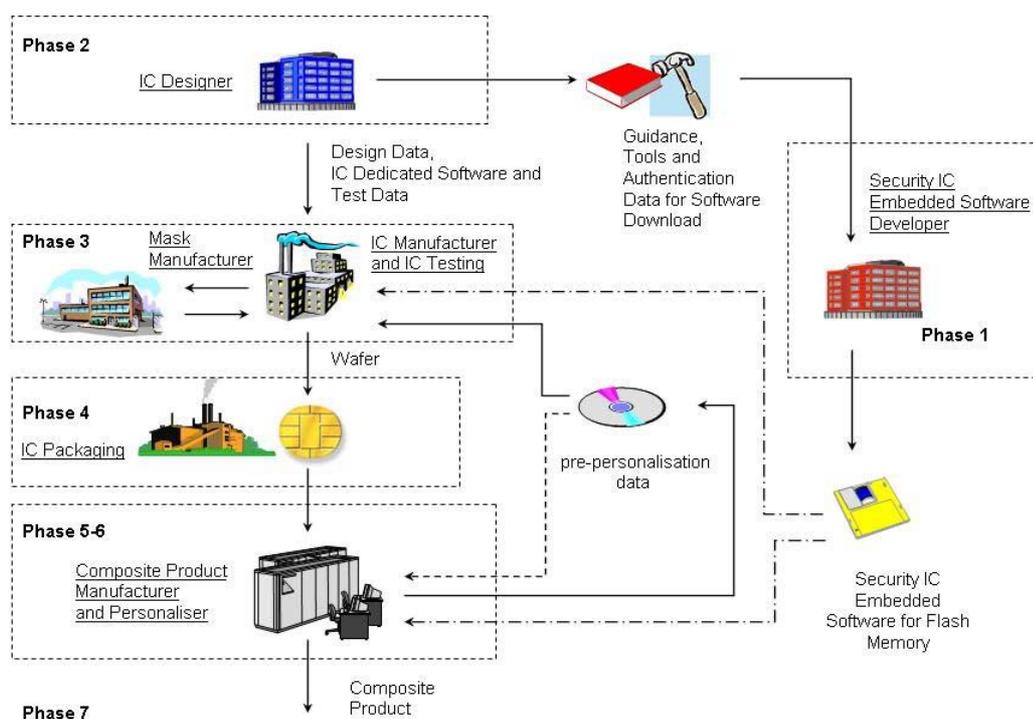


54      The life cycle phases are summarized in *Table 3*.

55      The sites potentially involved in the TOE life cycle are listed in *Table 16*.

56      The limit of the evaluation corresponds to phases 2, 3 and optionally 4, including the delivery and verification procedures of phase 1, and the TOE delivery either to the IC packaging manufacturer or to the composite product integrator ;  procedures corresponding to phases 1, 5, 6 and 7 are outside the scope of this evaluation.

57      In the following, the term "Composite product manufacturing" is uniquely used to indicate phases 1, optionally 4, 5 and 6 all together.
This ST also uses the term "Composite product manufacturer" which includes all roles responsible of the TOE during phases 1, optionally 4, 5 and 6.

58      The TOE is delivered after phase 3 in form of wafers or after phase 4 in packaged form, depending on the customer's order.

59    In the following, the term "TOE delivery" is uniquely used to indicate:

- after phase 3 (or before phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or
- after phase 4 (or before phase 5) if the TOE is delivered in form of packaged products.

60    The TOE is delivered in Admin (aka Issuer) or User configuration.

**Table 3.    Composite product life cycle phases**

| Phase | Name | Description |
|-------|------|-------------|
| 1 | Security IC embedded software development | security IC embedded software development<br>specification of IC pre-personalization requirements |
| 2 | IC development | IC design<br>IC dedicated software development |
| 3 | IC manufacturing and testing | integration and photomask fabrication<br>IC manufacturing<br>IC testing<br>IC pre-personalisation |
| 4 | IC packaging | security IC packaging (and testing)<br>pre-personalisation if necessary |
| 5 | Security IC product finishing process | composite product finishing process<br>composite product testing |
| 6 | Security IC personalisation | composite product personalisation<br>composite product testing |
| 7 | Security IC end usage | composite product usage by its issuers and consumers |

## 1.8    TOE environment

61    Considering the TOE, three types of environments are defined:

- Development environment corresponding to phase 2,
- Production environment corresponding to phase 3 and optionally 4,
- Operational environment, including phase 1 and from phase 4 or 5 to phase 7.

### 1.8.1    TOE Development Environment

62    To ensure security, the environment in which the development takes place is secured with controllable accesses having traceability. Furthermore, all authorized personnel involved fully understand the importance and the strict implementation of defined security procedures.

63    The development begins with the TOE's specification. All parties in contact with sensitive information are required to abide by Non-Disclosure Agreements.

64    Design and development of the IC then follows, together with the dedicated and engineering software and tools development. The engineers use secure computer systems (preventing unauthorized access) to make their developments, simulations, verifications and generation of the TOE's databases. Sensitive documents, files and tools, databases on tapes, and

printed circuit layout information are stored in appropriate locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

65     The development centres possibly involved in the development of the TOE are denoted by the activity "DEV" in *Table 16*.

66     Reticules and photomasks are generated from the verified IC databases; the former are used in the silicon Wafer-fab processing. As reticules and photomasks are generated off-site, they are transported and worked on in a secure environment. During the transfer of sensitive data electronically, procedures are established to ensure that the data arrive only at the destination and are not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies).

67     The authorized sub-contractors potentially involved in the TOE mask manufacturing are denoted by the activity "MASK" in *Table 16*.

### 1.8.2     TOE production environment

68     As high volumes of product commonly go through such environments, adequate control procedures are necessary to account for all product at all stages of production.

69     Production starts within the Wafer-fab; here the silicon wafers undergo the diffusion processing. Computer tracking at wafer level throughout the process is commonplace. The wafers are then taken into the test area. Testing and pre-personalization of each TOE occurs to assure conformance with the device specification and to load the customer information.

70     The authorized front-end plant possibly involved in the manufacturing of the TOE are denoted by the activity "FE" in *Table 16*.

71     The authorized EWS plant potentially involved in the testing of the TOE are denoted by the activity "EWS" in *Table 16*.

72     Wafers are then scribed and broken such as to separate the functional from the non-functional ICs. The latter is discarded in a controlled accountable manner. The good ICs are then packaged in phase 4, in a back-end plant. When testing, programming or deliveries are done offsite, ICs are transported and worked on in a secure environment with accountability and traceability of all (good and bad) products.

73     When the product is delivered after phase 4, the authorized back-end plants possibly involved in the packaging of the TOE are denoted by the activity "BE" in *Table 16*.

74     All sites denoted by the activity "WHS" in *Table 16* can be involved for the logistics.

### 1.8.3     TOE operational environment

75     A TOE operational environment is the environment of phases 1, optionally 4, then 5 to 7.

76     At phases 1, 4, 5 and 6, the TOE operational environment is a controlled environment.

77     End-user environments (phase 7): composite products are used in a wide range of applications to assure authorized conditional access. Examples of such are banking cards, brand protection, portable communication SIM cards, health cards, transportation cards, access management, identity and passport cards. The end-user environment therefore covers a wide range of very different functions, thus making it difficult to avoid and monitor any abuse of the TOE.

# 2     Conformance claims (ASE_CCL, ASE_ECD)

## 2.1     Common Criteria conformance claims

78     The ST33J2M0 D03 platform Security Target claims to be conformant to the Common Criteria version 3.1 revision 5.

79     Furthermore it claims to be CC Part 2 (*CCMB-2017-04-002*) extended and CC Part 3 (*CCMB-2017-04-003*) conformant.

80     The extended Security Functional Requirements are those defined in the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*):

- **FCS_RNG** Generation of random numbers,
- **FMT_LIM** Limited capabilities and availability,
- **FAU_SAS** Audit data storage,
- **FDP_SDC** Stored data confidentiality,
- **FIA_API** Authentication proof of identity .

The reader can find their certified definitions in the text of the "*BSI-CC-PP-0084-2014*" Protection Profile.

81     The assurance level for the ST33J2M0 D03 platform Security Target is **EAL 5** augmented by ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ASE_TSS.2, ATE_COV.3, ATE_FUN.2 and AVA_VAN.5.

## 2.2     PP Claims:

### 2.2.1     PP Reference

82     The ST33J2M0 D03 platform Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), for the part of the TOE covered by this PP (Security IC), as required by this Protection Profile.

83     The following packages have been selected from the *BSI-CC-PP-0084-2014*:

- Package "Authentication of the Security IC",
- Packages for Loader:
    - Package 1: Loader dedicated for usage in Secured Environment only,
    - Package 2: Loader dedicated for usage by authorized users only.

### 2.2.2    PP Additions

84    The main additions operated on the *BSI-CC-PP-0084-2014* are:

- Addition #4:    "Area based Memory Access Control"    from *AUG*,
- Addition #1:    "Support of Cipher Schemes"    from *AUG*,
- Specific additions for the Loader, to comply with *JIL SRFPDCL* and *ANSSI-CC-CER/F/06.003*,
- Specific additions for the Secure Diagnostic capability,
- Specific additions for M4M,
- Refinement of assurance requirements.

85    All refinements are indicated with type setting text ***as indicated here***, original text from the *BSI-CC-PP-0084-2014* being typeset as indicated here or ~~here~~. Text originating in *AUG* is typeset as indicated here. Text originating in *JIL SRFPDCL* and *ANSSI-CC-CER/F/06.003* is typeset as indicated here.

86    The security environment additions relative to the PP are summarized in *Table 4*.

87    The additional security objectives relative to the PP are summarized in *Table 5*.

88    A simplified presentation of the TOE Security Policy (TSP) is added.

89    The additional SFRs for the TOE relative to the PP are summarized in *Table 7*.

90    The additional SARs relative to the PP are summarized in *Table 10*.

### 2.2.3    PP Claims rationale

91    The differences between this Security Target security objectives and requirements and those of *BSI-CC-PP-0084-2014*, to which conformance is claimed, have been identified and justified in *Section 4* and in *Section 5*. They have been recalled in the previous section.

92    In the following, the statements of the security problem definition, the security objectives, and the security requirements are consistent with those of the *BSI-CC-PP-0084-2014*.

93    The security problem definition presented in *Section 3*, clearly shows the additions to the security problem statement of the PP.

94    The security objectives rationale presented in *Section 4.3* clearly identifies modifications and additions made to the rationale presented in the *BSI-CC-PP-0084-2014*.

95    Similarly, the security requirements rationale presented in *Section 5.4* has been updated with respect to the protection profile.

96    All PP requirements have been shown to be satisfied in the extended set of requirements whose completeness, consistency and soundness have been argued in the rationale sections of the present document.

# 3 Security problem definition (ASE_SPD)

97      This section describes the security aspects of the environment in which the TOE is intended to be used and addresses the description of the assets to be protected, the threats, the organisational security policies and the assumptions.

98      Note that the origin of each security aspect is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), section 3. Only those originating in *AUG* or in *JIL SRFPDCL* / *ANSSI-CC-CER/F/06.003*, and the ones introduced in this Security Target, are detailed in the following sections.

99      A summary of all these security aspects and their respective conditions is provided in *Table 4*.

**Table 4.      Summary of security aspects**

| | Label | Title |
|---|---|---|
| TOE threats | BSI.T.Leak-Inherent | Inherent Information Leakage |
| | BSI.T.Phys-Probing | Physical Probing |
| | BSI.T.Malfunction | Malfunction due to Environmental Stress |
| | BSI.T.Phys-Manipulation | Physical Manipulation |
| | BSI.T.Leak-Forced | Forced Information Leakage |
| | BSI.T.Abuse-Func | Abuse of Functionality |
| | BSI.T.RND | Deficiency of Random Numbers |
| | BSI.T.Masquerade-TOE | Masquerade the TOE |
| | AUG4.T.Mem-Access | Memory Access Violation |
| | ANSSI.T.Open-Samples-Diffusion | Diffusion of open samples |
| | T.Data-Modification-DESFire | Unauthorized data modification for M4M-DESFire |
| | T.Impersonate-DESFire | Impersonating authorized users during authentication for M4M-DESFire |
| | T.Cloning-DESFire | Cloning for M4M-DESFire |
| | T.Confid-Applic-Code-DESFire | M4M-DESFire code confidentiality |
| | T.Confid-Applic-Data-DESFire | M4M-DESFire data confidentiality |
| | T.Integ-Applic-Code-DESFire | M4M-DESFire code integrity |
| | T.Integ-Applic-Data-DESFire | M4M-DESFire data integrity |
| | T.Resource-DESFire | M4M-DESFire resource unavailability |

**Table 4.      Summary of security aspects (continued)**

| | Label | Title |
|---|---|---|
| **OSPs** | BSI.P.Process-TOE | Protection during TOE Development and Production |
| | BSI.P.Lim-Block-Loader | Limiting and blocking the loader functionality |
| | BSI.P.Ctrl-Loader | Controlled usage to Loader Functionality |
| | AUG1.P.Add-Functions | Additional Specific Security Functionality (Cipher Scheme Support) |
| | P.Confidentiality | Confidentiality during communication for M4M-DESFire |
| | P.Transaction | Transaction mechanism for M4M-DESFire |
| | P.No-Trace-DESFire | Un-traceability of end-users for M4M-DESFire |
| | P.Resp-Appl | Treatment of user data |
| **Assumptions** | BSI.A.Process-Sec-IC | Protection during Packaging, Finishing and Personalisation |
| | BSI.A.Resp-Appl | Treatment of User Data |
| | A.Secure-Values-DESFire | Usage of secure values for M4M-DESFire |
| | A.Terminal-Support-DESFire | Terminal support to ensure integrity and confidentiality for M4M-DESFire |
| | A.M4MFramework-Identification | Identification by M4M Framework |

## 3.1      Description of assets

100      Since this Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), the assets defined in section 3.1 of the Protection Profile are applied and the assets regarding threats are clarified in this Security Target.

101      The assets regarding the threats are:

- logical design data, physical design data, IC Dedicated Software, and configuration data,
- Initialisation data and pre-personalisation data, specific development aids, test and characterisation related data, material for software development support, and photomasks and product in any form,
- the TOE correct operation,
- the Security IC Embedded Software, stored in the TOE's protected memories and in operation,
- the security services provided by the TOE for the Security IC Embedded Software,
- the cryptographic co-processors for Triple-DES and AES, the random number generator,
- when M4M-DESFire is embedded, the special functions for the communication with an external interface device,
- the User Data comprising, especially when M4M-DESFire is embedded,
  – authentication data like keys,
  – issuer data like card holder name or processing options,
  – representation of monetary values, e.g. a stored value for transport applications,
- the TSF Data.

102        This Security Target includes optionally Security IC Embedded Software and therefore does contain more assets compared to *BSI-CC-PP-0084-2014*. These assets are described above.

103        Application note:
           The TOE providing a functionality for Security IC Embedded Software secure loading into NVM, the ES is considered as User Data being stored in the TOE's memories at this step, and the Protection Profile corresponding packages are integrated, as well as the requirements from *JIL SRFPDCL*.

## 3.2      Threats

104        The threats are described in the *BSI-CC-PP-0084-2014*, section 3.2.
           Only those originating in *AUG*, *ANSSI-CC-CER/F/06.003*, and those related to M4M-DESFire are detailed in the following section.

| | |
|---|---|
| BSI.T.Leak-Inherent | Inherent Information Leakage |
| BSI.T.Phys-Probing | Physical Probing |
| BSI.T.Malfunction | Malfunction due to Environmental Stress |
| BSI.T.Phys-Manipulation | Physical Manipulation |
| BSI.T.Leak-Forced | Forced Information Leakage |
| BSI.T.Abuse-Func | Abuse of Functionality |
| BSI.T.RND | Deficiency of Random Numbers |
| BSI.T.Masquerade-TOE | Masquerade the TOE |

AUG4.T.Mem-Access      Memory Access Violation:

Parts of the **Security IC** Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). Any restrictions are defined by the security policy of the specific application context and must be implemented by the **Security IC** Embedded Software.

Clarification: This threat does not address the proper definition and management of the security rules implemented by the Security IC Embedded Software, this being a software design and correctness issue. This threat addresses the reliability of the abstract machine targeted by the software implementation. To avert the threat, the set of access rules provided by this TOE should be undefeated if operated according to the provided guidance. The threat is not realized if the Security IC Embedded Software is designed or implemented to grant access to restricted information. It is realized if an implemented access denial is granted under unexpected conditions or if the execution machinery does not effectively control a controlled access.

Here the attacker is expected to (i) take advantage of flaws in the design and/or the implementation of the TOE memory access rules (refer to BSI.T.Abuse-Func but for functions available after TOE delivery), (ii) introduce flaws by forcing operational conditions (refer to BSI.T.Malfunction) and/or by physical manipulation (refer to BSI.T.Phys-Manipulation). This attacker is expected to have a high level potential of attack.

ANSSI.T.Open-Samples-Diffusion      Diffusion of open samples:

An attacker may get access to open samples of the TOE and use them to gain information about the TSF (loader, memory management unit, ROM code, …). He may also use the open samples to characterize the behavior of the IC and its security functionalities (for example: characterization of side channel profiles, perturbation cartography, …). The execution of a dedicated security features (for example: execution of a DES computation without countermeasures or by de-activating countermeasures) through the loading of an adequate code would allow this kind of characterization and the execution of enhanced attacks on the IC.

105      The following additional threats are related to M4M-DESFire. They are valid in case M4M-DESFire is embedded in the TOE.

T.Data-Modification-DESFire      Unauthorized data modification for M4M-DESFire:

User data stored by the TOE may be modified by unauthorized subjects. This threat applies to the processing of modification commands received by the TOE, it is not concerned with verification of authenticity.

| | |
|---|---|
| T.Impersonate-DESFire | Impersonating authorized users during authentication for M4M-DESFire: |
| | An unauthorized subject may try to impersonate an authorized subject during the authentication sequence, e.g. by a man-in-the middle or replay attack. |
| T.Cloning-DESFire | Cloning for M4M-DESFire: |
| | User and TSF data stored on the TOE (including keys) may be read out by an unauthorized subject in order to create a duplicate. |
| T.Confid-Applic-Code-DESFire | M4M-DESFire code confidentiality: |
| | M4M-DESFire Licensed product code must be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to memory area where the M4M-DESFire licensed product executable code is stored.<br>The attacker executes an application to disclose code belonging to M4M-DESFire Licensed product. |
| T.Confid-Applic-Data-DESFire | M4M-DESFire data confidentiality: |
| | M4M-DESFire Licensed product data must be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to the M4M-DESFire licensed product data by another application.<br>For example, the attacker executes an application that tries to read data  belonging to M4M-DESFire Licensed product. |
| T.Integ-Applic-Code-DESFire | M4M-DESFire code integrity: |
| | M4M-DESFire Licensed product code must be protected against unauthorized modification. This relates to attacks at runtime to gain write access to memory area where the M4M-DESFire licensed product executable code is stored.<br>The attacker executes an application that tries to alter (part of) the M4M-DESFire code. |
| T.Integ-Applic-Data-DESFire | M4M-DESFire data integrity: |
| | M4M-DESFire Licensed product data must be protected against unauthorized modification. This relates to attacks at runtime to gain write access to the M4M-DESFire Licensed product data by another application.<br>The attacker executes an application that tries to alter (part of) the M4M-DESFire Licensed product data. |
| T.Resource-DESFire | M4M-DESFire resource unavailability: |
| | The availability of resources for the M4M-DESFire Licensed product shall be controlled to prevent denial of service or malfunction.<br>An attacker prevents correct execution of M4M-DESFire through consumption of some resources of the card: e.g. RAM or non volatile RAM. |

## 3.3   Organisational security policies

106    The TOE provides specific security functionality that can be used by the *Security IC* Embedded Software. In the following specific security functionality is listed which is not

derived from threats identified for the TOE's environment because it can only be decided in the context of the *Security IC* application, against which threats the *Security IC* Embedded Software will use the specific security functionality.

107 ST applies the Protection policy during TOE Development and Production (*BSI.P.Process-TOE*) as specified below.

108 *BSI.P.Lim-Block-Loader* and *BSI.P.Ctrl-Loader* are dedicated to the Secure Flash Loader, and described in the *BSI-CC-PP-0084-2014* packages "Loader dedicated for usage in secured environment only" and "Loader dedicated for usage by authorized users only". *BSI.P.Ctrl-Loader* has been completed in accordance with *JIL SRFPDCL*.

109 *ST* applies the Additional Specific Security Functionality policy (*AUG1.P.Add-Functions*) as specified below.

110 New Organisational Security Policies (OSPs) are defined here below:

111 P.Confidentiality, P.Transaction and P.No-Trace-DESFire are related to M4M-DESFire, and valid in case M4M-DESFire is embedded in the TOE.

112 P.Resp-Appl is related to the ES that is part of the evaluation (NesLib and/or M4M-DESFire), and valid in case NesLib or M4M-DESFire are embbeded in the TOE.

| | |
|---|---|
| BSI.P.Process-TOE | Identification during TOE Development and Production: |
| | An accurate identification *is* established for the TOE. This requires that each instantiation of the TOE carries this unique identification. |
| BSI.P.Lim-Block-Loader | Limiting and blocking the loader functionality: |
| | The composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. He limits the capability and blocks the availability of the Loader[1] in order to protect stored data from disclosure and manipulation. |

1. Note that blocking the Loader is not required, as only authorized users can use the Loader as stated in BSI.P.Ctrl-Loader.

BSI.P.Ctrl-Loader    Controlled usage to Loader Functionality:

Authorized user controls the usage of the Loader functionality in order to protect stored and loaded user data from disclosure and manipulation.

The activation of the loaded Additional ~~Code~~ *user data* is possible if:
– integrity and authenticity of the Additional ~~Code~~ *user data* have been successfully checked;
– the loaded ~~Additional Code~~ *user data* is targeted to the Initial TOE (Identification ~~Data~~ of the Additional ~~Code~~ *user data* and the Initial TOE will be used for this check).
Identification ~~Data~~ of the resulting Final TOE shall identify the Initial TOE and the ~~activated~~ Additional ~~Code~~ *user data*. Identification Data shall be protected in integrity.
Note: Here, the term TOE denotes the TOE itself as well as the composite TOE which both may be maintained by loading of data.

AUG1.P.Add-Functions    Additional Specific Security Functionality:

The TOE shall provide the following specific security functionality to the Security IC Embedded Software:
– Triple Data Encryption Standard (TDES), if EDES+ is active,
– Advanced Encryption Standard (AES), if AES is active,
– **Elliptic Curves Cryptography,** if NesLib is embedded,
– **Secure Hashing (SHA-1**[1]**, SHA-2, SHA-3),** if NesLib is embedded,
– **Keccak,** if NesLib is embedded,
– **Keccak-p,** if NesLib is embedded,
– **Diffie-Hellman,** if NesLib is embedded,
– Rivest-Shamir-Adleman (RSA), if NesLib is embedded,
– **Deterministic Random Bit Generator (DRBG),** if NesLib is embedded,
– **Prime Number Generation,** if NesLib is embedded.

1.  Note that SHA-1 is no longer recommended as a cryptographic function in the context of smart card applications. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.

P.Confidentiality    Confidentiality during communication for M4M-DESFire:

The TOE shall provide the possibility to protect selected data elements from eavesdropping during contact-less communication. The TOE shall also provide the possibility to detect replay or man-in-the-middle attacks within a session.

P.Transaction    Transaction mechanism for M4M-DESFire:

The TOE shall provide the possibility to combine a number of data modification operations in one transaction, so that either all operations or no operation at all is performed.

| P.No-Trace-DESFire | Un-traceability of end-users for M4M-DESFire: |
|---|---|
| | The TOE shall provide the ability that authorized subjects can prevent that end-user of TOE may be traced by unauthorized subjects without consent. Tracing of end-users may happen by performing a contact-less communication with the TOE when the end-user is not aware of it. Typically this involves retrieving the UID or any freely accessible data element. |
| P.Resp-Appl | Treatment of user data: |
| | The Security IC Embedded Software, part of the TOE, treats user data according to the assumption A.Resp-Appl defined in *BSI-CC-PP-0084-2014*. |

## 3.4 Assumptions

113    The following assumptions are described in the *BSI-CC-PP-0084-2014*, section 3.4.

| BSI.A.Process-Sec-IC | Protection during Packaging, Finishing and Personalisation |
|---|---|
| BSI.A.Resp-Appl | Treatment of User Data of the Composite TOE |

114    The following assumptions are defined for M4M-DESFire only.
Thus, they do not contradict with the security problem definition of the *BSI-CC-PP-0084-2014*, as they are only related to assets which are out of the scope of this PP.

115    In consequence, the addition of these asumptions does not contradict with the strict conformance claim on the *BSI-CC-PP-0084-2014*.

116    The following assumptions are valid in case M4M-DESFire is embedded in the TOE.

| A.Secure-Values-DESFire | Usage of secure values for M4M-DESFire: |
|---|---|
| | Only confidential and secure keys shall be used to set up the authentication and access rights in M4M-DESFire. These values are generated outside the TOE and they are downloaded to the TOE. |
| A.Terminal-Support-DESFire | Terminal support to ensure integrity and confidentiality for M4M-DESFire: |
| | The terminal verifies information sent by the TOE in order to ensure integrity and confidentiality of the communication. |
| A.M4MFramework-Identification | Identification by M4M Framework: |
| | A subject getting access to M4M-DESFire through the M4M host interface is previously identified and authorized as specified in the M4M specification (*M4M specification*). |

# 4　　Security objectives (ASE_OBJ)

117　　The security objectives of the TOE cover principally the following aspects:

- integrity and confidentiality of assets,
- protection of the TOE and associated documentation during development and production phases,
- provide random numbers,
- provide cryptographic support and access control functionality.

118　　A summary of all security objectives is provided in *Table 5*.

119　　Note that the origin of each objective is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the *BSI-CC-PP-0084-2014*, sections 4.1 and 7.3. Only those which have been amended, those originating in *AUG*, those originating in *JIL SRFPDCL*, and the ones introduced in this Security Target, are detailed in the following sections.

