STMicroelectronics

ST33G1M2 C01
including optional cryptographic library NesLib, and optional technology MIFARE4Mobile®
Security Target for composition

Common Criteria for IT security evaluation

SMD_ST33G1M2_ST_19_002 Rev C01.3

October 2019

www.st.com

Contents

List of tables

List of figures

ST33G1M2 C01 platform Security Target for composition

Common Criteria for IT security evaluation

1 Introduction (ASE_INT)

1.1 Security Target reference

1 Document identification: ST33G1M2 C01 including optional cryptographic library NesLib, and optional technology MIFARE4Mobile® SECURITY TARGET FOR COMPOSITION.

2 Version number: Rev C01.3, issued in October 2019.

3 Registration: registered at ST Microelectronics under number SMD_ST33G1M2_ST_19_002.

1.2 TOE reference

4 This document presents **the Security Target for composition (ST)** of the **ST33G1M2 C01 (ST33G1M2 and ST33I1M2)** Security Integrated Circuit (IC), designed on the **ST33G platform of STMicroelectronics**, with firmware version 9 and A, optional cryptographic library **NesLib 6.3.4**, and optional technology **MIFARE4Mobile®** [a] **2.1.0**.

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*.

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

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 ALC_DVS.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.

The original text of this PP is typeset as indicated here, its augmentations from *AUG* as indicated here, when they are reproduced in this document.

This ST also instantiates the following package from the above mentioned PP:

- Loader dedicated for usage in secured environment 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***. 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* and ***AUG4*** for Addition #4 of *AUG*.

1.4 TOE identification

13 The Target of Evaluation (TOE) is the ST33G1M2 C01 platform.

14 “ST33G1M2 C01” 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 C01 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	IC version	Master identification number (1)	Firmware version	OST version	Optional NesLib crypto library version	Optional MIFARE4Mobile DESFire EV1 library Id(2)	Optional MIFARE4 Mobile version(3)
K8H0A	F	0061h (ST33G1M2) and 0105h (ST33I1M2)	9 and A	2.2	6.3.4	0x00000004 or 0x00000504 (combined)	2.1.0

1. Part of the product information.
2. See the ST33G Firmware User Manual referenced in *Chapter 7*.
3. See the MIFARE4Mobile User Manual referenced in *Chapter 7*.

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 TOE is a serial access Smartcard IC designed for secure mobile applications, based on 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 The TOE offers a high-speed User Flash memory, an internally generated clock, an MPU, an internal true random number generator (TRNG) and hardware accelerators for advanced cryptographic functions.

20 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, or composite product integration, or personnalisation process.

21 They 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.

22 The configuration of the derivative devices can impact the available IOs, the available NVM memory size, the availability of the crypto processors and the availability of the LPU, as detailed here below:

Table 2. Derivative devices configuration possibilities

Features	Possible values
SWP	Active, Inactive
SPI	Active, Inactive
IART	Active, Inactive
NVM size	Selectable by 128 Kbytes granularity from 1280 Kbytes to 384 Kbytes
Nescrypt	Active, Inactive
EDES+ accelerator	Active, Inactive
AES accelerator (HW-AES)	Active, Inactive
Library Protection Unit (LPU)	Active, Inactive
Crypto1	Active, Inactive

23 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.

24 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*.

25 The rest of this document applies to all possible configurations 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.

26 In a few words, the ST33G1M2 C01, offers a unique combination of high performances and very powerful features for high level security:

- Die integrity,
- Monitoring of environmental parameters,
- Protection mechanisms against faults,
- AIS20/AIS31 class PTG.2 compliant True Random Number Generator,
- Memory Protection Unit,
- ISO 13239 CRC calculation block,
- optional Hardware Security Enhanced DES accelerator,
- optional AES accelerator (HW-AES),
- optional Library Protection Unit,
- optional Next Step Cryptography accelerator (NESCRYPT),
- optional cryptographic library,
- optional secure MIFARE4Mobile library.

1.6 TOE description

1.6.1 TOE hardware description

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

If HW-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 Electronic CodeBook (ECB) or Cipher Block Chaining (CBC) modes.
If EDES+ is active, the 3-key triple DES accelerator (EDES+) supports efficiently the Data Encryption Standard (DES [2]), enabling Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes, and triple DES computation.
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]).

As randomness is a key stone in many applications, the ST33G1M2 C01 features a highly reliable True Random Number Generator (TRNG), compliant with PTG.2 Class of AIS20/AIS31 [1] and directly accessible thru dedicated registers.

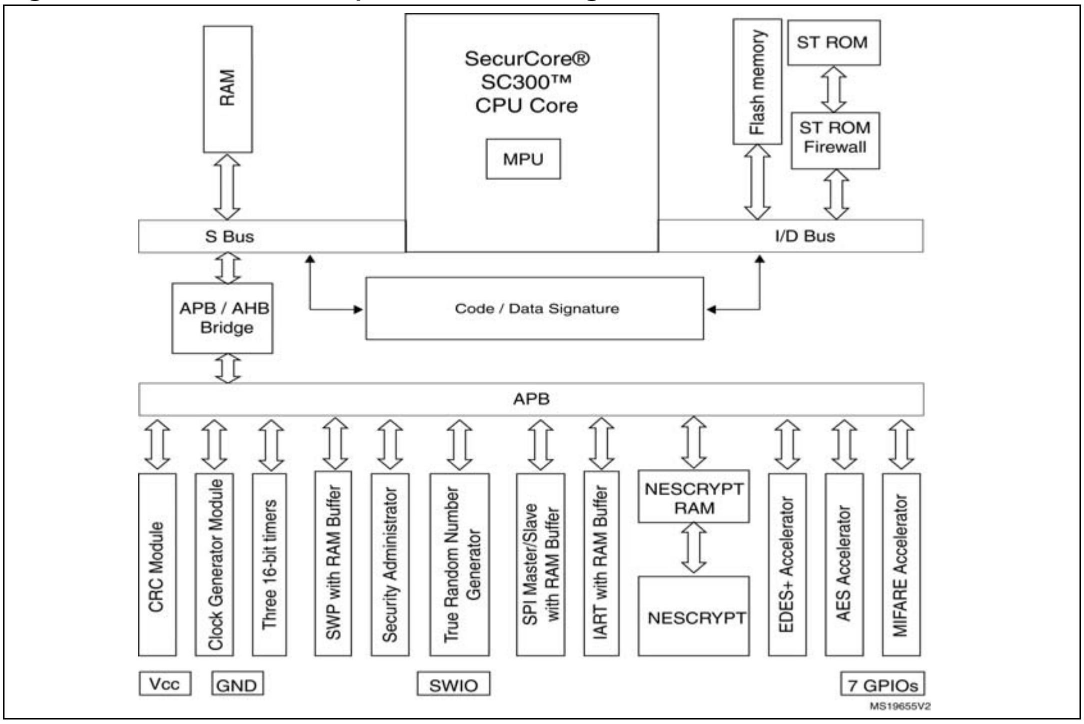
This device includes the ARM® SecurCore® SC300™ memory protection unit (MPU), which enables the user to define its own region organization with specific protection and access permissions. The MPU can be used to enforce various protection models, ranging from a basic code dump prevention model up to a full application confinement model.

28 The TOE offers 3 communication channels to the external world: a serial communication interface fully compatible with the ISO/IEC 7816-3 standard, a single-wire protocol (SWP) interface for communication with a near-field communication (NFC) router in SIM/NFC applications, and an alternative and exclusive SPI Slave interface for communication in non-SIM applications.

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

30 Figure 1 provides an overview of the ST33G1M2 C01 platform.

Figure 1. ST33G1M2 C01 platform block diagram



1.6.2 TOE software description

31 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.

32 The System ROM and ST NVM of the TOE contain a Dedicated Software which provides a very reduced set of commands for final test (operating system for final test, called "FTOS"), not intended for the Security IC Embedded Software (ES) usage, and not available in User configuration.

33 The System ROM and ST NVM of the TOE contain a Dedicated Support Software called 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 not available in User configuration.

34 The System ROM and ST NVM of the TOE contain a Dedicated Support Software, which provides 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 all through the product life-cycle.

35 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.

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 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]*.

36 The TOE optionally comprises a specific application in User NVM: this applicative Embedded Software is MIFARE4Mobile®, a MIFARE technology library *[29]*.
This library is configurable according to the customer's choice. It can include MIFARE®

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

Classic, or MIFARE® M4M-DESFire® EV1, or both.
The part of MIFARE4Mobile® featuring MIFARE® M4M-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 M4M-DESFire can only be used if the LPU, the EDES+ and the HW-AES are active.

37 In this Security Target, the terms:

- "M4M" means MIFARE4Mobile®[b],
- "M4M-DESFire" denotes the part of MIFARE4Mobile® featuring MIFARE® M4M-DESFire® EV1[c],
- "M4M-Classic" denotes the part of MIFARE4Mobile® featuring MIFARE® Classic.

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

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.

39 The user guidance documentation, part of the TOE, consists of:

- the product Data Sheet and die description,
- optionally the ST33G1M2 platform Technical Notes,
- the product family Security Guidance,
- the AIS31 user manuals,
- the Cortex M3 SC300 Technical Reference Manuals,
- the System ROM user manual,
- the Flash loader installation guide,
- optionally the NesLib user manual,
- optionally the MIFARE4Mobile® user manual.

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

1.7 TOE life cycle

41 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.

42 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.

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

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

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.

45 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.

46 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.

47 The TOE is delivered after Phase 3 in form of wafers or after Phase 4 in packaged form, depending on the customer’s order.

48 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.

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

1.8 TOE environment

50 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

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

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

53 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 unauthorised 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).