**Table 5.　　Summary of security objectives**

| | Label | Title |
|---|---|---|
| **TOE** | BSI.O.Leak-Inherent | Protection against Inherent Information Leakage |
| | BSI.O.Phys-Probing | Protection against Physical Probing |
| | BSI.O.Malfunction | Protection against Malfunctions |
| | BSI.O.Phys-Manipulation | Protection against Physical Manipulation |
| | BSI.O.Leak-Forced | Protection against Forced Information Leakage |
| | BSI.O.Abuse-Func | Protection against Abuse of Functionality |
| | BSI.O.Identification | TOE Identification |
| | BSI.O.RND | Random Numbers |
| | BSI.O.Cap-Avail-Loader | Capability and Availability of the Loader |
| | BSI.O.Ctrl_Auth_Loader | Access control and authenticity for the Loader |
| | ANSSI.O.Prot-TSF-Confidentiality | Protection of the confidentiality of the TSF |
| | ANSSI.O.Secure-Load-ACode | Secure loading of the Additional Code |
| | ANSSI.O.Secure-AC-Activation | Secure activation of the Additional Code |
| | ANSSI.O.TOE-Identification | Secure identification of the TOE |
| | O.Secure-Load-AMemImage | Secure loading of the Additional Memory Image |
| | O.MemImage-Identification | Secure identification of the Memory Image |
| | BSI.O.Authentication | Authentication to external entities |
| | AUG1.O.Add-Functions | Additional Specific Security Functionality |
| | AUG4.O.Mem-Access | *Dynamic* Area based Memory Access Control |

**Table 5.          Summary of security objectives (continued)**

| | Label | Title |
|---|---|---|
| **TOE** | *O.Access-Control-DESFire* | Access Control for M4M-DESFire |
| | *O.Authentication-DESFire* | Authentication for M4M-DESFire |
| | *O.Confidentiality-DESFire* | M4M-DESFire Confidential Communication |
| | *O.Type-Consistency-DESFire* | M4M-DESFire Data type consistency |
| | *O.Transaction-DESFire* | M4M-DESFire Transaction mechanism |
| | *O.No-Trace-DESFire* | Preventing Traceability for M4M-DESFire |
| | *O.Resp-Appl* | Treatment of user data for M4M-DESFire |
| | *O.Resource-DESFire* | Resource availability for M4M-DESFire |
| | *O.Firewall-DESFire* | M4M-DESFire firewall |
| | *O.Shr-Res-DESFire* | M4M-DESFire data cleaning for resource sharing |
| | *O.Verification-DESFire* | M4M-DESFire code integrity check |
| **Environments** | BSI.OE.Resp-Appl | Treatment of User Data of the Composite TOE |
| | BSI.OE.Process-Sec-IC | Protection during composite product manufacturing |
| | BSI.OE.Lim-Block-Loader | Limitation of capability and blocking the Loader |
| | BSI.OE.Loader-Usage | Secure communication and usage of the Loader |
| | BSI.OE.TOE-Auth | External entities authenticating of the TOE |
| | *OE.Composite-TOE-Id* | Composite TOE identification |
| | *OE.TOE-Id* | TOE identification |
| | *OE.Enable-Disable-Secure-Diag* | Enabling or disabling the Secure Diagnostic |
| | *OE.Secure-Diag-Usage* | Secure communication and usage of the Secure Diagnostic |
| | *OE.Secure-Values-DESFire* | Generation of secure values for M4M-DESFire |
| | *OE.Terminal-Support-DESFire* | Terminal support to ensure integrity and confidentiality for M4M-DESFire |
| | *OE.M4MFramework-Identification* | Identification by M4M Framework |

# 4.1     Security objectives for the TOE

BSI.O.Leak-Inherent          Protection against Inherent Information Leakage

BSI.O.Phys-Probing          Protection against Physical Probing

BSI.O.Malfunction          Protection against Malfunctions

BSI.O.Phys-Manipulation          Protection against Physical Manipulation

BSI.O.Leak-Forced          Protection against Forced Information Leakage

| BSI.O.Abuse-Func | Protection against Abuse of Functionality |
| BSI.O.Identification | TOE Identification |
| BSI.O.RND | Random Numbers |
| BSI.O.Cap-Avail-Loader | Capability and Availability of the Loader |
| BSI.O.Ctrl-Auth-Loader | Access control and authenticity for the Loader |
| BSI.O.Authentication | Authentication to external entities |

ANSSI.O.Prot-TSF-Confidentiality — Protection of the confidentiality of the TSF:

The TOE must provide protection against disclosure of confidential operations of the Security IC

(loader, memory management unit, …) through the use of a dedicated code loaded on open samples.

ANSSI.O.Secure-Load-ACode — Secure loading of the Additional Code:

The Loader of the ~~Initial~~ TOE shall check an evidence of authenticity and integrity of the loaded Additional Code.

The Loader enforces that only the allowed version of the Additional Code can be loaded on the Initial TOE. The Loader shall forbid the loading of an Additional Code not intended to be assembled with the Initial TOE.

During the Load Phase of an Additional Code, the TOE shall remain secure.

Note: Concretely, the TOE manages the Additional Code as a Memory Image.

ANSSI.O.Secure-AC-Activation — Secure activation of the Additional Code:

Activation of the Additional Code and update of the Identification Data shall be performed at the same time in an Atomic way.

All the operations needed for the code to be able to operate as in the Final TOE shall be completed before activation.

If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE), the Initial TOE shall remain in its initial state or fail secure.

ANSSI.O.TOE-Identification	Secure identification of the TOE:

The Identification Data identifies the Initial TOE and Additional Code. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data.

After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows identifications of Initial TOE and Additional TOE. The user shall be able to uniquely identify Initial TOE and Additional Code(s) which are embedded in the Final TOE.

O.Secure-Load-AMemImage	Secure loading of the Additional Memory Image:

The Loader of the TOE shall check an evidence of authenticity and integrity of the loaded Memory Image.

The Loader enforces that only the allowed version of the Additional Memory Image can be loaded after the Initial Memory Image. The Loader shall forbid the loading of an Additional Memory Image not intended to be assembled with the Initial Memory Image.

Note: This objective is similar to ANSSI.O.Secure-Load-ACode, applied to user data (e.g. embedded software).

O.MemImage-Identification	Secure identification of the Memory Image:

The Identification Data identifies the Initial Memory Image and Additional Memory Image. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data.

Storage of the Additional Memory Image and update of the Identification Data shall be performed at the same time in an Atomic way, otherwise (in case of interruption or incident which prevents this alignment), the Memory Image shall remain in its initial state or the TOE shall fail secure.

The Identification Data of the Final Memory Image allows identifications of Initial Memory Image and Additional Memory Image.

Note: This objective is similar to ANSSI.O.Secure-AC-Activation and ANSSI.O.TOE-Identification, applied to user data (e.g. embedded software).

AUG1.O.Add-Functions        Additional Specific Security Functionality:

The TOE must provide the following specific security functionality to the **Security IC** Embedded Software:
– Triple Data Encryption Standard (TDES), if EDES+ is active**,**
– Advanced Encryption Standard (AES), if AES is active**,**
– *Elliptic Curves Cryptography,* if NesLib is embedded**,**
– *Secure Hashing (SHA-1*[1]*, SHA-2, SHA-3),* if NesLib is embedded**,**
– *Keccak,* if NesLib is embedded,
– *Keccak-p,* if NesLib is embedded,
– *Diffie-Hellman,* if NesLib is embedded,
– Rivest-Shamir-Adleman (RSA)**,** if NesLib is embedded,
– *Deterministic Random Bit Generator (DRBG),* if NesLib is embedded,
– *Prime Number Generation,* if NesLib is embedded**.**

1. Note that SHA-1 is no longer recommended as a cryptographic function in the context of smart card applications. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.

AUG4.O.Mem-Access        *Dynamic* Area based Memory Access Control:

The TOE must provide the **Security IC** Embedded Software with the capability to define **dynamic memory segmentation and protection**. The TOE must then enforce **the defined access rules** so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

120        The following objectives are only valid in case M4M-DESFire is embedded:

O.Access-Control-DESFire        Access Control for M4M-DESFire:

The TOE must provide an access control mechanism for data stored by it. The access control mechanism shall apply to read, modify, create and delete operations for data elements and to reading and modifying security attributes as well as authentication data. It shall be possible to limit the right to perform a specific operation to a specific user. The security attributes (keys) used for authentication shall never be output.

O.Authentication-DESFire        Authentication for M4M-DESFire:

The TOE must provide an authentication mechanism in order to be able to authenticate authorized users. The authentication mechanism shall be resistant against replay and man-in-the-middle attacks.

O.Confidentiality-DESFire     M4M-DESFire Confidential Communication:

The TOE must be able to protect the communication by encryption. This shall be implemented by security attributes that enforce encrypted communication for the respective data element. The TOE shall also provide the possibility to detect replay or man-in-the-middle attacks within a session. This shall be implemented by checking verification data sent by the terminal and providing verification data to the terminal.

O.Type-Consistency-DESFire     M4M-DESFire Data type consistency:

The TOE must provide a consistent handling of the different supported data types. This comprises over- and underflow checking for values, for data file sizes and record handling.

O.Transaction-DESFire     M4M-DESFire Transaction mechanism:
The TOE must be able to provide a transaction mechanism that allows to update multiple data elements either all in common or none of them.

O.No-Trace-DESFire     Preventing Traceability for M4M-DESFire:

The TOE must be able to prevent that the TOE end-user can be traced. This shall be done by providing an option that disables the transfer of any information that is suitable for tracing an end-user by an unauthorized subject.

O.Resp-Appl     Treatment of user data:

Security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context.
For example the Security IC Embedded Software will not disclose security relevant user data to unauthorized users or processes when communicating with a terminal.

O.Resource-DESFire     Resource availability for M4M-DESFire:

The TOE shall control the availability of resources for M4M-DESFire Licensed product.

O.Firewall-DESFire     M4M-DESFire firewall:

The TOE shall ensure isolation of data and code between M4M-DESFire and the other applications. An application shall not read, write, compare any piece of data or code belonging to the M4M-DESFire Licensed product.

O.Shr-Res-DESFire      M4M-DESFire data cleaning for resource sharing:

It shall be ensured that any hardware resource, that is shared by M4M-DESFire and other applications or by any application which has access to such hardware resource, is always cleaned (using code that is part of the M4M-DESFire system and its certification) whenever M4M-DESFire is interrupted by the operation of another application. The only exception is buffers as long as these buffers do not contain other information than what is communicated over the contactless interface or has a form that is no different than what is normally communicated over the contacless interface.

For example, no data shall remain in a hardware crytographic coprocessor when M4M-DESFire is interrupted by another application.

O.Verification-DESFire      M4M-DESFire code integrity check:

The TOE shall ensure that M4M-DESFire code is verified for integrity and authenticity prior being executed.

## 4.2      Security objectives for the environment

121      Security Objectives for the Security IC Embedded Software development environment (phase 1):

BSI.OE.Resp-Appl      Treatment of User Data of the Composite TOE

122      Security Objectives for the operational Environment (phase 4 to 7):

BSI.OE.Process-Sec-IC      Protection during composite product manufacturing      Up to phase 6

BSI.OE.Lim-Block-Loader    Limitation of capability and blocking the Loader:      Up to phase 6

The Composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and, **_if desired,_** terminate irreversibly the Loader after intended usage of the Loader.

Note that blocking the Loader is not required, as only authorized users can use the Loader as stated in BSI.P.Ctrl-Loader.

| BSI.OE.Loader-Usage | Secure communication and usage of the Loader: | Up to phase 7 |
|---|---|---|
| | The authorized user must support the trusted communication channel with the TOE by confidentiality protection and authenticity proof of the data to be loaded and fulfilling the access conditions required by the Loader.<br>The authorized user must organize the maintenance transactions to ensure that the additional code (loaded as data) is able to operate as in the Final composite TOE. The authorized user must manage and associate unique Identification to the loaded data. | |
| BSI.OE.TOE-Auth | External entities authenticating of the TOE: | Up to phase 7 |
| | The operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE. | |
| OE.Composite-TOE-Id | Composite TOE identification: | Up to phase 7 |
| | The composite manufacturer must maintain a unique identification of a composite TOE under maintenance. | |
| OE.TOE-Id | TOE identification: | Up to phase 7 |
| | The IC manufacturer must maintain a unique identification of the TOE under maintenance. | |
| OE.Enable-Disable-Secure-Diag | Enabling or disabling the Secure Diagnostic: | Up to phase 7 |
| | If desired, the Composite Product Manufacturer will enable (or disable) irreversibly the Secure Diagnostic capability, thus enabling the IC manufacturer (or disabling everyone) to exercise the Secure Diagnostic capability. | |

| | | |
|---|---|---|
| OE.Secure-Diag-Usage | Secure communication and usage of the Secure Diagnostic: | Up to phase 7 |
| | The IC manufacturer must support the trusted communication channel with the TOE by fulfilling the access conditions required by the Secure Diagnostic. | |
| | The IC manufacturer must manage the Secure Diagnostic transactions so that they cannot be used to disclose critical user data of the Composite TOE, manipulate critical user data of the Composite TOE, manipulate Security IC Embedded Software or bypass, deactivate, change or explore security features or security services of the TOE | |

123    This section details the security objectives for the operational environment, related to M4M-DESFire, and to be enforced after TOE delivery up to phase 7.

124    The following security objectives for the operational environment are only valid if M4M-DESFire is embedded in the TOE:

| | |
|---|---|
| OE.Secure-Values-DESFire | Generation of secure values for M4M-DESFire: |
| | The environment shall generate confidential and secure keys for authentication purpose. These values are generated outside the TOE and they are downloaded to the TOE during the personalisation or usage in phase 5 to 7. |
| OE.Terminal-Support-DESFire | Terminal support to ensure integrity and confidentiality for M4M-DESFire: |
| | The terminal shall verify information sent by the TOE in order to ensure integrity and confidentiality of the communication. This involves checking of MAC values, verification of redundancy information according to the cryptographic protocol and secure closing of the communication session. |
| OE.M4MFramework-Identification | Identification by M4M Framework: |
| | The MIFAREforMobile Framework shall identify and authorize a user getting access to M4M-DESFire through the M4M host interface, as specified in the M4M specification (*M4M specification*). |

## 4.3    Security objectives rationale

125    The main line of this rationale is that the inclusion of all the security objectives of the *BSI-CC-PP-0084-2014* protection profile, together with those in *AUG*, and those introduced in

this ST, guarantees that all the security environment aspects identified in *Section 3* are addressed by the security objectives stated in this chapter.

126     Thus, it is necessary to show that:

  •     security environment aspects from *AUG* and from this ST, are addressed by security objectives stated in this chapter,

  •     security objectives from *AUG* and from this ST, are suitable (i.e. they address security environment aspects),

  •     security objectives from *AUG* and from this ST, are consistent with the other security objectives stated in this chapter (i.e. no contradictions).

127     The selected augmentations from *AUG* introduce the following security environment aspects:

  •     TOE threat "Memory Access Violation, (*AUG4.T.Mem-Access*)",

  •     organisational security policy "Additional Specific Security Functionality, (*AUG1.P.Add-Functions*)".

128     The augmentation made in this ST introduces the following security environment aspects:

  •     TOE threats "Diffusion of open samples, (*ANSSI.T.Open-Samples-Diffusion*)", "Unauthorized data modification for M4M-DESFire, (*T.Data-Modification-DESFire*)", "Impersonating authorized users during authentication for M4M-DESFire, (*T.Impersonate-DESFire*)", "Cloning for M4M-DESFire, (*T.Cloning-DESFire*)", "M4M-DESFire code confidentiality, (*T.Confid-Applic-Code-DESFire*)", "M4M-DESFire data confidentiality, (*T.Confid-Applic-Data-DESFire*)", "M4M-DESFire code integrity, (*T.Integ-Applic-Code-DESFire*)", "M4M-DESFire data integrity, (*T.Integ-Applic-Data-DESFire*)", and "M4M-DESFire resource unavailability, (*T.Resource-DESFire*)".

  •     organisational security policies "Confidentiality during communication for M4M-DESFire, (*P.Confidentiality*)", "Transaction mechanism for M4M-DESFire, (*P.Transaction*)", "Un-traceability of end-users for M4M-DESFire, (*P.No-Trace-DESFire*)", and "Treatment of user data, (*P.Resp-Appl*)".

  •     assumptions "Usage of secure values for M4M-DESFire, (*A.Secure-Values-DESFire*)", "Terminal support to ensure integrity and confidentiality for M4M-DESFire, (*A.Terminal-Support-DESFire*)", and "Identification by M4M Framework, (*A.M4MFramework-Identification*)".

129     The justification of the additional policies, additional threats, and additional assumptions provided in the next subsections shows that they do not contradict to the rationale already given in the protection profile *BSI-CC-PP-0084-2014* for the assumptions, policies and threats defined there.

130     In particular, the added assumptions do not contradict with the policies, threats and assumptions of the *BSI-CC-PP-0084-2014* Protection Profile, to which strict conformance is claimed, because they are all exclusively related to M4M-DESFire, which are out of the scope of this protection profile.

**Table 6.      Security Objectives versus Assumptions, Threats or Policies**

| Assumption, Threat or Organisational Security Policy | Security Objective | Notes |
|---|---|---|
| BSI.A.Resp-Appl | BSI.OE.Resp-Appl | Phase 1 |
| BSI.P.Process-TOE | BSI.O.Identification | Phase 2-3 optional Phase 4 |
| BSI.A.Process-Sec-IC | BSI.OE.Process-Sec-IC | Phase 5-6 optional Phase 4 |
| BSI.P.Lim-Block-Loader | BSI.O.Cap-Avail-Loader BSI.OE.Lim-Block-Loader | |
| BSI.P.Ctrl-Loader | BSI.O.Ctrl_Auth_Loader ANSSI.O.Secure-Load-ACode ANSSI.O.Secure-AC-Activation ANSSI.O.TOE-Identification O.Secure-Load-AMemImage O.MemImage-Identification BSI.OE.Loader-Usage OE.TOE-Id OE.Composite-TOE-Id | |
| A.Secure-Values-DESFire | OE.Secure-Values-DESFire | |
| A.Terminal-Support-DESFire | OE.Terminal-Support-DESFire | |
| A.M4MFramework-Identification | OE.M4MFramework-Identification | |
| AUG1.P.Add-Functions | AUG1.O.Add-Functions | |
| P.Confidentiality | O.Confidentiality-DESFire OE.Terminal-Support-DESFire | |
| P.Transaction | O.Transaction-DESFire | |
| P.No-Trace-DESFire | O.No-Trace-DESFire O.Access-Control-DESFire O.Authentication-DESFire | |
| P.Resp-Appl | O.Resp-Appl | |
| BSI.T.Leak-Inherent | BSI.O.Leak-Inherent | |
| BSI.T.Phys-Probing | BSI.O.Phys-Probing | |
| BSI.T.Malfunction | BSI.O.Malfunction | |
| BSI.T.Phys-Manipulation | BSI.O.Phys-Manipulation | |
| BSI.T.Leak-Forced | BSI.O.Leak-Forced | |

**Table 6.    Security Objectives versus Assumptions, Threats or Policies (continued)**

| Assumption, Threat or Organisational Security Policy | Security Objective | Notes |
|---|---|---|
| BSI.T.Abuse-Func | BSI.O.Abuse-Func<br>OE.Enable-Disable-Secure-Diag<br>OE.Secure-Diag-Usage | |
| BSI.T.RND | BSI.O.RND | |
| BSI.T.Masquerade-TOE | BSI.O.Authentication<br>BSI.OE.TOE-Auth | |
| AUG4.T.Mem-Access | AUG4.O.Mem-Access | |
| ANSSI.T.Open-Samples-Diffusion | ANSSI.O.Prot-TSF-Confidentiality<br>BSI.O.Leak-Inherent<br>BSI.O.Leak-Forced | |
| T.Data-Modification-DESFire | O.Access-Control-DESFire<br>O.Type-Consistency-DESFire<br>OE.Terminal-Support-DESFire | |
| T.Impersonate-DESFire | O.Authentication-DESFire | |
| T.Cloning-DESFire | O.Access-Control-DESFire<br>O.Authentication-DESFire | |
| T.Confid-Applic-Code-DESFire | O.Firewall-DESFire | |
| T.Confid-Applic-Data-DESFire | O.Firewall-DESFire | |
| T.Integ-Applic-Code-DESFire | O.Verification-DESFire<br>O.Firewall-DESFire | |
| T.Integ-Applic-Data-DESFire | O.Shr-Res-DESFire<br>O.Firewall-DESFire | |
| T.Resource-DESFire | O.Resource-DESFire | |

### 4.3.1    Assumption "Usage of secure values for M4M-DESFire"

131    The justification related to the assumption "Usage of secure values for M4M-DESFire, (*A.Secure-Values-DESFire*)" is as follows:

132    Since *OE.Secure-Values-DESFire* requires from the Administrator, Application Manager or the Application User to use secure values for the configuration of the authentication and access control as assumed in *A.Secure-Values-DESFire*, the assumption is covered by the objective.

133    *A.Secure-Values-DESFire* and *OE.Secure-Values-DESFire* do not contradict with the security problem definition of the *BSI-CC-PP-0084-2014*, because they are only related to M4M-DESFire, which is out of the scope of this protection profile.

### 4.3.2 Assumption "Terminal support to ensure integrity and confidentiality for M4M-DESFire"

134     The justification related to the assumption "Terminal support to ensure integrity and confidentiality for M4M-DESFire, (*A.Terminal-Support-DESFire*)" is as follows:

135     The objective *OE.Terminal-Support-DESFire* is an immediate transformation of the assumption *A.Terminal-Support-DESFire*, therefore it covers the assumption.

136     *A.Terminal-Support-DESFire* and *OE.Terminal-Support-DESFire* do not contradict with the security problem definition of the *BSI-CC-PP-0084-2014*, because they are only related to M4M-DESFire, which is out of the scope of this protection profile.

### 4.3.3 Assumption "Identification by M4M Framework"

137     The justification related to the assumption "Identification by M4M Framework, (*A.M4MFramework-Identification*)" is as follows:

138     The objective *OE.M4MFramework-Identification* is an immediate transformation of the assumption *A.M4MFramework-Identification*, therefore it covers the assumption.

139     *A.M4MFramework-Identification* and *OE.M4MFramework-Identification* do not contradict with the security problem definition of the BSI-PP-0084, because they are only related to M4M-DESFire, which is out of the scope of this protection profile.

### 4.3.4 TOE threat "Abuse of Functionality"

140     The justification related to the threat "Abuse of Functionality, (*BSI.T.Abuse-Func*)" is as follows:

141     The threat *BSI.T.Abuse-Func* is directly covered by the security objective *BSI.O.Abuse-Func,* supported by the security objectives for the operational environment *OE.Enable-Disable-Secure-Diag* and *OE.Secure-Diag-Usage* for the particular case of the Secure Diagnostic. Therefore *BSI.T.Abuse-Func* is covered by these three objectives.

### 4.3.5 TOE threat "Memory Access Violation"

142     The justification related to the threat "Memory Access Violation, (*AUG4.T.Mem-Access*)" is as follows:

143     According to *AUG4.O.Mem-Access* the TOE must enforce the **dynamic memory segmentation and protection** so that access of software to memory areas is controlled. Any restrictions are to be defined by the **Security IC** Embedded Software. Thereby security violations caused by accidental or deliberate access to restricted data (which may include code) can be prevented (refer to *AUG4.T.Mem-Access*). The threat *AUG4.T.Mem-Access* is therefore removed if the objective is met.

144     The added objective for the TOE *AUG4.O.Mem-Access* does not introduce any contradiction in the security objectives for the TOE.

### 4.3.6 TOE threat "Diffusion of open samples"

145     The justification related to the threat "Diffusion of open samples, (*ANSSI.T.Open-Samples-Diffusion*)" is as follows:

146     According to threat *ANSSI.T.Open-Samples-Diffusion*, the TOE shall provide protection against attacks using open samples of the TOE to characterize the behavior of the IC and its

security functionalities. The objective *ANSSI.O.Prot-TSF-Confidentiality* requires protection against disclosure of confidential operations of the Security IC through the use of a dedicated code loaded on open samples. Additionally, *BSI.O.Leak-Inherent* and *BSI.O.Leak-Forced* ensures protection against disclosure of confidential data processed in the Security IC. Therefore *ANSSI.T.Open-Samples-Diffusion* is covered by these three objectives.

147     The added objective for the TOE *ANSSI.O.Prot-TSF-Confidentiality* does not introduce any contradiction in the security objectives for the TOE.

### 4.3.7     TOE threat "Unauthorized data modification for M4M-DESFire"

148     The justification related to the threat "Unauthorized data modification for M4M-DESFire, (*T.Data-Modification-DESFire*)" is as follows:

149     According to threat *T.Data-Modification-DESFire*, the TOE shall avoid that user data stored by the TOE may be modified by unauthorized subjects. The objective *O.Access-Control-DESFire* requires an access control mechanism that limits the ability to modify data elements stored by the TOE. *O.Type-Consistency-DESFire* ensures that data types are adhered, so that data cannot be modified by abusing type-specific operations. The terminal must support this by checking the TOE responses, which is required by *OE.Terminal-Support-DESFire*. Therefore *T.Data-Modification-DESFire* is covered by these three objectives.

150     The added objectives for the TOE *O.Access-Control-DESFire* and *O.Type-Consistency-DESFire* do not introduce any contradiction in the security objectives for the TOE.

### 4.3.8     TOE threat "Impersonating authorized users during authentication for M4M-DESFire"

151     The justification related to the threat "Impersonating authorized users during authentication for M4M-DESFire, (*T.Impersonate-DESFire*)" is as follows:

152     The threat is related to the fact that an unauthorized subject may try to impersonate an authorized subject during authentication, e.g. by a man-in-the middle or replay attack. The goal of *O.Authentication-DESFire* is that an authentication mechanism is implemented in the TOE that prevents these attacks. Therefore the threat is covered by *O.Authentication-DESFire*.

153     The added objective for the TOE *O.Authentication-DESFire* does not introduce any contradiction in the security objectives for the TOE.

### 4.3.9     TOE threat "Cloning for M4M-DESFire"

154     The justification related to the threat "Cloning for M4M-DESFire, (*T.Cloning-DESFire*)" is as follows:

155     The concern of *T.Cloning-DESFire* is that all data stored on the TOE (including keys) may be read out in order to create a duplicate. The objective *O.Authentication-DESFire* together with *O.Access-Control-DESFire* requires that unauthorized users can not read any information that is restricted to the authorized subjects. The cryptographic keys used for the authentication are stored inside the TOE protected. *O.Access-Control-DESFire* states that no keys used for authentication shall ever be output. Therefore the two objectives cover *T.Cloning-DESFire*.

### 4.3.10    TOE threat "M4M-DESFire resource unavailability"

156      The justification related to the threat "M4M-DESFire resource unavailability, (*T.Resource-DESFire*)" is as follows:

157      The concern of *T.Resource-DESFire* is to prevent denial of service or malfunction of M4M-DESFire, that may result from an unavailability of resources. The goal of *O.Resource-DESFire* is to control the availability of resources for M4M-DESFire. Therefore the threat is covered by *O.Resource-DESFire*.

158      The added objective for the TOE *O.Resource-DESFire* does not introduce any contradiction in the security objectives for the TOE.

### 4.3.11    TOE threat "M4M-DESFire code confidentiality"

159      The justification related to the threat "M4M-DESFire code confidentiality, (*T.Confid-Applic-Code-DESFire*)" is as follows:

160      Since *O.Firewall-DESFire* requires that the TOE ensures isolation of code between M4M-DESFire and the other applications, the code of M4M-DESFire is protected against unauthorized disclosure, therefore *T.Confid-Applic-Code-DESFire* is covered by *O.Firewall-DESFire*.

161      The added objective for the TOE *O.Firewall-DESFire* does not introduce any contradiction in the security objectives for the TOE.

### 4.3.12    TOE threat "M4M-DESFire data confidentiality"

162      The justification related to the threat "M4M-DESFire data confidentiality, (*T.Confid-Applic-Data-DESFire*)" is as follows:

163      Since *O.Firewall-DESFire* requires that the TOE ensures isolation of data between M4M-DESFire and the other applications, the data of M4M-DESFire is protected against unauthorized disclosure, therefore *T.Confid-Applic-Data-DESFire* is covered by *O.Firewall-DESFire*.

### 4.3.13    TOE threat "M4M-DESFire code integrity"

164      The justification related to the threat "M4M-DESFire code integrity, (*T.Integ-Applic-Code-DESFire*)" is as follows:

165      The threat is related to the alteration of M4M-DESFire code by an attacker. *O.Verification-DESFire* requires that the TOE verifies the code integrity before its execution. Complementary, *O.Firewall-DESFire* requires that the TOE ensures isolation of code between M4M-DESFire and the other applications, thus protecting the code of M4M-DESFire against unauthorized modification. Therefore the threat is covered by *O.Verification-DESFire* together with *O.Firewall-DESFire*.

166      The added objective for the TOE *O.Verification-DESFire* does not introduce any contradiction in the security objectives for the TOE.

### 4.3.14    TOE threat "M4M-DESFire data integrity"

167      The justification related to the threat "M4M-DESFire data integrity, (*T.Integ-Applic-Data-DESFire*)" is as follows:

168    The threat is related to the alteration of M4M-DESFire data by an attacker. Since *O.Firewall-DESFire* and *O.Shr-Res-DESFire* require that the TOE ensures isolation of data between M4M-DESFire and the other applications, the data of M4M-DESFire is protected against unauthorized modification, therefore *T.Integ-Applic-Data-DESFire* is covered by *O.Firewall-DESFire* together with *O.Shr-Res-DESFire*.

169    The added objective for the TOE *O.Shr-Res-DESFire* does not introduce any contradiction in the security objectives for the TOE.

## 4.3.15    Organisational security policy "Controlled usage to Loader Functionality"

170    The justification related to the organisational security policy "Controlled usage to Loader Functionality, (*BSI.P.Ctrl-Loader*)" is as follows:

171    As stated in *BSI-CC-PP-0084-2014*, the organisational security policy "Controlled usage to Loader Functionality (*BSI.P.Ctrl-Loader*) is implemented by the security objective for the TOE "Access control and authenticity for the Loader (*BSI.O.Ctrl_Auth_Loader*)" and the security objective for the TOE environment "Secure communication and usage of the Loader (*BSI.OE.Loader-Usage*)".
The security objectives "Secure loading of the Additional Code (*ANSSI.O.Secure-Load-ACode*)", "Secure activation of the Additional Code (*ANSSI.O.Secure-AC-Activation*)", and "Secure identification of the TOE (*ANSSI.O.TOE-Identification*)" specified by *JIL SRFPDCL* additionally enforce this policy since they require authenticity, atomicity, identification of the loaded additional code, part of the TOE. "Secure identification of the TOE (*ANSSI.O.TOE-Identification*)" is supported by the security objective for the TOE environment "TOE identification (*OE.TOE-Id*)".
Similarly, the security objectives "Secure loading of the Additional Memory Image (*O.Secure-Load-AMemImage*)", and "Secure identification of the Memory Image (*O.MemImage-Identification*)", enforce this policy since they require authenticity, atomicity, identification of the loaded additional memory image for the user data (embedded software). "Secure identification of Memory Image (*O.MemImage-Identification*)" is supported by the security objective for the TOE environment "Composite TOE identification (*OE.Composite-TOE-Id*)".
Therefore the policy is covered by these nine objectives.

## 4.3.16    Organisational security policy "Additional Specific Security Functionality"

172    The justification related to the organisational security policy "Additional Specific Security Functionality, (*AUG1.P.Add-Functions*)" is as follows:

173    Since *AUG1.O.Add-Functions* requires the TOE to implement exactly the same specific security functionality as required by *AUG1.P.Add-Functions*, **and in the very same conditions,** the organisational security policy is covered by the objective.

174    Nevertheless the security objectives *BSI.O.Leak-Inherent*, *BSI.O.Phys-Probing*, , *BSI.O.Malfunction*, *BSI.O.Phys-Manipulation* and *BSI.O.Leak-Forced* define how to implement the specific security functionality required by *AUG1.P.Add-Functions*. (Note that these objectives support that the specific security functionality is provided in a secure way as expected from *AUG1.P.Add-Functions*.) Especially *BSI.O.Leak-Inherent* and *BSI.O.Leak-Forced* refer to the protection of confidential data (User Data or TSF data) in general. User Data are also processed by the specific security functionality required by *AUG1.P.Add-Functions*.

175        The added objective for the TOE *AUG1.O.Add-Functions* does not introduce any contradiction in the security objectives for the TOE.

## 4.3.17   Organisational security policy "Confidentiality during communication for M4M-DESFire"

176        The justification related to the organisational security policy "Confidentiality during communication for M4M-DESFire, (*P.Confidentiality*)" is as follows:

177        The policy *P.Confidentiality* requires the TOE to provide the possibility to protect selected data elements from eavesdropping during contact-less communication. In addition, the data transfer is protected in a way that injected and bogus commands, within the communication session before the protected data transfer, can be detected. The terminal must support this by checking the TOE responses, which is required by *OE.Terminal-Support-DESFire*. Since *O.Confidentiality-DESFire* requires that the security attribute for a data element contains an option that the communication related to this data element must be encrypted and protected, and because *OE.Terminal-Support-DESFire* ensures the support by the terminal, the two objectives cover the policy.

178        The added objective for the TOE *O.Confidentiality-DESFire* does not introduce any contradiction in the security objectives.

## 4.3.18   Organisational security policy "Transaction mechanism for M4M-DESFire"

179        The justification related to the organisational security policy "Transaction mechanism for M4M-DESFire, (*P.Transaction*)" is as follows:

180        According to this policy, the TOE shall be able to provide the possibility to combine a number of data modification operations in one transaction, so that either all operations or no operation at all is performed. This is exactly the goal of the objective *O.Transaction-DESFire*, therefore the policy *P.Transaction* is covered by *O.Transaction-DESFire*.

181        The added objective for the TOE *O.Transaction-DESFire* does not introduce any contradiction in the security objectives.

## 4.3.19   Organisational security policy "Un-traceability of end-users for M4M-DESFire"

182        The justification related to the organisational security policy "Un-traceability of end-users for M4M-DESFire, (*P.No-Trace-DESFire*)" is as follows:

183        The policy requires that the TOE has the ability to prevent tracing of end-users. Tracing can be performed with the UID or with any freely accessible data element stored by the TOE. The objective *O.No-Trace-DESFire* requires that the TOE shall provide an option to prevent the transfer of any information that is suitable for tracing an end-user by an unauthorized subject, which includes the UID. The objectives *O.Authentication-DESFire* and *O.Access-Control-DESFire* provide means to authorise subjects and to implement access control to data elements in a way that unauthorized subjects cannot read any element usable for tracing. Therefore the policy is covered by these three objectives.

184        The added objective for the TOE *O.No-Trace-DESFire* does not introduce any contradiction in the security objectives.

### 4.3.20 Organisational security policy "Treatment of user data"

185    The justification related to the organisational security policy "Treatment of user data, (*P.Resp-Appl*)" is as follows:

186    The policy states that the Security IC Embedded Software included in the TOE, treats user data according to the PP assumption *BSI.A.Resp-Appl*. *O.Resp-Appl* has the same objective as *BSI.OE.Resp-Appl* defined in the PP. Thus, the objective *O.Resp-Appl* covers the policy *P.Resp-Appl*.

187    The added objectives for the TOE *O.Resp-Appl* do not introduce any contradiction in the security objectives.

# 5        Security requirements (ASE_REQ)

188        This chapter on security requirements contains a section on security functional requirements (SFRs) for the TOE (*Section 5.1*), a section on security assurance requirements (SARs) for the TOE (*Section 5.2*), a section on the refinements of these SARs (*Section 5.3*) as required by the "*BSI-CC-PP-0084-2014*" Protection Profile. This chapter includes a section with the security requirements rationale (*Section 5.4*).

## 5.1        Security functional requirements for the TOE

189        Security Functional Requirements (SFRs) from the "*BSI-CC-PP-0084-2014*" Protection Profile (PP) are drawn from *CCMB-2017-04-002*, except the following SFRs, that are **extensions** to *CCMB-2017-04-002*:

   •   **FCS_RNG** Generation of random numbers,
   •   **FMT_LIM** Limited capabilities and availability,
   •   **FAU_SAS** Audit data storage,
   •   **FDP_SDC** Stored data confidentiality,
   •   **FIA_API** Authentication proof of identity .

   The reader can find their certified definitions in the text of the "*BSI-CC-PP-0084-2014*" Protection Profile.

190        All extensions to the SFRs of the "*BSI-CC-PP-0084-2014*" Protection Profile (PP) are **exclusively** drawn from *CCMB-2017-04-002*.

191        All iterations, assignments, selections, or refinements on SFRs have been performed according to section C.4 of *CCMB-2017-04-001*. They are easily identified in the following text as they appear **as indicated here**. Note that in order to improve readability, iterations are sometimes expressed within tables.

192        In order to ease the definition and the understanding of these security functional requirements, a simplified presentation of the TOE Security Policy (TSP) is given in the following section.

193        The selected security functional requirements for the TOE, their respective origin and type are summarized in *Table 7*.

**Table 7.        Summary of functional security requirements for the TOE**

| Label | Title | Addressing | Origin | Type |
|-------|-------|------------|--------|------|
| FRU_FLT.2 | Limited fault tolerance | Malfunction | *BSI-CC-PP-0084-2014* | *CCMB-2017-04-002* |
| FPT_FLS.1 | Failure with preservation of secure state | | | |

**Table 7.　Summary of functional security requirements for the TOE (continued)**

| Label | Title | Addressing | Origin | Type |
|---|---|---|---|---|
| FMT_LIM.1 / Test | Limited capabilities - Test | Abuse of Test functionality | BSI-CC-PP-0084-2014 | Extended |
| FMT_LIM.2 / Test | Limited availability - Test | | | |
| FAU_SAS.1 | Audit storage | Lack of TOE identification | BSI-CC-PP-0084-2014 Operated | |
| FDP_SDC.1 | Stored data confidentiality | Physical manipulation & probing | | CCMB-2017-04-002 |
| FDP_SDI.2 | Stored data integrity monitoring and action | | | |
| FPT_PHP.3 | Resistance to physical attack | | BSI-CC-PP-0084-2014 | |
| FDP_ITT.1 | Basic internal transfer protection | Leakage | | |
| FPT_ITT.1 | Basic internal TSF data transfer protection | | | |
| FDP_IFC.1 | Subset information flow control | | | |
| FCS_RNG.1 | Random number generation | Weak cryptographic quality of random numbers | BSI-CC-PP-0084-2014 Operated | Extended |
| FCS_COP.1 | Cryptographic operation | Cipher scheme support | AUG #1 Operated | CCMB-2017-04-002 |
| FCS_CKM.1 (if NesLib is embedded only) | Cryptographic key generation | | Security Target Operated | |
| FDP_ACC.2 / Memories | Complete access control - Memories | Memory access violation | Security Target Operated | |
| FDP_ACF.1 / Memories | Security attribute based access control - Memories | | AUG #4 Operated | |
| FMT_MSA.3 / Memories | Static attribute initialisation - Memories | Correct operation | | |
| FMT_MSA.1 / Memories | Management of security attributes - Memories | | | |
| FMT_SMF.1 / Memories | Specification of management functions - Memories | | Security Target Operated | |

**Table 7.     Summary of functional security requirements for the TOE (continued)**

| Label | Title | Addressing | Origin | Type |
|---|---|---|---|---|
| FIA_API.1 | Authentication Proof of Identity | Masquerade | *BSI-CC-PP-0084-2014* Operated | Extended |
| FMT_LIM.1 / Loader | Limited capabilities - Loader | Abuse of Loader functionality | | |
| FMT_LIM.2 / Loader | Limited availability - Loader | | | |
| FTP_ITC.1 / Loader | Inter-TSF trusted channel - Loader | Loader violation | *BSI-CC-PP-0084-2014* Operated | *CCMB-2017-04-002* |
| FDP_UCT.1 / Loader | Basic data exchange confidentiality - Loader | | | |
| FDP_UIT.1 / Loader | Data exchange integrity - Loader | | | |
| FDP_ACC.1 / Loader | Subset access control - Loader | | | |
| FDP_ACF.1 / Loader | Security attribute based access control - Loader | | | |
| FMT_MSA.3 / Loader | Static attribute initialisation - Loader | Correct Loader operation | Security Target Operated | |
| FMT_MSA.1 / Loader | Management of security attributes - Loader | | | |
| FMT_SMR.1 / Loader | Security roles - Loader | | | |
| FIA_UID.1 / Loader | Timing of identification - Loader | | | |
| FIA_UAU.1 / Loader | Timing of authentication - Loader | | | |
| FMT_SMF.1 / Loader | Specification of management functions - Loader | | | |
| FPT_FLS.1 / Loader | Failure with preservation of secure state - Loader | | | |
| FAU_SAR.1 / Loader | Audit review - Loader | Lack of TOE identification | | |
| FAU_SAS.1 / Loader | Audit storage - Loader | | | Extended |

**Table 7.　　Summary of functional security requirements for the TOE (continued)**

| Label | Title | Addressing | Origin | Type |
|---|---|---|---|---|
| FMT_SMR.1 / M4M-DESFire | Security roles - M4M-DESFire | M4M-DESFire access control (if M4M-DESFire is embedded only) | Security Target Operated | *CCMB-2017-04-002* |
| FDP_ACC.1 / M4M-DESFire | Subset access control - M4M-DESFire | | | |
| FDP_ACF.1 / M4M-DESFire | Security attribute based access control - M4M-DESFire | | | |
| FMT_MSA.3 / M4M-DESFire | Static attribute initialisation - M4M-DESFire | | | |
| FMT_MSA.1 / M4M-DESFire | Management of security attributes - M4M-DESFire | | | |
| FMT_SMF.1 / M4M-DESFire | Specification of management functions - M4M-DESFire | | | |
| FDP_ITC.2 / M4M-DESFire | Import of user data with security attributes - M4M-DESFire | | | |
| FPT_TDC.1 / M4M-DESFire | Inter-TSF basic TSF data consistency - M4M-DESFire | | | |
| FIA_UID.2 / M4M-DESFire | User identification before any action - M4M-DESFire | M4M-DESFire confidentiality and authentication (if M4M-DESFire is embedded only) | | |
| FIA_UAU.2 / M4M-DESFire | User authentication before any action - M4M-DESFire | | | |
| FIA_UAU.5 / M4M-DESFire | Multiple authentication mechanisms - M4M-DESFire | | | |
| FMT_MTD.1 / M4M-DESFire | Management of TSF data - M4M-DESFire | | | |
| FTP_TRP.1 / M4M-DESFire | Trusted path - M4M-DESFire | | | |
| FCS_CKM.4 / M4M-DESFire | Cryptographic key destruction - M4M-DESFire | | | |

**Table 7.**    **Summary of functional security requirements for the TOE (continued)**

| Label | Title | Addressing | Origin | Type |
|---|---|---|---|---|
| FDP_ROL.1 / M4M-DESFire | Basic rollback - M4M-DESFire | M4M-DESFire robustness (if M4M-DESFire is embedded only) | Security Target Operated | *CCMB-2017-04-002* |
| FPT_RPL.1 / M4M-DESFire | Replay detection - M4M-DESFire | | | |
| FPR_UNL.1 / M4M-DESFire | Unlinkability - M4M-DESFire | | | |
| FRU_RSA.2 / M4M-DESFire | Minimum and maximum quotas - M4M-DESFire | M4M-DESFire correct operation (if M4M-DESFire is embedded only) | | |
| FDP_RIP.1 / M4M-DESFire | Subset residual information protection - M4M-DESFire | M4M-DESFire intrinsic confidentiality and integrity (if M4M-DESFire is embedded only) | | |
| FTP_ITC.1 / Sdiag | Inter-TSF trusted channel - Secure Diagnostic | Abuse of Secure Diagnostic functionality | | |
| FAU_SAR.1 / Sdiag | Audit review - Secure Diagnostic | | | |
| FMT_LIM.1 / Sdiag | Limited capabilities - Secure Diagnostic | | | Extended |
| FMT_LIM.2 / Sdiag | Limited availability - Secure Diagnostic | | | |

### 5.1.1    Security Functional Requirements from the Protection Profile

**Limited fault tolerance (FRU_FLT.2)**

194    The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: ***exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1).***

**Failure with preservation of secure state (FPT_FLS.1)**

195    The TSF shall preserve a secure state when the following types of failures occur: ***exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur.***

*196*    *Refinements:*

*The term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.*

*Regarding application note 14 of BSI-CC-PP-0084-2014, the secure state is reached by an immediate interrupt or by a reset, depending on the current context.*

*Regarding application note 15 of BSI-CC-PP-0084-2014, the TOE provides information on the operating conditions monitored during Security IC Embedded Software*

*execution and after a warm reset. No audit requirement is however selected in this Security Target.*

### Limited capabilities (FMT_LIM.1) / Test

197　　The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: *Limited capability and availability Policy / Test*.

### Limited availability (FMT_LIM.2) / Test

198　　The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1) / Test" the following policy is enforced: *Limited capability and availability Policy / Test*.

*199*　　*SFP_1: Limited capability and availability Policy / Test*

*Deploying Test Features after TOE Delivery does not allow User Data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.*

### Audit storage (FAU_SAS.1)

200　　The TSF shall provide **the test process before TOE Delivery** with the capability to store the **Initialisation Data and/or Pre-personalisation Data and/or supplements of the Security IC Embedded Software** in the **NVM**.

### Stored data confidentiality (FDP_SDC.1)

201　　The TSF shall ensure the confidentiality of the information of the user data while it is stored in **all the memory areas where it can be stored**.

### Stored data integrity monitoring and action (FDP_SDI.2)

202　　The TSF shall monitor user data stored in containers controlled by the TSF for **integrity errors** on all objects, based on the following attributes: **user data stored in all possible memory areas, depending on the integrity control attributes**.

203　　Upon detection of a data integrity error, the TSF shall **signal the error and react**.

### Resistance to physical attack (FPT_PHP.3)

204　　The TSF shall resist **physical manipulation and physical probing,** to the **TSF** by responding automatically such that the SFRs are always enforced.

*205*　　*Refinement:*

*The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced. Hence, "automatic response" means here (i)assuming that there might be an attack at any time and (ii)countermeasures are provided at any time.*

### Basic internal transfer protection (FDP_ITT.1)

206     The TSF shall enforce the **Data Processing Policy** to prevent the **disclosure** of user data when it is transmitted between physically-separated parts of the TOE.

### Basic internal TSF data transfer protection (FPT_ITT.1)

207     The TSF shall protect TSF data from **disclosure** when it is transmitted between separate parts of the TOE.

***208***     ***Refinement:***

***The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE.***

***This requirement is equivalent to FDP_ITT.1 above but refers to TSF data instead of User Data. Therefore, it should be understood as to refer to the same Data Processing Policy defined under FDP_IFC.1 below.***

### Subset information flow control (FDP_IFC.1)

209     The TSF shall enforce the **Data Processing Policy** on **all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software**.

*210*     *SFP_2: Data Processing Policy*

*User Data of the Composite TOE and TSF data shall not be accessible from the TOE except when the Security IC Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security IC Embedded Software.*

### Random number generation (FCS_RNG.1)

211     The TSF shall provide a **physical** random number generator that implements:

- **(PTG.2.1) A total failure test detects a total failure of 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.**

- **(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. 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.**

212     The TSF shall provide **octets of bits** that meet

- **(PTG.2.6) Test procedure A 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.**

### 5.1.2 Additional Security Functional Requirements for the cryptographic services

#### Cryptographic operation (FCS_COP.1)

213     The TSF shall perform **the operations in** Table 8 in accordance with a specified cryptographic algorithm **in** Table 8 and cryptographic key sizes **of** Table 8 that meet the **standards in** Table 8**. The list of operations depends on the presence of cryptographic accelerators or NesLib, as indicated in** Table 8 **(Restrict).**

**Table 8.     FCS_COP.1 iterations (cryptographic operations)**

| Restrict | Iteration label | [assignment: list of cryptographic operations] | [assignment: cryptographic algorithm] | [assignment: cryptographic key sizes] | [assignment: list of standards] |
|---|---|---|---|---|---|
| If EDES+ | TDES | * encryption<br>* decryption<br>- in Cipher Block Chaining (CBC) mode<br>- in Electronic Code Book (ECB) mode | Triple Data Encryption Standard (TDES) | 168 bits | *NIST SP 800-67*<br>*NIST SP 800-38A* |
| If HW-AES | AES | * encryption (cipher)<br>* decryption (inverse cipher)<br>- in Cipher Block Chaining (CBC) mode<br>- in Electronic Code Book (ECB) mode | Advanced Encryption Standard | 128, 192 and 256 bits | *FIPS PUB 197* |
| If HW-AES and NesLib | | * Message authentication Code computation (CMAC)<br>* Authenticated encryption/decryption in Galois Counter Mode (GCM)<br>* Authenticated encryption/decryption in Counter with CBC-MAC (CCM) | | | *NIST SP 800-38B*<br>*NIST SP 800-38A*<br>*NIST SP 800-38D*<br>*NIST SP 800-38C* |

**Table 8.      FCS_COP.1 iterations (cryptographic operations) (continued)**

| Restrict | Iteration label | [assignment: list of cryptographic operations] | [assignment: cryptographic algorithm] | [assignment: cryptographic key sizes] | [assignment: list of standards] |
|---|---|---|---|---|---|
| If NesLib and Nescrypt | RSA | * RSA public key operation<br>* RSA private key operation without the Chinese Remainder Theorem<br>* RSA private key operation with the Chinese Remainder Theorem<br>* EMSA PSS and PKCS1 signature scheme coding<br>* RSA Key Encapsulation Method (KEM) | Rivest, Shamir & Adleman's | from 1024 to 4096 bits | *PKCS #1 V2.1* |
| If NesLib and Nescrypt | ECC on Weierstrass curves | * private scalar multiplication<br>* prepare Jacobian<br>* public scalar multiplication<br>* point validity check<br>* convert Jacobian to affine coordinates<br>* general point addition<br>* point expansion<br>* point compression<br>* Diffie-Hellman (ECDH) key agreement computation<br>* digital signature algorithm (ECDSA) generation and verification | Elliptic Curves Cryptography on GF(p) on curves in Weierstrass form | up to 640 bits | *IEEE 1363-2000, chapter 7*<br>*IEEE 1363a-2004*<br><br><br>*NIST SP 800-56A*<br><br>*FIPS PUB 186-4*<br>*ANSI X9.62, section 7* |
| If NesLib | ECC on Edwards curves | * ed25519 generation<br>* ed25519 verification<br>* ed25519 point decompression | Elliptic Curves Cryptography on GF(p) on curves in Edwards form, with curve 25519 | 256 bits | *EdDSA rfc*<br>*EDDSA*<br>*EDDSA2* |

**Table 8.    FCS_COP.1 iterations (cryptographic operations) (continued)**

| Restrict | Iteration label | [assignment: list of cryptographic operations] | [assignment: cryptographic algorithm] | [assignment: cryptographic key sizes] | [assignment: list of standards] |
|---|---|---|---|---|---|
| If NesLib | SHA | * SHA-1[1]<br>* SHA-224<br>* SHA-256<br>* SHA-384<br>* SHA-512<br>* Protected SHA-1[1]<br>* Protected SHA-256<br>* Protected SHA-384<br>* Protected SHA-512 | Secure Hash Algorithm | assignment pointless because algorithm has no key | *FIPS PUB 180-2* |
| | | * HMAC using Protected SHA-1[1] or Protected SHA-256 | | up to 512 bits | *FIPS PUB 198-1* |
| If NesLib | Keccak and SHA-3 | * SHAKE128,<br>* SHAKE256,<br>* SHA3-224,<br>* SHA3-256,<br>* SHA3-384,<br>* SHA3-512,<br>* Keccak[r,1600-r],<br>* protected SHAKE128,<br>* protected SHAKE256,<br>* protected SHA3-224,<br>* protected SHA3-256,<br>* protected SHA3-384,<br>* protected SHA3-512,<br>* Protected Keccak[r,1600-r] | Keccak | no key for plain functions, variable key length up to security level for protected functions (security level is last number in function names and 1600-c for Keccak) | *FIPS PUB 202* |
| If NesLib | Keccak-p | * Keccak-p[1600,n_r = 24],<br>* Keccak-p[1600, n_r=12],<br>* protected Keccak-p[1600,n_r = 24],<br>* protected Keccak-p[1600, n_r=12] | Keccak-p | no key for plain functions, any key length up to 256 bits for protected functions | *FIPS PUB 202* |
| If NesLib and Nescrypt | Diffie-Hellman | Diffie-Hellman | Diffie-Hellman | up to 4096 bits | *ANSI X9.42* |

**Table 8.        FCS_COP.1 iterations (cryptographic operations) (continued)**

| Restrict | Iteration label | [assignment: list of cryptographic operations] | [assignment: cryptographic algorithm] | [assignment: cryptographic key sizes] | [assignment: list of standards] |
|---|---|---|---|---|---|
| If NesLib | DRBG | * SHA-1[1]<br>* SHA-224<br>* SHA-256<br>* SHA-384<br>* SHA-512 | Hash-DRBG | none | *NIST SP 800-90*<br>*FIPS PUB 180-2* |
| | | *AES | CTR-DRBG | 128, 192 and 256 bits | *NIST SP 800-90*<br>*FIPS PUB 197* |

1.  Note that SHA-1 is no longer recommended as a cryptographic function in the context of smart card applications. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.