54 The development centres possibly involved in the development of the TOE are denoted by the activity “DEV” in *Table 16*.

55 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).

56 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

57 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.

58 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 of each TOE occurs to assure conformance with the device specification.

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

60 The authorized EWS plant potentially involved in the testing and pre-perso of the TOE are denoted by the activity “EWS” in *Table 16*.

61 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.

62 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*.

63 All sites denoted by the activity “WHS” in *Table 16* can be involved for the logistics.

1.8.3 TOE operational environment

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

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

66 End-user environments (phase 7): composite products are used in a wide range of applications to assure authorised conditional access. Examples of such are pay-TV, 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

67 The ST33G1M2 C01 platform Security Target claims to be conformant to the Common Criteria version 3.1 revision 5.

68 Furthermore it claims to be CC Part 2 (*CCMB-2017-04-002 R5*) extended and CC Part 3 (*CCMB-2017-04-003 R5*) conformant.

69 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.

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

70 The assurance level for the ST33G1M2 C01 platform Security Target is ***EAL5*** augmented by ALC_DVS.2 and AVA_VAN.5.

2.2 PP Claims

2.2.1 PP Reference

71 The ST33G1M2 C01 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.

2.2.2 PP Additions

72 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 Secure Flash Loader,
- Specific additions for M4M-DESFire,
- Refinement of assurance requirements.

73 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. Text originating in *AUG* is typeset as indicated here.

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

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

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

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

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

2.2.3 PP Claims rationale

79 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.

80 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*.

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

82 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*.

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

84 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)

85 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.

86 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*, and the ones introduced in this Security Target, are detailed in the following sections.

87 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
	AUG4.T.Mem-Access	Memory Access Violation
	T.Data-Modification-M4M	Unauthorised data modification for M4M-DESFire
	T.Impersonate-M4M	Impersonating authorised users during authentication for M4M-DESFire
	T.Cloning-M4M	Cloning for M4M-DESFire
	T.Confid-Applic-Code-M4M	M4M-DESFire code confidentiality
	T.Confid-Applic-Data-M4M	M4M-DESFire data confidentiality
	T.Integ-Applic-Code-M4M	M4M-DESFire code integrity
	T.Integ-Applic-Data-M4M	M4M-DESFire data integrity
	T.Resource-M4M	M4M-DESFire resource unavailability
OSPs	BSI.P.Process-TOE	Protection during TOE Development and Production
	BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality
	AUG1.P.Add-Functions	Additional Specific Security Functionality (Cipher Scheme Support)
	P.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software
	P.Confidentiality-M4M	Confidentiality during communication for M4M-DESFire
	P.Transaction-M4M	Transaction mechanism for M4M-DESFire
	P.No-Trace-M4M	Un-traceability of end-users for M4M-DESFire
	P.Resp-Appl	Treatment of user data

Table 4. Summary of security aspects (continued)

	Label	Title
Assumptions	BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
	BSI.A.Resp-Appl	Treatment of User Data
	A.Secure-Values-M4M	Usage of secure values for M4M-DESFire
	A.Terminal-Support-M4M	Terminal support to ensure integrity and confidentiality for M4M-DESFire
	A.M4M-Framework-Identification	Identification by M4M Framework

3.1 Description of assets

88 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.

89 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 (when they are active), 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.

90 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.

91 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 security concerns are extended accordingly.

3.2 Threats

92 The threats are described in the *BSI-CC-PP-0084-2014*, section 3.2.
Only those originating in *AUG* 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
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.

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

T.Data-Modification-M4M	Unauthorised data modification for M4M-DESFire: User data stored by the TOE may be modified by unauthorised subjects. This threat applies to the processing of modification commands received by the TOE, it is not concerned with verification of authenticity.

T.Impersonate-M4M	Impersonating authorised users during authentication for M4M-DESFire: An unauthorised subject may try to impersonate an authorised subject during the authentication sequence, e.g. by a man-in-the middle or replay attack.
T.Cloning-M4M	Cloning for M4M-DESFire: User and TSF data stored on the TOE (including keys) may be read out by an unauthorised subject in order to create a duplicate.
T.Confid-Applic-Code-M4M	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. The attacker executes an application to disclose code belonging to M4M-DESFire Licensed product.
T.Confid-Applic-Data-M4M	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. For example, the attacker executes an application that tries to read data belonging to M4M-DESFire Licensed product.
T.Integ-Applic-Code-M4M	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. The attacker executes an application that tries to alter (part of) the M4M-DESFire code.
T.Integ-Applic-Data-M4M	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. The attacker executes an application that tries to alter (part of) the M4M-DESFire Licensed product data.
T.Resource-M4M	M4M-DESFire resource unavailability: The availability of resources for the M4M-DESFire Licensed product shall be controlled to prevent denial of service or malfunction. 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

94 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.

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

96 *BSI.P.Lim-Block-Loader* is dedicated to the Secure Flash Loader, and described in the *BSI-CC-PP-0084-2014* package "Loader dedicated for usage in secured environment only".

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

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

99 P.Controlled-ES-Loading is related to the capability provided by the TOE to load Security IC Embedded Software into the NVM after TOE delivery, in a controlled manner, during composite product manufacturing. The use of this capability is optional, and depends on the customer's production organization.

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

101 P.Resp-Appl are 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 in order to protect stored data from disclosure and manipulation.

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), – Advanced Encryption Standard (AES), ***– Elliptic Curves Cryptography on GF(p),*** if NesLib is embedded***,*** ***– Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),*** if NesLib is embedded***,*** – Rivest-Shamir-Adleman (RSA)***,*** if NesLib is embedded, – ***Deterministic Random Bit Generator (DRBG),*** if NesLib is embedded, ***– Keccak,*** if NesLib is embedded, – ***Keccak-p,*** if NesLib is embedded, – ***Diffie-Hellman,*** if NesLib is embedded, – ***Prime Number Generation,*** if NesLib is embedded. Note that SHA-1 is no longer recommended as a cryptographic function. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.
P.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software: The TOE shall provide the capability to import the Security IC Embedded Software into the NVM, in a controlled manner, either before TOE delivery, under ST authority, either after TOE delivery, under the composite product manufacturer authority. This capability is not available in User configuration.
P.Confidentiality-M4M	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-M4M	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-M4M	Un-traceability of end-users for M4M-DESFire: The TOE shall provide the ability that authorised subjects can prevent that end-user of TOE may be traced by unauthorised 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

102 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

103 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.

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

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

A.Secure-Values-M4M	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-M4M	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.M4M-Framework-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)

106 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.

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

108 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 originating in *AUG*, 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
	AUG1.O.Add-Functions	Additional Specific Security Functionality
	AUG4.O.Mem-Access	***Dynamic*** Area based Memory Access Control
	O.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software
	O.Access-Control-M4M	Access Control for M4M-DESFire
	O.Authentication-M4M	Authentication for M4M-DESFire
	O.Confidentiality-M4M	M4M-DESFire Confidential Communication
	O.Type-Consistency-M4M	M4M-DESFire Data type consistency
	O.Transaction-M4M	M4M-DESFire Transaction mechanism
	O.No-Trace-M4M	Preventing Traceability for M4M-DESFire

Table 5. Summary of security objectives (continued)

	Label	Title
TOE	*O.Resp-Appl-M4M*	Treatment of user data for M4M-DESFire
	O.Resource-M4M	Resource availability for M4M-DESFire
	O.Firewall-M4M	M4M-DESFire firewall
	O.Shr-Res-M4M	M4M-DESFire data cleaning for resource sharing
	O.Verification-M4M	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
	OE.Secure-Values-M4M	Generation of secure values for M4M-DESFire
	OE.Terminal-Support-M4M	Terminal support to ensure integrity and confidentiality for M4M-DESFire
	OE.M4M-Framework-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

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), – Advanced Encryption Standard (AES), – ***Elliptic Curves Cryptography on GF(p),*** if NesLib is embedded***,*** – ***Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),*** if NesLib is embedded***,*** – Rivest-Shamir-Adleman (RSA)***,*** if NesLib is embedded, – ***Deterministic Random Bit Generator (DRBG),*** if NesLib is embedded, ***– Keccak,*** if NesLib is embedded, – ***Keccak-p,*** if NesLib is embedded, – ***Diffie-Hellman,*** if NesLib is embedded, – ***Prime Number Generation,*** if NesLib is embedded***.*** Note that SHA-1 is no longer recommended as a cryptographic function. 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.
O.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software: The TOE must provide the capability to load the Security IC Embedded Software into the NVM, either before TOE delivery, under ST authority, either after TOE delivery, under the composite product manufacturer authority. The TOE must restrict the access to these features. The TOE must provide control means to check the integrity of the loaded user data. This capability is not available in User configuration.

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

O.Access-Control-M4M	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-M4M	Authentication for M4M-DESFire: The TOE must provide an authentication mechanism in order to be able to authenticate authorised users. The authentication mechanism shall be resistant against replay and man-in-the-middle attacks.
O.Confidentiality-M4M	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-M4M	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-M4M	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-M4M	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 unauthorised subject.
O.Resp-Appl-M4M	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 unauthorised users or processes when communicating with a terminal.
O.Resource-M4M	Resource availability for M4M-DESFire: The TOE shall control the availability of resources for M4M-DESFire Licensed product.
O.Firewall-M4M	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-M4M	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-M4M	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

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

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

111 Security Objectives for the operational Environment (phase 4 up to 6):

BSI.OE.Process-Sec-IC	Protection during composite product manufacturing
BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the Loader

112 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.

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

OE.Secure-Values-M4M	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-M4M	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.M4M-Framework-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

114 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.

115 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).

116 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*)".

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

- TOE threats "Unauthorised data modification for M4M-DESFire, (*T.Data-Modification-M4M*)", "Impersonating authorised users during authentication for M4M-DESFire, (*T.Impersonate-M4M*)", "Cloning for M4M-DESFire, (*T.Cloning-M4M*)", "M4M-DESFire code confidentiality, (*T.Confid-Applic-Code-M4M*)", "M4M-DESFire data confidentiality, (*T.Confid-Applic-Data-M4M*)", "M4M-DESFire code integrity, (*T.Integ-Applic-Code-M4M*)", "M4M-DESFire data integrity, (*T.Integ-Applic-Data-M4M*)", and "M4M-DESFire resource unavailability, (*T.Resource-M4M*)".
- organisational security policies "Controlled loading of the Security IC Embedded Software, (*P.Controlled-ES-Loading*)", "Confidentiality during communication for M4M-DESFire, (*P.Confidentiality-M4M*)", "Transaction mechanism for M4M-DESFire, (*P.Transaction-M4M*)", "Un-traceability of end-users for M4M-DESFire, (*P.No-Trace-M4M*)", and "Treatment of user data, (*P.Resp-Appl*)".
- assumptions "Usage of secure values for M4M-DESFire, (*A.Secure-Values-M4M*)", and "Terminal support to ensure integrity, confidentiality for M4M-DESFire, (*A.Terminal-*

Support-M4M)", and "Identification by M4M Framework, (*A.M4M-Framework-Identification*)".

118 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, policy and threats defined there.

119 In particular, the added assumptions and objectives on the environment 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 is 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
A.M4M-Framework-Identification	*OE.M4M-Framework-Identification*	Phase 1
BSI.P.Process-TOE	*BSI.O.Identification*	Phase 2-3 optional Phase 4
BSI.P.Lim-Block-Loader	*BSI.O.Cap-Avail-Loader* *BSI.OE.Lim-Block-Loader*	Phase 5-6 optional Phase 4
BSI.A.Process-Sec-IC	*BSI.OE.Process-Sec-IC*	Phase 5-6 optional Phase 4
P.Controlled-ES-Loading	*O.Controlled-ES-Loading*	Phase 4-6
A.Secure-Values-M4M	*OE.Secure-Values-M4M*	Phases 5-7
A.Terminal-Support-M4M	*OE.Terminal-Support-M4M*	Phase 7
AUG1.P.Add-Functions	*AUG1.O.Add-Functions*	
P.Confidentiality-M4M	*O.Confidentiality-M4M* *OE.Terminal-Support-M4M*	
P.Transaction-M4M	*O.Transaction-M4M*	
P.No-Trace-M4M	*O.No-Trace-M4M* *O.Access-Control-M4M* *O.Authentication-M4M*	
P.Resp-Appl	*O.Resp-Appl-M4M*	
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*	
BSI.T.RND	*BSI.O.RND*	
AUG4.T.Mem-Access	*AUG4.O.Mem-Access*	
T.Data-Modification-M4M	*O.Access-Control-M4M* *O.Type-Consistency-M4M* *OE.Terminal-Support-M4M*	
T.Impersonate-M4M	*O.Authentication-M4M* *OE.M4M-Framework-Identification*	
T.Cloning-M4M	*O.Access-Control-M4M* *O.Authentication-M4M*	
T.Confid-Applic-Code-M4M	*O.Firewall-M4M*	
T.Confid-Applic-Data-M4M	*O.Firewall-M4M*	
T.Integ-Applic-Code-M4M	*O.Verification-M4M* *O.Firewall-M4M*	
T.Integ-Applic-Data-M4M	*O.Shr-Res-M4M* *O.Firewall-M4M*	
T.Resource-M4M	*O.Resource-M4M*	

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

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

121 Since *OE.Secure-Values-M4M* 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-M4M*, the assumption is covered by the objective.

122 *A.Secure-Values-M4M* and *OE.Secure-Values-M4M* 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"

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

124 The objective *OE.Terminal-Support-M4M* is an immediate transformation of the assumption *A.Terminal-Support-M4M*, therefore it covers the assumption.

125 *A.Terminal-Support-M4M* and *OE.Terminal-Support-M4M* 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”

126 The justification related to the assumption “Identification by M4M Framework, (*A.M4M-Framework-Identification*)” is as follows:

127 The objective *OE.M4M-Framework-Identification* is an immediate transformation of the assumption *A.M4M-Framework-Identification*, therefore it covers the assumption.

128 *A.M4M-Framework-Identification* and *OE.M4M-Framework-Identification* 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.

4.3.4 TOE threat "Memory Access Violation"

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

130 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.

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

4.3.5 TOE threat "Unauthorised data modification for M4M-DESFire"

132 The justification related to the threat “Unauthorised data modification for M4M-DESFire, (*T.Data-Modification-M4M*)” is as follows:

133 According to threat *T.Data-Modification-M4M*, the TOE shall avoid that user data stored by the TOE may be modified by unauthorised subjects. The objective *O.Access-Control-M4M* requires an access control mechanism that limits the ability to modify data elements stored by the TOE. *O.Type-Consistency-M4M* 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-M4M*. Therefore *T.Data-Modification-M4M* is covered by these three objectives.

134 The added objectives for the TOE *O.Access-Control-M4M* and *O.Type-Consistency-M4M* do not introduce any contradiction in the security objectives for the TOE.

4.3.6 TOE threat "Impersonating authorised users during authentication for M4M-DESFire"

135 The justification related to the threat “Impersonating authorised users during authentication for M4M-DESFire, (*T.Impersonate-M4M*)” is as follows:

136 The threat is related to the fact that an unauthorised subject may try to impersonate an authorised subject during authentication, e.g. by a man-in-the middle or replay attack. The goal of *O.Authentication-M4M* is that an authentication mechanism is implemented in the TOE that prevents these attacks. Additionally, *OE.M4M-Framework-Identification* requires that a subject getting access to M4M-DESFire through the M4M host interface is previously identified.Therefore the threat is covered by *O.Authentication-M4M* together with *OE.M4M-Framework-Identification*.

137 The added objective for the TOE *O.Authentication-M4M* does not introduce any contradiction in the security objectives for the TOE.

4.3.7 TOE threat "Cloning for M4M-DESFire"

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

139 The concern of *T.Cloning-M4M* is that all data stored on the TOE (including keys) may be read out in order to create a duplicate. The objective *O.Authentication-M4M* together with *O.Access-Control-M4M* requires that unauthorised users can not read any information that is restricted to the authorised subjects. The cryptographic keys used for the authentication are stored inside the TOE protected. *O.Access-Control-M4M* states that no keys used for authentication shall ever be output. Therefore the two objectives cover *T.Cloning-M4M*.

4.3.8 TOE threat "M4M-DESFire resource unavailability"

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

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

142 The added objective for the TOE *O.Resource-M4M* does not introduce any contradiction in the security objectives for the TOE.

4.3.9 TOE threat "M4M-DESFire code confidentiality"

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

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

145 The added objective for the TOE *O.Firewall-M4M* does not introduce any contradiction in the security objectives for the TOE.

4.3.10 TOE threat "M4M-DESFire data confidentiality"

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

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

4.3.11 TOE threat "M4M-DESFire code integrity"

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

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

150 The added objective for the TOE *O.Verification-M4M* does not introduce any contradiction in the security objectives for the TOE.

4.3.12 TOE threat "M4M-DESFire data integrity"

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

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

153 The added objective for the TOE *O.Shr-Res-M4M* does not introduce any contradiction in the security objectives for the TOE.

4.3.13 Organisational security policy "Additional Specific Security Functionality"

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

155 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.

156 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*.

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

4.3.14 Organisational security policy "Controlled loading of the Security IC Embedded Software"

158 The justification related to the organisational security policy "Controlled loading of the Security IC Embedded Software, (*P.Controlled-ES-Loading*)” is as follows:

159 Since *O.Controlled-ES-Loading* requires the TOE to implement exactly the same specific security functionality as required by *P.Controlled-ES-Loading*, and in the very same conditions, the organisational security policy is covered by the objective.

160 The added objective for the TOE *O.Controlled-ES-Loading* does not introduce any contradiction in the security objectives.

4.3.15 Organisational security policy "Confidentiality during communication for M4M-DESFire"

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

162 The policy *P.Confidentiality-M4M* 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-M4M*. Since *O.Confidentiality-M4M* 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-M4M* ensures the support by the terminal, the two objectives cover the policy.

163 The added objective for the TOE *O.Confidentiality-M4M* does not introduce any contradiction in the security objectives.

4.3.16 Organisational security policy "Transaction mechanism for M4M-DESFire"

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

165 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-M4M*, therefore the policy *P.Transaction-M4M* is covered by *O.Transaction-M4M*.

166 The added objective for the TOE *O.Transaction-M4M* does not introduce any contradiction in the security objectives.

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

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

168 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-M4M* 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 unauthorised subject, which includes the UID. The objectives *O.Authentication-M4M* and *O.Access-Control-M4M* provide means to authorise subjects and to implement access control to data elements in a way that unauthorised subjects cannot read any element usable for tracing. Therefore the policy is covered by these three objectives.

169 The added objective for the TOE *O.No-Trace-M4M* does not introduce any contradiction in the security objectives.

4.3.18 Organisational security policy "Treatment of user data"

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

171 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-M4M* has the same objective as *BSI.OE.Resp-Appl* defined in the PP. Thus, the objectives *O.Resp-Appl-M4M* covers the policy *P.Resp-Appl*.