### Cryptographic key generation (FCS_CKM.1)

214        If NesLib is embedded, the TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm*, in Table 9,* and specified cryptographic key sizes *of Table 9* that meet the following **standards in** *Table 9.*

**Table 9.        FCS_CKM.1 iterations (cryptographic key generation)**

| Iteration label | [assignment: cryptographic key generation algorithm] | [assignment: cryptographic key sizes] | [assignment: list of standards] |
|---|---|---|---|
| Prime generation | prime generation and RSA prime generation algorithm, optionally protected against side channel attacks, and/or optionally with conditions | up to 2048 bits | *FIPS PUB 140-2*<br>*FIPS PUB 186-4* |
| RSA key generation | RSA key pair generation algorithm, optionally protected against side channel attacks, and/or optionally with conditions | from 1024 to 4096 bits | *FIPS PUB 140-2*<br>*ISO/IEC 9796-2*<br>*PKCS #1 V2.1* |

## 5.1.3        Additional Security Functional Requirements for the memories protection

215        The following SFRs are extensions to "*BSI-CC-PP-0084-2014*" Protection Profile (PP), related to the memories protection.

### Static attribute initialisation (FMT_MSA.3) / Memories

216        The TSF shall enforce the **Dynamic Memory Access Control Policy** to provide **minimally protective**[e] default values for security attributes that are used to enforce the SFP.

---

e.  See the Datasheet referenced in *Section 7* for actual values.

217      The TSF shall allow **none** to specify alternative initial values to override the default values when an object or information is created.

Application note:
The security attributes are the set of access rights currently defined. They are dynamically attached to the subjects and objects locations, i.e. each logical address.

### Management of security attributes (FMT_MSA.1) / Memories

218      The TSF shall enforce the **Dynamic Memory Access Control Policy** to restrict the ability to **modify** the security attributes **current set of access rights** to **software running in privileged mode.**

### Complete access control (FDP_ACC.2) / Memories

219      The TSF shall enforce the **Dynamic Memory Access Control Policy** on **all subjects (software), all objects (data including code stored in memories)** and all operations among subjects and objects covered by the SFP.

220      The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

### Security attribute based access control (FDP_ACF.1) / Memories

221      The TSF shall enforce the **Dynamic Memory Access Control Policy** to objects based on the following: **software mode, the object location, the operation to be performed, and the current set of access rights.**

222      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 and only if the software mode, the object location and the operation matches an entry in the current set of access rights.**

223      The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

224      The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **in User configuration, any access (read, write, execute) to the OST ROM is denied,**
- **in User configuration, any write access to the ST NVM is denied,**
- **If** M4M-DESFire **is part of the TOE, another application cannot read, write, compare any piece of data or code belonging to** M4M-DESFire**.**

225      **Note**: It should be noted that this level of policy detail is not needed at the application level. The composite Security Target writer should describe the ES access control and information flow control policies instead. Within the ES High Level Design description, the chosen setting of IC security attributes would be shown to implement the described policies relying on the IC SFP presented here.

226      The following SFP **Dynamic Memory Access Control Policy** is defined for the requirement "Security attribute based access control (FDP_ACF.1) / Memories":

227      *SFP_3: Dynamic Memory Access Control Policy*

*The TSF must control read, write, execute accesses of software to data, based on the software mode and on the current set of access rights.*

**Specification of management functions (FMT_SMF.1) / Memories**

228    The TSF will be able to perform the following management functions: ***modification of the current set of access rights security attributes by software running in privileged mode, supporting the Dynamic Memory Access Control Policy.***

## 5.1.4    Additional Security Functional Requirements related to the loading and authentication capabilities

**Authentication Proof of Identity (FIA_API.1)**

The TSF shall provide a ***command based on a cryptographic mechanism*** to prove the identity of the TOE to an external entity.

**Limited capabilities (FMT_LIM.1) / Loader**

229    The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: ***Loader Limited Capability Policy.***

*230    SFP_4: Loader Limited Capability Policy*

*231    Deploying Loader functionality after **delivery** does not allow stored user data to be disclosed or manipulated by unauthorized user.*

**Limited availability (FMT_LIM.2) / Loader**

232    The TSF shall be designed and implemented in a manner that limits its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: ***Loader Limited Availability Policy.***

*233    SFP_5: Loader Limited Availability Policy*

*234    The TSF prevents deploying the Loader functionality after **blocking of the loader**.*

235    **Note**: Blocking the loader is just an option.

**Inter-TSF trusted channel (FTP_ITC.1) / Loader**

236    The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

237    The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

***238***    The TSF shall initiate communication via the trusted channel for ***Maintenance transaction***.

***239***    ***Refinement:***

***In practice, the communication is not initiated by the TSF.***

**Basic data exchange confidentiality (FDP_UCT.1) / Loader**

240    The TSF shall enforce the *Loader SFP* to receive user data in a manner protected from unauthorized disclosure.

### Data exchange integrity (FDP_UIT.1) / Loader

241     The TSF shall enforce the *Loader SFP* to receive user data in a manner protected from modification, deletion, insertion errors.

242     The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion has occurred.

### Subset access control (FDP_ACC.1) / Loader

243     The TSF shall enforce the *Loader SFP* on:

- the subjects **ST Loader, User Loader, and Delegated Loader,**
- the objects user data in **User NVM and ST data in ST NVM,**
- the operation **Maintenance transaction**.

### Security attribute based access control (FDP_ACF.1) / Loader

244     The TSF shall enforce the *Loader SFP* to objects based on the following: **all subjects, objects and attributes defined in the Loader SFP.**

245     The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **if the user authenticated role is allowed to perform the maintenance transaction and the maintenance transaction is legitimate and the loaded data emanates from an authorized originator.**

*Note that the term "data" also addresses Additional Code, as this code is seen as data by the TSF.*

246     The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none.**

247     The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none.**

248     The following SFP **Loader SFP** is defined for the requirements "Basic data exchange confidentiality (FDP_UCT.1) / Loader", "Data exchange integrity (FDP_UIT.1) / Loader", "Subset access control (FDP_ACC.1) / Loader", "Security attribute based access control (FDP_ACF.1) / Loader", "Static attribute initialisation (FMT_MSA.3) / Loader", and "Management of security attributes (FMT_MSA.1) / Loader":

*249*     *SFP_6: Loader SFP*

*250*     *The TSF must enforce that a maintenance transaction is performed if and only if **the user authenticated role is allowed to perform the maintenance transaction and the maintenance transaction is legitimate and the loaded data emanates from an authorized originator.***

*The TSF ruling is done according to a fixed access rights matrix, based on the subject, object and security attributes listed below.*

*The Security Function Policy (SFP) Loader SFP uses the following definitions:*

- *the subjects are the ST Loader, the User Loader, and the Delegated Loader,*
- *the objects are ST NVM and User NVM,*
- *the operation is Maintenance transaction,*
- *the security attributes linked to the subjects are the remaining sessions, the number of consecutive authentication failures, the allowed memory areas, the logging capacity, the transaction identification.*

*Note that subjects are authorized by cryptographic keys. These keys are considered as authentication data and not as security attributes.*

### Failure with preservation of secure state (FPT_FLS.1) / Loader

251    The TSF shall preserve a secure state when the following types of failures occur: ***the maintenance transaction is incomplete***.

### Static attribute initialisation (FMT_MSA.3) / Loader

252    The TSF shall enforce the **Loader SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

253    The TSF shall allow **none** to specify alternative initial values to override the default values when an object or information is created.

### Management of security attributes (FMT_MSA.1) / Loader

254    The TSF shall enforce the **Loader SFP** to restrict the ability to **modify** the security attributes **remaining sessions, transaction identification** to **the ST Loader or User Loader.**

### Specification of management functions (FMT_SMF.1) / Loader

255    The TSF will be able to perform the following management functions: ***change the role authentication data, change the remaining sessions, block a role, under the Loader SFP.***

### Security roles (FMT_SMR.1) / Loader

256    The TSF shall maintain the roles: ***ST Loader, User Loader, Delegated Loader, Secure Diagnostic, and Everybody***.

257    The TSF shall be able to associate users with roles.

### Timing of identification (FIA_UID.1) / Loader

258    The TSF shall allow ***boot, authentication command and non-critical queries*** on behalf of the user to be performed before the user is identified.

259    The TSF shall require each user to be successfully identified before allowing any other TSF mediated actions on behalf of that user.

### Timing of authentication (FIA_UAU.1) / Loader

260    The TSF shall allow ***boot, authentication command and non-critical queries*** on behalf of the user to be performed before the user is authenticated.

261       The TSF shall require each user to be successfully authenticated before allowing any other TSF mediated actions on behalf of that user.

### Audit storage (FAU_SAS.1) / Loader

262       The TSF shall provide **the Loader** with the capability to store the **transaction identification of the loaded data** in the **NVM**.

***263***       ***Refinement:***

***The TSF shall systematically store the transaction identification provided by the ST Loader or User Loader together with the loaded data.***

### Audit review (FAU_SAR.1) / Loader

264       The TSF shall provide **Everybody** with the capability to read the **Product information and the Identification of the last completed maintenance transaction, if any,** from the audit records.

265       The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

## 5.1.5    Additional Security Functional Requirements related to the Secure Diagnostic capabilities

### Limited capabilities (FMT_LIM.1) / Sdiag

266       The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: **Sdiag Limited Capability Policy.**

*267*       *SFP_7: Sdiag Limited Capability Policy*

*268*       *Deploying Secure Diagnostic capability does not allow stored user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.*

### Limited availability (FMT_LIM.2) / Sdiag

269       The TSF shall be designed and implemented in a manner that limits its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: **Sdiag Limited Availability Policy.**

*270*       *SFP_8: Sdiag Limited Availability Policy*

*271*       *The TSF prevents deploying the Secure Diagnostic capability unless the Secure Diagnostic mode is explicitly enabled by the authorized user. When the Secure Diagnostic capability is deployed, the TSF allows performing only authorized and authentic diagnostic transactions.*

***272***       ***Refinement:***

***By enabling the Secure Diagnostic capability, the Composite Product Manufacturer gives authority to the IC manufacturer to exercise the Secure Diagnostic capability known to abide by SFP_7.***

### Inter-TSF trusted channel (FTP_ITC.1) / Sdiag

273     The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

274     The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

*275*     The TSF shall initiate communication via the trusted channel for **Secure Diagnostic transaction**.

*276*     ***Refinement:***

        ***In practice, the communication is initiated by the trusted IT product.***

### Audit review (FAU_SAR.1) / Sdiag

277     The TSF shall provide **Everybody** with the capability to read the **Secure Diagnostic enable status,** from the audit records.

278     The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

## 5.1.6     Additional Security Functional Requirements related to M4M-DESFire

279     The following SFRs are extensions to "*BSI-CC-PP-0084-2014*" Protection Profile (PP), related to the capabilities and protections of M4M-DESFire.

280     They are only valid in case M4M-DESFire is embedded.

281     **Note**: M4M-DESFire library directly relies upon the following IC SFRs:
- FRU_FLT.2 in providing services as part of the security countermeasures implemented in the library,
- FPT_FLS.1 in order to generate a software reset,
- FCS_RNG.1 for the provision of random numbers,
- FCS_COP.1 / TDES for DES cryptographic operations,
- FCS_COP.1 / AES for AES cryptographic operations.

282     It also relies upon the other SFRs (except those of NesLib), which provide general low level security mechanisms.

### Security roles (FMT_SMR.1) / M4M-DESFire

283     The TSF shall maintain the roles **VC Administrator, VC Manager, Service Manager, Application Manager, Application User and Everybody.**

284     The TSF shall be able to associate users with roles.

285     **Note**: Based on the definition, Nobody is not considered as a role.

### Subset access control (FDP_ACC.1) / M4M-DESFire

286     The TSF shall enforce the **M4M-DESFire Access Control Policy** on **all subjects, objects, operations and attributes defined by the M4M-DESFire Access Control Policy.**

### Security attribute based access control (FDP_ACF.1) / M4M-DESFire

287    The TSF shall enforce the **M4M-DESFire Access Control Policy** to objects based on the following: **all subjects, objects and attributes**.

288    The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **The VC Manager can create virtual cards.**

- **The Service Manager can delete a virtual card.**

- **The VC Administrator of a virtual card can create and delete applications within this virtual card.**

- **The Service Manager can create and delete applications.**

- **The Application Manager of an application can delete this application, create data file and values within this application, delete data files and values within this application.**

- **An Application User can read or write a data file; read, increase or decrease a value based on the access control settings in the respective file attribute.**

289    The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **Everybody can create applications if this is allowed by a specific card attribute.**

- **Everybody can create and delete data files or values of a specific application if this is allowed by a specific application attribute.**

- **Everybody can read or write a data file; read, increase or decrease a value if this is allowed by a specific file attribute.**

290    The TSF shall explicitly deny access of subjects to objects based on the following additional rules*:*

- **Nobody can read or write a data file; read, increase or decrease a value if this is explicitly set for the respective operation on the respective data file or value.**

291    The following SFP **M4M-DESFire Access Control Policy** is defined for the requirement "Security attribute based access control (FDP_ACF.1) / M4M-DESFire":

292    *SFP 9: M4M-DESFire Access Control Policy*

*The Security Function Policy (SFP) M4M-DESFire Access Control Policy uses the following definitions:*

*The subjects are:*

- *The VC Manager i.e. the subject that owns or has access to a wholesale VC creation key.*

- *The Service Manager i.e. the subject that uses the M4M host interface without owning or having access to the VC creation key or a wholesale VC creation key.*

- *The VC Administrator i.e. the subject that owns or has access to the card master key.*

- *The Application Manager i.e. the subject that owns or has access to an application master key. Note that the TOE supports multiple applications and therefore multiple Application Managers, however for one application there is only one Application Manager.*

- *The Application User i.e. the subject that owns or has access to a key that allows to perform operations with application objects. Note that the TOE supports multiple*

*Application Users within each application and the assigned rights to the Application Users can be different, which allows to have more or less powerful Application Users.*

- *Any other subject belongs to the role Everybody. This includes the card holder (i.e. end-user) and any other subject e.g. an attacker. These subjects do not possess any key and can not perform operations that are restricted to the VC Administrator, VC Manager, Service Manager, Application Manager and Application User.*

- *The term Nobody will be used to explicitly indicate that no rights are granted to any subject.*

*The objects are:*

- *The MIFARE implementation itself.*

- *The MIFARE implementation can store a number of virtual cards.*

- *A virtual card can store a number of Applications.*

- *An application can store a number of Data Files of different types.*

- *One specific type of data file are Values.*

*Note that data files and values can be grouped in standard files and backup files, with values belonging to the group of backup files. When the term "file" is used without further information then both data files and values are meant.*

*The operations that can be performed with the objects are:*

- *read a value or data from a data file,*

- *write data to a data file,*

- *increase a value (with a limit or unlimited),*

- *decrease a value,*

- *create a virtual card, an application, a value or a data file,*

- *delete a virtual card, an application, a value or a data file and*

- *modify attribute of the MIFARE implementation, a virtual card, an application, a value or a data file.*

Note that 'freeze' will be used as specific form of modification that prevents any further modify.

*The security attributes are:*

- *Attributes of the MIFARE implementation, virtual cards, applications, values and data files.*

   *There is a set of attributes for the MIFARE implementation, a set of attributes for every virtual card, a set of attributes for every application and a set of attributes for every single file within an application.*

   *The term "MIFARE implementation attributes" will be used for the set of attributes related to the MIFARE implementation, the term "card attributes" will be used for the set of attributes related to a virtual card, the term "application attributes" will be used for the set of application attributes and the term "file attributes" will be used for the attributes of values and data files.*

*Note that subjects are authorized by cryptographic keys or the usage of the M4M host interface. These keys are considered as authentication data and not as security attributes. The MIFARE implementation has a VC creation key. Every virtual card has a card master key. Every application has an application master key and a variable number of keys used for operations on data files or values (all these keys are called application keys). The application keys within an application are numbered.*

*Implications of the M4M-DESFire Access Control Policy:*

*The M4M-DESFire Access Control Policy has some implications, that can be drawn from the policy and that are essential parts of the TOE security functions.*

- *The TOE end-user does normally not belong to the group of authorized users (VC Administrator, VC Manager, Service Manager, Application Manager, Application User), but regarded as 'Everybody' by the TOE. This means that the TOE cannot determine if it is used by its intended end-user (in other words: it cannot determine if the current card holder is the owner of the card).*

- *The VC Manager can create and associate virtual cards, and write the initial value of the card master key.*

- *The VC Administrator and the Service Manager can delete virtual cards.*

- *The VC Administrator can have the exclusive right to create and delete applications on the virtual card, however he can also grant this privilege to Everybody. Additionally, changing the virtual card attributes is reserved for the VC Administrator. Application keys, at delivery time should be personalized to a preliminary, temporary key only known to the VC Administrator and the Application Manager.*

- *At application personalization time, the Application Manager uses the preliminary application key in order to personalize the application keys, whereas all keys, except the application master key, can be personalized to a preliminary, temporary key only known to the Application Manager and the Application User. Furthermore, the Application Manager has the right to create files within his application scope.*

### Static attribute initialisation (FMT_MSA.3) / M4M-DESFire

293     The TSF shall enforce the **M4M-DESFire Access Control Policy** to provide **permissive** default values for security attributes that are used to enforce the SFP.

294     The TSF shall allow **no subject** to specify alternative initial values to override the default values when an object or information is created.

295     Application note:
The only initial attributes are the MIFARE implementation attributes. All other attributes have to be defined at the same time the respective object is created.

### Management of security attributes (FMT_MSA.1) / M4M-DESFire

296     The TSF shall enforce the **M4M-DESFire Access Control Policy** to restrict the ability to **modify or freeze** the security attributes **MIFARE implementation attributes, virtual card attributes, application attributes and file attributes** to the **VC Administrator,Application Manager and Application User, respectively**.

***297***     ***Refinement:***

***The detailed management abilities are:***

- ***The VC Administrator can modify the MIFARE implementation attributes. The MIFARE implementation attributes contain a flag that when set will prevent any***

*further change of the MIFARE implementation attributes, thereby allowing to freeze the MIFARE implementation attributes.*

- *The VC Administrator can modify the card attributes. The card attributes contain a flag that when set will prevent any further change of the card attributes, thereby allowing to freeze the card attributes.*

- *The Application Manager can modify the application attributes. The application attributes contain a flag that when set will prevent any further change of the application attributes, thereby allowing to freeze the application attributes.*

- *The Application Manager can decide to restrict the ability to modify the file attributes to the Application Manager, an Application User, Everybody or to Nobody. The restriction to Nobody is equivalent to freezing the file attributes.*

- *As an implication of the last rule, any subject that receives the modify abilities from the Application Manger gets these abilities transferred.*

- *The implication given in the previous rule includes the possibility for an Application User to modify the file attributes if the Application Manager decides to transfer this ability. If there is no such explicit transfer an Application User does not have the ability to modify the file attributes.*

### Specification of Management Functions (FMT_SMF.1) / M4M-DESFire

298      The TSF shall be capable of performing the following security management functions:

- *Authenticating a user,*

- *Invalidating the current authentication state based on the functions: Selecting an application or the virtual card, Changing a key, Occurrence of any error during the execution of a command, Reset,*

- *Changing a security attribute,*

- *Creating or deleting a virtual card, an application, a value or a data file.*

### Import of user data with security attributes (FDP_ITC.2) / M4M-DESFire

299      The TSF shall enforce the ***M4M-DESFire Access Control Policy*** when importing user data, controlled under the SFP, from outside of the TOE.

300      The TSF shall use the security attributes associated with the imported user data.

301      The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

302      The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

303      The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: ***no additional rules***.

### Inter-TSF basic TSF data consistency (FPT_TDC.1) / M4M-DESFire

304      The TSF shall provide the capability to consistently interpret ***data files and values*** when shared between the TSF and another trusted IT product.

305      The TSF shall use ***the rule: data files or values can only be modified by their dedicated type-specific operations honouring the type-specific boundaries*** when interpreting the TSF data from another trusted IT product.

Application note:
The TOE does not interpret the contents of the data, e.g. it can not determine if data stored

in a specific data file is an identification number that adheres to a specific format. Instead the TOE distinguishes different types of files and ensures that type-specific boundaries can not be violated, e.g. values do not overflow, single records are limited by their size and cyclic records are handled correctly.

### Cryptographic key destruction (FCS_CKM.4) / M4M-DESFire

306    The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting of memory** that meets the following: **none**.

### User identification before any action (FIA_UID.2) / M4M-DESFire

307    The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note:

The Service Manager is identified by the usage of the M4M host interface. Identification of the other users is performed upon an authentication request based on the currently selected context and the key number. For example, if an authentication request for key number 0 is issued after selecting a specific application, the user is identified as the Application Manager of the respective application. Before any authentication request is issued, the user is identified as 'Everybody'.

### User authentication before any action (FIA_UAU.2) / M4M-DESFire

308    The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note:

The Service Manager is the only user authenticated outside the TOE.

### Multiple authentication mechanisms (FIA_UAU.5) / M4M-DESFire

309    The TSF shall provide **'none' and cryptographic authentication** to support user authentication.

310    The TSF shall authenticate any user's claimed identity according to the **following rules:**

- **The 'none' authentication is performed with anyone who communicates with the TOE without issuing an explicit authentication request. The 'none' authentication implicitly and solely authorises the 'Everybody' subject.**

- **The cryptographic authentication is used to authorise the VC Administrator, VC Manager, Application Manager and Application User.**

### Management of TSF data (FMT_MTD.1) / M4M-DESFire

311    The TSF shall restrict the ability to **change_default, modify or freeze** the c**ard master key, application master keys and application keys** to **the VC Administrator, Application Manager and Application User.**

***312    Refinement:***

*The detailed management abilities are:*

- *The VC Administrator can modify the card master key. The virtual card attributes contain a flag that when set will prevent any further change of the card master key, thereby allowing to freeze the card master key.*
- *The VC Administrator can change the default key that is used for the application master key and for the application keys when an application is created.*
- *The Application Manager of an application can modify the application master key of this application. The application attributes contain a flag that when set will prevent any further change of the application master key, thereby allowing to freeze the application master key.*
- *The Application Manager can decide to restrict the ability to modify the application keys to the Application Manager, the Application Users or to Nobody. The restriction to Nobody is equivalent to freezing the application keys. The Application Users can either change their own keys or one Application User can be defined that can change all keys of the Application Users within an application.*
- *As an implication of the last rule, any subject that receives the modify abilities from the Application Manager gets these abilities transferred.*

### Trusted path (FTP_TRP.1) / M4M-DESFire

313    The TSF shall provide a communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **modification or disclosure**.

314    The TSF shall permit **remote users** to initiate communication via the trusted path.

315    The TSF shall require the use of the trusted path for **authentication requests with DES and AES, confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes**.

### Basic rollback (FDP_ROL.1) / M4M-DESFire

316    The TSF shall enforce **the M4M-DESFire Access Control Policy** to permit the rollback of the **operations that modify the value or data file objects** on the **backup files**.

317    The TSF shall permit operations to be rolled back within the **scope of the current transaction, which is defined by the following limitative events: chip reset, (re-) authentication (either successful or not), select command, explicit commit, explicit abort, command failure**.

### Replay detection (FPT_RPL.1) / M4M-DESFire

318    The TSF shall detect replay for the following entities: **authentication requests with DES and AES, confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes**.

319    The TSF shall perform **rejection of the request** when replay is detected.

### Unlinkability (FPR_UNL.1) / M4M-DESFire

320    The TSF shall ensure that **unauthorized subjects other than the card holder** are unable to determine whether **any operation of the TOE were caused by the same user**.

**Minimum and maximum quotas (FRU_RSA.2) / M4M-DESFire**

321     The TSF shall enforce maximum quotas of the following resources **NVM and RAM** that **subjects** can use **simultaneously**.

322     The TSF shall ensure the provision of minimum quantity of **the NVM and the RAM** that is available for **subjects** to use **simultaneously**.

Application note:
The subjects addressed here are M4M-DESFire, and all other applications running on the TOE.
The goal is to ensure that M4M-DESFire always have enough NVM and RAM for its own usage.

**Subset residual information protection (FDP_RIP.1) / M4M-DESFire**

323     The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **M4M-DESFire**.

# 5.2      TOE security assurance requirements

324     Security Assurance Requirements for the TOE for the evaluation of the TOE are those taken from the Evaluation Assurance Level **5** (EAL**5**) and augmented by taking the following components:

- ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.1, ALC_TAT.3, ASE_TSS.2, ATE_COV.3, ATE_FUN.2 and AVA_VAN.5**.**

325     Regarding application note 21 of *BSI-CC-PP-0084-2014*, the continuously increasing maturity level of evaluations of Security ICs justifies the selection of a higher-level assurance package.

326     The component ALC_FLR.1 is chosen as an augmentation in this ST because a solid flaw management is key for the continuous improvement of the security IC platforms, especially on markets which need highly resistant and long lasting products.

327     The component ASE_TSS.2 is chosen as an augmentation in this ST to give architectural information on the security functionality of the TOE.