172 The added objective for the TOE *O.Resp-Appl-M4M* does not introduce any contradiction in the security objectives.

5 Security requirements (ASE_REQ)

173 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

174 Security Functional Requirements (SFRs) from the "*BSI-CC-PP-0084-2014*" Protection Profile (PP) are drawn from *CCMB-2017-04-002 R5*, except the following SFRs, that are **extensions** to *CCMB-2017-04-002 R5*:

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

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

175 All extensions to the SFRs of the "*BSI-CC-PP-0084-2014*" Protection Profiles (PPs) are **exclusively** drawn from *CCMB-2017-04-002 R5*.

176 All <u>iterations</u>, <u>assignments</u>, <u>selections</u>, or <u>refinements</u> on SFRs have been performed according to section C.4 of *CCMB-2017-04-001 R5*. They are easily identified in the following text as they appear ***as indicated here***. Note that in order to improve readability, <u>iterations</u> are sometimes expressed within tables.

177 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.

178 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 R5*
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	Abuse of Test functionality	BSI-CC-PP-0084-2014	Extended
FMT_LIM.2 / Test	Limited availability			
FMT_LIM.1 / Loader	Limited capabilities	Abuse of Loader functionality	BSI-CC-PP-0084-2014 Operated	
FMT_LIM.2 / Loader	Limited availability			
FAU_SAS.1	Audit storage	Lack of TOE identification		
FDP_SDC.1	Stored data confidentiality	Physical manipulation & probing		
FDP_SDI.2	Stored data integrity monitoring and action			CCMB-2017-04-002 R5
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 R5
FCS_CKM.1 (if NesLib is embedded only)	Cryptographic key generation		Security Target Operated	
FDP_ACC.2 / Memories	Complete access control	Memory access violation	Security Target Operated	
FDP_ACF.1 / Memories	Security attribute based access control		AUG #4 Operated	
FMT_MSA.3 / Memories	Static attribute initialisation	Correct operation		
FMT_MSA.1 / Memories	Management of security attribute			
FMT_SMF.1 / Memories	Specification of management functions		Security Target Operated	

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

Label	Title	Addressing	Origin	Type
FDP_ITC.1 / Loader	Import of user data without security attributes	User data loading access violation	Security Target Operated	CCMB-2017-04-002 R5
FDP_ACC.1 / Loader	Subset access control			
FDP_ACF.1 / Loader	Security attribute based access control			
FMT_MSA.3 / Loader	Static attribute initialisation	Correct operation		
FMT_MSA.1 / Loader	Management of security attribute			
FMT_SMR.1 / Loader	Security roles	Abuse of Admin functionality		
FIA_UID.1 / Loader	Timing of identification			
FMT_SMF.1 / Loader	Specification of management functions			
FMT_SMR.1 / M4M-DESFire	Security roles	M4M-DESFire access control (if M4M-DESFire is embedded only)		
FDP_ACC.1 / M4M-DESFire	Subset access control			
FDP_ACF.1 / M4M-DESFire	Security attribute based access control			
FMT_MSA.3 / M4M-DESFire	Static attribute initialisation			
FMT_MSA.1 / M4M-DESFire	Management of security attribute			
FMT_SMF.1 / M4M-DESFire	Specification of management functions			
FDP_ITC.2 / M4M-DESFire	Import of user data with security attributes			
FPT_TDC.1 / M4M-DESFire	Inter-TSF basic TSF data consistency			

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

Label	Title	Addressing	Origin	Type
FIA_UID.2 / M4M-DESFire	User identification before any action	M4M-DESFire confidentiality and authentication (if M4M-DESFire is embedded only)	Security Target Operated	CCMB-2017-04-002 R5
FIA_UAU.2 / M4M-DESFire	User authentication before any action			
FIA_UAU.5 / M4M-DESFire	Multiple authentication mechanisms			
FMT_MTD.1 / M4M-DESFire	Management of TSF data			
FPT_TRP.1 / M4M-DESFire	Trusted path			
FCS_CKM.4 / M4M-DESFire	Cryptographic key destruction			
FDP_ROL.1 / M4M-DESFire	Basic rollback	M4M-DESFire robustness (if M4M-DESFire is embedded only)		
FPT_RPL.1 / M4M-DESFire	Replay detection			
FPR_UNL.1 / M4M-DESFire	Unlinkability			
FRU_RSA.2 / M4M-DESFire	Minimum and maximum quotas	M4M-DESFire correct operation (if M4M-DESFire is embedded only)		
FDP_RIP.1 / M4M-DESFire	Subset residual information protection	M4M-DESFire intrinsic confidentiality and integrity (if M4M-DESFire is embedded only)		
FDP_ACC.1 / APPLI_FWL	Subset access control	Application or M4M-DESFire intrinsic confidentiality and integrity		
FDP_ACF.1 / APPLI_FWL	Security attribute based access control			
FMT_MSA.3 / APPLI_FWL	Static attribute initialisation			

5.1.1 Security Functional Requirements from the Protection Profile

Limited fault tolerance (FRU_FLT.2)

179 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)

180 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.***

181 ***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

182 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

183 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***.

184 *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)

185 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)

186 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)

187 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***.

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

Resistance to physical attack (FPT_PHP.3)

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

190 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)

191 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)

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

193 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)

194 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***.

195 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)

196 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.***

197 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)

198 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 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+	EDES	* encryption * decryption - in Cipher Block Chaining (CBC) mode - in Electronic Code Book (ECB) mode	Triple Data Encryption Standard (TDES)	168 bits	*NIST SP 800-67* *NIST SP 800-38A*

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 HW-AES	AES	* encryption (cipher) * decryption (inverse cipher) - in Cipher Block Chaining (CBC) mode - 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) * Authenticated encryption/decryption in Galois Counter Mode (GCM) * Authenticated encryption/decryption in Counter with CBC-MAC (CCM)			*NIST SP 800-38B* *NIST SP 800-38A* *NIST SP 800-38D* *NIST SP 800-38C*
If NesLib	RSA	* RSA public key operation * RSA private key operation without the Chinese Remainder Theorem * RSA private key operation with the Chinese Remainder Theorem * EMSA PSS and PKCS1 signature scheme coding * RSA Key Encapsulation Method (KEM)	Rivest, Shamir & Adleman's	up to 4096 bits	*PKCS #1 V2.1*

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	ECC on Weierstrass curves	* private scalar multiplication * prepare Jacobian * public scalar multiplication * point validity check * convert Jacobian to affine coordinates * general point addition * point expansion * point compression	Elliptic Curves Cryptography on GF(p) on curves in Weierstrass form	up to 640 bits	*IEEE 1363-2000, chapter 7* *IEEE 1363a-2004*
		* Diffie-Hellman (ECDH) key agreement computation			*NIST SP 800-56A*
		* digital signature algorithm (ECDSA) generation and verification			*FIPS PUB 186-4* *ANSI X9.62, section 7*
If NesLib	ECC on Edwards curves	* ed25519 generation * ed25519 verification * ed25519 point decompression	Elliptic Curves Cryptography on GF(p) on curves in Edwards form, with curve 25519	256 bits	*EdDSA rfc* *EDDSA* *EDDSA2*
If NesLib	SHA	* SHA-1(1) * SHA-224 * SHA-256 * SHA-384 * SHA-512 * Protected SHA-1(1) * Protected SHA-256 * Protected SHA-384 * 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*

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	Keccak and SHA-3	* SHAKE128, * SHAKE256, * SHA3-224, * SHA3-256, * SHA3-384, * SHA3-512, * Keccak[r,1600-r], * protected SHAKE128, * protected SHAKE256, * protected SHA3-224, * protected SHA3-256, * protected SHA3-384, * protected SHA3-512, * 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], * Keccak-p[1600, n_r=12], * protected Keccak-p[1600,n_r = 24], * 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	Diffie-Hellman	Diffie-Hellman	Diffie-Hellman	up to 4096 bits	*ANSI X9.42*
If NesLib	DRBG	* SHA-1[(1)] * SHA-224 * SHA-256 * SHA-384 * SHA-512	Hash-DRBG	None	*NIST SP 800-90* *FIPS PUB 180-2*
		*AES	CTR-DRBG	128, 192 and 256 bits	*NIST SP 800-90* *FIPS PUB 197*

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

Cryptographic key generation (FCS_CKM.1)

199 If NesLib is embedded only, 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* *FIPS PUB 186-4*
RSA key generation	RSA key pair generation algorithm, optionally protected against side channel attacks, and/or optionally with conditions	up to 4096 bits	*FIPS PUB 140-2* *ISO/IEC 9796-2* *PKCS #1 V2.1*

5.1.3 Additional Security Functional Requirements for the memories protection

200 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

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

202 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

203 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

204 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.

205 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.

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

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

206 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.***

207 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.***

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

209 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***in Admin or User configuration, any access (read, write, execute) to the OST ROM is denied, and in User configuration, any write access to the ST NVM is denied.***

210 **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.

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

212 *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

213 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 possible availability of final test and loading capabilities in phases 4 to 6 of the TOE life-cycle

Limited capabilities (FMT_LIM.1) / Loader

214 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.***

215 *SFP_4: Loader Limited capability Policy*

216 *Deploying Loader functionality after blocking of the loader does not allow stored user data to be disclosed or manipulated by unauthorized user.*

Limited availability (FMT_LIM.2) / Loader

217 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.***

218 *SFP_5: Loader Limited availability Policy*

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

Import of user data without security attributes (FDP_ITC.1) / Loader

220 The TSF shall enforce the ***Loading Access Control Policy*** when importing user data, controlled under the SFP, from ouside of the TOE.