328     The set of security assurance requirements (SARs) is presented in *Table 10*, indicating the origin of the requirement.

**Table 10.      TOE security assurance requirements**

| Label | Title | Origin |
|---|---|---|
| ADV_ARC.1 | Security architecture description | EAL5/*BSI-CC-PP-0084-2014* |
| ADV_FSP.5 | Complete semi-formal functional specification with additional error information | EAL5 |
| ADV_IMP.2 | Complete mapping of the implementation representation of the TSF | Security Target |
| ADV_INT.3 | Minimally complex internals | Security Target |
| ADV_TDS.5 | Complete semiformal modular design | Security Target |

**Table 10.    TOE security assurance requirements (continued)**

| Label | Title | Origin |
|---|---|---|
| AGD_OPE.1 | Operational user guidance | EAL5/*BSI-CC-PP-0084-2014* |
| AGD_PRE.1 | Preparative procedures | EAL5/*BSI-CC-PP-0084-2014* |
| ALC_CMC.5 | Advanced support | Security Target |
| ALC_CMS.5 | Development tools CM coverage | EAL5 |
| ALC_DEL.1 | Delivery procedures | EAL5/*BSI-CC-PP-0084-2014* |
| ALC_DVS.2 | Sufficiency of security measures | *BSI-CC-PP-0084-2014* |
| ALC_FLR.1 | Basic flaw remediation | Security Target |
| ALC_LCD.1 | Developer defined life-cycle model | EAL5/*BSI-CC-PP-0084-2014* |
| ALC_TAT.3 | Compliance with implementation standards - all parts | Security Target |
| ASE_CCL.1 | Conformance claims | EAL5/*BSI-CC-PP-0084-2014* |
| ASE_ECD.1 | Extended components definition | EAL5/*BSI-CC-PP-0084-2014* |
| ASE_INT.1 | ST introduction | EAL5/*BSI-CC-PP-0084-2014* |
| ASE_OBJ.2 | Security objectives | EAL5/*BSI-CC-PP-0084-2014* |
| ASE_REQ.2 | Derived security requirements | EAL5/*BSI-CC-PP-0084-2014* |
| ASE_SPD.1 | Security problem definition | EAL5/*BSI-CC-PP-0084-2014* |
| ASE_TSS.2 | TOE summary specification with architectural summary | Security Target |
| ATE_COV.3 | Rigorous analysis of coverage | Security Target |
| ATE_DPT.3 | Testing: modular design | EAL5 |
| ATE_FUN.2 | Ordered functional testing | Security Target |
| ATE_IND.2 | Independent testing - sample | EAL5/*BSI-CC-PP-0084-2014* |
| AVA_VAN.5 | Advanced methodical vulnerability analysis | *BSI-CC-PP-0084-2014* |

## 5.3    Refinement of the security assurance requirements

329    As *BSI-CC-PP-0084-2014* defines refinements for selected SARs, these refinements are also claimed in this Security Target.

330    The main customizing is that the IC Dedicated Software is an operational part of the TOE after delivery, although it is mainly not available to the user.

331    Regarding application note 22 of *BSI-CC-PP-0084-2014*, the refinements for all the assurance families have been reviewed for the hierarchically higher-level assurance components selected in this Security Target.

332    The text of the impacted refinements of *BSI-CC-PP-0084-2014* is reproduced in the next sections.

333    For reader's ease, an impact summary is provided in *Table 11*.

**Table 11.    Impact of EAL5 selection on *BSI-CC-PP-0084-2014* refinements**

| Assurance Family | *BSI-CC-PP-0084-2014* Level | ST Level | Impact on refinement |
|---|---|---|---|
| ALC_DEL | 1 | 1 | New refinement related to the Loader |
| ALC_DVS | 2 | 2 | None |
| ALC_CMS | 4 | 5 | None, refinement is still valid |
| ALC_CMC | 4 | 5 | None, refinement is still valid |
| ADV_ARC | 1 | 1 | None |
| ADV_FSP | 4 | 5 | Presentation style changes, IC Dedicated Software is included |
| ADV_IMP | 1 | 2 | None, refinement is still valid |
| ATE_COV | 2 | 3 | IC Dedicated Software is included |
| AGD_OPE | 1 | 1 | None |
| AGD_PRE | 1 | 1 | New refinement related to the Loader |
| AVA_VAN | 5 | 5 | None |

## 5.3.1    Refinement regarding delivery procedure (ALC_DEL)

334    According to *JIL SRFPDCL*:

335    For the delivery of the Initial TOE, Additional Code and Final TOE, all the guidance describing the delivery procedures shall be taken into account.

336    They must especially describe the protection measures of the proof associated to the Additional Codes and the protection measures of the cryptographic keys used to generate this proof. The measures described in the guidance will have to be audited.

## 5.3.2    Refinement regarding functional specification (ADV_FSP)

337    ~~Although the IC Dedicated Test Software is a part of the TOE, the test functions of the IC Dedicated Test Software are not described in the Functional Specification because the IC Dedicated Test Software is considered as a test tool delivered with the TOE but not providing security functions for the operational phase of the TOE.~~ ***The IC Dedicated Software provides security functionalities as soon as the TOE becomes operational (boot software). These are properly identified in the delivered documentation.***

338    The Functional Specification ***refers to datasheet to*** trace security features that do not provide any external interface but that contribute to fulfil the SFRs e.g. like physical protection. Thereby they are part of the complete instantiation of the SFRs.

339    The Functional Specification ***refers to design specifications to detail the*** mechanisms against physical attacks ***described*** in a more general way only, but detailed enough to be able to support Test Coverage Analysis also for those mechanisms where inspection of the layout is of relevance or tests beside the TSFI may be needed.

340     The Functional Specification *refers to data sheet to* specify operating conditions of the TOE. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature.

341     All functions and mechanisms which control access to the functions provided by the IC Dedicated Test Software (refer to the security functional requirement (FMT_LIM.2)) *are part of the* Functional Specification. Details will be given in the document for ADV_ARC, refer to Section 6.2.1.5. In addition, all these functions and mechanisms *are* subsequently be refined according to all relevant requirements of the Common Criteria assurance class ADV because these functions and mechanisms are active after TOE Delivery and need to be part of the assurance aspects Tests (class ATE) and Vulnerability Assessment (class AVA). Therefore, all necessary information *is* provided to allow tests and vulnerability assessment.

342     Since the selected higher-level assurance component requires a security functional specification presented in a "semi-formal style" (ADV_FSP.5.2C) the changes affect the style of description, the *BSI-CC-PP-0084-2014* refinements can be applied with changes covering the IC Dedicated Test Software and are valid for ADV_FSP.5.

### 5.3.3     Refinement regarding test coverage (ATE_COV)

343     The TOE *is* tested under different operating conditions within the specified ranges. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature. This means that "Fault tolerance (FRU_FLT.2)" *is* proven for the complete TSF. The tests must also cover functions which may be affected by "ageing" (such as *NVM* writing).

344     The existence and effectiveness of measures against physical attacks (as specified by the functional requirement FPT_PHP.3) cannot be tested in a straightforward way. Instead *STMicroelectronics provides* evidence that the TOE actually has the particular physical characteristics (especially layout design principles). This *is* done by checking the layout (implementation or actual) in an appropriate way. The required evidence pertains to the existence of mechanisms against physical attacks (unless being obvious).

345     The IC Dedicated Test Software is seen as a "test tool" being delivered as part of the TOE. However, the Test Features do not provide security functionality. Therefore, Test Features need not to be covered by the Test Coverage Analysis but all functions and mechanisms which limit the capability of the functions (cf. FMT_LIM.1) and control access to the functions (cf. FMT_LIM.2) provided by the IC Dedicated Test Software must be part of the Test Coverage Analysis. *The IC Dedicated Software provides security functionalities as soon as the TOE becomes operational (boot software). These are part of the Test Coverage Analysis.*

### 5.3.4     Refinement regarding preparative procedures (AGD_PRE)

346     According to *JIL SRFPDCL*:

347     Preparative user guidance are intended to be used by persons responsible for the following tasks:
*   acceptance of the Initial TOE and of the Additional Code;
*   installation of the TOE: download of the Additional Code onto the Initial TOE, activation of the Additional Code, checking of the resulting Identification Data.

## 5.4       Security Requirements rationale

### 5.4.1       Rationale for the Security Functional Requirements

348       Just as for the security objectives rationale of *Section 4.3*, the main line of this rationale is that the inclusion of all the security requirements of the *BSI-CC-PP-0084-2014* protection profile, together with those in *AUG*, and with those introduced in this Security Target, guarantees that all the security objectives identified in *Section 4* are suitably addressed by the security requirements stated in this chapter, and that the latter together form an internally consistent whole.

**Table 12.       Security Requirements versus Security Objectives**

| Security Objective | TOE Security Functional and Assurance Requirements |
|---|---|
| *BSI.O.Leak-Inherent* | "*Basic internal transfer protection*" *FDP_ITT.1*<br>"*Basic internal TSF data transfer protection*" *FPT_ITT.1*<br>"*Subset information flow control*" *FDP_IFC.1* |
| *BSI.O.Phys-Probing* | "*Stored data confidentiality*" *FDP_SDC.1*<br>"*Resistance to physical attack*" *FPT_PHP.3* |
| *BSI.O.Malfunction* | "*Limited fault tolerance*" *FRU_FLT.2*<br>"*Failure with preservation of secure state*" *FPT_FLS.1* |
| *BSI.O.Phys-Manipulation* | "*Stored data integrity monitoring and action*" *FDP_SDI.2*<br>"*Resistance to physical attack*" *FPT_PHP.3* |
| *BSI.O.Leak-Forced* | All requirements listed for *BSI.O.Leak-Inherent*<br>*FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1*<br>plus those listed for *BSI.O.Malfunction* and *BSI.O.Phys-Manipulation*<br>*FRU_FLT.2*, *FPT_FLS.1*, *FDP_SDI.2*, *FPT_PHP.3* |
| *BSI.O.Abuse-Func* | "*Limited capabilities - Test*" *FMT_LIM.1 / Test*<br>"*Limited availability - Test*" *FMT_LIM.2 / Test*<br>"*Limited capabilities - Secure Diagnostic*" *FMT_LIM.1 / Sdiag*<br>"*Limited availability - Secure Diagnostic*" *FMT_LIM.2 / Sdiag*<br>"*Inter-TSF trusted channel - Secure Diagnostic*" *FTP_ITC.1 / Sdiag*<br>"*Audit review - Secure Diagnostic*" *FAU_SAR.1 / Sdiag*<br>plus those for *BSI.O.Leak-Inherent, BSI.O.Phys-Probing, BSI.O.Malfunction, BSI.O.Phys-Manipulation, BSI.O.Leak-Forced*<br>*FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1*, *FDP_SDC.1*, *FDP_SDI.2*, *FPT_PHP.3*, *FRU_FLT.2*, *FPT_FLS.1* |
| *BSI.O.Identification* | "*Audit storage*" *FAU_SAS.1* |
| *BSI.O.RND* | "*Random number generation*" *FCS_RNG.1*<br>plus those for *BSI.O.Leak-Inherent, BSI.O.Phys-Probing, BSI.O.Malfunction, BSI.O.Phys-Manipulation, BSI.O.Leak-Forced*<br>*FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1*, *FDP_IFC.1*, *FDP_SDC.1*, *FPT_PHP.3*, *FRU_FLT.2*, *FPT_FLS.1* |
| *BSI.OE.Resp-Appl* | Not applicable |

**Table 12. Security Requirements versus Security Objectives**

| Security Objective | TOE Security Functional and Assurance Requirements |
|---|---|
| *BSI.OE.Process-Sec-IC* | Not applicable |
| *BSI.OE.Lim-Block-Loader* | Not applicable |
| *BSI.OE.Loader-Usage* | Not applicable |
| *BSI.OE.TOE-Auth* | Not applicable |
| *OE.Enable-Disable-Secure-Diag* | Not applicable |
| *OE.Secure-Diag-Usage* | Not applicable |
| *BSI.O.Authentication* | "*Authentication Proof of Identity*" *FIA_API.1* |
| *BSI.O.Cap-Avail-Loader* | "*Limited capabilities - Loader*" *FMT_LIM.1 / Loader*<br>"*Limited availability - Loader*" *FMT_LIM.2 / Loader* |
| *BSI.O.Ctrl_Auth_Loader* | "*Inter-TSF trusted channel - Loader*" *FTP_ITC.1 / Loader*<br>"*Basic data exchange confidentiality - Loader*" *FDP_UCT.1 / Loader*<br>"*Data exchange integrity - Loader*" *FDP_UIT.1 / Loader*<br>"*Subset access control - Loader*" *FDP_ACC.1 / Loader*<br>"*Security attribute based access control - Loader*" *FDP_ACF.1 / Loader*<br>"*Static attribute initialisation - Loader*" *FMT_MSA.3 / Loader*<br>"*Management of security attributes - Loader*" *FMT_MSA.1 / Loader*<br>"*Specification of management functions - Loader*" *FMT_SMF.1 / Loader*<br>"*Security roles - Loader*" *FMT_SMR.1 / Loader*<br>"*Timing of identification - Loader*" *FIA_UID.1 / Loader*<br>"*Timing of authentication - Loader*" *FIA_UAU.1 / Loader* |
| *ANSSI.O.Prot-TSF-Confidentiality* | "*Inter-TSF trusted channel - Loader*" *FTP_ITC.1 / Loader*<br>"*Basic data exchange confidentiality - Loader*" *FDP_UCT.1 / Loader*<br>"*Data exchange integrity - Loader*" *FDP_UIT.1 / Loader*<br>"*Subset access control - Loader*" *FDP_ACC.1 / Loader*<br>"*Security attribute based access control - Loader*" *FDP_ACF.1 / Loader*<br>"*Static attribute initialisation - Loader*" *FMT_MSA.3 / Loader*<br>"*Management of security attributes - Loader*" *FMT_MSA.1 / Loader*<br>"*Specification of management functions - Loader*" *FMT_SMF.1 / Loader*<br>"*Security roles - Loader*" *FMT_SMR.1 / Loader*<br>"*Timing of identification - Loader*" *FIA_UID.1 / Loader*<br>"*Timing of authentication - Loader*" *FIA_UAU.1 / Loader* |

**Table 12.     Security Requirements versus Security Objectives**

| Security Objective | TOE Security Functional and Assurance Requirements |
|---|---|
| *ANSSI.O.Secure-Load-ACode* | "*Inter-TSF trusted channel - Loader*" *FTP_ITC.1 / Loader*<br>"*Basic data exchange confidentiality - Loader*" *FDP_UCT.1 / Loader*<br>"*Data exchange integrity - Loader*" *FDP_UIT.1 / Loader*<br>"*Subset access control - Loader*" *FDP_ACC.1 / Loader*<br>"*Security attribute based access control - Loader*" *FDP_ACF.1 / Loader*<br>"*Static attribute initialisation - Loader*" *FMT_MSA.3 / Loader*<br>"*Management of security attributes - Loader*" *FMT_MSA.1 / Loader*<br>"*Specification of management functions - Loader*" *FMT_SMF.1 / Loader*<br>"*Security roles - Loader*" *FMT_SMR.1 / Loader*<br>"*Timing of identification - Loader*" *FIA_UID.1 / Loader*<br>"*Timing of authentication - Loader*" *FIA_UAU.1 / Loader*<br>"*Audit storage - Loader*" *FAU_SAS.1 / Loader* |
| *ANSSI.O.Secure-AC-Activation* | "*Failure with preservation of secure state - Loader*" *FPT_FLS.1 / Loader* |
| *ANSSI.O.TOE-Identification* | "*Audit storage - Loader*" *FAU_SAS.1 / Loader*<br>"*Audit review - Loader*" *FAU_SAR.1 / Loader*<br>"*Stored data integrity monitoring and action*" *FDP_SDI.2* |
| *O.Secure-Load-AMemImage* | "*Inter-TSF trusted channel - Loader*" *FTP_ITC.1 / Loader*<br>"*Basic data exchange confidentiality - Loader*" *FDP_UCT.1 / Loader*<br>"*Data exchange integrity - Loader*" *FDP_UIT.1 / Loader*<br>"*Subset access control - Loader*" *FDP_ACC.1 / Loader*<br>"*Security attribute based access control - Loader*" *FDP_ACF.1 / Loader*<br>"*Static attribute initialisation - Loader*" *FMT_MSA.3 / Loader*<br>"*Management of security attributes - Loader*" *FMT_MSA.1 / Loader*<br>"*Specification of management functions - Loader*" *FMT_SMF.1 / Loader*<br>"*Security roles - Loader*" *FMT_SMR.1 / Loader*<br>"*Timing of identification - Loader*" *FIA_UID.1 / Loader*<br>"*Timing of authentication - Loader*" *FIA_UAU.1 / Loader*<br>"*Audit storage - Loader*" *FAU_SAS.1 / Loader* |
| *O.MemImage-Identification* | "*Failure with preservation of secure state - Loader*" *FPT_FLS.1 / Loader*<br>"*Audit storage - Loader*" *FAU_SAS.1 / Loader*<br>"*Audit review - Loader*" *FAU_SAR.1 / Loader*<br>"*Stored data integrity monitoring and action*" *FDP_SDI.2* |
| *OE.Composite-TOE-Id* | Not applicable |
| *OE.TOE-Id* | Not applicable |

**Table 12.    Security Requirements versus Security Objectives**

| Security Objective | TOE Security Functional and Assurance Requirements |
|---|---|
| *AUG1.O.Add-Functions* | "*Cryptographic operation*" *FCS_COP.1*<br>"*Cryptographic key generation*" *FCS_CKM.1* |
| *AUG4.O.Mem-Access* | "*Complete access control - Memories*" *FDP_ACC.2 / Memories*<br>"*Security attribute based access control - Memories*" *FDP_ACF.1 / Memories*<br>"*Static attribute initialisation - Memories*" *FMT_MSA.3 / Memories*<br>"*Management of security attributes - Memories*" *FMT_MSA.1 / Memories*<br>"*Specification of management functions - Memories*" *FMT_SMF.1 / Memories* |
| *O.Access-Control-DESFire* | "*Security roles - M4M-DESFire*" *FMT_SMR.1 / M4M-DESFire*<br>"*Subset access control - M4M-DESFire*" *FDP_ACC.1 / M4M-DESFire*<br>"*Security attribute based access control - M4M-DESFire*" *FDP_ACF.1 / M4M-DESFire*<br>"*Static attribute initialisation - M4M-DESFire*" *FMT_MSA.3 / M4M-DESFire*<br>"*Management of security attributes - M4M-DESFire*" *FMT_MSA.1 / M4M-DESFire*<br>"*Specification of management functions - M4M-DESFire*" *FMT_SMF.1 / M4M-DESFire*<br>"*Import of user data with security attributes - M4M-DESFire*" *FDP_ITC.2 / M4M-DESFire*<br>"*Cryptographic key destruction - M4M-DESFire*" *FCS_CKM.4 / M4M-DESFire*<br>"*Management of TSF data - M4M-DESFire*" *FMT_MTD.1 / M4M-DESFire* |
| *O.Authentication-DESFire* | "*Cryptographic operation* - DES" *FCS_COP.1 / DES*<br>"*Cryptographic operation* - AES" *FCS_COP.1 / AES*<br>"*User identification before any action - M4M-DESFire*" *FIA_UID.2 / M4M-DESFire*<br>"*User authentication before any action - M4M-DESFire*" *FIA_UAU.2 / M4M-DESFire*<br>"*Multiple authentication mechanisms - M4M-DESFire*" *FIA_UAU.5 / M4M-DESFire*<br>"*Trusted path - M4M-DESFire*" *FTP_TRP.1 / M4M-DESFire*<br>"*Replay detection - M4M-DESFire*" *FPT_RPL.1 / M4M-DESFire* |
| *O.Confidentiality-DESFire* | "*Cryptographic operation* - DES" *FCS_COP.1 / DES*<br>"*Cryptographic operation* - AES" *FCS_COP.1 / AES*<br>"*Trusted path - M4M-DESFire*" *FTP_TRP.1 / M4M-DESFire*<br>"*Replay detection - M4M-DESFire*" *FPT_RPL.1 / M4M-DESFire* |
| *O.Type-Consistency-DESFire* | "*Inter-TSF basic TSF data consistency - M4M-DESFire*" *FPT_TDC.1 / M4M-DESFire* |

**Table 12.     Security Requirements versus Security Objectives**

| Security Objective | TOE Security Functional and Assurance Requirements |
|---|---|
| O.Transaction-DESFire | "*Basic rollback - M4M-DESFire*" *FDP_ROL.1 / M4M-DESFire* |
| O.No-Trace-DESFire | "*Unlinkability - M4M-DESFire*" *FPR_UNL.1 / M4M-DESFire* |
| O.Resp-Appl | All SFRs defined additionnaly in the ST |
| O.Resource-DESFire | "*Minimum and maximum quotas - M4M-DESFire*" *FRU_RSA.2 / M4M-DESFire* |
| O.Verification-DESFire | "*Complete access control - Memories*" *FDP_ACC.2 / Memories*<br>"*Security attribute based access control - Memories*" *FDP_ACF.1 / Memories*<br>"*Static attribute initialisation - Memories*" *FMT_MSA.3 / Memories*<br>"*Failure with preservation of secure state*" *FPT_FLS.1* |
| O.Firewall-DESFire | "*Complete access control - Memories*" *FDP_ACC.2 / Memories*<br>"*Security attribute based access control - Memories*" *FDP_ACF.1 / Memories*<br>"*Static attribute initialisation - Memories*" *FMT_MSA.3 / Memories* |
| O.Shr-Res-DESFire | "*Subset residual information protection - M4M-DESFire*" *FDP_RIP.1 / M4M-DESFire* |
| OE.Secure-Values-DESFire | Not applicable |
| OE.Terminal-Support-DESFire | Not applicable |
| OE.M4MFramework-Identification | Not applicable |

349     As origins of security objectives have been carefully kept in their labelling, and origins of security requirements have been carefully identified in *Table 7* and *Table 12*, it can be verified that the justifications provided by the *BSI-CC-PP-0084-2014* protection profile and *AUG* can just be carried forward to their union.

350     From *Table 5*, it is straightforward to identify additional security objectives for the TOE (*AUG1.O.Add-Functions* and *AUG4.O.Mem-Access*) tracing back to *AUG*, additional objectives (*ANSSI.O.Prot-TSF-Confidentiality*, *ANSSI.O.Secure-Load-ACode*, *ANSSI.O.Secure-AC-Activation* and *ANSSI.O.TOE-Identification*) tracing back to *JIL SRFPDCL* / *ANSSI-CC-CER/F/06.003*,and additional objectives (*O.Secure-Load-AMemImage*, *O.MemImage-Identification*, *O.Access-Control-DESFire*, *O.Authentication-DESFire*, *O.Confidentiality-DESFire*, *O.Type-Consistency-DESFire*, *O.Transaction-DESFire*, *O.No-Trace-DESFire*, *O.Resp-Appl*, *O.Resource-DESFire*, *O.Verification-DESFire*, *O.Firewall-DESFire* and *O.Shr-Res-DESFire*) introduced in this Security Target. This rationale must show that security requirements suitably address them all.

351      Furthermore, a careful observation of the requirements listed in *Table 7* and *Table 12* shows that:

- there are security requirements introduced from *AUG* (*FCS_COP.1*, *FDP_ACC.2 / Memories*, *FDP_ACF.1 / Memories*, *FMT_MSA.3 / Memories* and *FMT_MSA.1 / Memories*),

- there are additional security requirements introduced by this Security Target (*FCS_CKM.1*, *FMT_MSA.3 / Loader*, *FMT_MSA.1 / Loader*, *FMT_SMF.1 / Loader*, *FMT_SMR.1 / Loader*, *FIA_UID.1 / Loader*, *FIA_UAU.1 / Loader*, *FPT_FLS.1 / Loader*, *FAU_SAS.1 / Loader*, *FAU_SAR.1 / Loader*, *FMT_SMF.1 / Memories*, *FMT_SMR.1 / M4M-DESFire*, *FDP_ACC.1 / M4M-DESFire*, *FDP_ACF.1 / M4M-DESFire*, *FMT_MSA.3 / M4M-DESFire*, *FMT_MSA.1 / M4M-DESFire*, *FMT_SMF.1 / M4M-DESFire*, *FDP_ITC.2 / M4M-DESFire*, *FPT_TDC.1 / M4M-DESFire*, *FIA_UID.2 / M4M-DESFire*, *FIA_UAU.2 / M4M-DESFire*, *FIA_UAU.5 / M4M-DESFire*, *FMT_MTD.1 / M4M-DESFire*, *FTP_TRP.1 / M4M-DESFire*, *FCS_CKM.4 / M4M-DESFire*, *FDP_ROL.1 / M4M-DESFire*, *FPT_RPL.1 / M4M-DESFire*, *FPR_UNL.1 / M4M-DESFire*, *FRU_RSA.2 / M4M-DESFire*, *FDP_RIP.1 / M4M-DESFire*, *FTP_ITC.1 / Sdiag*, *FAU_SAR.1 / Sdiag*, *FMT_LIM.1 / Sdiag*, *FMT_LIM.2 / Sdiag*, and various assurance requirements of EAL5+).

352      Though it remains to show that:

- security objectives from this Security Target, from *JIL SRFPDCL* / *ANSSI-CC-CER/F/06.003* and from *AUG* are addressed by security requirements stated in this chapter,

- additional security requirements from this Security Target and from *AUG* are mutually supportive with the security requirements from the *BSI-CC-PP-0084-2014* protection profile, and they do not introduce internal contradictions,

- all dependencies are still satisfied.

353      The justification that the additional security objectives are suitably addressed, that the additional security requirements are mutually supportive and that, together with those already in *BSI-CC-PP-0084-2014*, they form an internally consistent whole, is provided in the next subsections.

## 5.4.2      Extended security objectives are suitably addressed

**Security objective "Dynamic Area based Memory Access Control (*AUG4.O.Mem-Access*)"**

354      The justification related to the security objective "***Dynamic*** Area based Memory Access Control (*AUG4.O.Mem-Access*)" is as follows:

355      The security functional requirements "*Complete access control (FDP_ACC.2) / Memories*" ***and** "Security attribute based access control (FDP_ACF.1) / Memories"*, with the related Security Function Policy (SFP) "***Dynamic Memory Access Control Policy***" exactly require to implement a ***Dynamic*** area based memory access control as demanded by *AUG4.O.Mem-Access*. Therefore, *FDP_ACC.2 / Memories* **and** *FDP_ACF.1 / Memories* with **their** SFP **are** suitable to meet the security objective.