221 The TSF shall ignore any security attributes associated with the User data when imported from outside of the TOE.

222 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside of the TOE:

- ***the integrity of the loaded user data is checked at the end of each loading session,***
- ***the loaded user data is received encrypted, internally decrypted, then stored into the NVM.***

Static attribute initialisation (FMT_MSA.3) / Loader

223 The TSF shall enforce the ***Loading Access Control Policy*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

224 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

225 The TSF shall enforce the ***Loading Access Control Policy*** to restrict the ability to ***modify*** the security attributes ***remaining loading sessions*** to ***the Loader Administrator.***

Subset access control (FDP_ACC.1) / Loader

226 The TSF shall enforce the ***Loading Access Control Policy*** on ***all subjects, object NVM and all commands***.

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

227 The TSF shall enforce the ***Loading Access Control Policy*** to objects based on the following: ***the TOE mode, the user authenticated role, the remaining loading sessions and the requested command, according to the fixed loader access rights.***

228 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***the command is allowed if and only if the TOE mode, the user authenticated role, the remaining loading sessions and the requested command match an entry in the fixed loader access rights.***

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

230 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***in User mode, no loader command is deployed.***

231 The following SFP ***Loading Access Control Policy*** is defined for the requirement "Security attribute based access control (FDP_ACF.1) / Loader":

232 *SFP_6: Loading Access Control Policy*

233 *The TSF must enforce that only authorised users are allowed to download User code and data into the User NVM or to set the product profile.*
The TSF must enforce that only authorised users are allowed to be administrator of the provided loader functionality.
The TSF controls access to the loader functionality based on the TOE mode, the user authenticated role, the remaining loading sessions and the requested command according to the fixed loader access rights.

Specification of management functions (FMT_SMF.1) / Loader

234 The TSF will be able to perform the following management functions: ***change the TOE mode, change the user role, change the remaining sessions.***

Security roles (FMT_SMR.1) / Loader

235 The TSF shall maintain the roles: ***Loader and Loader Administrator***.

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

Timing of identification (FIA_UID.1) / Loader

237 The TSF shall allow ***boot and authentication command*** on behalf of the user to be performed before the user is identified.

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

5.1.5 Additional Security Functional Requirements related to M4M-DESFire

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

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

241 **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 / EDES for DES cryptographic operations,
- FCS_COP.1 / AES for AES cryptographic operations.

242 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

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

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

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

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

246 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

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

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

- ***The VC Administrator or 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.***

249 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.***

250 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.***

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

252 *SFP_7: 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 Administrator, 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 preve*nts 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.

253 *Note that subjects are authorised 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 authorised 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 Administrator and 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

254 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.

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

256 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

257 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***.

258 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

259 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

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

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

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

263 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.

264 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

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

266 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

267 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

268 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 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

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

269 The TSF shall provide ***‘none’ and cryptographic authentication*** to support user authentication.

270 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

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

272 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

273 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***.

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

275 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

276 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***.

277 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

278 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***.

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

Unlinkability (FPR_UNL.1) / M4M-DESFire

280 The TSF shall ensure that ***unauthorised 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

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

282 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

283 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***.

Subset access control (FDP_ACC.1) / APPLI_FWL

284 The TSF shall enforce the ***Protected Application Firewall Access Control Policy*** on ***the Protected Application code and data.***

Security attribute based access control (FDP_ACF.1) / APPLI_FWL

285 The TSF shall enforce the ***Protected Application Firewall Access Control Policy*** to objects based on the following: ***Protected Application code and data***.

286 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***An application cannot read, write, compare any piece of data or code belonging to the Protected Application.***

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

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

- ***Another application cannot read, write, compare any piece of data or code belonging to the Protected Application.***

289 The following SFP ***Protected Application Firewall Access Control Policy*** is defined for the requirement "Security attribute based access control (FDP_ACF.1) / APPLI_FWL":

290 *SFP_8: Protected Application Firewall Access Control Policy*

291 *Another application cannot read, write, compare any piece of data or code belonging to the Protected Application.*

Application Note:
When M4M is embedded, M4M is the (only) Protected Application.

Static attribute initialisation (FMT_MSA.3) / APPLI_FWL

292 The TSF shall enforce the ***Protected Application Firewall Access Control Policy*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

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

5.2 TOE security assurance requirements

294 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:

- ALC_DVS.2 and AVA_VAN.5.

295 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.

296 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.1	Implementation representation of the TSF	EAL5/*BSI-CC-PP-0084-2014*
ADV_INT.2	Well-stuctured internals	EAL5
ADV_TDS.4	Semiformal modular design	EAL5
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.4	Production support, acceptance procedures and automation	EAL5/*BSI-CC-PP-0084-2014*
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_LCD.1	Developer defined life-cycle model	EAL5/*BSI-CC-PP-0084-2014*
ALC_TAT.2	Compliance with implementation standards	EAL5
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.1	TOE summary specification	EAL5/*BSI-CC-PP-0084-2014*
ATE_COV.2	Analysis of coverage	EAL5/*BSI-CC-PP-0084-2014*
ATE_DPT.3	Testing: modular design	EAL5
ATE_FUN.1	Functional testing	EAL5/*BSI-CC-PP-0084-2014*

Table 10. TOE security assurance requirements (continued)

Label	Title	Origin
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

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

298 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.

299 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.

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

301 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
ADO_DEL	1	1	None
ALC_DVS	2	2	None
ALC_CMS	4	5	None, refinement is still valid
ALC_CMC	4	4	None
ADV_ARC	1	1	None
ADV_FSP	4	5	Presentation style changes, IC Dedicated Software is included
ADV_IMP	1	1	None
ATE_COV	2	2	IC Dedicated Software is included
AGD_OPE	1	1	None
AGD_PRE	1	1	None
AVA_VAN	5	5	None

5.3.1 Refinement regarding functional specification (ADV_FSP)

302 ~~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.

303 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.

304 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.

305 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.

306 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.

307 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.

5.3.2 Refinement regarding test coverage (ATE_COV)

308 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 EEPROM writing).

309 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).

310 ~~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.***

5.4 Security Requirements rationale

5.4.1 Rationale for the Security Functional Requirements

311 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* *Basic internal TSF data transfer protection FPT_ITT.1* *Subset information flow control FDP_IFC.1*
BSI.O.Phys-Probing	*Stored data confidentiality FDP_SDC.1* *Resistance to physical attack FPT_PHP.3*
BSI.O.Malfunction	*Limited fault tolerance FRU_FLT.2* *Failure with preservation of secure state FPT_FLS.1*
BSI.O.Phys-Manipulation	*Stored data integrity monitoring and action FDP_SDI.2* *Resistance to physical attack FPT_PHP.3*
BSI.O.Leak-Forced	All requirements listed for *BSI.O.Leak-Inherent* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1* plus those listed for *BSI.O.Malfunction* and *BSI.O.Phys-Manipulation* *FRU_FLT.2*, *FPT_FLS.1*, *FDP_SDI.2*, *FPT_PHP.3*
BSI.O.Abuse-Func	*Limited capabilities FMT_LIM.1 / Test* *Limited availability FMT_LIM.2 / Test* plus those for *BSI.O.Leak-Inherent*, *BSI.O.Phys-Probing*, *BSI.O.Malfunction*, *BSI.O.Phys-Manipulation*, *BSI.O.Leak-Forced* *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* plus those for *BSI.O.Leak-Inherent*, *BSI.O.Phys-Probing*, *BSI.O.Malfunction*, *BSI.O.Phys-Manipulation*, *BSI.O.Leak-Forced* *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
BSI.OE.Process-Sec-IC	Not applicable
AUG1.O.Add-Functions	*Cryptographic operation FCS_COP.1* *Cryptographic key generation FCS_CKM.1*

Table 12. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
AUG4.O.Mem-Access	*Complete access control FDP_ACC.2 / Memories* *Security attribute based access control FDP_ACF.1 / Memories* *Static attribute initialisation FMT_MSA.3 / Memories* *Management of security attribute FMT_MSA.1 / Memories* *Specification of management functions FMT_SMF.1 / Memories*
BSI.O.Cap-Avail-Loader	*Limited capabilities FMT_LIM.1 / Loader* *Limited availability FMT_LIM.2 / Loader*
O.Controlled-ES-Loading	*Import of user data without security attributes FDP_ITC.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* *Management of security attribute FMT_MSA.1 / Loader* *Specification of management functions FMT_SMF.1 / Loader* *Security roles FMT_SMR.1 / Loader* *Timing of identification FIA_UID.1 / Loader*
O.Access-Control-M4M	*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 attribute FMT_MSA.1 / M4M-DESFire* *Specification of management functions 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* *Management of TSF data FMT_MTD.1 / M4M-DESFire*
O.Authentication-M4M	*Cryptographic operation FCS_COP.1* / EDES *Cryptographic operation FCS_COP.1* / AES *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* *Trusted path FPT_TRP.1 / M4M-DESFire* *Replay detection FPT_RPL.1 / M4M-DESFire*
O.Confidentiality-M4M	*Cryptographic operation FCS_COP.1* / AES *Trusted path FPT_TRP.1 / M4M-DESFire* *Replay detection FPT_RPL.1 / M4M-DESFire*
O.Type-Consistency-M4M	*Inter-TSF basic TSF data consistency FPT_TDC.1 / M4M-DESFire*
O.Transaction-M4M	*Basic rollback FDP_ROL.1 / M4M-DESFire*
O.No-Trace-M4M	*Unlinkability FPR_UNL.1 / M4M-DESFire*
O.Resp-Appl-M4M	All SFRs defined additionnaly in the ST

Table 12. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
O.Resource-M4M	*Minimum and maximum quotas FRU_RSA.2 / M4M-DESFire*
O.Verification-M4M	*Subset access control FDP_ACC.1 / APPLI_FWL* *Security attribute based access control FDP_ACF.1 / APPLI_FWL* *Static attribute initialisation FMT_MSA.3 / APPLI_FWL* *Failure with preservation of secure state FPT_FLS.1*
O.Firewall-M4M	*Subset access control FDP_ACC.1 / APPLI_FWL* *Security attribute based access control FDP_ACF.1 / APPLI_FWL* *Static attribute initialisation FMT_MSA.3 / APPLI_FWL*
O.Shr-Res-M4M	*Subset residual information protection FDP_RIP.1 / M4M-DESFire*
OE.Secure-Values-M4M	Not applicable
OE.Terminal-Support-M4M	Not applicable
OE.M4M-Framework-Identification	Not applicable

312 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.

313 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*, and additional objectives (*O.Controlled-ES-Loading*, *O.Access-Control-M4M*, *O.Authentication-M4M*, *O.Confidentiality-M4M*, *O.Type-Consistency-M4M*, *O.Transaction-M4M*, *O.No-Trace-M4M*, *O.Resp-Appl-M4M*, *O.Resource-M4M*, *O.Verification-M4M*, *O.Firewall-M4M* and *O.Shr-Res-M4M*) introduced in this Security Target. This rationale must show that security requirements suitably address them all.

314 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*, *FDP_ITC.1 / Loader*, *FDP_ACC.1 / Loader*, *FDP_ACF.1 / Loader*, *FMT_MSA.3 / Loader*, *FMT_MSA.1 / Loader*, *FMT_SMF.1 / Loader*, *FMT_SMR.1 / Loader*, *FIA_UID.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*, *FPT_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*, *FDP_ACC.1 / APPLI_FWL*, *FDP_ACF.1 / APPLI_FWL*, and *FMT_MSA.3 / APPLI_FWL*, and various assurance requirements of EAL5+).

315 Though it remains to show that:

- security objectives from this Security Target 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.

316 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 Additional security objectives are suitably addressed

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

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

318 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.

319 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*)"

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

321 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 "Controlled loading of the Security IC Embedded Software (*O.Controlled-ES-Loading*)"

322 The justification related to the security objective "Controlled loading of the Security IC Embedded Software (*O.Controlled-ES-Loading*)" is as follows:

323 The security functional requirements "*Import of user data without security attributes (FDP_ITC.1) / Loader*", "*Subset access control (FDP_ACC.1) / Loader*" and "*Security attribute based access control (FDP_ACF.1) / Loader*", with the related Security Function

Policy (SFP) “Loading Access Control Policy” exactly require to implement a controlled loading of the Security IC Embedded Software as demanded by *O.Controlled-ES-Loading*. Therefore, *FDP_ITC.1 / Loader*, *FDP_ACC.1 / Loader* and *FDP_ACF.1 / Loader* with their SFP are suitable to meet the security objective.

324 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*" and "*Timing of identification (FIA_UID.1) / Loader*" specifies the roles that the TSF recognises and the actions authorised 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.

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

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

326 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 authorised 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-M4M*), 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-M4M*.

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

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

328 The two security functional requirements "*Cryptographic operation (FCS_COP.1)* / EDES" 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-M4M*.

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

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

330 The two security functional requirements "*Cryptographic operation (FCS_COP.1)* / AES" requires 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-M4M*.

Security objective “M4M-DESFire Data type consistency (*O.Type-Consistency-M4M*)”

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

332 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-M4M*.

Security objective “M4M-DESFire Transaction mechanism (*O.Transaction-M4M*)”

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

334 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-M4M*.

Security objective “Preventing traceability for M4M-DESFire (*O.No-Trace-M4M*)”

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

336 The security functional requirement "*Unlinkability (FPR_UNL.1) / M4M-DESFire*" requires that unauthorised 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-*

M4M.

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

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

338 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-M4M* is fulfilled by the additional ST SFRs.

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

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

340 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-M4M*.

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

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

342 The security functional requirements "*Subset access control (FDP_ACC.1) / APPLI_FWL*" and "*Security attribute based access control (FDP_ACF.1) / APPLI_FWL*", supported by "*Static attribute initialisation (FMT_MSA.3) / APPLI_FWL*", require that M4M-DESFire code integrity is protected. 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-M4M*.

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

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

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

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

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

346 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-M4M*.

5.4.3 Additional security requirements are consistent

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

347 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*)"

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

"Import of user data without security attribute (*FDP_ITC.1 / Loader*),
Static attribute initialisation (*FMT_MSA.3 / Loader*),
Management of security attributes (*FMT_MSA.1 / Loader*),
Subset access control (*FDP_ACC.1 / Loader*),
Security attribute based access control (*FDP_ACF.1 / Loader*),
Specification of management function (*FMT_SMF.1 / Loader*),
Security roles (*FMT_SMR.1 / Loader*),
Timing of identification(*FIA_UID.1 / Loader*)"

349 These security requirements have already been argued in *Section : Security objective "Controlled loading of the Security IC Embedded Software (O.Controlled-ES-Loading)"* 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*)"

350 These security requirements have already been argued in *Section : Security objective "Access control for M4M-DESFire (O.Access-Control-M4M)"* 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*)"

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

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

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

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

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

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

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

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

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

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

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

"Subset access control (*FDP_ACC.1 / APPLI_FWL*),
Security attribute based access control (*FDP_ACF.1 / APPLI_FWL*),
Static attribute initialisation (*FMT_MSA.3 / APPLI_FWL*),

357 These security requirements have already been argued in *Section : Security objective "M4M-DESFire firewall (O.Firewall-M4M)"* above.

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

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

5.4.4 Dependencies of Security Functional Requirements

359 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 *FMT_MSA.3 / APPLI_FWL* on FMT_MSA.1 and FMT_SMR.1 (see discussion below).

360 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*

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_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*
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*
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, by FDP_ITC.1 and FCS_CKM.1, see 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 R5*
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***	

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_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 R5*
	FMT_SMR.1 / Memories	No, see *AUG* ***#4***	Yes, *AUG* ***#4***
FMT_SMF.1 / Memories	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FMT_ITC.1 / Loader	[FDP_ACC.1 / Loader or FDP_IFC.1]	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_MSA.3 / Loader	Yes	
FDP_ACC.1 / Loader	FDP_ACF.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
FDP_ACF.1 / Loader	FDP_ACC.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_MSA.3 / Loader	Yes	
FMT_MSA.3 / Loader	FMT_MSA.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_SMR.1 / Loader	Yes	
FMT_MSA.1 / Loader	[FDP_ACC.1 / Loader or FDP_IFC.1]	Yes	***No,*** *CCMB-2017-04-002 R5*
	FDP_SMF.1 / Loader	Yes	
	FDP_SMR.1 / Loader	Yes	
FMT_SMR.1 / Loader	FIA_UID.1 / Loader	Yes	***No,*** *CCMB-2017-04-002 R5*
FIA_UID.1 / Loader	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FDP_SMF.1 / Loader	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FMT_SMR.1 / M4M-DESFire	FIA_UID.1 / M4M-DESFire	Yes, by FIA_UID.2 / M4M-DESFire	***No,*** *CCMB-2017-04-002 R5*

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_ACC.1 / M4M-DESFire	FDP_ACF.1 / M4M-DESFire	Yes	***No,*** *CCMB-2017-04-002 R5*
FDP_ACF.1 / M4M-DESFire	FDP_ACC.1 / M4M-DESFire	Yes	***No,*** *CCMB-2017-04-002 R5*
	FMT_MSA.3 / M4M-DESFire	Yes	
FMT_MSA.3 / M4M-DESFire	FMT_MSA.1 / M4M-DESFire	Yes	***No,*** *CCMB-2017-04-002 R5*
	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 R5*
	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 R5*
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 R5*
	[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 R5*
FIA_UID.2 / M4M-DESFire	None	No dependency	***No,*** *CCMB-2017-04-002 R5*
FIA_UAU.2 / M4M-DESFire	FIA_UID.1	Yes, by FIA_UID.2 / M4M-DESFire	***No,*** *CCMB-2017-04-002 R5*
FIA_UAU.5 / M4M-DESFire	None	No dependency	***No,*** *CCMB-2017-04-002 R5*

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 R5*
	FMT_SMF.1 / M4M-DESFire	Yes	
FPT_TRP.1 / M4M-DESFire	None	No dependency	**No,** *CCMB-2017-04-002 R5*
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 R5*
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 R5*
FPT_RPL.1 / M4M-DESFire	None	No dependency	**No,** *CCMB-2017-04-002 R5*
FPR_UNL.1 / M4M-DESFire	None	No dependency	**No,** *CCMB-2017-04-002 R5*
FRU_RSA.2 / M4M-DESFire	None	No dependency	**No,** *CCMB-2017-04-002 R5*
FDP_ACC.1 / APPLI_FWL	FDP_ACF.1 / APPLI_FWL	Yes	**No,** *CCMB-2017-04-002 R5*
FDP_ACF.1 / APPLI_FWL	FDP_ACC.1 / APPLI_FWL	Yes	**No,** *CCMB-2017-04-002 R5*
	FMT_MSA.3 / APPLI_FWL	Yes	
FMT_MSA.3 / APPLI_FWL	FMT_MSA.1	No, see discussion below	**No,** *CCMB-2017-04-002 R5*
	FMT_SMR.1	No, see discussion below	
FDP_RIP.1 / M4M-DESFire	None	No dependency	**No,** *CCMB-2017-04-002 R5*

361 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, both "*Cryptographic key generation (FCS_CKM.1)*" and "*Import of user data without security attributes (FDP_ITC.1) / Loader*" 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.

362 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.