356      The security functional requirement "*Static attribute initialisation (FMT_MSA.3) / Memories*" requires that the TOE provides default values for security attributes. The ability to update the security attributes is restricted to privileged subject(s) ***as further detailed in the security functional requirement "****Management of security attributes (FMT_MSA.1) /*

*Memories"*. These management functions ensure that the required access control can be realised using the functions provided by the TOE.

### Security objective "Additional Specific Security Functionality (*AUG1.O.Add-Functions*)"

357     The justification related to the security objective "Additional Specific Security Functionality (*AUG1.O.Add-Functions*)" is as follows:

358     The security functional requirements "*Cryptographic operation (FCS_COP.1)*" **and** "*Cryptographic key generation (FCS_CKM.1)*" exactly require those functions to be implemented that are demanded by *AUG1.O.Add-Functions.* Therefore, *FCS_COP.1* is suitable to meet the security objective, **together with** *FCS_CKM.1*.

### Security objective "Protection against Abuse of Functionality (*BSI.O.Abuse-Func*)"

359     This objective states that abuse of functions (especially provided by the IC Dedicated Test Software, for instance in order to read secret data) must not be possible in Phase 7 of the life-cycle. There are two possibilities to achieve this: (i) They cannot be used by an attacker (i. e. its availability is limited) or (ii) using them would not be of relevant use for an attacker (i. e. its capabilities are limited) since the functions are designed in a specific way. The first possibility is specified by "*Limited availability (FMT_LIM.2) / Test*" **and** "*Limited availability (FMT_LIM.2) / Sdiag*", and the second one by "*Limited capabilities (FMT_LIM.1) / Test*" **and** "*Limited capabilities (FMT_LIM.1) / Sdiag*". Since these requirements are combined to support the policy, which is suitable to fulfil O.Abuse-Func, **these** security functional requirements together are suitable to meet the objective.

360     Other security functional requirements which prevent attackers from circumventing the functions implementing these two security functional requirements (for instance by manipulating the hardware) also support the objective. The relevant **Security Functional requirements** are also listed in *Table 12*.

### Security objective "Access control and authenticity for the Loader (*BSI.O.Ctrl_Auth_Loader*)"

361     The justification related to the security objective "Access control and authenticity for the Loader (*BSI.O.Ctrl_Auth_Loader*)" is as follows:

362     The **security functional requirement** "*Subset access control (FDP_ACC.1) / Loader*" defines the subjects, objects and operations of the Loader SFP enforced by the SFR *FTP_ITC.1 / Loader, FDP_UCT.1 / Loader, FDP_UIT.1 / Loader* and *FDP_ACF.1 / Loader*. The **security functional requirement** "*Inter-TSF trusted channel (FTP_ITC.1) / Loader*" requires the TSF to establish a trusted channel with assured identification of its end points and protection of the channel data from modification or disclosure. The **security functional requirement** "*Basic data exchange confidentiality (FDP_UCT.1) / Loader*" requires the TSF to receive data protected from unauthorized disclosure. The **security functional requirement** "*Data exchange integrity (FDP_UIT.1) / Loader*" requires the TSF to verify the integrity **and the rightfulness** of the received data. The **security functional requirement** "*Security attribute based access control (FDP_ACF.1) / Loader*" requires the TSF to implement access control for the Loader functionality. Therefore, *FTP_ITC.1 / Loader*, *FDP_UCT.1 / Loader*, *FDP_UIT.1 / Loader*, *FDP_ACC.1 / Loader* and *FDP_ACF.1 / Loader* with their SFP are suitable to meet the security objective.

363     Complementary, the security functional requirement "*Static attribute initialisation (FMT_MSA.3) / Loader*" requires that the TOE provides default values for security attributes. The ability to update the security attributes is restricted to privileged subject(s) as further detailed in the security functional requirement "*Management of security attributes (FMT_MSA.1) / Loader*"
The security functional requirements "*Security roles (FMT_SMR.1) / Loader*", "*Timing of identification (FIA_UID.1) / Loader*" and "*Timing of authentication (FIA_UAU.1) / Loader*" specify the roles that the TSF recognises and the actions authorized before their identification.
The security functional requirement "*Specification of management functions (FMT_SMF.1) / Loader*" provides additional controlled facility for adapting the loader behaviour to the user's needs. These management functions ensure that the required access control, associated to the loading feature, can be realized using the functions provided by the TOE.

**Security objectives "Protection of the confidentiality of the TSF (*ANSSI.O.Prot-TSF-Confidentiality*)", "Secure loading of the Additional Code (*ANSSI.O.Secure-Load-ACode*)" and "Secure loading of the Additional Memory Image (*O.Secure-Load-AMemImage*)"**

364     The justification related to the security objectives **"Protection of the confidentiality of the TSF (*ANSSI.O.Prot-TSF-Confidentiality*)", "Secure loading of the Additional Code (*ANSSI.O.Secure-Load-ACode*)" and "Secure loading of the Additional Memory Image (*O.Secure-Load-AMemImage*)"** is as follows:

365     The security functional requirement "*Subset access control (FDP_ACC.1) / Loader*" defines the subjects, objects and operations of the Loader SFP enforced by the SFR FTP_ITC.1, FDP_UCT.1, FDP_UIT.1 and FDP_ACF.1/Loader.
The security functional requirement "*Inter-TSF trusted channel (FTP_ITC.1) / Loader*" requires the TSF to establish a trusted channel with assured identification of its end points and protection of the channel data from modification or disclosure.
The security functional requirement "*Basic data exchange confidentiality (FDP_UCT.1) / Loader*" requires the TSF to receive data protected from unauthorized disclosure.
The security functional requirement "*Data exchange integrity (FDP_UIT.1) / Loader*" requires the TSF to verify the integrity of the received data.
The security functional requirement "*Security attribute based access control (FDP_ACF.1) / Loader*" requires the TSF to implement access control for the Loader functionality.
The security functional requirement "*Static attribute initialisation (FMT_MSA.3) / Loader*" requires that the TOE provides default values for security attributes.
The ability to update the security attributes is restricted to privileged subject(s) as further detailed in the security functional requirement "*Management of security attributes (FMT_MSA.1) / Loader*".
The security functional requirements "*Security roles (FMT_SMR.1) / Loader*", "*Timing of identification (FIA_UID.1) / Loader*" and "*Timing of authentication (FIA_UAU.1) / Loader*" specify the roles that the TSF recognises and the actions authorized before their identification.
The security functional requirement "*Specification of management functions (FMT_SMF.1) / Loader*" provides additional controlled facility for adapting the loader behaviour to the user's needs. These management functions ensure that the required access control, associated to the loading feature, can be realised using the functions provided by the TOE.
The security functional requirement "*Audit storage (FAU_SAS.1) / Loader*" requires to store the identification data needed to enforce that only the allowed version of the Additional Memory Image can be loaded on the Initial TOE.

366      Therefore, *FTP_ITC.1 / Loader*, *FDP_UCT.1 / Loader*, *FDP_UIT.1 / Loader*, *FDP_ACC.1 / Loader*, *FDP_ACF.1 / Loader* together with *FMT_MSA.3 / Loader*, *FMT_MSA.1 / Loader*, *FMT_SMR.1 / Loader*, *FMT_SMF.1 / Loader*, *FIA_UID.1 / Loader*, *FIA_UAU.1 / Loader,* and *FAU_SAS.1 / Loader* are suitable to meet these security objectives.

### Security objective "Secure activation of the Additional Code (*ANSSI.O.Secure-AC-Activation*)"

367      The justification related to the security objective "Secure activation of the Additional Code (*ANSSI.O.Secure-AC-Activation*)" is as follows:

368      The security functional requirement "*Audit storage (FAU_SAS.1) / Loader*" requires the TSF to fail secure unless the Loading of the Additional Memory Image, including update of the Identification data, is comprehensive, as specified by *ANSSI.O.Secure-AC-Activation*.

369      Therefore, *FPT_FLS.1 / Loader* is suitable to meet this security objective.

### Security objective "Secure identification of the TOE (*ANSSI.O.TOE-Identification*)"

370      The justification related to the security objective "Secure identification of the TOE (*ANSSI.O.TOE-Identification*)" is as follows:

371      The security functional requirement "*Audit storage (FAU_SAS.1) / Loader*" requires the TSF to store the Identification Data of the Memory Images.
The security functional requirement "*Stored data integrity monitoring and action (FDP_SDI.2)*" requires the TSF to detect the integrity errors of the stored data and react in case of detected errors.
The security functional requirement "*Audit review (FAU_SAR.1) / Loader*" allows any user to read this Identification Data.

372      Therefore, *FAU_SAS.1 / Loader*, and *FAU_SAR.1 / Loader* together with *FDP_SDI.2* are suitable to meet this security objective.

### Security objective "Secure identification of the Memory Image (*O.MemImage-Identification*)"

373      The justification related to the security objective "Secure identification of the Memory Image (*O.MemImage-Identification*)" is as follows:

374      The security functional requirement "*Audit storage (FAU_SAS.1) / Loader*" requires the TSF to store the Identification Data of the Memory Images.
The security functional requirement "*Stored data integrity monitoring and action (FDP_SDI.2)*" requires the TSF to detect the integrity errors of the stored user data and react in case of detected errors.
The security functional requirement "*Audit review (FAU_SAR.1) / Loader*" allows any user to read this Identification Data.
The security functional requirement "*Audit storage (FAU_SAS.1) / Loader*" requires the TSF to fail secure unless the Loading of the Additional Memory Image, including update of the Identification data, is comprehensive, as specified by *ANSSI.O.Secure-AC-Activation*.

375      Therefore, *FAU_SAS.1 / Loader*, *FAU_SAR.1 / Loader* together with *FDP_SDI.2* and *FPT_FLS.1 / Loader* are suitable to meet this security objective.

**Security objective "Access control for M4M-DESFire (*O.Access-Control-DESFire*)"**

376     The justification related to the security objective "Access control for M4M-DESFire (*O.Access-Control-DESFire*)" is as follows:

377     The security functional requirement "*Security roles (FMT_SMR.1) / M4M-DESFire*" defines the roles of the M4M-DESFire Access Control Policy.
The security functional requirements "*Subset access control (FDP_ACC.1) / M4M-DESFire*" and "*Security attribute based access control (FDP_ACF.1) / M4M-DESFire*" define the rules and "*Static attribute initialisation (FMT_MSA.3) / M4M-DESFire*" and "*Management of security attributes (FMT_MSA.1) / M4M-DESFire*" the attributes that the access control is based on.
The security functional requirement "*Management of TSF data (FMT_MTD.1) / M4M-DESFire*" provides the rules for the management of the authentication data.
The management functions are defined by "*Specification of Management Functions (FMT_SMF.1) / M4M-DESFire*".
Since the TOE stores data on behalf of the authorized subjects, import of user data with security attributes is defined by "*Import of user data with security attributes (FDP_ITC.2) / M4M-DESFire*".
Since cryptographic keys are used for authentication (refer to *O.Authentication-DESFire*), these keys have to be removed if they are no longer needed for the access control (i.e. an application is deleted). This is required by "*Cryptographic key destruction (FCS_CKM.4) / M4M-DESFire*". These nine SFRs together provide an access control mechanism as required by the objective *O.Access-Control-DESFire*.

**Security objective "Authentication for M4M-DESFire (*O.Authentication-DESFire*)"**

378     The justification related to the security objective "Authentication for M4M-DESFire (*O.Authentication-DESFire*)" is as follows:

379     The two security functional requirements "*Cryptographic operation (FCS_COP.1) / DES*" and "*Cryptographic operation (FCS_COP.1) / AES*" require that the TOE provides the basic cryptographic algorithms that can be used to perform the authentication.
The security functional requirements "*User identification before any action (FIA_UID.2) / M4M-DESFire*", "*User authentication before any action (FIA_UAU.2) / M4M-DESFire*" and "*Multiple authentication mechanisms (FIA_UAU.5) / M4M-DESFire*" together define that users must be identified and authenticated before any action. The 'none' authentication of "*Multiple authentication mechanisms (FIA_UAU.5) / M4M-DESFire*" also ensures that a specific subject is identified and authenticated before an explicit authentication request is sent to the TOE.
"*Trusted path (FTP_TRP.1) / M4M-DESFire*" requires a trusted communication path between the TOE and remote users; FTP_TRP.1.3 especially requires "authentication requests".
Together with "*Replay detection (FPT_RPL.1) / M4M-DESFire*" which requires a replay detection for these authentication requests, the seven security functional requirements fulfil the objective *O.Authentication-DESFire*.

**Security objective "M4M-DESFire Confidential Communication (*O.Confidentiality-DESFire*)"**

380     The justification related to the security objective "M4M-DESFire Confidential communication (*O.Confidentiality-DESFire*)" is as follows:

381    The two security functional requirements "*Cryptographic operation (FCS_COP.1)* / DES" and "*Cryptographic operation (FCS_COP.1)* / AES" require that the TOE provides the basic cryptographic algorithm AES that can be used to protect the communication by encryption. "*Trusted path (FTP_TRP.1) / M4M-DESFire*" requires a trusted communication path between the TOE and remote users; FTP_TRP.1.3 especially requires "confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes".
Together with "*Replay detection (FPT_RPL.1) / M4M-DESFire*" which requires a replay detection for these data transfers, the three security functional requirements fulfil the objective *O.Confidentiality-DESFire*.

### Security objective "M4M-DESFire Data type consistency (*O.Type-Consistency-DESFire*)"

382    The justification related to the security objective "M4M-DESFire Data type consistency (*O.Type-Consistency-DESFire*)" is as follows:

383    The security functional requirement "*Inter-TSF basic TSF data consistency (FPT_TDC.1) / M4M-DESFire*" requires the TOE to consistently interpret data files and values. The TOE will honour the respective file formats and boundaries (i.e. upper and lower limits, size limitations). This meets the objective *O.Type-Consistency-DESFire*.

### Security objective "M4M-DESFire Transaction mechanism (*O.Transaction-DESFire*)"

384    The justification related to the security objective "M4M-DESFire Transaction mechanism (*O.Transaction-DESFire*)" is as follows:

385    The security functional requirement "*Basic rollback (FDP_ROL.1) / M4M-DESFire*" requires the possibility to rollback a set of modifying operations on backup files in total. The set of operations is defined by the scope of the transaction, which is itself limited by some boundary events. This fulfils the objective *O.Transaction-DESFire*.

### Security objective "Preventing traceability for M4M-DESFire (*O.No-Trace-DESFire*)"

386    The justification related to the security objective "Preventing traceability for M4M-DESFire (*O.No-Trace-DESFire*)" is as follows:

387    The security functional requirement "*Unlinkability (FPR_UNL.1) / M4M-DESFire*" requires that unauthorized subjects other than the card holder are unable to determine whether any operation of the TOE were caused by the same user. This meets the objective *O.No-Trace-DESFire*.

### Security objective "Treatment of user data for M4M-DESFire (*O.Resp-Appl*)"

388    The justification related to the security objective "Treatment of user data for M4M-DESFire (*O.Resp-Appl*)" is as follows:

389    The objective was translated from an environment objective in the PP into a TOE objective in this ST. The objective is that "Security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context." The application context is defined by the security environment described in this ST. The additional SFRs defined in this ST do address the additional TOE objectives of the ST based on the ST security environment, therefore *O.Resp-Appl* is fulfilled by the additional ST SFRs.

**Security objective "NVM resource availability for M4M-DESFire (*O.Resource-DESFire*)"**

390     The justification related to the security objective "Resource availability for M4M-DESFire (*O.Resource-DESFire*)" is as follows:

391     The security functional requirement "*Minimum and maximum quotas (FRU_RSA.2) / M4M-DESFire*" requires that sufficient parts of the NVM and RAM are reserved for M4M-DESFire use. This fulfils the objective *O.Resource-DESFire*.

**Security objective "M4M-DESFire code integrity check (*O.Verification-DESFire*)"**

392     The justification related to the security objective "M4M-DESFire code integrity check (*O.Verification-DESFire*)" is as follows:

393     The security functional requirements "*Complete access control (FDP_ACC.2) / Memories*" **and "***Security attribute based access control (FDP_ACF.1) / Memories***"**, supported by "*Static attribute initialisation (FMT_MSA.3) / Memories*", require that M4M-DESFire code integrity is protected when it is part of the TOE. In addition, the security functional requirement "*Failure with preservation of secure state (FPT_FLS.1)*" requires that in case of error on NVM, M4M-DESFire execution is stopped. This meets the objective *O.Verification-DESFire*.

**Security objective "M4M-DESFire firewall (*O.Firewall-DESFire*)"**

394     The justification related to the security objective "M4M-DESFire firewall (*O.Firewall-DESFire*)" is as follows:

395     The security functional requirements "*Complete access control (FDP_ACC.2) / Memories*" and "*Security attribute based access control (FDP_ACF.1) / Memories*", supported by "*Static attribute initialisation (FMT_MSA.3) / Memories*", require that no application can read, write, compare any piece of data or code belonging to M4M-DESFire. This meets the objective *O.Firewall-DESFire*.

**Security objective "M4M-DESFire data cleaning for resource sharing (*O.Shr-Res-DESFire*)"**

396     The justification related to the security objective "M4M-DESFire data cleaning for resource sharing (*O.Shr-Res-DESFire*)" is as follows:

397     The security functional requirement "*Subset residual information protection (FDP_RIP.1) / M4M-DESFire*" requires that the information content of a resource is made unavailable upon its deallocation from M4M-DESFire. This meets the objective *O.Shr-Res-DESFire*.

## 5.4.3     Additional security requirements are consistent

**"Cryptographic operation (*FCS_COP.1*) & key generation (*FCS_CKM.1*)"**

398     These security requirements have already been argued in *Section : Security objective "Additional Specific Security Functionality (AUG1.O.Add-Functions)"* above.

**"Static attribute initialisation (*FMT_MSA.3 / Memories*),**
**Management of security attributes (*FMT_MSA.1 / Memories*),**
**Complete access control (*FDP_ACC.2 / Memories*),**
**Security attribute based access control (*FDP_ACF.1 / Memories*)"**

399     These security requirements have already been argued in *Section : Security objective "Dynamic Area based Memory Access Control (AUG4.O.Mem-Access)"* above.

**"Static attribute initialisation (*FMT_MSA.3 / Loader*),**
**Management of security attributes (*FMT_MSA.1 / Loader*),**
**Specification of management function (*FMT_SMF.1 / Loader*),**
**Security roles (*FMT_SMR.1 / Loader*),**
**Timing of identification (*FIA_UID.1 / Loader*),**
**Timing of authentication (*FIA_UAU.1 / Loader*)"**

400     These security requirements have already been argued in *Section : Security objective "Access control and authenticity for the Loader (BSI.O.Ctrl_Auth_Loader)"* and *Section : Security objectives "Protection of the confidentiality of the TSF (ANSSI.O.Prot-TSF-Confidentiality)", "Secure loading of the Additional Code (ANSSI.O.Secure-Load-ACode)" and "Secure loading of the Additional Memory Image (O.Secure-Load-AMemImage)"* above.

**"Audit storage (*FAU_SAS.1 / Loader*),**
**Audit review (*FAU_SAR.1 / Loader*)"**

401     These security requirements have already been argued in *Section : Security objective "Secure identification of the TOE (ANSSI.O.TOE-Identification)"* and *Section : Security objective "Secure identification of the Memory Image (O.MemImage-Identification)"* above.

**"Failure with preservation of secure state (*FPT_FLS.1 / Loader*)"**

402     This security requirement has already been argued in *Section : Security objective "Secure activation of the Additional Code (ANSSI.O.Secure-AC-Activation)"* and *Section : Security objective "Secure identification of the Memory Image (O.MemImage-Identification)"* above.

**"Inter-TSF trusted channel(*FTP_ITC.1 / Sdiag*),**
**Audit review (*FAU_SAR.1 / Sdiag*),**
**Limited capabilities (*FMT_LIM.1 / Sdiag*),**
**Limited availability (*FMT_LIM.2 / Sdiag*)**

403     These security requirements have already been argued in *Section : Security objective "Protection against Abuse of Functionality (BSI.O.Abuse-Func)"* above.

**"Security roles (*FMT_SMR.1 / M4M-DESFire*),
Subset access control  (*FDP_ACC.1 / M4M-DESFire*),
Security attribute based access control (*FDP_ACF.1 / M4M-DESFire*),
Static attribute initialisation (*FMT_MSA.3 / M4M-DESFire*),
Management of security attributes (*FMT_MSA.1 / M4M-DESFire*),
Specification of TSF data (*FMT_MTD.1 / M4M-DESFire*)
Specification of management function (*FMT_SMF.1 / M4M-DESFire*)
Import of user data with security attributes (*FDP_ITC.2 / M4M-DESFire*)
Cryptographic key destruction (*FCS_CKM.4 / M4M-DESFire*)"**

404        These security requirements have already been argued in *Section : Security objective "Secure activation of the Additional Code (ANSSI.O.Secure-AC-Activation)"* above.

**"User identification before any action (*FIA_UID.2 / M4M-DESFire*),
User authentication before any action (*FIA_UAU.2 / M4M-DESFire*),
Multiple authentication mechanisms (*FIA_UAU.5 / M4M-DESFire*)"**

405        These security requirements have already been argued in *Section : Security objective "Authentication for M4M-DESFire (O.Authentication-DESFire)"* above.

**"Trusted path (*FTP_TRP.1 / M4M-DESFire*),
Replay detection (*FPT_RPL.1 / M4M-DESFire*)"**

406        These security requirements have already been argued in *Section : Security objective "M4M-DESFire Confidential Communication (O.Confidentiality-DESFire)"* above.

**"Inter-TSF basic TSF data consistency (*FPT_TDC.1 / M4M-DESFire*)"**

407        This security requirement has already been argued in *Section : Security objective "M4M-DESFire Data type consistency (O.Type-Consistency-DESFire)"* above.

**"Basic rollback (*FDP_ROL.1 / M4M-DESFire*)"**

408        This security requirement has already been argued in *Section : Security objective "M4M-DESFire Transaction mechanism (O.Transaction-DESFire)"* above.

**"Unlinkability (*FPR_UNL.1 / M4M-DESFire*)"**

409        This security requirement has already been argued in *Section : Security objective "Preventing traceability for M4M-DESFire (O.No-Trace-DESFire)"* above.

**"Minimum and maximum quotas (*FRU_RSA.2 / M4M-DESFire*)"**

410        This security requirement has already been argued in *Section : Security objective "NVM resource availability for M4M-DESFire (O.Resource-DESFire)"* above.

**"Subset residual information protection (*FDP_RIP.1 / M4M-DESFire*)"**

411        This security requirement has already been argued in *Section : Security objective "M4M-DESFire data cleaning for resource sharing (O.Shr-Res-DESFire)"* above.

### 5.4.4 Dependencies of Security Functional Requirements

412 All dependencies of Security Functional Requirements have been fulfilled in this Security Target except :

- those justified in the *BSI-CC-PP-0084-2014* protection profile security requirements rationale,
- those justifed in *AUG* security requirements rationale,
- the dependency of *FCS_COP.1* and *FCS_CKM.1* on FCS_CKM.4 (see discussion below),
- the dependency of *FAU_SAR.1 / Loader* on FAU_GEN.1 (see discussion below),
- the dependency of *FAU_SAR.1 / Sdiag* on FAU_GEN.1 (see discussion below).

413 Details are provided in *Table 13* below.

**Table 13.    Dependencies of security functional requirements**

| Label | Dependencies | Fulfilled by security requirements in this Security Target | Dependency already in *BSI-CC-PP-0084-2014* or in *AUG* |
|---|---|---|---|
| FRU_FLT.2 | FPT_FLS.1 | Yes | Yes, *BSI-CC-PP-0084-2014* |
| FPT_FLS.1 | None | No dependency | Yes, *BSI-CC-PP-0084-2014* |
| FMT_LIM.1 / Test | FMT_LIM.2 / Test | Yes | Yes, *BSI-CC-PP-0084-2014* |
| FMT_LIM.2 / Test | FMT_LIM.1 / Test | Yes | Yes, *BSI-CC-PP-0084-2014* |
| FMT_LIM.1 / Loader | FMT_LIM.2 / Loader | Yes | Yes, *BSI-CC-PP-0084-2014* |
| FMT_LIM.2 / Loader | FMT_LIM.1 / Loader | Yes | Yes, *BSI-CC-PP-0084-2014* |
| FMT_LIM.1 / Sdiag | FMT_LIM.2 / Sdiag | Yes | Yes, *BSI-CC-PP-0084-2014* |
| FMT_LIM.2 / Sdiag | FMT_LIM.1 / Sdiag | Yes | Yes, *BSI-CC-PP-0084-2014* |
| FAU_SAS.1 | None | No dependency | Yes, *BSI-CC-PP-0084-2014* |
| FDP_SDC.1 | None | No dependency | Yes, *BSI-CC-PP-0084-2014* |
| FDP_SDI.2 | None | No dependency | Yes, *BSI-CC-PP-0084-2014* |
| FPT_PHP.3 | None | No dependency | Yes, *BSI-CC-PP-0084-2014* |
| FDP_ITT.1 | FDP_ACC.1 or FDP_IFC.1 | Yes | Yes, *BSI-CC-PP-0084-2014* |
| FPT_ITT.1 | None | No dependency | Yes, *BSI-CC-PP-0084-2014* |
| FDP_IFC.1 | FDP_IFF.1 | No, see *BSI-CC-PP-0084-2014* | Yes, *BSI-CC-PP-0084-2014* |
| FCS_RNG.1 | None | No dependency | Yes, *BSI-CC-PP-0084-2014* |

**Table 13.     Dependencies of security functional requirements (continued)**

| Label | Dependencies | Fulfilled by security requirements in this Security Target | Dependency already in *BSI-CC-PP-0084-2014* or in *AUG* |
|---|---|---|---|
| FCS_COP.1 | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | Yes, by FCS_CKM.1, see also discussion below | Yes, *AUG #1* |
| | FCS_CKM.4 | No, see discussion below | |
| FCS_CKM.1 | [FDP_CKM.2 or FCS_COP.1] | Yes, by FCS_COP.1 | |
| | FCS_CKM.4 | No, see discussion below | |
| FDP_ACC.2 / Memories | FDP_ACF.1 / Memories | Yes | ***No, CCMB-2017-04-002*** |
| FDP_ACF.1 / Memories | FDP_ACC.1 / Memories | Yes, by FDP_ACC.2 / Memories | Yes, *AUG #4* |
| | FMT_MSA.3 / Memories | Yes | |
| FMT_MSA.3 / Memories | FMT_MSA.1 / Memories | Yes | Yes, *AUG #4* |
| | FMT_SMR.1 / Memories | No, see *AUG #4* | |
| FMT_MSA.1 / Memories | [FDP_ACC.1 / Memories or FDP_IFC.1] | Yes, by FDP_ACC.2 / Memories and FDP_IFC.1 | Yes, *AUG #4* |
| | FMT_SMF.1 / Memories | Yes | ***No, CCMB-2017-04-002*** |
| | FMT_SMR.1 / Memories | No, see *AUG #4* | Yes, *AUG #4* |
| FMT_SMF.1 / Memories | None | No dependency | ***No, CCMB-2017-04-002*** |
| FIA_API.1 | None | No dependency | Yes, *BSI-CC-PP-0084-2014* |
| FTP_ITC.1 / Loader | None | No dependency | Yes, *BSI-CC-PP-0084-2014* |
| FDP_UCT.1 / Loader | [FTP_ITC.1 / Loader or FTP_TRP.1 / Loader] | Yes, by FTP_ITC.1 / Loader | Yes, *BSI-CC-PP-0084-2014* |
| | [FDP_ACC.1 / Loader or FDP_IFC.1 / Loader] | Yes, by FDP_ACC.1 / Loader | |

**Table 13.     Dependencies of security functional requirements (continued)**

| Label | Dependencies | Fulfilled by security requirements in this Security Target | Dependency already in *BSI-CC-PP-0084-2014* or in *AUG* |
|---|---|---|---|
| FDP_UIT.1 / Loader | [FTP_ITC.1 / Loader or FTP_TRP.1 / Loader] | Yes, by FTP_ITC.1 / Loader | Yes, *BSI-CC-PP-0084-2014* |
| | [FDP_ACC.1 / Loader or FDP_IFC.1 / Loader] | Yes, by FDP_ACC.1 / Loader | |
| FDP_ACC.1 / Loader | FDP_ACF.1 / Loader | Yes | Yes, *BSI-CC-PP-0084-2014* |
| FDP_ACF.1 / Loader | FDP_ACC.1 / Loader | Yes | Yes, *BSI-CC-PP-0084-2014* |
| | FMT_MSA.3 / Loader | Yes | |
| FMT_MSA.3 / Loader | FMT_MSA.1 / Loader | Yes | **No,** *CCMB-2017-04-002* |
| | FMT_SMR.1 / Loader | Yes | |
| FMT_MSA.1 / Loader | [FDP_ACC.1 / Loader or FDP_IFC.1] | Yes, by FDP_ACC.1 / Loader | **No,** *CCMB-2017-04-002* |
| | FDP_SMF.1 / Loader | Yes | |
| | FDP_SMR.1 / Loader | Yes | |
| FMT_SMR.1 / Loader | FIA_UID.1 / Loader | Yes | **No,** *CCMB-2017-04-002* |
| FIA_UID.1 / Loader | None | No dependency | **No,** *CCMB-2017-04-002* |
| FIA_UAU.1 / Loader | FIA_UID.1 / Loader | Yes | **No,** *CCMB-2017-04-002* |
| FDP_SMF.1 / Loader | None | No dependency | **No,** *CCMB-2017-04-002* |
| FPT_FLS.1 / Loader | None | No dependency | **No,** *CCMB-2017-04-002* |
| FAU_SAS.1 / Loader | None | No dependency | Yes, *BSI-CC-PP-0084-2014* |
| FAU_SAR.1 / Loader | FAU_GEN.1 | No, by FAU_SAS.1 / Loader instead, see discussion below | **No,** *CCMB-2017-04-002* |
| FTP_ITC.1 / Sdiag | None | No dependency | **No,** *CCMB-2017-04-002* |
| FAU_SAR.1 / Sdiag | FAU_GEN.1 | No, see discussion below | **No,** *CCMB-2017-04-002* |

**Table 13.     Dependencies of security functional requirements (continued)**

| Label | Dependencies | Fulfilled by security requirements in this Security Target | Dependency already in *BSI-CC-PP-0084-2014* or in *AUG* |
|---|---|---|---|
| FMT_SMR.1 / M4M-DESFire | FIA_UID.1 / M4M-DESFire | Yes, by FIA_UID.2 / M4M-DESFire | ***No,*** *CCMB-2017-04-002* |
| FDP_ACC.1 / M4M-DESFire | FDP_ACF.1 / M4M-DESFire | Yes | ***No,*** *CCMB-2017-04-002* |
| FDP_ACF.1 / M4M-DESFire | FDP_ACC.1 / M4M-DESFire | Yes | ***No,*** *CCMB-2017-04-002* |
| | FMT_MSA.3 / M4M-DESFire | Yes | |
| FMT_MSA.3 / M4M-DESFire | FMT_MSA.1 / M4M-DESFire | Yes | ***No,*** *CCMB-2017-04-002* |
| | FMT_SMR.1 / M4M-DESFire | Yes | |
| FMT_MSA.1 / M4M-DESFire | [FDP_ACC.1 / M4M-DESFire or FDP_IFC.1] | Yes, by FDP_ACC.1 / M4M-DESFire | ***No,*** *CCMB-2017-04-002* |
| | FMT_SMF.1 / M4M-DESFire | Yes | |
| | FMT_SMR.1 / M4M-DESFire | Yes | |
| FMT_SMF.1 / M4M-DESFire | None | No dependency | ***No,*** *CCMB-2017-04-002* |
| FDP_ITC.2 / M4M-DESFire | [FDP_ACC.1 / M4M-DESFire or FDP_IFC.1] | Yes, by FDP_ACC.1 / M4M-DESFire | ***No,*** *CCMB-2017-04-002* |
| | [FTP_ITC.1 or FPT_TRP.1 / M4M-DESFire] | Yes, by FPT_TRP.1 / M4M-DESFire | |
| | FPT_TDC.1 / M4M-DESFire | Yes | |
| FPT_TDC.1 / M4M-DESFire | None | No dependency | ***No,*** *CCMB-2017-04-002* |
| FIA_UID.2 / M4M-DESFire | None | No dependency | ***No,*** *CCMB-2017-04-002* |
| FIA_UAU.2 / M4M-DESFire | FIA_UID.1 | Yes, by FIA_UID.2 / M4M-DESFire | ***No,*** *CCMB-2017-04-002* |
| FIA_UAU.5 / M4M-DESFire | None | No dependency | ***No,*** *CCMB-2017-04-002* |

**Table 13. Dependencies of security functional requirements (continued)**

| Label | Dependencies | Fulfilled by security requirements in this Security Target | Dependency already in *BSI-CC-PP-0084-2014* or in *AUG* |
|---|---|---|---|
| FMT_MTD.1 / M4M-DESFire | FMT_SMR.1 / M4M-DESFire | Yes | ***No,** CCMB-2017-04-002* |
| | FMT_SMF.1 / M4M-DESFire | Yes | |
| FPT_TRP.1 / M4M-DESFire | None | No dependency | ***No,** CCMB-2017-04-002* |
| FCS_CKM.4 / M4M-DESFire | [FDP_ITC.1 or FDP_ITC.2 / M4M-DESFire or FCS_CKM.1] | Yes, by FDP_ITC.2 / M4M-DESFire | ***No,** CCMB-2017-04-002* |
| FDP_ROL.1 / M4M-DESFire | [FDP_ACC.1 / M4M-DESFire or FDP_IFC.1] | Yes, by FDP_ACC.1 / M4M-DESFire | ***No,** CCMB-2017-04-002* |
| FPT_RPL.1 / M4M-DESFire | None | No dependency | ***No,** CCMB-2017-04-002* |
| FPR_UNL.1 / M4M-DESFire | None | No dependency | ***No,** CCMB-2017-04-002* |
| FRU_RSA.2 / M4M-DESFire | None | No dependency | ***No,** CCMB-2017-04-002* |
| FDP_RIP.1 / M4M-DESFire | None | No dependency | ***No,** CCMB-2017-04-002* |

414      Part 2 of the Common Criteria defines the dependency of "*Cryptographic operation (FCS_COP.1)*" on "Import of user data without security attributes (FDP_ITC.1)" or "Import of user data with security attributes (FDP_ITC.2)" or "Cryptographic key generation (FCS_CKM.1)". In this particular TOE, "*Cryptographic key generation (FCS_CKM.1)*" may be used for the purpose of creating cryptographic keys, but also, the ES has all possibilities to implement its own creation function, in conformance with its security policy.

415      Part 2 of the Common Criteria defines the dependency of "*Cryptographic operation (FCS_COP.1)*" and "*Cryptographic key generation (FCS_CKM.1)*" on "Cryptographic key destruction (FCS_CKM.4)". In this particular TOE, there is no specific function for the destruction of the keys. The ES has all possibilities to implement its own destruction function, in conformance with its security policy. Therefore, FCS_CKM.4 is not defined in this ST.

416      Part 2 of the Common Criteria defines the dependency of "*Audit review (FAU_SAR.1) / Loader*" on "Audit data generation (FAU_GEN.1)". In this particular TOE, "*Audit storage (FAU_SAS.1) / Loader*" is used to ensure the storage of audit data, because FAU_GEN.1 is too comprehensive to be used in this context. Therefore this dependency is fulfilled by "*Audit storage (FAU_SAS.1) / Loader*" instead.

417      Part 2 of the Common Criteria defines the dependency of "*Audit review (FAU_SAR.1) / Sdiag*" on "Audit data generation (FAU_GEN.1)". In this particular TOE, there is no specific

function for audit data generation, the data to be audited are just stored. Therefore, FAU_GEN.1 is not defined in this ST.

## 5.4.5      Rationale for the Assurance Requirements

### Security assurance requirements added to reach EAL5 (*Table 10*)

418      Regarding application note 21 of *BSI-CC-PP-0084-2014*, this Security Target chooses EAL5 because developers and users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

419      EAL5 represents a meaningful increase in assurance from EAL4 by requiring semiformal design descriptions, a more structured (and hence analyzable) architecture, extensive testing, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered during development.

420      The assurance components in an evaluation assurance level (EAL) are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL5. Therefore, these components add additional assurance to EAL5, but the mutual support of the requirements and the internal consistency is still guaranteed.

421      Note that detailed and updated refinements for assurance requirements are given in *Section 5.3*.

### Dependencies of assurance requirements

422      Dependencies of security assurance requirements are fulfilled by the EAL5 package selection.

423      The augmentation to this package identified in paragraph *324* does not introduce dependencies not already satisfied by the EAL5 package, and is considered as consistent augmentation:

- ALC_FLR.1 has no dependency.
- ASE_TSS.2 dependencies (ASE_INT.1, ASE_REQ.1 and ADV_ARC.1) are fulfilled by the assurance requirements claimed by this ST.

# 6  TOE summary specification (ASE_TSS)

424     This section demonstrates how the TOE meets each Security Functional Requirement, which will be further detailed in the ADV_FSP documents.

## 6.1  Limited fault tolerance (FRU_FLT.2)

425     The TSF provides limited fault tolerance, by managing a certain number of faults or errors that may happen, related to random number generation, power supply, data flows and cryptographic operations, thus preventing risk of malfunction.

## 6.2  Failure with preservation of secure state (FPT_FLS.1)

426     The TSF provides preservation of secure state by detecting and managing the following events, resulting in an immediate interruption or reset:

- Die integrity violation detection,
- Errors on memories and registers,
- Glitches,
- High voltage supply,
- CPU errors,
- MMU errors,
- Faults on crypto processors or libraries.

427     The ES can generate a software reset.

## 6.3  Limited capabilities (FMT_LIM.1) / Test, Limited capabilities (FMT_LIM.1) / Sdiag, Limited capabilities (FMT_LIM.1) / Loader, Limited availability (FMT_LIM.2) / Test, Limited availability (FMT_LIM.2) / Sdiag & Limited availability (FMT_LIM.2) / Loader

428     The TOE is either in Test, Admin or User configuration.

429     The TOE may also be in Basic Diagnostic (aka Diagnostic), Secure Diagnostic or Genuine Check volatile configuration.

430     The Test and Diagnostics configurations are reserved to ST.

431     The TSF ensures the switching and the control of TOE configuration, the corresponding access control and the control of the corresponding capabilities.The transition controls rely on several strong mechanisms including fuse, authentication and control registers. Part of the transitions are only possible in the STMicroelectronics audited environment.

432     The TSF reduces the available features depending on the TOE configuration.

433     The customer can choose to disable irreversibly the Loading capability.

434 The customer can choose to irreversibly enable or disable the Secure Diagnostic capability. Only if the customer enables it, for quality investigation purpose, ST can exercise the Secure Diagnostic capability with a secure protocol, in an audited environment.

## 6.4 Inter-TSF trusted channel (FTP_ITC.1) / Sdiag

435 In Secure Diagnostic volatile configuration, the System Firmware provides a secure channel to allow another IT product to operate a Secure Diagnostic transaction.

## 6.5 Audit review (FAU_SAR.1) / Sdiag

436 The System Firmware allows to read the Secure Diagnostic status (permanently disabled, permanently enabled, disabled but still configurable).

## 6.6 Stored data confidentiality (FDP_SDC.1)

437 The TSF ensures confidentiality of the User Data, thanks to the following features:
- Memories scrambling and encryption,
- Protection of NVM sectors,
- MMU,
- LPU.

## 6.7 Stored data integrity monitoring and action (FDP_SDI.2)

438 The TSF ensures integrity of the stored data, thanks to the following features:
- Memories parity control,
- Protection of NVM sectors,
- MMU,
- LPU.

## 6.8 Audit storage (FAU_SAS.1)

439 In User configuration, the TOE provides commands to store data and/or pre-personalisation data and/or supplements of the ES in the NVM. These commands are only available to authorized processes before delivery.

## 6.9 Resistance to physical attack (FPT_PHP.3)

440 The TSF ensures resistance to physical tampering, thanks to the following features:
- The TOE implements a set of countermeasures that reduce the exploitability of physical probing.
- The TOE is physically protected by active shields that command an automatic reaction on die integrity violation detection.

## 6.10 Basic internal transfer protection (FDP_ITT.1), Basic internal TSF data transfer protection (FPT_ITT.1) & Subset information flow control (FDP_IFC.1)

441     The TSF prevents the disclosure of internal and user data thanks to:

- Memories scrambling and encryption,
- Bus encryption,
- Mechanisms for operation execution concealment,
- Leakage protection in libraries.

## 6.11 Random number generation (FCS_RNG.1)

442     The TSF provides 8-bit true random numbers that can be qualified with the test metrics required by the *BSI-AIS20/AIS31* standard for a PTG.2 class device.

## 6.12 Cryptographic operation: DES operation (FCS_COP.1) / TDES if EDES+

443     The TOE provides optionally an EDES+ accelerator that has the capability to perform Triple DES encryption and decryption in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode conformant to *NIST SP 800-67* and *NIST SP 800-38A*.

If NesLib is embedded, the cryptographic library NesLib instantiates the same standard DES cryptographic operations, in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode.

444     The M4M-DESFire library uses Triple DES as cryptographic operation (EDES+ accelerator). Cryptographic operations are used for setting up the mutual authentication, for encryption and message authentication.

## 6.13 Cryptographic operation: AES operation (FCS_COP.1) / AES if HW_AES

445     The TOE provides optionally an AES accelerator allowing the following standard AES cryptographic operations for key sizes of 128, 192 and 256 bits, conformant to *FIPS PUB 197* with intrinsic counter-measures against attacks:

- cipher,
- inverse cipher.

446     The AES accelerator can operate in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode.

447      If NesLib is embedded, the cryptographic library NesLib instantiates the same standard AES cryptographic operations, in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode, and additionally provides:

- message authentication Code computation (CMAC),
- authenticated encryption/decryption in Galois Counter Mode (GCM),
- authenticated encryption/decryption in Counter with CBC-MAC (CCM).

448      The M4M-DESFire library uses AES as cryptographic operation (AES accelerator). Cryptographic operations are used for setting up the mutual authentication, for encryption and message authentication.

## 6.14 Cryptographic operation: RSA operation (FCS_COP.1) / RSA if NesLib

449      The cryptographic library NesLib provides to the ES developer the following RSA functions, all conformant to *PKCS #1 V2.1*:

- RSA public key cryptographic operation for modulus sizes from 1024 to 4096 bits,
- RSA private key cryptographic operation with or without CRT for modulus sizes from 1024 to 4096 bits,
- RSA signature formatting,
- RSA Key Encapsulation Method.

## 6.15 Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1) / ECC if NesLib

450      The cryptographic library NesLib provides to the ES developer the following efficient basic functions for Elliptic Curves Cryptography over prime fields, all conformant to *IEEE 1363-2000* and *IEEE 1363a-2004*, including:

- private scalar multiplication,
- preparation of Elliptic Curve computations in affine coordinates,
- public scalar multiplication,
- point validity check,
- Jacobian conversion to affine coordinates,
- general point addition,
- point expansion and compression.

451      Additionally, the cryptographic library NesLib provides functions dedicated to the two most used elliptic curves cryptosystems:

- Elliptic Curve Diffie-Hellman (ECDH), as specified in *NIST SP 800-56A*,
- Elliptic Curve Digital Signature Algorithm (ECDSA) generation and verification, as stipulated in *FIPS PUB 186-4* and specified in *ANSI X9.62,* section 7.

452    The cryptographic library NesLib provides to the ES developer the following efficient basic functions for Elliptic Curves Cryptography over prime fields on curves in Edwards form, with curve 25519, all conformant to *EdDSA rfc*, including:

- generation,
- verification,
- point decompression.

## 6.16    Cryptographic operation: SHA-1 & SHA-2 operation (FCS_COP.1) / SHA, if NesLib

453    The cryptographic library NesLib provides the SHA-1[f], SHA-224, SHA-256, SHA-384, SHA-512 secure hash functions conformant to *FIPS PUB 180-2*.

454    The cryptographic library NesLib provides the SHA-1[e],SHA-256, SHA-384, SHA-512 secure hash functions conformant to *FIPS PUB 180-2*, and offering resistance against side channel and fault attacks.

455    Additionally, the cryptographic library NesLib offers support for the HMAC mode of use, as specified in *FIPS PUB 198-1*, to be used in conjunction with the protected versions of SHA-1[e] and SHA-256.

## 6.17    Cryptographic operation: Keccak & SHA-3 operation (FCS_COP.1) / Keccak, if NesLib

456    The cryptographic library NesLib provides the operation of the following extendable output functions conformant to *FIPS PUB 202*:

- SHAKE128,
- SHAKE256,
- Keccak[r,c] with choice of r < 1600 and c = 1600 - r.

457    The cryptographic library NesLib provides the operation of the following hash functions, conformant to *FIPS PUB 202*:

- SHA3-224,
- SHA3-256,
- SHA3-384,
- SHA3-512.

458    The cryptographic library NesLib provides the operation of the following extendable output functions conformant to *FIPS PUB 202*, offering resistance against side channel and fault attacks:

- SHAKE128,
- SHAKE256,
- Keccak[r,c] with choice of r < 1600 and c = 1600 - r.

---

f.    Note that SHA-1 is no longer recommended as a cryptographic function in the context of smart card applications. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.

459    The cryptographic library NesLib provides the operation of the following hash functions, conformant to *FIPS PUB 202*, offering resistance against side channel and fault attacks:

- SHA3-224,
- SHA3-256,
- SHA3-384,
- SHA3-512.

## 6.18 Cryptographic operation: Keccak-p operation (FCS_COP.1) / Keccak-p, if NesLib

460    The cryptographic library NesLib provides a toolbox for building modes on top of the following permutations, conformant to *FIPS PUB 202*:

- Keccak-p[1600,n_r = 24],
- Keccak-p[1600,n_r = 12].

461    The cryptographic library NesLib provides a toolbox for building modes on top of the following permutations, conformant to *FIPS PUB 202,* offering resistance against side channel and fault attacks:

- Keccak-p[1600,n_r = 24],
- Keccak-p[1600,n_r = 12].

## 6.19 Cryptographic operation: Diffie-Hellman operation (FCS_COP.1) / Diffie-Hellman, if NesLib

462    The cryptographic library NesLib provides the Diffie-Hellman key establishment operation over GF(p) for size of modulus p up to 4096 bits, conformant to *ANSI X9.42*.

## 6.20 Cryptographic operation: DRBG operation (FCS_COP.1) / DRBG, if NesLib

463    The cryptographic library NesLib gives support for a DRBG generator, based on cryptographic algorithms specified in *NIST SP 800-90*.

464    The cryptographic library NesLib implements two of the DRBG specified in *NIST SP 800-90*:

- Hash-DRBG,
- CTR-DRBG.

## 6.21 Cryptographic key generation: Prime generation (FCS_CKM.1) / Prime-generation, if NesLib

465    The cryptographic library NesLib provides prime numbers generation for prime sizes up to 2048 bits conformant to *FIPS PUB 140-2* and *FIPS PUB 186-4*, optionally with conditions and/or optionally offering resistance against side channel and fault attacks*.*

## 6.22 Cryptographic key generation: RSA key generation (FCS_CKM.1) / RSA-key-generation, if NesLib

466    The cryptographic library NesLib provides standard RSA public and private key computation for key sizes from 1024 to 4096 bits conformant to *FIPS PUB 140-2, ISO/IEC 9796-2* and *PKCS #1 V2.1*, optionally with conditions and/or optionally offering resistance against side channel and fault attacks.

## 6.23 Static attribute initialisation (FMT_MSA.3) / Memories

467    The TOE enforces a default memory management policy when none other is programmed by the ES.
Additionally, at product start all the LPU static attributes are initialised, allowing to protect the segments where M4M-DESFire code and data are stored, if M4M-DESFire is part of the TOE.

## 6.24 Management of security attributes (FMT_MSA.1) / Memories & Specification of management functions (FMT_SMF.1) / Memories

468    The TOE provides a dynamic Memory Management Unit (MMU), that can be configured by the ES.

469    Other complementary memory protections are also available to the ES (LPU, NVM sector protection, limitation in unprivileged mode).

## 6.25 Complete access control (FDP_ACC.2) / Memories & Security attribute based access control (FDP_ACF.1) / Memories

470    The TOE enforces the dynamic memory management policy for data access and code access thanks to a dynamic Memory Management Unit (MMU), a Library Protection Unit (LPU), and complementary protection mechanisms, programmed by the ES.
In case M4M-DESFire is present, the Library Protection Unit is reserved to ST usage to isolate the M4M-DESFire firmware (code and data) from the rest of the code embedded in the device.

471    Overriding the MMU and LPU set of access rights, depending on the TOE configuration, the TOE enforces additional protections on specific parts of the memories.

## 6.26 Authentication Proof of Identity (FIA_API.1)

472    In Admin configuration or Genuine check configuration, the System Firmware provides commands based on a cryptographic mechanism which allows another IT product to check that the TOE is a genuine TOE.

## 6.27 Inter-TSF trusted channel (FTP_ITC.1) / Loader, Basic data exchange confidentiality (FDP_UCT.1) / Loader, Data exchange integrity (FDP_UIT.1) / Loader & Audit storage (FAU_SAS.1) / Loader

473    In Admin configuration, the System Firmware provides a secure channel to allow another IT product to operate a maintenance transaction.

474    The ciphered data is automatically decrypted then stored in the requested memory.

475    A maintenance transaction can end only after a successful integrity check of the loaded data or an erase. The identification data associated with the memory update is automatically logged during the session,

## 6.28 Subset access control (FDP_ACC.1) / Loader & Security attribute based access control (FDP_ACF.1) / Loader

476    In Admin configuration, during a maintenance transaction, the System Firmware verifies if the Loader access conditions are satisfied and returns an error when this is not the case.

477    In particular, the additional memory update must be intended to be assembled with the memory update previously loaded.

## 6.29 Failure with preservation of secure state (FPT_FLS.1) / Loader

478    In Admin configuration, the System Firmware enforces that a maintenance transaction can only end when it is consistent or canceled by an erase.

## 6.30 Static attribute initialisation (FMT_MSA.3) / Loader

479    In Admin configuration, the System Firmware provides restrictive default values for the Flash Loader security attributes.

## 6.31 Management of security attributes (FMT_MSA.1) / Loader & Specification of management functions (FMT_SMF.1) / Loader

480    In Admin configuration, the System Firmware provides the capability for an authorized user to change part of the Flash Loader security attributes.

## 6.32 Security roles (FMT_SMR.1) / Loader

481    The System Firmware supports the assignment of roles to users through the assignment of different keys for the different roles. This allows to distinguish between the roles of ST Loader, User Loader, Delegated Loader, Secure Diagnostic, and Everybody.

## 6.33    Timing of identification (FIA_UID.1) / Loader & Timing of authentication (FIA_UAU.1) / Loader

482    The System Firmware identifies the user through the key selected for authentication. This is performed by verifying an encryption, thus preventing to unveil the key.

483    After this authentication, both parties share a session key.

484    A limited number of operations is allowed on behalf of the user before the user is identified and authenticated, such as boot, authentication and non-critical queries.

## 6.34    Audit review (FAU_SAR.1) / Loader

485    In Admin configuration, the System Firmware allows to read the product information and the identification data of all memory updates previously loaded on the TOE.

## 6.35    Security roles (FMT_SMR.1) / M4M-DESFire

486    M4M-DESFire supports the assignment of roles to users through the assignment of different keys for the different roles and through the structure and configuration of the access rights. This allows to distinguish between the roles of VC Administrator, VC Manager, Application Manager, Application User, and Everybody.

## 6.36    Subset access control (FDP_ACC.1) / M4M-DESFire

487    For each M4M-DESFire command subject to access control, the M4M-DESFire library verifies if the M4M-DESFire access conditions are satisfied and returns an error when this is not the case.