363 Part 2 of the Common Criteria defines the dependency of "*Static attribute initialisation (FMT_MSA.3) / APPLI_FWL*" on "Management of security attributes (FMT_MSA.1)" and "Security roles (FMT_SMR.1)". For this particular instantiation of the access control attributes aimed at protecting M4M-DESFire code and data from unauthorised accesses, the security attributes are only static, initialized at product start. Therefore, there is no need to identify management capabilities and associated roles in form of Security Functional Requirements "FMT_MSA.1" and "FMT_SMR.1".

5.4.5 Rationale for the Assurance Requirements

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

364 Regarding application note 21 of *BSI-CC-PP-0084-2014*, this Security Target chooses EAL5 with augmentations 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.

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

366 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. All dependencies introduced by the requirements chosen for augmentation are fulfilled. Therefore, these components add additional assurance to EAL5, but the mutual support of the requirements and the internal consistency is still guaranteed.

367 Note that detailed and updated refinements for assurance requirements are given in *Section 5.3*.

Dependencies of assurance requirements

368 Dependencies of security assurance requirements are fulfilled by the EAL5 package selection.

369 The augmentation to this package are identified in paragraph *294* and do not introduce dependencies not already satisfied by the EAL5 package.

6 TOE summary specification (ASE_TSS)

370 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)

371 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)

372 The TSF provides preservation of secure state by detecting and managing the following failures:

- High voltage supply,
- Glitches,
- Die integrity violation detection,
- External clock incorrect frequency,
- Errors on memories and registers
- MPU errors,
- CPU errors,
- Watchdog reset,
- Faults on crypto processors or libraries,
- etc...

373 The secure state is reached by an immediate reset and run.

374 The ES can generate a software reset.

6.3 Limited capabilities (FMT_LIM.1) / Test

375 The TSF ensures that only very limited test capabilities are available in User configuration, in accordance with SFP_1: Limited capability and availability Policy / Test.

6.4 Limited capabilities (FMT_LIM.1) / Loader

376 The TSF ensures that the Secure Flash Loader and the final test capabilities are unavailable in User configuration, in accordance with SFP_4: Loader Limited capability Policy.

6.5 Limited availability (FMT_LIM.2) / Test & (FMT_LIM.2) / Loader

377 The TOE is either in Test, Admin (aka Issuer) or User configuration.

378 The only authorised TOE configuration modifications are:

- Test to Admin configuration,
- Test to User configuration,
- Admin to User configuration.

379 The TSF ensures the switching and the control of TOE configuration.

380 The TSF reduces the available features depending on the TOE configuration:

- the full test features are unavailable in User and Admin configuration,
- the Secure Flash Loader and the Final Test OS are unavailable in User configuration,
- the diagnosis test features are protected in User configuration.

6.6 Stored data confidentiality (FDP_SDC.1)

381 The TSF ensures confidentiality of the User Data, thanks to the following features:

- Memories scrambling and encryption,
- Protection of NVM sectors,
- MPU,
- LPU.

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

382 The TSF ensures stored data integrity, thanks to the following features:

- Memories parity control,
- Protection of NVM sectors,
- MPU,
- LPU.

6.8 Audit storage (FAU_SAS.1)

383 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, and only until phase 6.

6.9 Resistance to physical attack (FPT_PHP.3)

384 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)

385 The TSF prevents the disclosure of internal and user data thanks to:

- Memories scrambling and encryption,
- Bus encryption,
- RAM content destruction and register cleaning upon reset,
- Clocks jittering,
- Mechanisms for operation execution concealment.

6.11 Random number generation (FCS_RNG.1)

386 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: EDES operation (FCS_COP.1) / EDES, only if EDES+

387 If EDES+ is active, the TOE provides optionally an EDES+ accelerator that has the capability to perform 3-key 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.

388 The M4M-DESFire library uses Triple DES as cryptographic operation. 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, only if HW_AES

389 If HW-AES is active, the AES accelerator provides 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.

390 The AES accelerator can operate in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode.

391 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).

392 The M4M-DESFire library uses AES as cryptographic operation. 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, only if NesLib

393 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 up to 4096 bits,
- RSA private key cryptographic operation with or without CRT for modulus sizes up to 4096 bits,
- RSA signature formatting,
- RSA Key Encapsulation Method.

6.15 Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1) / ECC, only if NesLib

394 The cryptographic library NesLib provides to the ES developer the following efficient basic functions for Elliptic Curves Cryptography over prime fields on curves in Weierstrass form, 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.

395 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.

396 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, only if NesLib

397 The cryptographic library NesLib provides the SHA-1[e], SHA-224, SHA-256, SHA-384, SHA-512 secure hash functions conformant to *FIPS PUB 180-2*.

398 The cryptographic library NesLib provides the SHA-1, SHA-256, SHA-384, SHA-512 secure hash functions conformant to *FIPS PUB 180-2*, and offering resistance against side channel and fault attacks.

399 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 or SHA-256.

6.17 Cryptographic operation: Keccak & SHA-3 operation (FCS_COP.1) / Keccak, only if NesLib

400 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.

401 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.

402 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.

e. 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.

403 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, only if NesLib

404 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].
- 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, only if NesLib

405 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, only if NesLib

406 The cryptographic library NesLib gives support for a DRBG generator, based on cryptographic algorithms specified in *NIST SP 800-90*.

407 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, only if NesLib

408 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, only if NesLib

409 The cryptographic library NesLib provides standard RSA public and private key computation for key sizes upto 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

410 The TOE enforces a default memory protection policy when none other is programmed by the ES.

6.24 Management of security attributes (FMT_MSA.1) / Memories & Specification of management functions (FMT_SMF.1) / Memories

411 The TOE provides a dynamic Memory Protection Unit (MPU), that can be configured by the ES.

6.25 Complete access control (FDP_ACC.2) / Memories & Security attribute based access control (FDP_ACF.1) / Memories

412 The TOE enforces the dynamic memory protection policy for data access and code access thanks to a dynamic Memory Protection Unit (MPU), and complementary protection mechanisms, programmed by the ES.

6.26 Static attribute initialisation (FMT_MSA.3) / Loader

413 In Admin configuration, the System Firmware provides restrictive default values for the Flash Loader security attributes.

6.27 Management of security attributes (FMT_MSA.1) / Loader & Specification of management functions (FMT_SMF.1) / Loader

414 In Admin configuration, the System Firmware provides the capability to change part of the Flash Loader security attributes, only once in the product lifecycle.

6.28 Subset access control (FDP_ACC.1) / Loader, Security attribute based access control (FDP_ACF.1) / Loader, Security roles (FMT_SMR.1) / Loader & Timing of identification (FIA_UID.1) / Loader

415 In Admin configuration, the System Firmware grants access to the Flash Loader functions, only after presentation of the required valid passwords.

6.29 Import of user data without security attributes (FDP_ITC.1) / Loader

416 In Admin configuration, the System Firmware provides the capability of loading user data into the NVM, while ensuring confidentiality and integrity of the loaded data.

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

417 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.

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

418 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.

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

419 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.

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

420 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.

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

421 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.

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

422 The M4M-DESFire library implements the management functions defined by the M4M-DESFire interface specifications for authentication, changing security attributes and creating or deleting an application, a value or a data file.

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

423 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.

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

424 The M4M-DESFire library implements the M4M-DESFire interface specifications, supporting consistent interpretation and modification control of inter-TSF exchanges.

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

425 The M4M-DESFire library erases key values from memory after their context becomes obsolete.

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

426 The M4M-DESFire library identifies the user through the key selected for authentication or the usage of the M4M host interface as specified by the M4M-DESFire Interface Specification.

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

427 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.

428 After this authentication, both parties share a session key.

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

429 The M4M-DESFire library implements the M4M-DESFire Interface Specification, that has a mechanism to authenticate the VC Administrator, VC Manager, Application Manager and Application User, while Everybody is assumed when there is no valid authentication state.

430 Two types of authentication are supported: the native M4M-DESFire 3-pass authentication and the ISO authentication.

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

431 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.

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

432 The M4M-DESFire library implements the M4M-DESFire Interface Specification allowing to establish and enforce a trusted path between itself and remote users.

433 The mechanisms include encryption on commands and CMAC on responses.

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

434 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. The transaction mechanism applies to all files except the standard data files.

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

435 The M4M-DESFire library implements the M4M-DESFire authentication command, and authenticated commands, that allow replay detection.

6.46 Unlinkability (FPR_UNL.1) / M4M-DESFire

436 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.

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

437 The M4M-DESFire library ensures the memory required for its operation is available.

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

438 At the end of commands execution or upon interrupt, the M4M-DESFire library cleans the confidential data from crypto-processors and CPU registers it uses.

6.49 Subset access control (FDP_ACC.1) / APPLI_FWL & Security attribute based access control (FDP_ACF.1) / APPLI_FWL

439 The Library Protection Unit is used to isolate the protected application or M4M-DESFire firmware (code and data) from the rest of the code embedded in the device.

6.50 Static attribute initialisation (FMT_MSA.3) / APPLI_FWL

440 At product start, all the static attributes are initialised, which are needed to protect the segments where the Protected Application or M4M-DESFire code and data are stored.