## 6.37    Security attribute based access control (FDP_ACF.1) / M4M-DESFire

488    The M4M-DESFire library verifies the M4M-DESFire security attributes during the execution of M4M-DESFire commands to enforce the Access Control Policy defined by the M4M-DESFire interface specification.

489    On Virtual Card level, the security attributes define:

- if change of card configuration is allowed,
- if administrator master authentication is required for create/delete applications,
- if change of card master key is allowed,
- the type of master key used: Single DES, 2 Key Triple DES, 3 Key Triple DES or AES.[g]
- if format card is allowed,
- if random UID is enabled.

---

g.   Note that DES is no longer recommended as an encryption function in the context of smart card applications. Hence, Security IC Embedded Software may need to use triple DES to achieve a suitable strength.

490    On Application level, the security attributes define:

- the key identifier and the conditions for changing the application manager key,
- if change of application configuration is allowed,
- if application manager authentication is required for create/delete applications,
- if application manager authentication is required for directory access,
- if change of application manager key is allowed,
- the type of application key used: Single DES, 2 Key Triple DES, 3 Key Triple DES or AES.[f]

491    On File level, the security attributes define:

- the type of file:
- standard data file (without rollback),
- value file (with rollback),
- backup data file (with rollback),
- linear record file (with rollback),
- cyclic record file (with rollback),
- the communication settings: plain, with MACing or enciphered,
- the Application user identifier or Nobody or Everybody,
- the type of master key used: Single DES, 2 Key Triple DES, 3 Key Triple DES or AES.[f]

492    On Value file level, the security attributes define:

- the lower limit,
- the upper limit,
- the limited credit limit,
- if the limited credit is enabled.

## 6.38    Static attribute initialisation (FMT_MSA.3) / M4M-DESFire

493    The M4M-DESFire library initialises all the static attributes to the values defined by M4M-DESFire interface specifications before they can be used by the Embedded Software.

## 6.39    Management of security attributes (FMT_MSA.1) / M4M-DESFire

494    The M4M-DESFire library verifies the M4M-DESFire security attributes during the execution of M4M-DESFire commands to enforce the Access Control Policy on the security attributes.

## 6.40    Specification of Management Functions (FMT_SMF.1) / M4M-DESFire

495    The M4M-DESFire library implements the management functions defined by the M4M-DESFire interface specifications for authentication, changing security attributes and creating or deleting a virtual card, an application, a value or a data file.

## 6.41 Import of user data with security attributes (FDP_ITC.2) / M4M-DESFire

496    The M4M-DESFire library implements the M4M-DESFire interface specifications and enforces the Access Control Policy to associate the user data to the security attributes.

## 6.42 Inter-TSF basic TSF data consistency (FPT_TDC.1) / M4M-DESFire

497    The M4M-DESFire library implements the M4M-DESFire interface specifications, supporting consistent interpretation and modification control of inter-TSF exchanges.

## 6.43 Cryptographic key destruction (FCS_CKM.4) / M4M-DESFire

498    The M4M-DESFire library erases key values from memory after their context becomes obsolete.

## 6.44 User identification before any action (FIA_UID.2) / M4M-DESFire

499    The M4M-DESFire library identifies the user through the key selected for authentication as specified by the M4M-DESFire Interface Specification.

## 6.45 User authentication before any action (FIA_UAU.2) / M4M-DESFire

500    During the authentication, the M4M-DESFire library verifies that the user knows the selected key. This is performed by verifying an encryption, thus preventing to unveil the key.

501    After this authentication, both parties share a session key.

## 6.46 Multiple authentication mechanisms (FIA_UAU.5) / M4M-DESFire

502    The M4M-DESFire library implements the M4M-DESFire Interface Specification, that has a mechanism to authenticate VC Administrator, VC Manager, Application Manager and Application User, while Everybody is assumed when there is no valid authentication state.

503    Two types of authentication are supported: the native M4M-DESFire 3-pass authentication and the ISO authentication.

## 6.47 Management of TSF data (FMT_MTD.1) / M4M-DESFire

504    The M4M-DESFire library implements the M4M-DESFire Interface Specification, restricting key modifications in ways configurable through the security attributes to authenticated users, or disabling key modification capabilities.

## 6.48    Trusted path (FTP_TRP.1) / M4M-DESFire

505    The M4M-DESFire library implements the M4M-DESFire Interface Specification allowing to establish and enforce a trusted path between itself and remote users.

## 6.49    Basic rollback (FDP_ROL.1) / M4M-DESFire

506    The M4M-DESFire library implements the M4M-DESFire transaction mechanism ensuring that either all or none of the (modifying) file commands within a transaction are performed. If not, they are rolled back.

## 6.50    Replay detection (FPT_RPL.1) / M4M-DESFire

507    The M4M-DESFire library implements the M4M-DESFire authentication command, and authenticated commands, that allow replay detection.

## 6.51    Unlinkability (FPR_UNL.1) / M4M-DESFire

508    M4M-DESFire provides an Administrator option to use random UID during the ISO 14443 anti-collision sequence, preventing the traceability through UID. At higher level, the M4M-DESFire access control - when configured for this purpose - provides traceability protection.

## 6.52    Minimum and maximum quotas (FRU_RSA.2) / M4M-DESFire

509    The M4M-DESFire library ensures the memory required for its operation is available.

## 6.53    Subset residual information protection (FDP_RIP.1) / M4M-DESFire

510    At the end of commands execution or upon interrupt, the M4M-DESFire library cleans the confidential data from registers it uses.

# 7      Identification

**Table 14.    TOE components**

| IC Maskset name | Master identification number [1] | IC version | Firmware version | Optional NesLib crypto library version | Optional MIFARE4Mobile version |
|---|---|---|---|---|---|
| K500A | 0137h | H | 3.2.5 and 3.3.0 | 6.3.4 | 2.2.9 and 2.2.10 |
|  |  | I | 3.3.0 |  |  |

1. Part of the product information.

**Table 15.    Guidance documentation**

| Component description | Reference | Version |
|---|---|---|
| ST33J2M0 datasheet: Secure MCU with 32-bit SecurCore SC300 CPU with SWP, ISO, SPI, I2C & Flash | DS_ST33J2M0 | 9 |
| ST33J Secure MCU platforms Security Guidance | AN_SECU_ST33J | 10 |
| ARM® SC300 r0p1 Technical Reference Manual | ARM_DDI_0447 | A |
| ARM® Cortex M3 r2p0 Technical Reference Manual | ARM DDI 0337F3c | F3c |
| ARM® SecurCore SC300 Errata | PR326-PRDC-009983 | 11 |
| ST33J2M0 firmware V3 User manual | UM_ST33J2M0_FWv3 | 20 |
| ST33J platform - AIS31 compliant random number - User manual | UM_ST33J_AIS31 | 1 |
| ST33J platform - AIS Reference implementation: Startup, on-line and total failure tests - AN | AN_ST33J_AIS1 | 1 |
| NesLib cryptographic library NesLib 6.3 - User manual | UM_NesLib_6.3 | 4 |
| ST33J secure MCU platforms NesLib 6.3 security recommendations - Application note | AN_SECU_ST33J_NESLIB_6.3 | 5 |
| NesLib 6.3.4 for ST33 Lockstep platforms – Release note | RN_ST33J_NESLIB_6.3.4 | 4 |
| MIFARE4Mobile® library 2.2 for the ST33J platform - User manual | UM_33J_MIFARE4MOBILE-2.2 | 4 |
| MIFARE4Mobile® library 2.2.9 for the ST33J platform - Application note | AN_ST33J_M4M_Lib | 1 |
| MIFARE4Mobile® library 2.2.10 for the ST33J platform - Application note | AN_ST33J_M4M_Lib | 2 |

**Table 16. Sites list**

| Site | Address | Activities[1] |
|------|---------|---------------|
| ST Rousset | STMicroelectronics<br>190 Avenue Célestin Coq, ZI,<br>13106 Rousset Cedex<br>France | DEV<br>EWS<br>WHS |
| ST Crolles | STMicroelectronics<br>850 rue Jean Monnet<br>38926 Crolles<br>France | DEV<br>FE<br>MASK |
| ST AMK1 | STMicroelectronics<br>5A Serangoon North Avenue 5<br>Singapore 554574 | DEV |
| ST Zaventem | STMicroelectronics<br>Green Square, Lambroekstraat 5, Building B 3d floor<br>1831 Diegem/Machelen<br>Belgium | DEV |
| ST Grenoble | STMicroelectronics<br>12 rue Jules Horowitz, BP 217<br>38019 Grenoble Cedex<br>France | DEV |
| ST Ljubljana | STMicroelectronics d.o.o. Ljubljana<br>Tehnoloski park 21,<br>1000 Ljubljana,<br>Slovenia | DEV |
| ST Rennes | STMicroelectronics<br>10 rue de Jouanet, ePark<br>35700 Rennes<br>France | DEV |
| ST Sophia | STMicroelectronics<br>Sky Sophia, Bât B, 776 Rue Albert Caquot,<br>06410 Biot,<br>France | DEV |
| ST Gardanne | CMP Georges Charpak<br>880 Avenue de Mimet<br>13541 Gardanne<br>France | BE |

**Table 16. Sites list (continued)**

| Site | Address | Activities[1] |
|---|---|---|
| ST Toa Payoh | STMicroelectronics<br>629 Lorong 4/6 Toa Payoh<br>319521 Singapore<br>Singapore | EWS |
| STS Shenzhen | STS Microelectronics<br>16 Tao hua Rd.<br>Futian free trade zone<br>518038 Shenzhen<br>P.R. China | BE |
| ST Bouskoura | STMicroelectronics<br>101 Boulevard des Muriers – BP97<br>20180 Bouskoura<br>Maroc | BE<br>WHS |
| ST Calamba | STMicroelectronics<br>9 Mountain Drive, LISP II, Brgy La mesa<br>Calamba<br>4027 Philippines | BE<br>WHS |
| ST Loyang | STMicroelectronics<br>7 Loyang Drive<br>508938 Singapore | WHS |
| ST AMK6 | STMicroelectronics<br>18 Ang Mo Kio Industrial park 2<br>569505 Singapore | WHS |
| ST Tunis | STMicroelectronics<br>Elgazala Technopark, Raoued, Gouvernorat de l'Ariana,<br>PB21, 2088 cedex, Ariana,<br>Tunisia | IT |
| AMKOR ATP3/4 | AMKOR Technology<br>ATP3/4: 119 N. Science Avenue,<br>Laguna Technopark, Binan, Laguna,<br>4024 Philippines | BE |
| AMKOR ATP1 | AMKOR Technology<br>ATP1: Km 22 East Service Rd.,<br>South Superhighway, Muntipula City<br>1771 Philippines | BE |

**Table 16.    Sites list  (continued)**

| Site | Address | Activities[1] |
|---|---|---|
| AMKOR ATT1 | AMKOR Technology Taiwan, Inc.<br>T1: N°1, Kao-Ping Sec, Chung-Feng Rd,<br>Lungtan Township, Taoyuan County,<br>Taiwan, R.O.C. | BE |
| AMKOR ATT3 | AMKOR Technology Taiwan, Inc.<br>T3: 11 Guangfu Road, Hsinchu Industrial Park<br>Hukou County, HSINCHU 303<br>Taiwan, R.O.C. | BE |
| AMKOR ATT6 | AMKOR Technology Taiwan, Inc.<br>T6: No. 333, Longyuan 1st Rd., Hsinchu Science Park,<br>Longtan Dist., Taoyuan City,<br>Taiwan, R.O.C. | BE |
| WINSTEK | Winstek Semiconductor Co., Ltd.<br>No 176-5, 6 Ling, Hualung Chun, Chiung Lin,<br>307 Hsinchu, Taïwan | BE |
| STATS JSCC | STATS ChipPAC Semiconductor Jiangyin CO. Ltd<br>No. 78 Changshan Road, Jiangyin,<br>214437, Jiangsu<br>P.R. China | BE |
| FEILIKS | Feili Logistics (Shenzhen) CO., Ltd<br>Zhongbao Logistics Building,<br>No. 28 Taohua Road, FFTZ,<br>Shenzhen, Guangdong 518038,<br>China | WHS |
| DNP | Dai Nippon printing Co ltd.<br>2-2-1 Kami-Fukuoka, Fujimino-shi,<br>Saitama,356-8507<br>Japan | MASK |
| DPE | Dai Printing Europe<br>Via C. Olivetti, 2/A,<br>I-20041 Agrate,<br>Italy | MASK |
| AMTC / Toppan Dresden | Advanced Mask Technology Center Gmbh & Co KG<br>Rahnitzer Allee 9<br>01109 Dresden<br>Germany | MASK |

1. DEV = development, FE = front end manufacturing, EWS = electrical wafer sort and pre-perso, BE = back end manufacturing, MASK = mask manufacturing, WHS = warehouse

# 8 References

**Table 17. Common Criteria**

| Component description | Reference | Version |
|---|---|---|
| Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, April 2017 | CCMB-2017-04-001 | 3.1 Rev 5 |
| Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, April 2017 | CCMB-2017-04-002 | 3.1 Rev 5 |
| Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, April 2017 | CCMB-2017-04-003 | 3.1 Rev 5 |

**Table 18. Protection Profile**

| Component description | Reference | Version |
|---|---|---|
| Eurosmart - Security IC Platform Protection Profile with Augmentation Packages | BSI-CC-PP-0084-2014 | 1.0 |

**Table 19. Other standards**

| Ref | Identifier | Description |
|---|---|---|
| [1] | BSI-AIS20/AIS31 | A proposal for: Functionality classes for random number generators,<br>W. Killmann & W. Schindler<br>BSI, Version 2.0, 18-09-2011 |
| [2] | NIST SP 800-67 | NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised January 2012, National Institute of Standards and Technology |
| [3] | FIPS PUB 140-2 | FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), up to change notice December 3, 2002 |
| [4] | FIPS PUB 180-2 | FIPS PUB 180-2 Secure Hash Standard with Change Notice 1 dated February 25,2004, National Institute of Standards and Technology, U.S.A., 2004 |
| [5] | FIPS PUB 186-4 | FIPS PUB 186-4, Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST), July 2013 |
| [6] | FIPS PUB 197 | FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001 |
| [7] | ISO/IEC 9796-2 | ISO/IEC 9796, Information technology - Security techniques - Digital signature scheme giving message recovery - Part 2: Integer factorization based mechanisms, ISO, 2002 |

**Table 19.    Other standards**

| Ref | Identifier | Description |
|-----|-----------|-------------|
| [8] | NIST SP 800-38A | NIST SP 800-38A Recommendation for Block Cipher Modes of Operation, 2001, with Addendum Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, October 2010 |
| [9] | NIST SP 800-38B | NIST special publication 800-38B, Recommandation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology (NIST), May 2005 |
| [10] | NIST SP 800-38C | NIST special publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, National Institute of Standards and Technology (NIST), May 2004 |
| [11] | NIST SP 800-38D | NIST special publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter mode (GCM) and GMAC, National Institute of Standards and Technology (NIST), November 2007 |
| [12] | ISO/IEC 14888 | ISO/IEC 14888, Information technology - Security techniques - Digital signatures with appendix - Part 1: General (1998), Part 2: Identity-based mechanisms (1999), Part 3: Certificate based mechanisms (2006), ISO |
| [13] | AUG | Smartcard Integrated Circuit Platform Augmentations, Atmel, Hitachi Europe, Infineon Technologies, Philips Semiconductors, Version 1.0, March 2002. |
| [14] | MIT/LCS/TR-212 | On digital signatures and public key cryptosystems, Rivest, Shamir & Adleman Technical report MIT/LCS/TR-212, MIT Laboratory for computer sciences, January 1979 |
| [15] | IEEE 1363-2000 | IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, 2000 |
| [16] | IEEE 1363a-2004 | IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004 |
| [17] | PKCS #1 V2.1 | PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002 |
| [18] | MOV 97 | Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997 |
| [19] | NIST SP 800-90 | NIST Special Publication 800-90, Recommendation for random number generation using deterministic random bit generators (Revised), National Institute of Standards and Technology (NIST), March 2007 |

**Table 19.**     **Other standards**

| Ref | Identifier | Description |
|-----|-----------|-------------|
| [20] | FIPS PUB 198-1 | FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC), National Institute of Standards and Technology (NIST), July 2008 |
| [21] | NIST SP 800-56A | NIST SP 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, National Institute of Standards and Technology (NIST), May 2013 |
| [22] | ANSI X9.31 | ANSI X9.31, Digital Signature Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), American National Standard for Financial Services, 1998 |
| [23] | ANSI X9.42 | ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, American National Standard for Financial Services, 2003 (R2013) |
| [24] | ANSI X9.62 | ANSI X9.62, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standard for Financial Services, 2005 |
| [25] | FIPS PUB 202 | FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015 |
| [26] | EdDSA rfc | S. Josefsson and I. Liusvaara,, Edwards-curve Digital Signature Algorithm (EdDSA) draft-irtf-cfrg-eddsa-08, Network Working Group Internet-Draft, IETF, August 19, 2016, available from *https://tools.ietf.org/html/draft-irtf-cfrg-eddsa-08* |
| [27] | EDDSA | Bernstein, D., Duif, N., Lange, T., Schwabe, P., and B. Yang, "High-speed high-security signatures", *http://ed25519.cr.yp.to/ed25519-20110926.pdf* September 2011 |
| [28] | EDDSA2 | Bernstein, D., Josefsson, S., Lange, T., Schwabe, P., and B. Yang, "EdDSA for more curves", WWW *http://ed25519.cr.yp.to/eddsa-20150704.pdf* July 2015 |
| [29] | NOTE 12.1 | Note d'application: Modélisation formelle des politiques de sécurité d'une cible d'évaluation NOTE/12.1, N°587/SGDN/DCSSI/SDR DCSSI, 25-03-2008 |
| [30] | M4M specification | MIFARE4Mobile specification v2.1.1, MIFARE4Mobile Industry Group, 2013 |
| [31] | JIL SRFPDCL | Security requirements for post-delivery code loading, Joint Interpretation Library, Version 1.0, February 2016 |
| [32] | ANSSI-CC-CER/F/06.003 | PP0084: Interpretations, ANSSI, June 2016 |

# Appendix A Glossary

## A.1 Terms

**Additional Code**

From the loader perspective, code activated by the Atomic Activation on the Initial TOE to generate the final TOE. For instance, Additional Code could: correct flaws, add new functionalities, update the operating system. An Additional Code is a particular « memory image » that has been activated in an authorized way on behalf of the TOE owner.

**Authorized user**

A user who may, in accordance with the TSP, perform an operation.

**Composite product**

Security IC product which includes the Security Integrated Circuit (i.e. the TOE) and the Embedded Software and is evaluated as composite target of evaluation.

**End-consumer**

User of the Composite Product in Phase 7.

**Final TOE**

From the loader perspective, the Final TOE is generated from the Initial TOE and the Additional Code. It is the resulting product of the Atomic Activation of the Additional Code onto the Initial TOE. Here the term TOE denotes the TOE itself as well as the composite TOE considered as a memory image which both may be maintained by a maintenance transaction.

**Integrated Circuit (IC)**

Electronic component(s) designed to perform processing and/or memory functions.

**IC Dedicated Software**

IC proprietary software embedded in a Security IC (also known as IC firmware) and developed by *ST*. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).

**IC Dedicated Test Software**

That part of the IC Dedicated Software which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.

**IC developer**

Institution (or its agent) responsible for the IC development.

**IC manufacturer**

Institution (or its agent) responsible for the IC manufacturing, testing, and pre-personalization.

**IC packaging manufacturer**

Institution (or its agent) responsible for the IC packaging and testing.

**Initial TOE**

From the loader perspective, the Initial TOE is the product on which the Additional Code is loaded and with the Loader as part of the embedded software. Here the term TOE denotes the TOE itself as well as the composite TOE which both may be maintained by loading of an additional memory image.

**Initialisation data**

Initialisation Data defined by the TOE Manufacturer to identify the TOE and to keep track of the Security IC's production and further life-cycle phases are considered as belonging to the TSF data. These data are for instance used for traceability and for TOE identification (identification data)

**Loader**

The Loader is the software developed by the Product Manufacturer. It is used to load and activate the Additional Code into the Product FLASH ~~or EEPROM~~ memory. The Loader is included in the ~~embedded~~ dedicated software and is ~~considered as~~ part of the ~~Initial~~ TOE.

**Maintenance transaction**

Modification of an initial memory image by an additional memory image resulting in a final memory image.

**Memory image**

Set of mappings of memory addresses onto data.

**Object**

An entity within the TSC that contains or receives information and upon which subjects perform operations.

**Packaged IC**

Security IC embedded in a physical package such as micromodules, DIPs, SOICs or TQFPs.

**Pre-personalization data**

Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases. If "Package 2: Loader dedicated for usage by authorized users only" is used the Pre-personalisation Data may contain the authentication reference data or key material for the trusted channel between the TOE and the authorized users using the Loader.

**Secret**

Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.

**Security IC**

Composition of the TOE, the Security IC Embedded Software, User Data, and the package.

**Security IC Embedded Software (ES)**

Software embedded in the Security IC and not developed by the IC designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the Security IC in Phase 3.

**Security IC embedded software (ES) developer**

Institution (or its agent) responsible for the security IC embedded software development and the specification of IC pre-personalization requirements, if any.

**Security attribute**

Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

**Sensitive information**

Any information identified as a security relevant element of the TOE such as:

– the application data of the TOE (such as IC pre-personalization requirements, IC and system specific data),

– the security IC embedded software,

– the IC dedicated software,

– the IC specification, design, development tools and technology.

**Smartcard**

A card according to ISO 7816 requirements which has a non volatile memory and a processing unit embedded within it.

**Subject**

An entity within the TSC that causes operations to be performed.

**Test features**

All features and functions (implemented by the IC Dedicated Software and/or hardware) which are designed to be used before TOE Delivery only and delivered as part of the TOE.

**TOE Delivery**

The period when the TOE is delivered which is after Phase 3 *or Phase 4 in this Security target*.

**TSF data**

Data created by and for the TOE, that might affect the operation of the TOE.

**User**

Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

**User data**

All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.

# A.2 Abbreviations

**Table 20. List of abbreviations**

| Term | Meaning |
|------|---------|
| AIS | Application notes and Interpretation of the Scheme (BSI). |
| BE | Back End manufacturing. |
| BSI | Bundesamt für Sicherheit in der Informationstechnik. |
| CBC | Cipher Block Chaining. |
| CC | Common Criteria. |
| CPU | Central Processing Unit. |
| CRC | Cyclic Redundancy Check. |
| DCSSI | Direction Centrale de la Sécurité des Systèmes d'Information. |
| DES | Data Encryption Standard. |

**Table 20.    List of abbreviations (continued)**

| Term | Meaning |
|------|---------|
| DESFire | MIFARE® DESFire® EV1. |
| DEV | Development. |
| DIP | Dual-In-Line Package. |
| DRBG | Deterministic Random Bit Generator. |
| EAL | Evaluation Assurance Level. |
| ECB | Electronic Code Book. |
| EDES | Enhanced DES. |
| EEPROM | Electrically Erasable Programmable Read Only Memory. |
| ES | Security IC Embedded Software. |
| EWS | Electrical Wafer Sort. |
| FE | Front End manufacturing. |
| FIPS | Federal Information Processing Standard. |
| I/O | Input / Output. |
| IC | Integrated Circuit. |
| ISO | International Standards Organisation. |
| IT | Information Technology. |
| LPU | Library Protection Unit. |
| MASK | Mask manufacturing. |
| MMU | Memory Management Unit. |
| M4M | MIFARE4Mobile®. |
| NESCRYPT | Next Step Cryptography Accelerator. |
| NIST | National Institute of Standards and Technology. |
| NVM | Non Volatile Memory. |
| OSP | Organisational Security Policy. |
| OST | Operating System for Test. |
| PP | Protection Profile. |
| PUB | Publication Series. |
| RAM | Random Access Memory. |
| RF | Radio Frequency. |
| ROM | Read Only Memory. |
| RSA | Rivest, Shamir & Adleman. |
| SAR | Security Assurance Requirement. |
| SFP | Security Function Policy. |

**Table 20.    List of abbreviations (continued)**

| Term | Meaning |
|------|---------|
| SFR | Security Functional Requirement. |
| SOIC | Small Outline IC. |
| ST | Context dependent : STMicroelectronics or Security Target. |
| TDES | Triple Data Encryption Standard |
| TOE | Target of Evaluation. |
| TQFP | Thin Quad Flat Package. |
| TRNG | True Random Number Generator. |
| TSC | TSF Scope of Control. |
| TSF | TOE Security Functionality. |
| TSFI | TSF Interface. |
| TSP | TOE Security Policy. |
| TSS | TOE Summary Specification. |
| WHS | Warehouse. |

**Please Read Carefully:**

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST's terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST'S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

ST PRODUCTS ARE NOT DESIGNED OR AUTHORIZED FOR USE IN: (A) SAFETY CRITICAL APPLICATIONS SUCH AS LIFE SUPPORTING, ACTIVE IMPLANTED DEVICES OR SYSTEMS WITH PRODUCT FUNCTIONAL SAFETY REQUIREMENTS; (B) AERONAUTIC APPLICATIONS; (C) AUTOMOTIVE APPLICATIONS OR ENVIRONMENTS, AND/OR (D) AEROSPACE APPLICATIONS OR ENVIRONMENTS. WHERE ST PRODUCTS ARE NOT DESIGNED FOR SUCH USE, THE PURCHASER SHALL USE PRODUCTS AT PURCHASER'S SOLE RISK, EVEN IF ST HAS BEEN INFORMED IN WRITING OF SUCH USAGE, UNLESS A PRODUCT IS EXPRESSLY DESIGNATED BY ST AS BEING INTENDED FOR "AUTOMOTIVE, AUTOMOTIVE SAFETY OR MEDICAL" INDUSTRY DOMAINS ACCORDING TO ST PRODUCT DESIGN SPECIFICATIONS. PRODUCTS FORMALLY ESCC, QML OR JAN QUALIFIED ARE DEEMED SUITABLE FOR USE IN AEROSPACE BY THE CORRESPONDING GOVERNMENTAL AGENCY.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.

Information in this document supersedes and replaces all information previously supplied.

The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.