7 Identification

Table 14. TOE components

IC Maskset name	IC version	Master identification number	Firmware version	OST version	Optional NesLib crypto library version	Optional MIFARE4Mobile DESFire EV1 library Id	Optional MIFARE4 Mobile version
K8H0A	F	0061h and 0105h	9 and A	2.2	6.3.4	0x00000004 or 0x00000504 (combined)	2.1.0

Table 15. Guidance documentation

Component description	Reference	Version
ST33G1M2 ST33I1M2 datasheet Secure MCU with 32-bit ARM SecurCore SC300 - Datasheet	DS_ST33G_I	2
ST33G1M2 platform: BP and BM specific product profiles - Technical note	TN_ST33G1M2_01	2
ST33G1M2 platform: LS, LC and BS specific product profiles - Technical note	TN_ST33G1M2_02	2
ST33G1M2 family extension: BP and BM specific product profiles	TN_ST33G1M2_04	1
ST33G1M2 family extension: LS, LC and BS specific product profiles	TN_ST33G1M2_05	1
ST33G1M2: CMOS M10+ 80-nm technology die and wafer delivery description	DD_ST33G1M2	4
ARM® Cortex SC300 r0p0 Technical Reference Manual	ARM DDI 0337F	F
ARM® Cortex M3 r2p0 Technical Reference Manual	ARM DDI 0337F3c	F3c
ARM® SC300 r0p0 SecurCore Technical Reference Manual Supplement 1A	ARM DDI 0337 Supp 1A	A
ARM® SecurCore® SC300	ES_SC300	1
ST33G1M2 Firmware user manual	UM_ST33G1M2_FW	14
ST33G1M2 and derivatives Flash loader installation guide	UM_33G_FL	4
ST33G and ST33H Firmware support for LPU regions - application note	AN_33G_33H_LPU	1
ST33G and ST33H Secure MCU platforms - Security Guidance	AN_SECU_ST33	9

Table 15. Guidance documentation (continued)

Component description	Reference	Version
ST33G and ST33H Power supply glitch detector characteristics - application note	AN_33_GLITCH	2
ST33G and ST33H - AIS31 Compliant Random Number - User Manual	UM_33G_33H_AIS31	3
ST33G and ST33H - AIS31 - Ref. impl.: Start-up, on-line and total failure tests - Application note	AN_33G_33H_AIS31	1
ST33 ARM Execute-only memory support for SecurCore® SC300 devices - Application note	AN_33_EXE	2
ST33 uniform timing application note	AN_33_UT	2
NesLib cryptographic library NesLib 6.3 - User manual	UM_NesLib_6.3	4
ST33G and ST33H secure MCU platforms - NesLib 6.3 security recommendations - Application note	AN_SECU_ST33G_H_NESLIB_6.3	5
NesLib 6.3.4 for ST33G, ST33H and ST33I platforms - Release note	RN_ST33_NESLIB_6.3.4	2
MIFARE4Mobile® library 2.1 - User manual	UM_33_MIFARE4Mobile-2.1	5
MIFARE4Mobile® library 2.1.0 for ST33G1M2 - Application note	AN_ST33G1M2_M4M_Lib	1

Table 16. Sites list

Site	Address	Activities(1)
Amkor ATP1	AMKOR ATP1 Km 22 East Service Road, South Superhighway, Muntinlupa City, 1771 Philippines	BE
Amkor ATP3/4	AMKOR ATP3/4 119 North Science Avenue, Laguna Technopark, Binan, Laguna, 4024 Philippines	BE
Amkor ATT1	AMKOR TECHNOLOGY TAIWAN, INC. (ATT) - T1 1F, No.1, Kao-Ping Sec, Chung-Feng Rd., Lungtan Township, Taoyuan County 325, Taiwan, R.O.C.	BE
Amkor ATT3	AMKOR TECHNOLOGY TAIWAN, INC. (ATT) - T3 11 Guangfu Road, Hsinchu Industrial Park, Hukou County, Hsinchu 303, Taiwan, R.O.C.	BE

Table 16. Sites list (continued)

Site	Address	Activities[1]
DNP Japan	DNP (Dai Nippon printing Co ltd.) 2-2-1 Kami-Fukuoka, Fujimino-shi, Saitama,356-8507, Japan	MASK
DPE Italy	DPE (Dai Printing Europe) Via C. Olivetti, 2/A, I-20041 Agrate, Italy	MASK
Feiliks	Feili Logistics (Shenzhen) CO., Ltd Zhongbao Logistics Building, No. 28 Taohua Road, FFTZ, Shenzhen, Guangdong 518038, China	WHS
Smartflex	Smartflex Technology 37A Tampines Street 92, Singapore 528886	BE
ST AMK1	STMicroelectronics 5A Serangoon North Avenue 5, Singapore 554574	DEV
ST AMK6	STMicroelectronics 18 Ang Mo Kio Industrial park 2, Singapore 569505	WHS
ST Bouskoura	STMicroelectronics 101 Boulevard des Muriers – BP97, 20180 Bouskoura, Maroc	BE WHS
ST Calamba	STMicroelectronics 9 Mountain Drive, LISP II, Brgy La mesa, Calamba, Philippines 4027	BE WHS
ST Crolles	STMicroelectronics 850 rue Jean Monnet, 38926 Crolles, France	DEV MASK FE
ST Gardanne	CMP Georges Charpak 880 Avenue de Mimet, 13541 Gardanne, France	BE

Table 16. Sites list (continued)

Site	Address	Activities[1]
ST Grenoble	STMicroelectronics 12 rue Jules Horowitz, BP 217, 38019 Grenoble Cedex, France	DEV
ST Ljubljana	STMicroelectronics d.o.o. Ljubljana Tehnoloski park 21, 1000 Ljubljana, Slovenia	DEV
ST Loyang	STMicroelectronics 7 Loyang Drive, Singapore 508938	WHS
ST Rennes	STMicroelectronics 10 rue de Jouanet, ePark, 35700 Rennes, France	DEV
ST Rousset	STMicroelectronics 190 Avenue Célestin Coq, Z.I., 13106 Rousset Cedex, France	DEV EWS WHS FE
ST Shenzen	STS Microelectronics 16 Tao hua Rd., Futian free trade zone, Shenzhen, P.R. China 518038	BE
ST Sophia	STMicroelectronics 635 route des lucioles, 06560 Valbonne, France	DEV
ST Toa Payoh	STMicroelectronics 629 Lorong 4/6 Toa Payoh, Singapore 319521	EWS
ST Tunis	STMicroelectronics Tunis Elgazala Technopark, Raoued, Gouvernorat de l'Ariana, PB21, 2088 cedex, Ariana, Tunisia	IT
ST Zaventem	STMicroelectronics Green Square, Lambroekstraat 5, Building B, 3d floor, 1831 Diegem/Machelen, Belgium	DEV

Table 16. Sites list (continued)

Site	Address	Activities(1)
STATS JSCC	STATS ChipPAC Semiconductor Jiangyin CO. Ltd (JSCC) No. 78 Changshan Road, Jiangyin, Jiangsu, China, Postal code: 214437	BE
TSMC F2/F5	TSMC FAB 2-5 121 Park Avenue 3, Hsinchu science park, Hsinchu 300-77, Taiwan, ROC	MASK FE
TSMC F14	TSMC FAB 14 1-1 Nan Ke N. Rd. Tainan science park, Tainan 741_44, Taiwan, ROC	MASK FE
TSMC F8	TSMC FAB 8 25, Li-Hsin Road, Hsinchu Science Park, Hsinchu 300-78, Taiwan ROC	MASK FE
Winstek	WINSTEK STATS ChipPAC (SCT) No 176-5, 6 Ling, Hualung Chun, Chiung Lin, 307 Hsinchu, Taiwan	BE

1. DEV = development, FE = front end manufacturing, EWS = electrical wafer sort, 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 R5	3.1 Rev 5
Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, April 2017	CCMB-2017-04-002 R5	3.1 Rev 5
Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, April 2017	CCMB-2017-04-003 R5	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, W. Killmann & W. Schindler 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 800-90A 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]	M4M specification	MIFARE4Mobile specification v2.1.1, MIFARE4Mobile Industry Group, 2013
[30]	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

Appendix A Glossary

A.1 Terms

Authorised 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.

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.

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)

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.

Secret

Information that must be known only to authorised 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
AES	Advanced Encryption Standard
AIS	Application notes and Interpretation of the Scheme (BSI).
ALU	Arithmetical and Logical Unit.
BE	Back End manufacturing.
BSI	Bundesamt für Sicherheit in der Informationstechnik.
CBC	Cipher Block Chaining.
CBC-MAC	Cipher Block Chaining Message Authentication Code.
CC	Common Criteria Version 3.1. R5.
CPU	Central Processing Unit.
CRC	Cyclic Redundancy Check.
DCSSI	Direction Centrale de la Sécurité des Systèmes d’Information.
DES	Data Encryption Standard.
DEV	Development.
DIP	Dual-In-Line Package.
DRBG	Deterministic Random Bit Generator.
EAL	Evaluation Assurance Level.
ECB	Electronic Code Book.
ECC	Elliptic Curve Cryptography.
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.
FTOS	Final Test Operating System.
GPIO	General Purpose I/O.
HMAC	Keyed-Hash Message Authentication Code.
I/O	Input / Output.
IC	Integrated Circuit.
ISO	International Standards Organisation.
IT	Information Technology.

Table 20. List of abbreviations (continued)

Term	Meaning
LPU	Library Protection Unit.
M4M	MIFARE4Mobile®
MASK	Mask manufacturing.
MPU	Memory Protection Unit.
NESCRYPT	Next Step Cryptography Accelerator.
NFC	Near Field Communication.
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.
RF UART	Radio Frequency Universal Asynchronous Receiver Transmitter.
ROM	Read Only Memory.
RSA	Rivest, Shamir & Adleman.
SAR	Security Assurance Requirement.
SFP	Security Function Policy.
SFR	Security Functional Requirement.
SHA	Secure Hash Algorithm.
SIM	Subscriber Identity Module.
SOIC	Small Outline IC.
SPI	Serial Peripheral Interface.
ST	Context dependent : STMicroelectronics or Security Target.
SWP	Single Wire Protocol.
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.

Table 20. List of abbreviations (continued)

Term	Meaning
TSS	TOE Summary Specification.
UID	User Identification.
WHS	Warehouse.